Ciencias Matemáticas, Vol. 29, No. 1, Pag. 61-67, 2015
Recibido 06-2015

Toro algebraico de tipo Norma sobre una extensión abeliana de Galois
Algebraic norm type tori defined over abelian Galois extension

Huber Martínez Rodríguez[1]*, Pedro Luis Del Angel Rodríguez[2], Jorge Estrada Sarlabous[3]

Resumen El toro algebraico de tipo norma introducido para aplicaciones criptográficas por Karl Rubin y Alice Silverberg, ha sido estudiado sobre una extensión cíclica finita L/k y más específicamente cuando $k=\mathbb{F}_q$ y $L=\mathbb{F}_{q^n}$. El presente artículo brinda una descripción algebraica del toro de tipo norma cuando es definido sobre L y L/k es una extensión finita, abeliana y no cíclica con grupo de Galois G isomorfo a $C_{p^r}\times C_{p^s}$. Por otro lado, describe el grupo de puntos L-racionales y los k-racionales para diferentes primos p cuando G es isomorfo a $C_p\times C_p$. Además, se demuestra que el grupo de puntos L-racionales es un subespacio vectorial en el espacio vectorial $\mathbb{F}_{p^{p^2}}$ sobre $\mathbb{F}_p$ y más aún se muestra que el grupo de puntos k-racionales es isomorfo a $(\mathbb{F}_p,+)$. Finalmente se construye un ejemplo donde se muestra cómo obtener sobre los campos p-ádicos una extensión de Galois con grupo $C_p\times C_p$.

Abstract The algebraic norm type torus introduced for cryptographic applications by Karl Rubin and Alice Silverberg has been studied over a finite cyclic extension L/k and more specifically when $k=\mathbb{F}_q$ and $L=\mathbb{F}_{q^n}$. This paper provides an algebraic norm type torus description when it is defined over L and L/k is finite, abelian and non-cyclic extension with Galois group G isomorphic to $C_{p^r}\times C_{p^s}$. On the other hand, describe the L-rational points group and the k-rational points group for different prime p when G is isomorphic to $C_p\times C_p$. Besides, it is shown that the L-rational points group is a subspace in the vector space $\mathbb{F}_{p^{p^2}}$ over $\mathbb{F}_p$ and moreover the k-rational points group is isomorphic to $(\mathbb{F}_p,+)$. Finally, is showed through an example, how to construct over the p-adic fields a Galois extension with group $C_p\times C_p$.

Palabras Clave
Group Scheme, Algebraic Tori, Torus-based Cryptography, Local fields

[1] *Departamento de Matemática, Universidad Máximo Gómez Báez, Cuba, huber@informatica.unica.cu*
[2] *Centro de Investigación en Matemáticas A.C, Gto. México, luis@cimat.mx*
[3] *Inst. de Cibern. Matemática y Física, La Habana, Cuba, jestrada@icimaf.cu*
***Autor para Correspondencia**

1. Introduction

The study of mathematical objects for cryptographic applications and codes theory is a preponderant thematic in the actual researches. Starting from the second half of the twenty century , the numeric groups played an essential role in its applications to the cryptography and codes theory. At the end of the same century, began to appear geometric objects for cryptographic applications. The most clear examples are the elliptic curves and hyperelliptic curves. The elliptic curves are essential in the current standard applications named Elliptic Curve Cryptography [2] [6] [3]. At the beginning of this century other geometric objects are introduced for cryptographic applications like algebraic norm type tori [10], this topic was named Torus-Based Cryptography introduced in [7] [8]. The algebraic norm type tori will be the study object in this paper.

In the works [7] and [8] the authors studied the torus

$$\mathscr{T}_{L/k}:=\mathscr{T}_L=ker\left[R_{L/k}\mathbb{G}_m \overset{\oplus N_{L/k,k}}{\longrightarrow} \bigoplus_{k\subseteq M\subsetneq L} R_{L/M}\mathbb{G}_m\right]$$

when L/k is a cyclic extension and proposed this for cryptographic applications. They say that the k-rational points are infinity when k has characteristic zero and finity when k has characteristic p i.e the field $\mathbb{F}_q$ with q a power of p. When $k=\mathbb{F}_q$ and $L=\mathbb{F}_{q^n}$ then L/k is a cyclic extension and the torus k-rational points can be applied to the cryptography. The k-rational points are given by

$$\mathscr{T}_L(k)\cong\{\alpha\in L^\times : N_{L/M}(\alpha)=1 \ \ whenever \ \ k\subseteq M\subsetneq L\}.$$

The present paper describes the torus $\mathscr{T}_{L/k}$ when L/k is a finite, abelian and non-cyclic extension with Galois group G

isomorphic to $C_{p^r} \times C_{p^s}$. To do so, the structure of the article is as follows. In the first section are given the preliminary results for this work. Section 2 offers a complete torus descriptions for this extensions and is proved that the torus has dimension zero (i.e a finite number of rational points). As a particular case, section 3 discloses the L-rational points for the torus $\mathscr{T}_{L/k}$ when L/k has Galois group isomorphic to $C_p \times C_p$. Also it is shown trough of examples for a lot of primes p, that the L-rational points form a subspace in the vector space $L = \mathbb{F}_{p^{p^2}}$ over $\mathbb{F}_p$. To construct the examples was programmed in SAGE[1] two functions. The first function returns the torus matrix definition named A and the second function returns for a prime p, the rank of A and the dimension of its null space. The final section contains the k-rational points description for the torus $\mathscr{T}_{L/k}$ when L/k has Galois group isomorphic to $C_{p^r} \times C_{p^s}$ and is demonstrated that the k-rational points group is isomorphic to the group $(\mathbb{F}_p, +)$. The difficulty here is to find extensions with Galois group isomorphic to $C_p \times C_p$, an example over the p-adic fields is given to show how to construct these extensions.

2. Preliminary

Fix a field k and let k_s be a separable extension. Let $\mathbb{A}^d$ denote d-dimensional affine space, on the other hand let V be a variety and D a set, then

$$V^D := \otimes_{\delta \in D} V \cong V^{|D|}.$$

If D is a group, then D acts by permutations over the summands of V^D. $\mathbb{G}_m$ denotes the multiplicative k-group, the reader can see [10][1] for further information.

Definition 1 *L/k be a Galois extension and let V be a variety defined over L then the Weil restriction of V over k is defines as $R_{L/k}V$. $R_{L/k}V$ is a variety over k such that its k-rational points are isomorphic to the L-rational points of V, for more details see [10] p. 37.*

In [7] is given the following proposition that describes some properties about Weil restriction that is given here without proof.

Proposition 2 *Let L/k be a Galois extension, V a variety defined over L and $H = Gal(L/k)$. Then*

I. *for every field F containing k, there is a functorial bijection*
$$(R_{L/k}V)(F) \cong V(F \otimes_k L).$$

II. *there are functorial morphisms $\pi_\gamma : R_{L/k}V \longrightarrow V$ for all $\gamma \in H$, defined over L, such that the direct sum*
$$\oplus \pi_\gamma : R_{L/k}V \cong V^H$$
is an isomorphism over L,

III. *H acts on $R_{L/k}V$ in fact there is a homomorphism $H \longrightarrow Aut_k(R_{L/k}V)$ compatible with the isomorphism of (i) and (ii), where in (i), H acts on the second factor of $F \otimes_k L$,*

IV. *if V is an algebraic group, then so is $R_{L/k}V$, and all the above maps preserve the group structure as well.*

If $V = \mathbb{G}_m$, then $R_{L/k}V = R_{L/k}\mathbb{G}_m$ and by (i) we have that $(R_{L/k}\mathbb{G}_m)(k) = \mathbb{G}_m(L) = L^*$.

Definition 3 *An algebraic torus over k is an algebraic group defined over k such that over k_s it is isomorphic to $\mathbb{G}_m^d$, where d is the dimension.*

Each torus T has associated a character group $\widehat{T} = Hom_{k_s}(T, \mathbb{G}_m)$. The group $\mathscr{G} = Gal(k_s/k)$ acts continuously over $\widehat{T}$ also $Gal(L/k)$ does the same for any field L where T is split. Let T and T' be tori over k, then $Hom_k(T, T') \cong Hom_{\mathscr{G}}(\widehat{T}, \widehat{T'})$ furthermore $T \cong T'$ over k if and only if $\widehat{T} \cong \widehat{T'}$ as a $\mathscr{G}$-module.

By Prop. 2. (ii), there is an isomorphism over L between the torus $\mathscr{T}_L$ and the torus

$$\mathbb{T}_G := Ker \begin{bmatrix} \mathbb{G}_m^G & \overset{\oplus N_H}{\longrightarrow} & \bigoplus_{1 \neq H \subseteq G} \mathbb{G}_m^{G/H} \end{bmatrix}, \qquad (1)$$

with $N_H : \mathbb{G}_m^G \longrightarrow \mathbb{G}_m^{G/H}$ sending

$$(\alpha_g)_{g \in G} \longmapsto (\prod_{\gamma \in gH} \alpha_\gamma)_{gH \in G/H}.$$

Thus, it is similar to study the torus $\mathbb{T}_G$ over L than $\mathscr{T}_L$ over L.

3. The algebraic torus $\mathbb{T}_G$ over L

All elements in G can be written as $\sigma^i \tau^j$ for $0 \leq i \leq p^r - 1$ and $0 \leq j \leq p^s - 1$. The cyclic subgroups in G have the form $Z = \langle \sigma^h \tau^k \rangle$ for some $0 \leq h \leq p^r - 1$ and $0 \leq k \leq p^s - 1$. In this case the group order is

$$l = |\langle \sigma^h \tau^k \rangle| = max\left\{ ord(\sigma^h), ord(\tau^k) \right\} = max\left\{ \frac{p^r}{gcd(h, p^r)}, \frac{p^s}{gcd(k, p^s)} \right\},$$

where l is a power of p.

Now, the torus $\mathbb{T}_G$ over L will be studied (i.e $\mathscr{T}_L$ over L), when G is an abelian noncyclic p-primary group $C_{p^r} \times C_{p^s}$. To prove that the torus $\mathscr{T}_L$ over L has dimension zero and additionally that $\mathbb{T}_G$ is a subset in $\mu_p^{|G|}$ with μ_p the kernel of $r : \mathbb{G}_m \to \mathbb{G}_m$ assigning $\beta \mapsto \beta^p$, the following theorem is given.

Theorem 4 *Let $G \cong C_{p^r} \times C_{p^s}$ be a finite non cyclic abelian group, whose generators are σ, τ such that $\sigma^{p^r} = 1 = \tau^{p^s}$,*

[1] Open Source Mathematics Software. www.sagemath.org

then the torus $\mathbb{T}_G$ is finite i.e with dimension zero and can be written in the form:

$$\mathbb{T}_G = \left\{ \begin{array}{c} \beta = (\beta_g)_{g\in G} \in \mathbb{G}_m^G : \\ \prod_{j=0}^{p-1} \beta_{g\left(\sigma^h\tau^k\right)^j} = 1 \ \ \forall g \in G \ \textit{and} \\ \forall H = \langle \sigma^h\tau^k\rangle < G \ \textit{with} \ \ |H| = p \end{array} \right\}. \quad (2)$$

Also, if $\beta = (\beta_g)_{g\in G} \in \mathbb{T}_G$, then $\beta_g^p = 1$ for all $g \in G$.

Proof. The torus $\mathbb{T}_G$ defined in (1) can be written as

$$\mathbb{T}_G = \bigcap_{1\neq H\leq G} Ker\, N_H = \left\{\beta \in \mathbb{G}_m^G : N_H(\beta) = 1 \ \forall \text{ non trivial } H \leq G\right\}.$$

On the other hand, if H_1 and H_2 are subgroups of G and $H_1 \subset H_2$, then $Ker\, N_{H_1} \subset Ker\, N_{H_2}$, so the intersection of the N_H's kernels for all nontrivial subgroups H is the same as the intersection for all minimal subgroups H, i.e the subgroups H with $|H| = p$. According to the norm function definition in (1) and using the quotient between the group G and the minimals subgroups H with $|H| = p$ is obtained the defining torus equations in (2). In the definition (2) all elements in G are used as representatives, thus there are redundant equations, but this no affect the torus definition.

Now, the affirmation $\beta_g^p = 1$ is proven. Let us take $g \in G$ arbitrary and let H_1, H_2, ..., H_{p+1} be the subgroups of G with order p. It is known by [9] that there are $p+1$ order p subgroups in G, then g can be chosen as coset representative in the quotient G/H_i for each $i = 1,\ldots,p+1$. Now, the cosets of g for each quotient are

$$\begin{array}{cccc} \left[g(\sigma^{h_1}\tau^{k_1})^0, g(\sigma^{h_1}\tau^{k_1})^1, \ldots, g(\sigma^{h_1}\tau^{k_1})^{p-1}\right] \\ \left[g(\sigma^{h_2}\tau^{k_2})^0, g(\sigma^{h_2}\tau^{k_2})^1, \ldots, g(\sigma^{h_2}\tau^{k_2})^{p-1}\right] \\ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ \left[g(\sigma^{h_{p+1}}\tau^{k_{p+1}})^0, g(\sigma^{h_{p+1}}\tau^{k_{p+1}})^1, \ldots, g(\sigma^{h_{p+1}}\tau^{k_{p+1}})^{p-1}\right]. \end{array}$$

By the representation 4 is satisfied that

$$\left(\prod_{j=0}^{p-1} \beta_{g\left(\sigma^{h_i}\tau^{k_i}\right)^j}\right)_{i=1,\ldots,p+1} = 1$$

and consequently, multiplying for every i the equation

$$\prod_{i=1}^{p+1}\prod_{j=0}^{p-1} \beta_{g\left(\sigma^{h_i}\tau^{k_i}\right)^j} = 1$$

is obtained. For $j = 0$, β_g is included in each term and taking it as a common factor the following equation is achieved

$$\beta_g^{p+1}\prod_{i=1}^{p+1}\prod_{j=1}^{p-1} \beta_{g\left(\sigma^{h_i}\tau^{k_i}\right)^j} = 1.$$

If $\langle\sigma^h\tau^k\rangle$ is a cardinality p cyclic subgroup of G, then

$$|\langle\sigma^h\tau^k\rangle| = \max\left\{ord(\sigma^h), ord(\tau^k)\right\} = p.$$

Now, let us suppose that $ord(\sigma^h) = p$ then $ord(\tau^k) = 0$ or $ord(\tau^k) = p$. It is known that the subgroup $\langle\sigma^0\tau^{p^{s-1}}\rangle$ has cardinality p in G and hence it is the only one with $h = 0$, consequently in the above product there is one i where $h_i = 0$ and $k_i = p^{s-1}$. Without loss of generality suppose that $i = p+1$ and so the product takes the form

$$\left(\beta_g^{p+1}\prod_{j=1}^{p-1} \beta_{g\left(\tau^{p^{s-1}}\right)^j}\right)\prod_{i=1}^{p}\prod_{j=1}^{p-1} \beta_{g\left(\sigma^{h_i}\tau^{k_i}\right)^j} = 1.$$

Note that all $\sigma^{h_i}\tau^{k_i}$ have $ord(\sigma^{h_i}) = p$, otherwise it would be zero and this was extracted from the product. The above implies that $ord(\tau^{k_i}) = 0$ or $ord(\tau^{k_i}) = p$, for this reason $k_i = lp^{s-1}$ with l taking values $0,1,\ldots,p-1$. In this way k_i runs through the cardinality p subgroups generators except one i.e. the extracted subgroups, hence there are $p+1$ subgroups. Under the above considerations and interchange the product the equation

$$\left(\beta_g^{p+1}\prod_{j=1}^{p-1} \beta_{g\left(\tau^{p^{s-1}}\right)^j}\right)\prod_{j=1}^{p-1}\prod_{i=1}^{p} \beta_{\left(g\sigma^{j\,p^r-1}\right)\left(\tau^{j\,p^{s-1}}\right)^{i-1}} = 1$$

is obtained.

In the last equality $\tau^{jp^{s-1}}$ has order p, and so taking $H = \langle\tau^{jp^{s-1}}\rangle < G$ and $g\sigma^{j\,p^r-1}$ as representative in the quotient G/H for each fixed j the equation

$$\prod_{j=1}^{p-1}\prod_{i=1}^{p} \beta_{\left(g\sigma^{j\,p^r-1}\right)\left(\tau^{j\,p^{s-1}}\right)^{i-1}} = 1$$

is achieved. Now, the equality

$$\beta_g^{p+1}\prod_{j=1}^{p-1} \beta_{g\left(\tau^{p^{s-1}}\right)^j} = 1$$

can be written as

$$\beta_g^{p}\prod_{j=0}^{p-1} \beta_{g\left(\tau^{p^{s-1}}\right)^j} = 1.$$

It is known by (2) that the product $\prod_{j=0}^{p-1} \beta_{g\left(\tau^{p^{s-1}}\right)^j} = 1$, hence $\beta_g^p = 1$. ■

Proposition 5 *Let L/k be an extension that contains the p-th roots of unity with generator w and let $n \in \mathbb{N}$, then the map*

$$\psi : \mu_p^n(L) \longrightarrow \mathbb{F}_p[x]/\langle f(x)\rangle \cong \mathbb{F}_p(\gamma)$$

that sends $(w^{i_j})_{j=0,\ldots,n-1} \longmapsto \sum_{j=0}^{n-1} i_j\,\gamma^j$ is a group isomorphism between $(\mu_p^n(L),\cdot)$ and $(\mathbb{F}_p[x]/\langle f(x)\rangle,+)$. The polynomial $f(x)$ with n degree in $\mathbb{F}_p[x]$, is irreducible over $\mathbb{F}_p$ and γ is a primitive element that satisfies $f(\gamma) = 0$.

Proof. First, it is proven that $\psi : \mu_p^n(L) \longrightarrow \mathbb{F}_p(\gamma)$ is compatible with the operations of each group, indeed

$$\psi((w^{i_j}\cdot w^{k_j})_{j=0,\ldots,n-1}) = \psi((w^{i_j+k_j})_{j=0,\ldots,n-1}) = \sum_{j=0}^{n-1}(i_j+k_j)\,\gamma^j = \sum_{j=0}^{n-1} i_j\alpha^j + \sum_{j=0}^{n-1} k_j\,\alpha^j = \psi((w^{i_j})_{j=0,\ldots,n-1}) + \psi((w^{k_j})_{j=0,\ldots,n-1}),$$

thus the morphism transform the product of two elements in the sum of its transformed. Also,

$$\psi((1)_{j=1,\ldots,n}) = \psi((w^0)_{j=1,\ldots,n}) = \sum_{j=0}^{n-1} 0\,\gamma^j = 0,$$

so ψ sends neutral element in the group $(\mu_p^n(L),\cdot)$ to neutral element in the group $(\mathbb{F}_p[x]/\langle f(x)\rangle,+)$. Let $y=0$, $y\in\mathbb{F}_p(\gamma)$ in this way $y=\sum_{j=0}^{n-1}0\,\gamma^j$, if we take $x=(w^0)_{j=0,\ldots,n-1}$, then it is satisfies that $\psi((w^0)_{j=1,\ldots,n})=\sum_{j=0}^{n-1}0\,\gamma^j=y$, beside if there is $x'=(w^{i_j})_{j=0,\ldots,n-1}$ such that $\psi(x')=\sum_{j=0}^{n-1}0\,\gamma^j=y$, then

$$\psi(x') = \psi((w^{i_j})_{j=0,\ldots,n-1}) = \sum_{j=0}^{n-1} i_j\gamma^j = \sum_{j=0}^{n-1} 0\,\gamma^j = y.$$

As $i_j\geq 0$ for all j then the last equality is possible if and only if all $i_j=0$, hence $x=x'$ and ψ is injective. To prove the surjectivity let $y\in\mathbb{F}_p(\gamma)$ be arbitrary and write this as $y=\sum_{j=0}^{n-1} i_j\gamma^j$ then $\psi((w^{i_j})_{j=0,\ldots,n-1})=y$. Note that $i_j\in\mathbb{F}_p$ for all j, i.e $0\leq i_j\leq p-1$ and so $w^{i_j}\in\mu_p(L)$ that proves the surjectivity. ■

Let $g_0,g_1,\ldots,g_{|G|-1}$ be the elements of G, then by the Proposition 5 is concluded that $\mathbb{T}_G(L)\subset\mathbb{F}_p(\gamma)$ and $\mathbb{T}_G(L)$ can be written as

$$\mathbb{T}_G(L) = \left\{ \sum_{i=0}^{|G|-1} \alpha_{g_i}\gamma^i \in \mathbb{F}_p(\gamma) : \begin{array}{c} \sum_{j=0}^{p-1}\alpha_{g_i(\sigma^h\tau^k)^j}=0 \\ \text{for } i=0,\ldots,|G|-1 \\ \text{and} \\ \forall H=\langle\sigma^h\tau^k\rangle<G \\ \text{with } |H|=p \end{array} \right\}. \tag{3}$$

Observe in the previous torus definition that each $g\in G$ was taken as a representative in the quotient G/H with $H<G$ such that $|H|=p$, this induces redundant equations because several $g_i\in G$ correspond with the same coset in the quotient G/H. Also the defining torus equations is transformed from the product form to additive form, which is better for calculation.

In the present paper a particular case is studied, i.e the torus $\mathbb{T}_G$ defined by $G\cong C_p\times C_p$ with p prime.

4. The torus $\mathbb{T}_G$ defined by $G\cong C_p\times C_p$ with p prime

In the first time, to study the torus $\mathbb{T}_G$ for the group $G\cong C_p\times C_p$ it is necessary to see the structure of all subgroups H of order p in G, and secondly to know which are the forms of the cosets in the quotients G/H for each H. Let $G=\langle\sigma,\tau\rangle$ where σ and τ are the generators of G with $\sigma^p=\tau^p=1$. The order p subgroups in G have the form $\langle\sigma\tau^k\rangle$ for $k=0,\ldots,p-1$ including the subgroup $\langle\tau\rangle$. Keep in mind that G has $p+1$ order p subgroups.

Let us denote $H_0=\langle\tau\rangle$ and $H_k=\langle\sigma\tau^k\rangle$ for $k=1,2,\ldots,p-1$, for these subgroups the cardinality l is equal to p, thus the elements $g\in G$ given by

$$g=\sigma^0,\ldots,\sigma^{p-1}$$

can be taken as coset representatives of the quotients G/H_0 and G/H_k respectively. Similarly, when $k=0$ we have $H_p=\langle\sigma\rangle$, $l=p$ and $g=\tau^0,\ldots,\tau^{p-1}$ as coset representatives. Using the fact that g and $g'\in G$ are in the same coset in the quotient G/H_k (i.e $gH_k=g'H_k$) if and only if $g^{-1}.g'\in H_k$, it is easy to prove that the coset representatives proposed previously are inducing different cosets.

Now, let G/H_0 be the quotient defined in matrix form as:

$$(h_{ij}^{(0)}) = \begin{pmatrix} \sigma^0(\tau)^0 & \sigma^0(\tau)^1 & \ldots & \sigma^0(\tau)^{p-1} \\ \sigma^1(\tau)^0 & \sigma^1(\tau)^1 & \ldots & \sigma^1(\tau)^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{p-1}(\tau)^0 & \sigma^{p-1}(\tau)^1 & \ldots & \sigma^{p-1}(\tau)^{p-1} \end{pmatrix},$$

the rows are denoting the quotient cosets of G/H_0. It is easy to note that

$$h_{ij}^{(k)} = h_{i+j \bmod p,\, kj \bmod p}^{(0)}$$

where the rows of the matrix $(h_{ij}^{(k)})$ represent the cosets of the quotient G/H_k for $k=1,\ldots,p-1$. Finally, $h^{(p)}=h^{(0)^T}$ i.e. the transpose of $h^{(0)}$, where the rows denote the cosets of the quotient G/H_p. Each row in the above matrices induce a torus defining equation over $\mathbb{F}_p$ by 3.

Each matrix that represent the quotient G/H_k contains by definition all elements of G distributed in cosets. The L-rational points for $\mathbb{T}_G$ according to 3 are the elements

$$\sum_{i=0}^{|G|-1}\alpha_{g_i}\gamma^i\in\mathbb{F}_p(\gamma)$$

that satisfied the following equations system relating the coefficients α_g for all $g\in G$. The equations

$$\sum_{j=0}^{p-1}\alpha_{g_i(\sigma\tau)^j}=0, \sum_{j=0}^{p-1}\alpha_{g_i(\sigma\tau^2)^j}=0,\ldots, \sum_{j=0}^{p-1}\alpha_{g_i(\sigma\tau^{p-1})^j}=0, \sum_{j=0}^{p-1}\alpha_{g_i(\tau)^j}=0$$

with $g_i=\sigma^i$ for i varying from $0,\ldots,p-1$ that correspond to the quotients $G/H_1,G/H_2,\ldots,G/H_{p-1}$ and G/H_0 respectively. Besides, the equations $\sum_{j=0}^{p-1}\alpha_{g_i(\sigma)^j}=0$ with $g_i=\tau^i$ for i varying from $0,\ldots,p-1$ that correspond with G/H_p.

Hence the torus $\mathbb{T}_G$ can be described in details from these equations. Note that, as we are using a representative of each coset without repetitions, then in the torus definition 3, the redundant equations disappear and we have $p(p+1)$ equations in total.

Now, let us take A as the matrix that produces the equations system $A\alpha = 0$ defining the torus $\mathbb{T}_G$ with

$$\alpha = (\alpha_{g_1}, \alpha_{g_2}, \ldots, \alpha_{g_{p^2}}) \in \mathbb{F}_{p^{p^2}}$$

the variables vector. Each column in the matrix A corresponds with the variables α_{g_i}, and the same time these are organized using the column disposition in $h^{(0)}$ (it is known that $h^{(0)}$ contains all elements of G organized in cosets) i.e.

$$g_1 = h^{(0)}_{0,0}, g_2 = h^{(0)}_{1,0}, \ldots, g_p = h^{(0)}_{p-1,0}$$

$$g_{p+1} = h^{(0)}_{0,1}, g_{p+2} = h^{(0)}_{1,1}, \ldots, g_{2p} = h^{(0)}_{p-1,1}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$g_{(p-1)p+1} = h^{(0)}_{0,p-1}, g_{(p-1)p+2} = h^{(0)}_{1,p-1}, \ldots, g_{p^2} = h^{(0)}_{p-1,p-1},$$

for each $\alpha_{g_1}, \alpha_{g_1}, \ldots, \alpha_{g_{p^2}}$ over the finite field $\mathbb{F}_p$. The matrix A is created in the order of the matrices $h^{(k)}$ for $k = 0, \ldots, p$; the first p rows correspond to the equations defined by each coset in $h^{(0)}$, the second p rows to the equations defined by $h^{(1)}$ and so on. The matrix A contains as consequence only zeros and one in each row, it are placed depending of the variables that appear in each equation.

The function $TorusMatrix(p)$ was programmed by the authors in SAGE to construct the matrix A corresponding with the above descriptions. This function returns the matrix A associated with the torus $\mathbb{T}_G$ given the prime p that defines the group $C_p \times C_p$ as argument.

```
def TorusMatrix(p):
   lis=[[[i,j] for j in range(0,p)] for i in range(0,p)]
   lis_aux=[[lis[i][j] for j in range(0,p)] for i in range(0,p)]
   m=[ ]
   for k in range(0,p):
       for i in range(0,p):
           aux=[0 for j in range(0,p^2)]
           for j in range(0,p):
               aux[lis_aux[i][j][1]*p+lis_aux[i][j][0]]=1
           m.append(aux)
       for i in range(0,p):
           for j in range(0,p):
               lis_aux[i][j]=lis[(i+j) % p][((k+1)*j) % p]
   lis_aux=[[lis[j][i] for j in range(0,p)] for i in range(0,p)]
   for i in range(0,p):
           aux=[0 for j in range(0,p^2)]
           for j in range(0,p):
               aux[lis_aux[i][j][1]*p+lis_aux[i][j][0]]=1
           m.append(aux)
   return m
```

Other auxiliary function is defined to return the parameters list $[p,r,d]$. The parameters r and d represent the rank of the matrix A and the dimension of the torus respectively.

```
def TorusParameters(p):
  m1=matrix(GF(p),p*(p+1),p^2,TorusMatrix(p));
  r=m1.rank();
  Torus=m1.right_kernel();
  d=Torus.dimension();
  return [p,r,d]
```

Now, it is shown how to use the above functions in SAGE.

```
TorusParameters(2)
Output:
[2, 3, 1]

TorusParameters(7)
Output:
[7, 28, 21]

TorusParameters(11)
Output:
[11, 66, 55]
```

The table bellow contains several calculations for different primes p using the function $TorusParameters(p)$. It is important to remark that the torus $\mathbb{T}_G$ has p^d elements for each prime p, this fact proves the non-triviality of the torus.

Primes	A Rank	Torus dimension	L-Rat. P. Q.
2	3	1	2^1
3	6	3	3^3
5	15	10	5^{10}
7	28	21	7^{21}
11	66	55	11^{55}
13	91	78	13^{78}
17	153	136	17^{136}
19	190	171	19^{171}
23	276	253	23^{253}
29	435	406	29^{406}
31	496	465	31^{465}

Table 1. Torus parameters for different prime p. Column header L-Rat. P. Q. means L-Rational points quantity

From the above table we can to establish as conjecture that the rank of A satisfied the relation $p(p+1)/2$ and as consequence the torus dimension is $p^2-p(p+1)/2=(p^2-p)/2$.

It is shown in the Table 1 that the set $\mathbb{T}_G(L)\subset\mathbb{F}_{p^{p^2}}$ is a subspace over $\mathbb{F}_p$ with dimension $(p^2-p)/2$ for $G\cong C_p\times C_p$. The $\mathbb{T}_G(L)$ subspace is defined by the right kernel of the matrix A, i.e.

$$\mathbb{T}_G(L)=\mathbb{F}_p[v_1]\oplus\mathbb{F}_p[v_2]\oplus\ldots\oplus\mathbb{F}_p[v_{(p^2-p)/2}]$$

where $\{v_i\}$ is a subspace basis and so the group $\mathbb{T}_G(L)$ is isomorphic to $(\mathbb{F}_{p^{((p^2-p)/2)}},+)$.

Using the above facts, for the prime $p=2$ the torus L-rational points group $\mathbb{T}_G(L)$ takes the form

$$\mathbb{T}_G(L)=\mathbb{F}_2\,[v_1]$$

with 2^1 elements. When $p=3$ the torus L-rational points group is written as

$$\mathbb{T}_G(L)=\mathbb{F}_3\,[v_1]\oplus\mathbb{F}_3\,[v_2]\oplus\mathbb{F}_3\,[v_3]$$

with 3^3 elements and so on for different prime p.

5. The k-rational points for $\mathscr{T}_L$ with L/k a Galois extension with group $G\cong C_{p^r}\times C_{p^s}$

It is known after the works [7] and [8] that the k-rational points for $\mathscr{T}_L$ are infinite when k has characteristic zero and L/k is cyclic. Specifically, when $k=\mathbb{F}_q$ and $L=\mathbb{F}_{q^n}$ the k-rational points are used in cryptography. Now, we consider an extension L/k with Galois groups $G\cong C_{p^r}\times C_{p^s}$ and we want to find the k-rational points for this case.

Lemma 6 *Let k be a field containing the p-th roots of unity and L/k an extension with Galois group $G\cong C_p\times C_p$, then $\mathscr{T}_L(k)$ is equal to $\mu_p(k)$.*

Proof. The k-rational points in the torus $\mathscr{T}_L$ are

$$\mathscr{T}_L(k)\cong\{\alpha\in L^\times : N_{L/M}(\alpha)=1 \ \textit{whenever}\ k\subseteq M\subsetneq L\}.$$

Let G be generated by σ and τ with $\sigma^p=\tau^p=1$, it is known that every strict subgroup of G has the form $H_j=\langle\sigma\tau^j\rangle$ when j varies in the range $0,\ldots,p-1$ and $H_p=\langle\tau\rangle$. Now, consider the subextensions $M_j\subset L$ fixed by H_j when, j takes the values $j=0,\ldots,p$, we need to find all $\alpha\in L^*$ such that $N_{L/M_j}(\alpha)=1$ whenever $k\subseteq M_j\subsetneq L$. The above considerations implies the following equations for each H_j,

$$N_{L/M_j}(\alpha)=\alpha\sigma\tau^j(\alpha)(\sigma\tau^j)^2(\alpha)\ldots(\sigma\tau^j)^{p-1}(\alpha)=1$$

for $j=0,\ldots,p-1$, for $j=p$ the equation

$$\alpha\tau(\alpha)(\tau)^2(\alpha)\ldots(\tau)^{p-1}(\alpha)=1$$

and the equation

$$N_{L/k}(\alpha)=\frac{\alpha\sigma(\alpha)\ldots\sigma^{p-1}\sigma\tau(\alpha)\ldots}{\sigma^{p-1}\tau(\alpha)\sigma\tau^{p-1}(\alpha)\ldots\sigma^{p-1}\tau^{p-1}(\alpha)}=1 \tag{4}$$

by the inclusion of field k fixed by G.

Recalling that all H_j are different and the union of H_j are the elements of G without repetitions except the identity, then multiplying the first $p+1$ equations it follows that

$$\alpha^p\alpha\sigma(\alpha)\ldots\sigma^{p-1}\sigma\tau(\alpha)\ldots \sigma^{p-1}\tau(\alpha)\sigma\tau^{p-1}(\alpha)\ldots\sigma^{p-1}\tau^{p-1}(\alpha)=1.$$

From the last equation and using 4 we have $\alpha^p=1$ being a necessary condition. If the field k contains the p-th roots of unity, then $\alpha^p=1$ turns out to be a sufficient condition, consequently $\mathscr{T}_L(k)$ is equal to $\mu_p(k)$. ■

Theorem 7 *Under the hypothesis of Lemma 6 with $G\cong C_{p^r}\times C_{p^s}$ and $r,s\geq 1$, then $\mathscr{T}_L(k)$ is equal to $\mu_p(k)$.*

Proof. To prove the theorem consider G generated by σ and τ with $\sigma^{p^r}=\tau^{p^s}=1$. The group $G\cong C_{p^r}\times C_{p^s}$ contains the subgroup $C_p\times C_p$ generated by $\sigma^{p^{r-1}}$ and $\tau^{p^{s-1}}$ and so the equation $\alpha^p=1$ appears again using similar argument that the

Lemma 6. This equation shows that the solutions must be the p-th roots of unity, but we need to prove that these satisfies the equations $N_{L/M_i}(\alpha) = 1$ for M_i fixed by the other subgroups in G that are not contained in $C_p \times C_p$. As k contains the p-th roots of unity and G fixes any element in k, then the subgroups in G that are not contained in $C_p \times C_p$ induce equations in the form $\alpha^{p^{k_i}} = 1$ for $2 \leq k_i \leq r+s$. The last equations contain in its solutions the p-th roots of unity hence these are the only solutions that satisfy all the equations. ■

The example below illustrates these cases, besides show how to construct a p-adic field extension with Galois group $G \cong C_p \times C_p$:

Example 8 *This example is constructing an extension L/k being Galois, abelian and splitting with group $G \cong C_3 \times C_3$. Consider $k/\mathbb{Q}_5$ an extension non-ramified of $\mathbb{Q}_5$ of degree 2, in fact $k = \mathbb{Q}_5(w)$ with w a primitive (5^2-1)-th root of unity, thus it is ensured that k contains the 3-th roots of unity . Now, consider L/k a tamely ramified extension with ramification index $e = 3$ and residual degree $f = 3$ constructed as $L = k(w, \sqrt[3]{5})$. Using the theorem in ([4], p.251) with $r = 0$ it is easy to prove that this extension is Galois and abelian. On the other hand [5] proved that L/k split if and only if L contains a prime $\overline{\pi}$ such that $\overline{\pi}^{\mathfrak{e}} = \pi$ with π a prime in k which yields $\mathscr{G} \cong J \times H$ with H the Galois group associated with the extension $L/k(\sqrt[\mathfrak{e}]{\pi})$ that is non-ramified and then cyclic, i.e. both H and J are cyclic groups (J is the group associated to the Kummer extension K/K_0). In this case $H \cong C_3$ and $J \cong C_3$ therefore $G \cong C_3 \times C_3$. Now, the k-rational points of $\mathscr{T}_L$ are equal to the k-rational points of μ_p, then by Proposition 5*

$$\mathscr{T}_L(k) = (\mu_p(k), \cdot) \cong (\mathbb{F}_p, +).$$

References

[1] A. Borel. *Linear Algebraic Groups*. Grad. Texts in Math. Springer-Verlag, segunda edition, (1991).

[2] A. Menezes D. Hankerson and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, first edition, (2004).

[3] G. Frey et al. H. Cohen. *Handbook ok Elliptic and Hyperelliptic Curve Cryptography*. Chatman and Hall/CRC, first edition, (2006).

[4] H. Hasse. *Number Theory*. Springer-Verlag, tercera edition, (1969).

[5] K. Iwasawa. On galois groups of local fields. *Trans. Amer. Math. Soc.*, **80**:448–469, 1965.

[6] A. Menezes and S. Vanstone. The implementation of elliptic curve cryptosystems. In *Advances in Cryptology-AUSCRYPT' 90*, pages 2–13, (1990).

[7] K. Rubin and A. Silverberg. Torus-based cryptography. in crypto 2003. *Lecture Notes in Comput. Sci.*, **2729**:349–365, 2003.

[8] K. Rubin and A. Silverberg. Algebraic tori in cryptography. In *High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, number 41 in Field institute Communications, pages 317–326. American Mathematical Society, Providence, RI, (2004).

[9] M. Tarnauceanu. An arithmetic method of counting the subgroups of a finite abelian group. *Bull. Math. Soc. Sci. Math. Roumanie*, **53**(4):373–386, 2010.

[10] V. E. Voskresenskii. *Algebraic Groups and Their Birational Invariants*. Number 179 in Transl. Math. Monogr. American Mathematical Society, (1998).