To appear in Serdica Math. J. **44** (2018)

**Serdica**
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

# LOCALLY FINITE MODULES WITH NOETHER NORMALIZATION*

Azniv Kasparian, Vasil Magaranov

*Communicated by V. Drensky*

Abstract. The aim of this note is to show that if a finite field $k$ with absolute Galois group $\mathfrak{G}$ acts on a set $M$ with finite orbits and for some $m$ there is a $\mathfrak{G}$-equivariant map $\xi : M \to \overline{k}^m$, whose fibres are of bounded cardinality, then $M$ admits a $\mathfrak{G}$-equivariant embedding in an affine space $\overline{k}^n$ of sufficiently large dimension $n$.

## 1. Introduction.

Grothendieck has noticed that the Galois theory of fields is related to the Galois theory of coverings through the bijective correspondence between the finite coverings $f : Y \to X$ of algebraic varieties over a field $k$ and the finite extensions $k(X) \subset k(Y)$ of function fields. This led him to the notion of a Galois category (cf. [1], [7], [4] or [3]). To any connected scheme $X$ Grothendieck associates a profinite group $\pi^{\mathrm{et}}(X)$, called the etale fundamental group of $X$ and shows that the category of the finite etale coverings of $X$ is equivalent to the category of the finite sets with discrete topology, acted continuously by $\pi_1^{\mathrm{et}}(X)$. In particular, if $k$ is a perfect field with algebraic closure $\overline{k}$ then the

2010 *Mathematics Subject Classification:* 14G15, 14R20.
*Key words:* Affine varieties, locally finite modules, Noether normalization.

*This research is partially supported by Contract 80-10-135/25.04.2018 with the Scientific Foundation of Sofia University " St. Kliment Ohridski".

etale fundamental group $\pi_1^{\text{et}}(k) = \text{Gal}(\overline{k}/k)$ coincides with the absolute Galois group of $k$.

Note that $\text{Gal}(\overline{k}/k)$ acts on any algebraic variety $X$, defined over $k$ and the finite extensions $k_1 \supset k$ induce finite separable extensions $k_1(X) \supset k(X)$ of function fields. For the interplay between $k(X) \subset k_1(X)$ and the finite separable extensions $k(X) \subset k(Y)$, arising from finite coverings $Y \to X$see [6] or [5]. In general, the absolute Galois group $\text{Gal}(\overline{k}/k)$ of a perfect field $k$ is quite complicated. However, for a finite field $k = \mathbb{F}_q$, the group $\mathfrak{G} = \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}}$ is the profinite completion of the infinite cyclic group, generated by the Frobenius automorphism $\Phi_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, $\Phi_q(\alpha) = \alpha^q$. The $\mathfrak{G}$-orbits $\text{Orb}_{\mathfrak{G}}(p)$ on a smooth projective curve $C \ni p$, defined over $\mathbb{F}_q$ correspond to the discrete valuation rings $\mathcal{O}_p(C)$ of $\mathbb{F}_q(X)$ in such a way that the cardinality of $\text{Orb}_{\mathfrak{G}}(p)$ equals the degree $[\mathcal{O}_p(C)/\mathfrak{M}_p(C) : \mathbb{F}_q]$ of its associated valuation. Based on this fact, [2] introduces the Hasse-Weil $\zeta$-function $\zeta_M(t)$ of a set $M$, acted by $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with finite orbits. By a combinatorial argument it derives a sufficient condition for the Riemann Hypothesis Analogue on $\zeta_M(t)$.

The present note studies to what extent the $\mathfrak{G} = \text{Gal}(\overline{k}/k)$-action on an affine variety $X \subseteq \overline{k}^n$, defined over $k = \mathbb{F}_q$, determines the geometric properties of $X$. We say that a set $M$ with a $\mathfrak{G}$-action is a locally finite $\mathfrak{G}$-module if all $\mathfrak{G}$-orbits on $M$ are finite and there are finitely many $\mathfrak{G}$-orbits of fixed cardinality. An arbitrary $\mathfrak{G}$-equivariant map $f : M \to \overline{k}^m$ with fibres of cardinality $\leq s$, $s \in \mathbb{N}$ is called a Noether normalization of $M$. By a combinatorial argument we prove that any locally finite $\mathfrak{G}$-module $M$ with a Noether normalization admits a $\mathfrak{G}$-equivariant embedding $M \hookrightarrow \overline{k}^n$ in an affine space of sufficiently large dimension $n$. The affine varieties $X \subset \overline{k}^n$, defined over $k$ are locally finite $\mathfrak{G}$-modules with a Noether normalization, as well as all $\mathfrak{G}$-submodules $M \subset X$. By specific examples we show that the category of the locally finite $\mathfrak{G}$-modules with a Noether normalization (whose morphisms are the $\mathfrak{G}$-equivariant maps) contains strictly the category of the quasi-affine varieties.

**2. The absolute Galois group of a finite field and its action on the affine varieties.** Let us start with some properties of the action of the absolute Galois group $\mathfrak{G} = \text{Gal}(\overline{k}, k)$ of a finite field $k = \mathbb{F}_q$, on an affine variety $X \subseteq \overline{k}^n$, defined over $k$. If $a = (a_1, \ldots, a_n) \in X$ then $a_i \in \mathbb{F}_{q^m}$ for some $m \in \mathbb{N}$ and all $1 \leq i \leq n$. An arbitrary $\varphi \in \mathfrak{G} = \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ transforms $a$ into $\varphi(a) \in \mathbb{F}_{q^m}^n$, so that $|\text{Orb}_{\mathfrak{G}}(a_1, \ldots, a_n)| \leq q^{mn}$ and all the $\mathfrak{G}$-orbits on $X$ are finite. We refer to the number of elements of an orbit as of its degree. Since $\mathbb{F}_{q^m} \supset \mathbb{F}_q$ is a normal extension, the orbits $\text{Orb}_{\mathfrak{G}}(a_1, \ldots a_n) = \text{Orb}_{\text{Gal}(\mathbb{F}_{q^m}/F_q)}(a_1, \ldots a_n)$ coincide. The Galois group $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \Phi_q \rangle / \langle \Phi_q^m \rangle$ is cyclic of order $m$

and generated by the Frobenius automorphism $\Phi_q(x) = x^q$. If the $\mathfrak{G}$-orbit of $(a_1, \ldots, a_n) \in X$ is of degree $s$ then $(a_1^{q^s}, \ldots, a_n^{q^s}) = \Phi_q^s(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$, whereas $(a_1, \ldots a_n) \in \mathbb{F}_{q^s}^n$. Thus, $X$ has finitely many $\mathfrak{G}$-orbits of fixed degree $s$.

The absolute Galois group $\mathfrak{G} = \mathrm{Gal}(\overline{k}/k)$ is profinite as a projective limit of the finite Galois groups $\mathrm{Gal}(L/k)$ of the finite Galois extensions $L \supseteq k$. In the case of a finite field $k$, any extension $L \supseteq k$ of degree $[L : k] = m$ is Galois and its Galois group $\mathrm{Gal}(L/k) = \langle \Phi_q \rangle / \langle \Phi_q^m \rangle \simeq \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ is a finite quotient group of the infinite cyclic group $\langle \Phi_q \rangle \simeq (\mathbb{Z}, +)$. That is why the absolute Galois group $\mathfrak{G} = \mathrm{Gal}(\overline{k}/k) = \widehat{\langle \Phi_q \rangle} \simeq \widehat{\mathbb{Z}}$ is the profinite completion of $\langle \Phi_q \rangle \simeq (\mathbb{Z}, +)$. Let us endow the finite Galois groups $\mathrm{Gal}(L/k)$ with the discrete topology. Then the induced product topology on $\prod \mathrm{Gal}(L/k)$ is compact and totally disconnected. The closed subgroup $\mathfrak{G}$ of $\prod \mathrm{Gal}(L/k)$ is compact and totally disconnected, as well. The next proposition establishes the continuity of the $\mathfrak{G}$-action on an affine variety $X$ with respect to the Zariski topology.

**Proposition 1.** *If $X \subset \overline{k}^n$ is an affine variety, defined over a finite field $k$ then the action $\mu : \mathfrak{G} \times X \to X$ of $\mathfrak{G} = \mathrm{Gal}(\overline{k}/k)$ on $X$ is continuous with respect to the Zariski topology on $X$.*

Proof. The $\mathfrak{G}$-action on the algebraic closure $\overline{k}$ induces a $\mathfrak{G}$-action on the polynomials $\overline{k}[x_1, \ldots, x_n]$, which fixes all the variables $x_1, \ldots, x_n$. Let $\mu : \mathfrak{G} \times \overline{k}^n \to \overline{k}^n$ be the $\mathfrak{G}$-action on the affine space $\overline{k}^n$ and $V(f) = \{a \in \overline{k}^n | f(a) = 0\}$ for $f \in \overline{k}[x_1, \ldots, x_n]$. Since $X$ is a closed subset of $\overline{k}^n$, it suffices to show that $\mu^{-1}(V(f)) \subset \mathfrak{G} \times \overline{k}^n$ is a closed subset for any polynomial $f$, in order to conclude that $\mu^{-1}(V(f)) \cap (\mathfrak{G} \times X)$ is a closed subset of $\mathfrak{G} \times X$ and to prove the proposition. Note that $f$ has finitely many coefficients and there is a finite extension $L \supseteq k$ with $f \in L[x_1, \ldots, x_n]$. The closed normal subgroup $\mathrm{Gal}(\overline{k}/L)$ of $\mathfrak{G} = \mathrm{Gal}(\overline{k}/k)$ of index $[\mathfrak{G} : \mathrm{Gal}(\overline{k}/L)] = |\mathrm{Gal}(L/k)| = [L : k] = m$ fixes $f$. If $\mathfrak{G} = \cup_{i=1}^m \mathrm{Gal}(\overline{k}/L)\varphi_i$ is the decomposition of $\mathfrak{G}$ into a disjoint union of cosets modulo $\mathrm{Gal}(\overline{k}/L)$ then

$$\mu^{-1}(V(f)) = \cup_{\varphi \in \mathfrak{G}} (\varphi \times V(\varphi^{-1}(f)) = \cup_{i=1}^m Gal(\overline{k}/L)\varphi_i \times V(\varphi_i^{-1}(f))$$

is a closed subset of $\mathfrak{G} \times \overline{k}^n$, as far as $\mathrm{Gal}(\overline{k}/L)\varphi_i$ is a closed subset of $\mathfrak{G} = \mathrm{Gal}(\overline{k}/k)$ and $V(\varphi_i^{-1}(f))$ is a closed subset of $\overline{k}^n$. □

Note that the Zariski topology on an affine variety $X \subseteq \overline{k}^n$ is $T_1$ since the points are closed subsets of $X$. Generalizing the properties of the $\mathfrak{G}$-action on an affine variety $X \subseteq \overline{k}^n$, defined over $k$, we give the following

**Definition 2.** *A set $M$ with an action of $\mathfrak{G}$ is called a $\mathfrak{G}$-module.*

*A $\mathfrak{G}$-module is locally finite if all $\mathfrak{G}$-orbits on $M$ are finite and for any $s \in \mathbb{N}$ there are finitely many $\mathfrak{G}$-orbits on $M$ of cardinality $s$.*

*A $\mathfrak{G}$-module $M$ is $T_1$-continuous if there is a $T_1$-topology on $M$, with respect to which the $\mathfrak{G}$-action $\mathfrak{G} \times M \to M$ is a continuous map.*

**3. Noether normalization.** In the present section we start our study of the morphisms of $\mathfrak{G}$-modules, i.e., of the $\mathfrak{G}$-equivariant maps of $\mathfrak{G}$-modules.

**Definition 3.** *Let $\xi : M \to N$ be a morphism of $\mathfrak{G}$-modules.*

- *If all the fibres of $\xi$ are finite sets then $\xi$ is called a finite morphism.*
- *If there exists $d \in \mathbb{N}$, such that all the fibres of $\xi$ are of cardinality $\leq d$ then $\xi$ is said to be of bounded degree $d$.*
- *A morphism $\xi : M \to N$ in a $\mathfrak{G}$-submodule $N \subseteq \overline{k}^n$ of an affine space is dominant if the Zariski closure $\overline{\xi(M)} = N$ of the image of $\xi$ coincides with $N$.*

**Definition 4.** *If $M$ is a $\mathfrak{G}$-module then any $\mathfrak{G}$-equivariant map $\xi : M \to \overline{k}^n$ of bounded degree with Zariski dense image $\overline{\xi(M)} = \overline{k}^n$ is called a Noether normalization of $M$.*

**Proposition 5.** *Let $M \subseteq \overline{\mathbb{F}_q}^n$ be a $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-submodule of $\overline{\mathbb{F}_q}^n$ with an irreducible Zariski closure $\overline{M} \subseteq \overline{\mathbb{F}_q}^n$ of dimension $d$. Then there exist $m \in \mathbb{N}$, a $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-submodule $M_1 \subseteq M$ with the same Zariski closure $\overline{M_1} = \overline{M}$ and a finite morphism $\xi : M_1 \to \overline{k}^d$ of $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-modules of bounded degree with Zariski dense image $\overline{\xi(M_1)} = \overline{k}^d$.*

P r o o f. The function field $\overline{k}(X)$ of the affine variety $X = \overline{M}$ is a finite extension of the function field $\overline{k}(y_1, \dots, y_d)$ of $\overline{k}^d$ and there exists a non-empty Zariski open subset $U \subseteq X$ with a dominant regular map $\xi : U \to \overline{k}^d$, whose fibres are of cardinality $t := [\overline{k}(X) : \overline{k}(y_1, \dots, y_d)]$. For a sufficiently small $U$ the map $\xi = \left(\frac{f_1}{g_1}, \dots, \frac{f_d}{g_d}\right)$ is given by an ordered $d$-tuple of rational functions $\frac{f_i}{g_i} \in \overline{k}(x_1, \dots, x_n)$. Any Zariski open subset $U \subseteq X$ is a finite union $U = \cup_{1 \leq j \leq s} U_{h_j}$ of principal Zariski open subsets $U_{h_j} = \{(a_1, \dots, a_n) \in X | h_j(a_1, \dots, a_n) \neq 0\}$, determined by polynomials $h_j \in \overline{k}[x_1, \dots, x_n]$. If all the coefficients of $f_i, g_i$, $1 \leq i \leq n$ and of $h_j$, $1 \leq j \leq s$ are contained in $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q = k$ for some $m \in \mathbb{N}$ then $\xi : U \to \overline{k}^d$ is a $\mathrm{Gal}(\overline{k}/\mathbb{F}_{q^m})$-equivariant map of the $\mathrm{Gal}(\overline{k}/\mathbb{F}_{q^m})$-submodule $U$ of $X$. The restriction $\xi|_{M \cap U} : M \cap U \to \overline{k}^d$ is a morphism of $\mathrm{Gal}(\overline{k}/\mathbb{F}_{q^m})$-modules of degree $\leq t$. There remains to be shown that $\overline{M \cap U} = X$ and $\overline{\xi(M \cap U)} = \overline{k}^d$.

An arbitrary non-empty open set $\emptyset \neq W \subseteq X$ has non-empty open intersection with $U$, due to the irreducibility of $X$. Consequently, $\emptyset \neq U \cap W \cap M$ since $M$ is dense in $X$. This proves the Zariski density of $M \cap U$ in $X$. Let us assume that $\xi(M \cap U)$ is not Zariski dense in $\overline{k}^d$. Then there is a non-empty Zariski open subset $V \subseteq \overline{k}^d$ with $\xi(M \cap U) \cap V = \emptyset$. The Zariski open subset $\xi^{-1}(V) \subseteq X$ intersects the Zariski dense subset $M \cap U \subseteq X$ and any $x \in \xi^{-1}(V) \cap M \cap U$ maps to $\xi(x) \in V \cap \xi(M \cap U)$. That contradicts the assumption $\xi(M \cap U) \cap V = \emptyset$ and proves the Zariski density of $\xi(M \cap U)$ in $\overline{k}^d$. □

The above proposition establishes that the submodules of affine spaces have a Noether normalization. We are going to show that any locally finite $T_1$-continuous module with a Noether normalization admits an equivariant embedding in an affine space.

**4. Affine embeddings of locally finite $T_1$-continuous modules with a Noether normalization.** We claim that if $M$ is a locally finite $T_1$-continuous module over $\mathfrak{G} = \widehat{\langle \Phi_q \rangle}$, then the orbits $\mathrm{Orb}_{\mathfrak{G}}(x) = \mathrm{Orb}_{\langle \Phi_q \rangle}(x)$ coincide. On one hand, $\langle \Phi_q \rangle$ is residually finite and embeds in $\mathfrak{G}$, so that $\mathrm{Orb}_{\langle \Phi_q \rangle}(x) \subseteq \mathrm{Orb}_{\mathfrak{G}}(x)$. If $\left| \mathrm{Orb}_{\langle \Phi_q \rangle}(x) \right| = m$ then $\mathrm{Stab}_{\langle \Phi_q \rangle}(x)$ is of index $[\langle \Phi_q \rangle : \mathrm{Stab}_{\langle \Phi_q \rangle}(x)] = m$, whereas $\mathrm{Stab}_{\langle \Phi_q \rangle}(x) = \langle \Phi_q^m \rangle$. The continuity of the action $\mu : \mathfrak{G} \times M \to M$ with respect to a $T_1$-topology on $M$ implies the continuity of the maps $\mu_y : \mathfrak{G} \to M$, $\mu_y(\varphi) = \varphi(y)$ for all $y \in M$. The points $y \in M$ form closed subsets $\{y\} \subset M$ with respect to any $T_1$-topology on $M$, so that $\mu_y^{-1}(y) = \mathrm{Stab}_{\mathfrak{G}}(y)$ are closed subgroups of $\mathfrak{G}$. The closure of $\langle \Phi_q^m \rangle$ in $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ coincides with the profinite completion $\mathfrak{G}_m = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$ of $\langle \Phi_q^m \rangle$, so that $\langle \Phi_q^m \rangle \subseteq \mathrm{Stab}_{\mathfrak{G}}(x)$ implies $\mathfrak{G}_m \subseteq \mathrm{Stab}_{\mathfrak{G}}(x)$. As a result, $m = [\mathfrak{G} : \mathfrak{G}_m] \geq [\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(x)] = |\mathrm{Orb}_{\mathfrak{G}}(x)| \geq \left| \mathrm{Orb}_{\langle \Phi_q \rangle}(x) \right| = m$, whereas $\mathrm{Orb}_{\mathfrak{G}}(x) = \mathrm{Orb}_{\langle \Phi_q \rangle}(x)$. Thus, the degree of $\mathrm{Orb}_{\mathfrak{G}}(x)$ is the minimal natural number $m$ with $\Phi_q^m(x) = x$.

**Definition 6.** *Let $M$ be a locally finite $T_1$-continuous $\mathfrak{G}$-module. Then*

- $M^{\Phi_q^k} := \left\{ x \in M \mid \Phi_q^k(x) = x \right\}$ *is called the set of the $\mathbb{F}_{q^k}$-rational points of $M$;*
- $N_k(M) := \left| M^{\Phi_q^k} \right|$ *is the number of the $\mathbb{F}_{q^k}$-rational points of $M$;*
- $\mathfrak{B}_k(M) := \{ x \in M \mid |\mathrm{Orb}_{\mathfrak{G}}(x)| = k \}$ *is the set of the points of $M$, whose $\mathfrak{G}$-orbits are of degree $k$ and*
- $B_k(M) := \dfrac{1}{k} |\mathfrak{B}_k(M)|$ *is the number of the $\mathfrak{G}$-orbits on $M$ of degree $k$.*

Note that $\mathfrak{B}_k(M)$ and $M^{\Phi_q^k}$ are $\mathfrak{G}$-modules, as far as $\mathfrak{G}$ is an abelian group and all the points from some $\mathfrak{G}$-orbit have coinciding stabilizers. Moreover, $\mathfrak{B}_k(M) \subseteq M^{\Phi_q^k}$, so that $kB_k(M) \leq N_k(M)$.

**Proposition 7.** *Let $L$ be a locally finite $\mathfrak{G}$-module and $k, n \in \mathbb{N}$ be natural numbers. Then for any $1 \leq i \leq n$ the set*

$$L_k^{(i)} := (L^{\Phi_q^k})^{i-1} \times \mathfrak{B}_k(L) \times (L^{\Phi_q^k})^{n-i} \subset (L^{\Phi_q^k})^n = (L^n)^{\Phi_q^k}$$

*is contained in the $\mathfrak{G}$-submodule $\mathfrak{B}_k(L^n)$ of $L^n$ and there holds the inequality*

$$kB_k(L^n) \geq \left| \bigcup_{1\leq i\leq n} L_k^{(i)} \right| = N_k(L)^n - [N_k(L) - kB_k(L)]^n \tag{1}$$

Proof. If $(a_1, \dots, a_n) \in L_k^{(i)}$ then $d = |\operatorname{Orb}_{\mathfrak{G}}(a_1, \dots, a_n)|$ is the minimal natural number with $\Phi_q^d(a_1, \dots, a_n) = (a_1^{q^d}, \dots, a_n^{q^d}) = (a_1, \dots, a_n)$, so that $d \leq k$. Since $k$ is the minimal natural number with $\Phi_q^k(a_i) = a_i$, there follow $k = d$ and $L_k^{(i)} \subseteq \mathfrak{B}_k(L^n)$. Combining $\bigcup_{1\leq i\leq n} L_k^{(i)} \subseteq \mathfrak{B}_k(L^n)$ with

$$\bigcup_{1\leq i\leq n} L_k^{(i)} = (L^{\Phi_q^k})^n \setminus \left[ (L^{\Phi_q^k})^n \setminus \bigcup_{1\leq i\leq n} L_k^{(i)} \right] =$$

$$= (L^{\Phi_q^k})^n \setminus \left\{ \cap_{1\leq i\leq n} [(L^{\Phi_q^k})^n \setminus L_k^{(i)}] \right\} =$$

$$= (L^{\Phi_q^k})^n \setminus \left\{ \cap_{1\leq i\leq n} (L^{\Phi_q^k})^{i-1} \times [L^{\Phi_q^k} \setminus \mathfrak{B}_k(L)] \times (L^{\Phi_q^k})^{n-i} \right\} =$$

$$= (L^{\Phi_q^k})^n \setminus \left\{ \left[ L^{\Phi_q^k} \setminus \mathfrak{B}_k(L) \right]^n \right\},$$

one derives (1). □

For an arbitrary morphism $\xi : M \to L$ of $\mathfrak{G}$-modules and an arbitrary point $x \in M$ one has $\operatorname{Stab}_{\mathfrak{G}}(x) \leq \operatorname{Stab}_{\mathfrak{G}}(\xi(x))$. Moreover, if the $\mathfrak{G}$-action on $M$ has finite orbits then one defines the inertia map

$$e_\xi : M \to \mathbb{Q},$$

$$e_\xi(x) := \frac{\deg \operatorname{Orb}_{\mathfrak{G}}(x)}{\deg \operatorname{Orb}_{\mathfrak{G}}(\xi(x))} = \frac{[\mathfrak{G} : \operatorname{Stab}_{\mathfrak{G}}(x)]}{[\mathfrak{G} : \operatorname{Stab}_{\mathfrak{G}}(\xi(x))]} = [\operatorname{Stab}_{\mathfrak{G}}(\xi(x)) : \operatorname{Stab}_{\mathfrak{G}}(x)] \in \mathbb{N}$$

and notes that it takes natural values. As far as the inertia map is constant on the $\mathfrak{G}$-orbits of $M$, the set $M^{[t]} = \{x \in M \mid e_\xi(x) = t\}$ is a $\mathfrak{G}$-submodule of $M$.

Let $\xi : M \to L$ be a morphism of bounded degree $d$ between locally finite $T_1$-continuous $\mathfrak{G}$-modules. Then

$$\mathfrak{B}_k(M^{[s]}) = \{x \in M | k = \deg \mathrm{Orb}_{\mathfrak{G}}(x) = s \deg \mathrm{Orb}_{\mathfrak{G}}(\xi(x))\} \neq \emptyset$$

only when $s \in \mathbb{N}$ divides $k \in \mathbb{N}$. If so, then $\xi(\mathfrak{B}_k(M^{[s]})) \subseteq \mathfrak{B}_{\frac{k}{s}}(L) \cap \xi(M^{[s]}) = \mathfrak{B}_{\frac{k}{s}}(\xi(M^{[s]}))$. Conversely, if $y \in \mathfrak{B}_{\frac{k}{s}}(\xi(M^{[s]}))$ then $y = \xi(x)$ for some $x \in M^{[s]}$. As a result, $\deg \mathrm{Orb}_{\mathfrak{G}}(x) = s \deg \mathrm{Orb}_{\mathfrak{G}}(\xi(x)) = k$, so that $x \in \mathfrak{B}_k(M^{[s]})$. That justifies $\mathfrak{B}_{\frac{k}{s}}(\xi(M^{[s]})) \subseteq \xi(\mathfrak{B}_k(M^{[s]}))$ and

$$\xi(\mathfrak{B}_k(M^{[s]})) = \mathfrak{B}_{\frac{k}{s}}(\xi(M^{[s]})).$$

In particular, $\xi(\mathfrak{B}_k(M^{[s]})) \subseteq \mathfrak{B}_{\frac{k}{s}}(L)$, so that $\mathfrak{B}_k(M^{[s]}) \subseteq \xi^{-1}(\mathfrak{B}_{\frac{k}{s}}(L))$ and there holds $kB_k(M^{[s]}) \leq d\dfrac{k}{s}B_{\frac{k}{s}}(L)$. Therefore

$$B_k(M^{[s]}) \leq \frac{d}{s} B_{\frac{k}{s}}(L).$$

Note that $\xi(\mathrm{Orb}_{\mathfrak{G}}(x)) \subseteq \mathrm{Orb}_{\mathfrak{G}}(\xi(x))$ implies $\mathrm{Orb}_{\mathfrak{G}}(x) \subseteq \xi^{-1}(\mathrm{Orb}_{\mathfrak{G}}(\xi(x))$, whereas $\deg \mathrm{Orb}_{\mathfrak{G}}(x) \leq d \deg \mathrm{Orb}_{\mathfrak{G}}(\xi(x))$. Therefore $e_{\xi}(x) \leq d$. That allows to split $M$ into a disjoint union $M = \bigcup\limits_{1 \leq i \leq d} M^{[i]}$ and to observe that

$$B_k(M) = \sum_{1 \leq i \leq d} B_k(M^{[i]}) = \sum_{i \leq d;\ i/k} B_k(M^{[i]}) \leq \sum_{i \leq d;\ i/k} \frac{d}{i} B_{\frac{k}{i}}(L) =$$
$$\frac{d}{k} \sum_{i \leq d;\ i/k} \frac{k}{i} B_{\frac{k}{i}}(L) \leq \frac{d}{k} N_k(L)$$

In such a way, we have derived

$$B_k(M) \leq \frac{d}{k} N_k(L). \tag{2}$$

The inequalities (1) and (2) will be used for showing that an arbitrary locally finite $T_1$-continuous $\mathfrak{G}$-module with a Noether normalization admits a $\mathfrak{G}$-equivariant embedding in an affine space of sufficiently large dimension. Prior to that, we derive a lower bound on $B_k(\overline{\mathbb{F}_q})$.

**Proposition 8.** *For any $k \in \mathbb{N}$ there holds*

$$kB_k(\overline{\mathbb{F}_q}) \geq q^{k/2} \tag{3}$$

P r o o f. Let $a$ be a generator of the multiplicative group $\mathbb{F}_{q^k}^* = \langle a \rangle$. Then $q^k - 1 \in \mathbb{N}$ is the minimal natural number with $a^{q^k - 1} = 1$ and $k \in \mathbb{N}$

is the minimal natural number with $a^{q^k} = a$, so that $\mathrm{Stab}_{\langle \Phi_q \rangle}(a) = \langle \Phi_q^k \rangle$ and $\mathrm{Orb}_{\langle \Phi_q \rangle}(a) = \mathrm{Orb}_{\mathfrak{G}}(a)$ is of degree $\deg \mathrm{Orb}_{\mathfrak{G}}(a) = [\langle \Phi_q \rangle : \langle \Phi_q^k \rangle] = k$. For an arbitrary natural number $1 \leq s \leq q^k - 1$, if $\deg \mathrm{Orb}_{\mathfrak{G}}(a^s) = \deg \mathrm{Orb}_{\langle \Phi_q \rangle}(a^s) = d$ then

$$\langle \Phi_q^d \rangle = \mathrm{Stab}_{\langle \Phi_q \rangle}(a^s) \geq \mathrm{Stab}_{\langle \Phi_q \rangle}(a) = \langle \Phi_q^k \rangle,$$

whereas $\Phi_q^k \in \langle \Phi_q^d \rangle$ and $d$ divides $k$. In particular, $d \leq k$ and $q^d - 1$ divides $q^k - 1$. On the other hand, $\Phi_q^d \in \mathrm{Stab}_{\langle \Phi_q \rangle}(a^s)$ implies $(a^s)^{q^d} = a^s$, whereas $a^{s(q^d-1)} = 1$. Therefore the order $q^k - 1$ of $a$ divides $s(q^d - 1)$ and, in particular, $q^k - 1 \leq s(q^d - 1)$. As a result,

$$s \geq \frac{q^k - 1}{q^d - 1} = q^{k-d} + q^{k-2d} + \ldots + q^d + 1 \geq q^{k-d} + 1.$$

If $d < k$ then $k/d \in \mathbb{N}$, $k/d > 1$, whereas $k/d \geq 2$, which is equivalent to $k/2 \geq d$. Therefore

$$s \geq q^{k-d} + 1 \geq q^{k-k/2} + 1 > q^{k/2}$$

whenever $d < k$. In other words, for any $1 \leq s \leq q^{k/2}$ the orbit $\mathrm{Orb}_{\mathfrak{G}}(a^s)$ is of degree $\deg \mathrm{Orb}_{\mathfrak{G}}(a^s) = k$ and $a^s \in \mathfrak{B}_k(\overline{\mathbb{F}_q})$. That implies (3). □

Now, we are ready to prove our main result:

**Theorem 9.** *Let $M$ be a locally finite $T_1$-continuous $\mathfrak{G}$-module with a $\mathfrak{G}$-equivariant map $\xi : M \to \overline{\mathbb{F}_q}^m$ of bounded degree $d$ (i.e $\xi$ is a Noether normalization of $M$). Then there exists a $\mathfrak{G}$-equivariant embedding $\mu : M \to \overline{\mathbb{F}_q}^n$ for a sufficiently large $n \in \mathbb{N}$.*

Proof. For any $k \in \mathbb{N}$ inequality (2) implies that

$$B_k(M) \leq \frac{d}{k} N_k(\overline{\mathbb{F}_q}^m) = \frac{d}{k} N_k(\overline{\mathbb{F}_q})^m = \frac{d}{k}(q^k)^m = \frac{d}{k} q^{km}.$$

On the other hand, by (3) from Proposition 8 and (1) there follows

$$B_k(\overline{\mathbb{F}_q}^n) \geq \frac{N_k(\overline{\mathbb{F}_q})^n - [N_k(\overline{\mathbb{F}_q}) - kB_k(\overline{\mathbb{F}_q})]^n}{k} =$$

$$= \frac{q^{kn} - [q^k - kB_k(\overline{\mathbb{F}_q})]^n}{k} \geq \frac{q^{kn} - (q^k - q^{k/2})^n}{k}.$$

We are going to show the existence of a natural number $n \in \mathbb{N}$ with

$$dq^{km} \leq q^{kn} - (q^k - q^{k/2})^n \quad \text{for all} \quad k \in \mathbb{N}, \tag{4}$$

in order to have $\mathfrak{G}$-equivariant embeddings $\mu_k : \mathfrak{B}_k(M) \to \mathfrak{B}_k(\overline{\mathbb{F}_q}^n)$ for all $k \in \mathbb{N}$, which give rise to a $\mathfrak{G}$-equivariant embedding $\mu : M \to \overline{\mathbb{F}_q}^n$. Note that (4) is equivalent to

$$q^{k(n-m)} - q^{k(n/2-m)} \left(q^{k/2} - 1\right)^n - d \geq 0$$

and consider the function

$$f(x) := q^{x(n-m)} - q^{x(n/2-m)} \left(q^{x/2} - 1\right)^n - d.$$

It suffices to prove that $f(x)$ is an increasing function of a real variable $x \in [1, +\infty)$ with $f(1) \geq 0$ for a sufficiently large $n \in \mathbb{N}$, in order to establish that $f(k) \geq 0$ for all $k \in \mathbb{N}$ and to conclude the proof of the theorem. To this end, let us introduce $t := q^{x/2}$ and note that

$$f(x) = t^{2(n-m)} - t^{n-2m}(t-1)^n - d = t^{n-2m}[t^n - (t-1)^n] - d.$$

The function $h(t) := t^n - (t-1)^n$ takes positive values and increases for $t \geq q^{1/2}$, as far as its derivative $h'(t) = n[t^{n-1} - (t-1)^{n-1}] \geq 0$. For $n > 2m$ the function $t^{n-2m}$ is non-negative and increasing, as well. Therefore $f(x)$ is a non-negative increasing function on $t \geq q^{1/2}$ and according to $\frac{d}{dx}t = \frac{d}{dx}q^{x/2} = \frac{\log(q)}{2}q^{x/2} \geq 0$, one has $\frac{d}{dx}f(x) = \frac{d}{dt}f(x)\frac{dt}{dx} \geq 0$ for all $x \geq 1$. That suffices for $f(x)$ to be an increasing function on $x \in [1, +\infty)$, whenever $n > 2m$.

There remains to be shown the existence of $n \in \mathbb{N}$, $n > 2m$ with

$$f(1) = q^{n-m} - q^{n/2-m} \left(q^{1/2} - 1\right)^n - d \geq 0.$$

To this end, it suffices to prove that the auxiliary function

$$g(x) := q^{x-m} - q^{x/2-m} \left(q^{1/2} - 1\right)^x = q^{x/2-m} \left[q^{x/2} - \left(q^{1/2} - 1\right)^x\right]$$

tends to $+\infty$ as $x \to +\infty$. We denote by $r$ the constant $q^{\frac{1}{2}}$ and show that

$$G(x) := \frac{r^x}{q^m}\left[r^x - (r-1)^x\right]$$

has $\lim_{x \to +\infty} G(x) = +\infty$ for any fixed $r > 1$. The function $g_1(x) := r^x - (r-1)^x$ is strictly increasing, as far as it has a strictly positive derivative

$$\frac{d}{dx}g_1(x) = \log(r)r^x - \log(r-1)(r-1)^x =$$

$$= \log(r)[r^x - (r-1)^x] + [\log(r) - \log(r-1)](r-1)^x > 0.$$

Therefore $\lim_{x \to +\infty} g_1(x) = +\infty$, whereas

$$\lim_{x \to +\infty} G(x) = \left(\lim_{x \to +\infty} \frac{r^x}{q^m}\right) \left(\lim_{x \to +\infty} g_1(x)\right) = +\infty$$

for any fixed $r > 1$. In particular, for a sufficiently large $n \in \mathbb{N}$ one has $f(1) = g(n) \geq 0$. $\Box$

**5. Some distinctions between the morphisms of $\mathfrak{G}$-modules and the morphisms of affine varieties.** It is well known that if $f : X \to \overline{\mathbb{F}_q}$ is a finite morphism of affine varieties then $X$ is a curve, $f$ is of bounded degree $d$ and $f$ has a finite branch locus

$$R := \{z \in f(X) | \left|f^{-1}(z)\right| < d\}.$$

The present section provides an example of a finite morphism $\xi : M \to \overline{\mathbb{F}_q}$ of locally finite $\mathfrak{G}$-modules of unbounded degree and an example of a finite morphism $\eta : N \to \overline{\mathbb{F}_q}$ of locally finite $\mathfrak{G}$-modules of bounded degree $d$ with an infinite branch locus $R$. These examples reveal that the locally finite $T_1$-continuous $\mathfrak{G}$-action allows a larger diversity of morphisms than the Zariski topology.

Let us consider the $\mathfrak{G}$-submodules

$$M := \{(a, b) \in \overline{\mathbb{F}_q}^2 | \deg \mathrm{Orb}_{\mathfrak{G}}(a) \neq \deg \mathrm{Orb}_{\mathfrak{G}}(b)\}$$

of $\overline{\mathbb{F}_q}^2$ and $\overline{\mathbb{F}_q}' := \overline{\mathbb{F}_q} \setminus \mathbb{F}_q = \bigcup_{i \geq 2} \mathfrak{B}_i(\overline{\mathbb{F}_q})$ of $\overline{\mathbb{F}_q}$. The map

$$\xi : M \longrightarrow \overline{\mathbb{F}_q}', \quad \xi(a, b) = \begin{cases} a \text{ for } \deg \mathrm{Orb}_{\mathfrak{G}}(a) > \deg \mathrm{Orb}_{\mathfrak{G}}(b), \\ b \text{ for } \deg \mathrm{Orb}_{\mathfrak{G}}(b) > \deg \mathrm{Orb}_{\mathfrak{G}}(a) \end{cases}$$

is $\mathfrak{G}$-equivariant and has finite fibres

$$\xi^{-1}(a) = \left[ \bigcup_{1 \leq i < \deg \mathrm{Orb}_{\mathfrak{G}}(a)} \mathfrak{B}_i(\overline{\mathbb{F}_q}) \times \{a\} \right] \bigcup \left[ \{a\} \times \bigcup_{1 \leq i < \deg \mathrm{Orb}_{\mathfrak{G}}(a)} \mathfrak{B}_i(\overline{\mathbb{F}_q}) \right]$$

of unbounded degree.

Let $d \in \mathbb{N}$ be coprime to $q$, $X_o := \{(y^d, y) | y \in \overline{\mathbb{F}_q}\}$ and $\eta : X_o \to \overline{\mathbb{F}_q}$, $\eta(y^d, y) = y^d$ be the first canonical projection. Then $X_o$ is a $\mathfrak{G}$-submodule of $\overline{\mathbb{F}_q}^2$ and $\eta$ is a morphism of $X_o$ onto $\overline{\mathbb{F}_q}$. All the fibres of $\eta$ except $\eta^{-1}(0) = (0, 0)$ are of cardinality $d$. We are going to show that if $\delta \in \mathbb{N}$, $\delta > \log_q(d - 1)$ and $\beta$ is a generator of $\mathbb{F}^*_{q^{d\delta}} = \langle \beta \rangle$ then the inertia index of $\eta : X_o \to \overline{\mathbb{F}_q}$ at $(\beta^d, \beta) \in X_o$ is $e_\eta(\beta^d, \beta) < d$. Therefore $\eta^{-1} \mathrm{Orb}_{\mathfrak{G}}(\beta^d) \supsetneqq \mathrm{Orb}_{\mathfrak{G}}(\beta^d, \beta)$ and

$$N := X_o \setminus \left[ \bigcup_{\langle \beta \rangle = \mathbb{F}^*_{q^{d\delta}}, \delta > \log_q(d-1)} \mathrm{Orb}_{\mathfrak{G}}(\beta^d, \beta) \right]$$

is a $\mathfrak{G}$-submodule of $X_o$ with a finite morphism $\eta : N \to \overline{\mathbb{F}_q}$, whose branch locus

$$R := \{z \in \overline{\mathbb{F}_q} \,|\, \left|\eta^{-1}(z) \cap N\right| < d\} \supseteq \bigcup_{\langle\beta\rangle = \mathbb{F}^*_{q^{d\delta}}, \delta > \log_q(d-1)} \mathrm{Orb}_{\mathfrak{G}}(\beta^d)$$

is infinite. Note that there are infinitely many fibres of $\eta : N \to \overline{\mathbb{F}_q}$ of cardinality $d$. For instance, for any natural number $1 \leq r \leq d-1$ and any generator $\gamma_{r,\delta}$ of $\mathbb{F}^*_{q^{d\delta+r}} = \langle \gamma_{r,\delta} \rangle$ the fibre $\eta^{-1}(\gamma^d_{r,\delta})$ is of cardinality $d$ and there are infinitely many such $\gamma_{r,\delta}$ with $\delta > \log_q(d-1)$. Towards $e_\eta(\beta^d, \beta) < d$, note that if $\beta$ is a generator of $\mathbb{F}^*_{q^{d\delta}} = \langle\beta\rangle$ then $\deg \mathrm{Orb}_{\mathfrak{G}}(\beta^d, \beta) = \deg \mathrm{Orb}_{\mathfrak{G}}(\beta) = d\delta$ and $\beta^d \in \mathbb{F}^*_{q^{d\delta}}$ is of order

$$\mathrm{ord}(\beta^d) = \frac{\mathrm{ord}(\beta)}{GCD(\mathrm{ord}(\beta), d)} = \frac{q^{d\delta} - 1}{GCD(q^{d\delta} - 1, d)}.$$

If $e_\eta(\beta^d, \beta) = d$ then

$$\deg \mathrm{Orb}_{\mathfrak{G}}(\beta^d) = \frac{\deg \mathrm{Orb}_{\mathfrak{G}}(\beta^d, \beta)}{e_\eta(\beta^d, \beta)} = \frac{d\delta}{d} = \delta,$$

so that $\mathrm{Stab}_{\mathfrak{G}}(\beta^d) = \langle \Phi^\delta_q \rangle$ and $(\beta^d)^{q^\delta} = \beta^d$. As a result, $(\beta^d)^{q^\delta - 1} = 1$ and the order $\mathrm{ord}(\beta^d)$ of $\beta^d \in \mathbb{F}^*_{q^{d\delta}}$ divides $q^\delta - 1$, i.e.,

$$\frac{q^{d\delta} - 1}{GCD(q^{d\delta} - 1, d)} r = q^\delta - 1 \quad \text{for some} \quad r \in \mathbb{N}.$$

Now,

$$q^\delta + 1 \leq q^{d\delta - \delta} + q^{d\delta - 2\delta} + \ldots + q^\delta + 1 =$$
$$= \frac{q^{d\delta} - 1}{q^\delta - 1} \leq \frac{q^{d\delta} - 1}{q^\delta - 1} r = GCD(q^{d\delta} - 1, d) \leq d$$

implies that $\delta \leq \log_q(d-1)$. In such a way we have shown that if $e_\eta(\beta^d, \beta) = d$ for a generator $\beta$ of $\mathbb{F}^*_{q^{d\delta}} = \langle\beta\rangle$ then $\delta \leq \log_q(d-1)$. Bearing in mind that $e_\eta(\beta^d, \beta) \leq d$ for all $\beta \in \overline{\mathbb{F}_q}$, one concludes that $e_\eta(\beta^d, \beta) < d$ for any generator $\beta$ of $\mathbb{F}^*_{q^{d\delta}} = \langle\beta\rangle$ with $\delta > \log_q(d-1)$.

In the light of the previous example of a morphism $\eta : N \to \overline{\mathbb{F}_q}$ of bounded degree with infinite branch locus, one questions the existence of Noether normalizations $\xi_1 : M \to \overline{\mathbb{F}_q}^{m_1}$, $\xi_2 : M \to \overline{\mathbb{F}_q}^{m_2}$ of one and a same locally finite $\mathfrak{G}$-module $M$ with images of different dimensions $m_1 \neq m_2$.

## REFERENCES

[1] Revêtements étales et groupe fondamental. Séminaire de géométrie algébrique du Bois Marie, 1960–1961, dirigé par A. Grothendieck. Lecture Notes in Mathematics vol **224**, Berlin, Springer-Verlag, 1971.

[2] A. Kasparian, I. Marinov. Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field *Annuaire de l' Universite de Sofia* **104** (2017), 99–137.

[3] H. W. Lenstra. Galois Theory for Schemes. `http://hdl.handle.net/1887/2138`.

[4] J. P. Murre. Lectures on an introduction to Grothendieck's theory of the fundamental group. Tata Institute of Fundamental Research, Lectures on Mathematics vol. **40**, Bombay, 1967.

[5] H. Niederreiter, Ch. Xing. Algebraic Geometry in Coding Theory and Cryptography. Princeton, NJ, Princeton University Press, 2009.

[6] H. Stichtenoth. Algebraic Function Fields and Codes. Universitext. Berlin, Springer-Verlag, 1993.

[7] T. Szamuely. Galois Groups and Fundamental Groups. Cambridge Studies in Advanced Mathematics, vol. **117**. Cambridge, Cambridge University Press, 2009.

*Faculty of Mathematics and Informatics*
*Sofia University "St. Kliment Ohridski"*
*5, J. Bouchier Blvd*
*1164 Sofia, Bulgaria*
*e-mail:* `kasparia@fmi.uni-sofia.bg` *(Azniv Kasparian)*
*e-mail:* `magaranov@abv.bg` *(Vasil Magaranov)*