A CONSTRUCTIVE APPROACH TO A CONJECTURE BY VOSKRESENSKII

MATHIEU FLORENCE AND MICHEL VAN GARREL

ABSTRACT. Voskresenskii conjectured that stably rational tori are rational. Klyachko proved this assertion for a wide class of tori by general principles. We re-prove Klyachko's result by providing simple explicit birational isomorphisms, and elaborate on some links to torus-based cryptography.

CONTENTS

1. INTRODUCTION

Let k be an infinite field of any characteristic. We denote by $\overline{k}$ an algebraic closure of k. A variety X over k is said to be *rational* if it is birational to a projective space $\mathbb{P}_k^n$. A strictly weaker notion is that of stable rationality.

Definition 1.1. Let X be a variety over k. X is said to be *stably rational* if $X \times_k \mathbb{P}_k^m$ is rational for some $m \geq 0$.

Let T be a linear (=affine) algebraic group over k. Then T is said to be an *algebraic torus* if, over an algebraic closure of k, it becomes isomorphic to a product of $\mathbb{G}_m$'s. A conjecture of Voskresenskii (see [5, p. 68]) states that a stably rational torus over k ought to be rational. This conjecture is widely open. A result of Klyachko ([2], see also

[5, sec. 6.3]) gives a positive answer for a special type of stably rational tori, which we describe now (see section 2 for a more detailed description).

Let A and B be étale k-algebras of coprime dimension over k. Denote by $\mathrm{GL}_1(A)$ the algebraic group of invertible elements in A. Let T be the quotient of $\mathrm{GL}_1(A \otimes_k B)$ by the subgroup generated by $\mathrm{GL}_1(A)$ and $\mathrm{GL}_1(B)$. Then T is a stably rational k-torus and Klyachko shows that it is in fact rational. However, his proof by general principles does not provide a simple explicit birational isomorphism from T to a projective space.

We remedy to this by re-proving Klyachko's result, constructing a simple birational map from T to a projective space. We expect our construction to generalize to the situation where A and B are *any* not necessarily commutative finite-dimensional k-algebras, of coprime dimension over k (in that case T is not necessarily a torus, or even an algebraic group).

Finally, in section 4, we explore applications of our explicit birational maps to torus-based cryptography. Following the methods developed by Rubin-Silverberg in [4], we propose more general compression algorithms.

2. Setup and statement of results

Let k be an infinite field of any characteristic and let V be a finite-dimensional k-vector space. We start by recalling some k-schemes that are associated to V. The *affine space of V*, denoted by $\mathbb{A}(V)$, is defined as the functor

$$X \mapsto \mathbb{A}(V)(X) := V \otimes_k \Gamma(X, \mathcal{O}_X),$$

from k-schemes to sets. It is represented by the affine scheme $\mathrm{Spec}\,(\mathrm{Sym}\,V^*)$.
The *projective space of V*, denoted $\mathbb{P}(V)$, represents the (functor of) locally free submodules of rank one $N \subset V$, such that the quotient V/N is locally free. It is defined to be

$$\mathbb{P}(V) := (\mathbb{A}(V) - \{0\}) / \mathbb{G}_m = \mathrm{Proj}\,(\mathrm{Sym}\,V^*)\,.$$

Let A be a not necessarily commutative (unital) k-algebra of finite dimension. The linear algebraic group $\mathrm{GL}_1(A)$ is defined as the functor

$$X \mapsto \mathrm{GL}_1(A)(X) := (A \otimes_k \Gamma(X, \mathcal{O}_X))^\times,$$

from k-schemes to groups. It is represented by the closed subscheme of $\mathbb{A}(A \oplus A)$ given by the equation $xy = 1$. One has a canonical injective homomorphism of algebraic groups

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathrm{GL}_1(A).$$

One can then form the quotient

$$\mathrm{PGL}_1(A) := \mathrm{GL}_1(A)/\mathbb{G}_m;$$

it is a linear algebraic group.

For the remainder, assume that A is commutative.

Then, $\mathrm{GL}_1(A)$ is canonically isomorphic to the Weil restriction of scalars $\mathrm{Res}_{A/k}(\mathbb{G}_m)$. Let M be an A-module, which is locally free of finite rank. Then, we can build the projective space $\mathbb{P}(M)$; it is defined over $\mathrm{Spec}(A)$. In this work, it shall be viewed as a k-variety, by Weil scalar restriction. More explicitly, we set

$$\mathbb{P}_A(M) := \mathrm{Res}_{A/k}(\mathbb{P}(M)).$$

Consider two finite-dimensional commutative k-algebras A and B. We have an exact sequence

$$1 \longrightarrow \mathbb{G}_m \xrightarrow{\ i\ } \mathrm{GL}_1(A) \times \mathrm{GL}_1(B) \xrightarrow{\ j\ } \mathrm{GL}_1(A \otimes_k B),$$
$$i(x) = (x, x^{-1}),\ j(a, b) = a \otimes b.$$

Put $H(A, B) = \mathrm{im}(j)$. We will consider the quotient

$$Q(A, B) := \mathrm{GL}_1(A \otimes_k B)/H(A, B).$$

It follows from [5, section 6.1, theorem 1] that $Q(A, B)$ is stably rational.

Recall that a k-algebra A is said to be étale if one of the two following equivalent conditions holds:

- $A \cong \prod_{i=1}^n k_i$, where the k_i are finite separable field extensions of k.
- $A \otimes_k \overline{k}$, as a $\overline{k}$-algebra, is isomorphic to a finite product of copies of $\overline{k}$.

The main result of this paper is to re-prove, in a constructive fashion, the following result.

Theorem 2.1 (Klyachko in [2], see also [5], section 6.3). *Let k be an infinite field of any characteristic and let A and B be two étale k-algebras of finite dimension. Assume that $\dim(A)$ and $\dim(B)$ are coprime. Then $Q(A, B)$ is k-rational.*

Note that the proof of theorem 2.1 that we provide in section 3 is via explicit birational isomorphisms, whereas Klyachko's original proof is by general principles.

Recall that an algebraic k-torus of dimension d is a k-group scheme T such that

$$T \times_k \overline{k} \cong \mathbb{G}_{m,\overline{k}}^d.$$

The following conjecture states that for algebraic tori, stable rationality is equivalent to rationality.

Conjecture 2.2 (Voskresenskii, see [5], section 6.2)**.** *Stably rational k-tori are k-rational.*

Theorem 2.1 thus provides a positive proof of conjecture 2.2, in a particular case.

3. PROOF OF THE THEOREM

Let A and B be étale k-algebras of coprime dimensions (over k) a and b, respectively. Being invertible is an open condition, so that $\mathrm{GL}_1(A \otimes B)$ is a nonempty open subvariety of $\mathbb{A}(A \otimes B)$. Choose integers $0 < u \leq b$ and $0 < v \leq a$ such that

$$ua + vb = ab + 1.$$

This is possible since a and b are chosen to be coprime to each other. For a k-vector subspace $W \subset A \otimes_k B$, containing 1, denote by

$$\mathbb{P}_1(W) \subset \mathbb{P}(W)$$

the non-empty open subvariety consisting of lines directed by an invertible element of W.

Proposition 3.1. *There exist k-vector subspaces $U \in \mathrm{Gr}(u, B)(k)$ and $V \in \mathrm{Gr}(v, A)(k)$, both containing 1, such that the morphism below is a birational isomorphism:*

$$
\begin{aligned}
\phi_1 \ :\ \mathbb{P}_1(V \otimes_k B) \times \mathbb{P}_1(A \otimes_k U) \quad &\dashrightarrow \quad \mathbb{P}_1(A \otimes_k B) = \mathrm{PGL}_1(A \otimes_k B), \\
(x, y) \quad &\longmapsto \quad xy^{-1}.
\end{aligned}
$$

(3.1)

Proof in the case of fields. We first prove the assertion in the case that A and B are fields. Then $A \otimes_k B$ is a field as well, because a and b are coprime. Take arbitrary U and V as in the statement. We claim that ϕ_1 then is a birational isomorphism. Consider the fibers of ϕ_1. An invertible k-rational point of $\mathrm{PGL}_1(A \otimes_k B)$ is given by the class of $t \in (A \otimes_k B)^*$. The fiber of that class consists of (the projectivization of)

$$\{(x, y) \in (V \otimes_k B) \oplus (A \otimes_k U) \mid x = yt\},$$

where $(V \otimes_k B) \oplus (A \otimes_k U)$ is a vector k-space of dimension $vb + au = ab + 1$. Hence the equation $x = yt$ in $A \otimes_k B$ breaks down into a homogeneous linear system of ab equations in $ab + 1$ variables. It follows that it has a non-trivial solution (x, y) over k. Since $A \otimes_k B$ is a field, both x and y are invertible. This shows that the fiber of ϕ_1 at t is non-empty, even isomorphic to a non-empty open of a projective space. But one may base-change from k to the function field K of $\mathrm{PGL}_1(A \otimes_k B)$, and reproduce the previous arguments with K instead of k (note that K/k is purely transcendental,

hence $A \otimes_k K$ and $B \otimes_k K$ are still fields). We thus get that the generic fiber of ϕ_1 is K-rational. But the source and target of ϕ_1 have the same dimension $ab - 1$. Hence, as asserted, ϕ_1 is a birational isomorphism. $\square$

Proof in the general case. It is a specialization argument as follows. We start by introducing the polynomial algebra (in $a + b$ variables)

$$\mathcal{K} := k[x_0, \ldots, x_{a-1}, y_0, \ldots y_{b-1}],$$

and denote by $\tilde{\mathcal{K}}$ its field of fractions. Set

$$\mathcal{A} := K[T]/< T^a + x_{a-1}T^{a-1} + \ldots + x_1 T + x_0 >$$

and

$$\mathcal{B} := K[T]/< T^b + y_{b-1}T^{b-1} + \ldots + y_1 T + y_0 >,$$

and put

$$\tilde{\mathcal{A}} := \mathcal{A} \otimes_{\mathcal{K}} \tilde{\mathcal{K}}$$

as well as

$$\tilde{\mathcal{B}} := \mathcal{B} \otimes_{\mathcal{K}} \tilde{\mathcal{K}}.$$

Then $\tilde{\mathcal{A}}$ (resp. $\tilde{\mathcal{B}}$) is an étale $\tilde{\mathcal{K}}$-algebra of degree a (resp. b). It is clearly a field. Pick $\tilde{\mathcal{K}}$-subspaces $\tilde{\mathcal{U}} \in \mathrm{Gr}(u, \tilde{\mathcal{B}})(\tilde{\mathcal{K}})$ and $\tilde{\mathcal{V}} \in \mathrm{Gr}(v, \tilde{\mathcal{A}})(\tilde{\mathcal{K}})$, both containing 1. By what precedes, the $\tilde{\mathcal{K}}$-morphism

$$\tilde{\Phi}_1 \; : \; \mathbb{P}_1(\tilde{\mathcal{V}} \otimes_{\tilde{\mathcal{K}}} \tilde{\mathcal{B}}) \times \mathbb{P}_1(\tilde{\mathcal{A}} \otimes_{\tilde{\mathcal{K}}} \tilde{\mathcal{U}}) \; \dashrightarrow \; \mathbb{P}_1(\tilde{\mathcal{A}} \otimes_{\tilde{\mathcal{K}}} \tilde{\mathcal{B}}),$$
$$(x, y) \longmapsto xy^{-1}$$

is a birational isomorphism. Since all above schemes are of finite presentation over $\tilde{\mathcal{K}}$, they, as well as Φ_1, are actually defined over a nonempty open subscheme of $\mathrm{Spec}(\mathcal{K})$. More precisely, there exists a nonzero element $F \in \mathcal{K}$, such that, denoting by $\mathcal{K}_{(F)}$ the k-algebra obtained by inverting F in $\mathcal{K}$, the following holds:

(a) The $\mathcal{K}_{(F)}$-algebras $\mathcal{A}_{(F)}$ and $\mathcal{B}_{(F)}$ are étale.
(b) The subspaces $\tilde{\mathcal{U}}$ and $\tilde{\mathcal{V}}$ are defined over $\mathcal{K}_{(F)}$, i.e., are given by elements $\mathcal{U} \in \mathrm{Gr}(u, \mathcal{B})(\mathcal{K}_{(F)})$ and $\mathcal{V} \in \mathrm{Gr}(u, \mathcal{A})(\mathcal{K}_{(F)})$, respectively.
(c) The $\mathcal{K}_{(F)}$-morphism

$$\Phi_1 \; : \; \mathbb{P}_1(\mathcal{V} \otimes_{\mathcal{K}_{(F)}} \mathcal{B}_{(F)}) \times \mathbb{P}_1(\mathcal{A}_{(F)} \otimes_{\mathcal{K}_{(F)}} \mathcal{U}) \; \dashrightarrow \; \mathbb{P}_1(\mathcal{A}_{(F)} \otimes_{\mathcal{K}_{(F)}} \mathcal{B}_{(F)}),$$
$$(x, y) \longmapsto xy^{-1}$$

is a birational isomorphism.

But the étale $\tilde{\mathcal{K}}$-algebras $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ are *versal*, in the sense of [1, Def. 5.1, see also section 24.6]. Hence, there exists a k-morphism

$$\theta : \mathcal{K}_{(F)} \longrightarrow k$$

such that $\mathcal{A}_{(F)} \otimes_\theta k$ is isomorphic to A (resp. such that $\mathcal{B}_{(F)} \otimes_\theta k$ is isomorphic to B). Put $V := \mathcal{V} \otimes_\theta k$ and $U := \mathcal{U} \otimes_\theta k$. Then U (resp. V) belongs to $\mathrm{Gr}(u, B)(k)$ (resp. to $\mathrm{Gr}(v, A)(k)$), and the specialization of Φ_1 via θ yields the birational isomorphism ϕ_1. This finishes the proof of proposition 3.1. $\qquad\square$

Note that $\mathbb{P}_1(V \otimes_k B) \times \mathbb{P}_1(A \otimes_k U)$ is open in $\mathbb{P}(V \otimes_k B) \times \mathbb{P}(A \otimes_k U)$, and that $\mathbb{P}_1(A \otimes_k B)$ is open in $\mathbb{P}(A \otimes_k B)$. Hence the map ϕ_1 of (3.1) extends to a birational isomorphism

$$(3.2) \qquad \phi \ : \ \mathbb{P}(V \otimes_k B) \times \mathbb{P}(A \otimes_k U) \quad \dashrightarrow \quad \mathbb{P}(A \otimes_k B).$$

We quotient out both sides of (3.2). Note the following identifications as birational quotients:

$$\mathbb{P}(V \otimes_k B)/\mathrm{GL}_1(B) \equiv (V \otimes_k B/\mathbb{G}_m) / (\mathrm{GL}_1(B)/\mathbb{G}_m)$$
$$\equiv (V \otimes_k B) / \mathrm{GL}_1(B) \equiv \mathbb{P}_B(V \otimes_k B).$$

Since $\mathrm{GL}_1(B)/\mathbb{G}_m$ acts freely on $V \otimes_k B/\mathbb{G}_m$, we conclude that $\dim \mathbb{P}_B(V \otimes_k B) = vb - b$. Similarly,

$$\mathbb{P}(A \otimes_k U)/\mathrm{GL}_1(A) \equiv \mathbb{P}_A(A \otimes_k U)$$

is of dimension $au - a$.

On the right hand side of the map of (3.2), we take the following birational quotient:

$$\mathbb{P}(A \otimes_k B) / {\mathrm{GL}_1(A) \times \mathrm{GL}_1(B)} \ \equiv \ (A \otimes_k B/\mathbb{G}_m) / {\mathrm{GL}_1(A) \times \mathrm{GL}_1(B)}$$
$$\equiv \ (A \otimes_k B/\mathbb{G}_m) / {(\mathrm{GL}_1(A)/\mathbb{G}_m) \times (\mathrm{GL}_1(B)/\mathbb{G}_m)}$$

Both $\mathrm{GL}_1(B)/\mathbb{G}_m$ and $\mathrm{GL}_1(A)/\mathbb{G}_m$ act freely on $A \otimes_k B/\mathbb{G}_m$, so that the dimension of the birational quotient is $ab - a - b + 1$. For an A-module M, recall from section 2 that we defined $\mathbb{P}_A(M)$ to be the Weil scalar restriction $\mathrm{Res}_{A/k}(\mathbb{P}(M))$.

Lemma 3.2. *The map ϕ of* (3.2) *induces a birational isomorphism*

$$(3.3) \qquad \overline{\phi} \ : \ \mathbb{P}_B(V \otimes_k B) \times \mathbb{P}_A(A \otimes_k U) \quad \dashrightarrow \quad \mathbb{P}(A \otimes_k B) / {\mathrm{GL}_1(A) \times \mathrm{GL}_1(B)}.$$

Proof. The dimensions of both quotients agree. Since the map is a birational isomorphism before taking the quotient, we only need to show that it descends to the quotient. But that is clear since the map is given by taking the inverse and multiplication. $\qquad\square$

Finally, note that $\mathbb{P}(A \otimes_k B) / {\mathrm{GL}_1(A) \times \mathrm{GL}_1(B)}$ is birational to $Q(A, B)$. This then completes the proof of Theorem 2.1, as both $\mathbb{P}_B(V \otimes_k B)$ and $\mathbb{P}_A(A \otimes_k U)$ are rational.

4. An application to cryptography

Our explicit birational maps open up some new examples for torus-based cryptography. Using finite cyclic groups for public key encryption is an old idea, cf. [3, chapter 8]. Rubin-Silverberg in [4] suggested using rational algebraic tori defined over finite fields. The advantage is in term of computational gains. Representing most elements of the torus as elements of an affine space over a finite field yields efficiency gains in the transmitted information. Let q be a prime power and choose $n \geq 1$. Following [4], consider

$$G_{q,n} := \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m(\mathbb{F}_q).$$

For encryption purpuses, $G_{q,n}$ is the cryptographically most significant part of $\mathbb{F}_{q^n}^{\times}$ and $G_{q,n}$, albeit smaller, inherits the security of $\mathbb{F}_{q^n}^{\times}$. See [4] for more details. $G_{q,n}$ is a torus over $\mathbb{F}_q$ of dimension $\phi(n)$, where ϕ denotes the Euler phi function. Assuming that it is rational, one then would like to (computationally) compress elements of $G_{q,n}$ via a *compression map*

$$f \ : \ G_{q,n} \quad \dashrightarrow \quad \mathbb{F}_q^{\varphi(n)}$$

that has an efficiently computable inverse j. Since $G_{q,n} < \mathbb{F}_{q^n}^{\times}$, the latter being of dimension n over $\mathbb{F}_q$, sending $f(x)$ instead of $x \in G_{q,n}$ yields an efficiency gain (in bits) of $n/\phi(n)$. Based on this idea, Rubin-Silverberg introduce two compression algorithms inducing efficient public key cryptosystems that they call CEILIDH and $\mathbb{T}_2$. Note that they restrict their encryption to the open part of $G_{q,n}$ where f and j are actual inverse isomorphisms.

Our methods allow to produce more general compression algorithms. The torus that we consider is $Q(A, B)$ as above, for any finite-dimensional étale commutative $\mathbb{F}_q$-algebras A and B of coprime dimension. Recall that we introduced the decompression map

$$\phi(A, B) \ : \ \mathbb{P}_B(V \otimes_{\mathbb{F}_q} B) \times \mathbb{P}_A(A \otimes_{\mathbb{F}_q} U) \quad \dashrightarrow \quad Q(A, B),$$

which is induced as in formula (3.1) by

$$\phi_1 \ : \ \mathbb{P}_1(V \otimes_{\mathbb{F}_q} B) \times \mathbb{P}_1(A \otimes_{\mathbb{F}_q} U) \quad \dashrightarrow \quad \mathbb{P}_1(A \otimes_{\mathbb{F}_q} B) = \mathrm{PGL}_1(A \otimes_{\mathbb{F}_q} B),$$
$$(x, y) \quad \longmapsto \quad xy^{-1}.$$

We describe the birational inverse to ϕ_1. Both maps then descend to the quotients of lemma 3.2. Let $[z] \in \mathrm{PGL}_1(A \otimes_{\mathbb{F}_q} B)$ be a generic element given by $z \in \mathrm{GL}_1(A \otimes_{\mathbb{F}_q} B)$. Since z is generic and $ua + vb = ab + 1$,

$$(V \otimes_{\mathbb{F}_q} B) \cap z(A \otimes_{\mathbb{F}_q} U) \subset V \otimes_{\mathbb{F}_q} B$$

is a line, hence an element $[s] \in \mathbb{P}_1(V \otimes_{\mathbb{F}_q} B)$. Similarly,

$$z^{-1}\left((V \otimes_{\mathbb{F}_q} B) \cap z(A \otimes_{\mathbb{F}_q} U)\right) \subset A \otimes_{\mathbb{F}_q} U$$

is a line $[t] \in \mathbb{P}_1(A \otimes_{\mathbb{F}_q} U)$. Solving these equations equations amounts to solving linear equations, hence yielding an efficient computation. Finally, after descending to the quotients, finding rational parametrizations of $\mathbb{P}_B(V \otimes_k B) \times \mathbb{P}_A(A \otimes_k U)$ is standard.

Now the torus-based Diffie-Hellman key agreement, the torus-based ElGamal encryption and the torus-based ElGamal signatures can be performed as described in [4].

References

[1] S. Garibaldi, A. Merkurjev and J.-P. Serre, *Cohomological Invariants in Galois Cohomology*, University Lecture Series, Vol. 28, AMS, 2003.

[2] A. A. Klyachko, *On rationality of tori with a cyclic splitting field*, Arithmetic and Geometry of Varieties, Kuibyshev Univ. Press, Kuibyshev, 1988, pp. 73-78 (Russian).

[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[4] K. Rubin and A. Silverberg, *Compression in finite fields and torus-based cryptography*, SIAM J. Comput., Vol. 37, No. 5 (2008), pp. 1401-1428.

[5] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, Translations of mathematical monographs, Vol. 179, AMS, 1998.

INSTITUT DE MATHÉMATIQUES DE JUSSIEU, UNIVERSITÉ PARIS 6, PLACE JUSSIEU 4, 75005 PARIS, FRANCE
E-mail address: florence@math.jussieu.fr

KIAS, 85 HOEGIRO, DONGDAEMUN-GU, SEOUL 02455, REPUBLIC OF KOREA
E-mail address: vangarrel@kias.re.kr