A short proof of Klyachko’s theorem about rational algebraic tori

Mathieu Florence

Abstract
In this paper, we give another proof of a theorem by Klyachko ([?]), which asserts that Zariski’s conjecture holds for a special class of tori over an arbitrary ground field.

1 Introduction
The main purpose of this paper is to give a much simpler proof of a theorem due to Klyachko ([?]; see also [?], chap. 2, 6.3), which is here theorem ???. To achieve this, we first prove a generalization of a theorem due to Voskresenskii ([?], chap. 2, 5.1, corollary). To be more precise, we show stable rationality for a certain class of algebraic tori over a given field k, strictly containing the cyclotomic ones. What is more, we give an effective way of presenting the character module of these tori as the kernel of a surjection between permutation modules (that is, lattices that contain a basis which is permuted by the action of the absolute Galois group of k). Recall that, according to loc. cit., chap. 2, 4.7, theorem 2, the existence of such a surjection is a necessary and sufficient condition for a torus to be stably rational. All the basic material concerning algebraic tori and rationality questions related to these is contained in loc. cit., chap.2; we shall assume that the reader is familiar with this reference.

In the following section, the symbol ⊗ alone means ⊗Z. If k is a field with separable closure ks, we denote by Γk the profinite group Gal(ks/k). Let Γ be a profinite group. By a Γ-lattice, we mean a free Z-module of finite rank, endowed with a continuous action of Γ. We will say simply ’exact sequence’ instead of ’exact sequence of Γ-lattices’.

2 Stably rational and rational algebraic tori
To begin this section, we prove an elementary but crucial lemma.
Lemma 2.1  Let $\Gamma$ be a profinite group. Let $A_i, B_i, C_i$, $i = 1, 2$ be $\Gamma$-lattices, fitting into two exact sequences

$$0 \rightarrow A_i \xrightarrow{j_i} B_i \xrightarrow{\pi_i} C_i \rightarrow 0.$$ 

Assume we are given $s_i : C_i \rightarrow B_i$, and $d_1, d_2$ two coprime integers, such that $\pi_i \circ s_i = d_i Id$, $i = 1, 2$. Let

$$A_3 = A_1 \otimes A_2,$$

$$B_3 = (B_1 \otimes B_2) \oplus (C_1 \otimes C_2),$$

and

$$C_3 = (C_1 \otimes B_2) \oplus (B_1 \otimes C_2).$$

Then there is an exact sequence

$$0 \rightarrow A_3 \xrightarrow{j_3} B_3 \xrightarrow{\pi_3} C_3 \rightarrow 0,$$

together with a morphism $s_3 : C_3 \rightarrow B_3$, satisfying $\pi_3 \circ s_3 = d_1 d_2 Id$.

Proof. We have an exact sequence

$$0 \rightarrow A_1 \otimes A_2 \rightarrow B_1 \otimes B_2 \xrightarrow{(\pi_1 \otimes Id) \oplus (Id \otimes \pi_2)} (C_1 \otimes B_2) \oplus (B_1 \otimes C_2) \xrightarrow{\pi} C_1 \otimes C_2 \rightarrow 0,$$

where $\pi = Id \otimes \pi_2 - \pi_1 \otimes Id$.

Select integers $u, v$ such that $vd_2 - ud_1 = 1$. Then the map

$$s : C_1 \otimes C_2 \rightarrow (C_1 \otimes B_2) \oplus (B_1 \otimes C_2),$$

$$c_1 \otimes c_2 \mapsto (vc_1 \otimes s_2(c_2), us_1(c_1) \otimes c_2)$$

is a splitting of $\pi$. Hence we have an exact sequence

$$0 \rightarrow A_3 \xrightarrow{j_3} B_3 \xrightarrow{\pi_3} C_3 \rightarrow 0$$

as stated, where

$$\pi_3 : (B_1 \otimes B_2) \oplus (C_1 \otimes C_2) \xrightarrow{((\pi_1 \otimes Id) \oplus (Id \otimes \pi_2), s)} (C_1 \otimes B_2) \oplus (B_1 \otimes C_2).$$

The last assertion is obvious: if $r_i : B_i \rightarrow A_i$ ($i = 1, 2$) are such that $r_i \circ j_i = d_i Id$, then

$$r_3 := (r_1 \otimes r_2, 0) : B_3 \rightarrow A_3$$

satisfies $r_3 \circ j_3 = d_1 d_2 Id. \Box$

From this we can derive the following
Theorem 2.2 Let $k$ be a field, and $X_1, \ldots, X_r$ be finite $\Gamma_k$-sets. For $i = 1, \ldots, r$, denote by $J_i$ the kernel of the canonical surjection $\mathbb{Z}^{X_i} \twoheadrightarrow \mathbb{Z}$. Let $J = \oplus_i J_i$. If the orders of the $X_i$ are two by two coprime, then we have an exact sequence

$$0 \rightarrow J \rightarrow \bigoplus_{I \in J_0} \mathbb{Z}^{\Pi_{i \in I} X_i} \rightarrow \bigoplus_{I \in J_1} \mathbb{Z}^{\Pi_{i \in I} X_i} \rightarrow 0,$$

where $J_i$ is the set of subsets of $\{1, \ldots, r\}$ whose cardinality is congruent to $r - i \mod 2$. In particular, a $k$-torus with character module isomorphic to $J$ is stably rational over $k$. What is more, let $d$ denote the product of the orders of the $X_i$, $i = 1, \ldots, r$. Then there exists

$$s : \bigoplus_{I \in J_1} \mathbb{Z}^{\Pi_{i \in I} X_i} \rightarrow \bigoplus_{I \in J_0} \mathbb{Z}^{\Pi_{i \in I} X_i}$$

such that $\pi \circ s = dId$.

Proof. For $i = 1, \ldots, r$, we have a canonical map

$$s_i : \mathbb{Z} \rightarrow \mathbb{Z}^{X_i},$$

$$1 \mapsto \sum_{x \in X_i} x,$$

which satisfies $\pi_i \circ s_i = d_i Id$, where $d_i$ is the order of $X_i$. The proof is then an easy induction using the previous lemma and the obvious isomorphism $\mathbb{Z}^X \otimes \mathbb{Z}^Y \simeq \mathbb{Z}^{X \times Y}$, for any two finite sets $X$ and $Y$. □

As a particular case of this theorem, we recover a result due to Voskresenskii ([?], chap. 2, 5.1 corollary).

Corollary 2.3 Let $k$ be a field, and $l/k$ a Galois extension with cyclic Galois group $G$ of order $n = p_1 \ldots p_r$, where the $p_i$ are prime numbers. Let $\sigma$ be a generator of this Galois group, and $T/k$ the $n^{th}$ cyclotomic torus, i.e. the torus with character group isomorphic to $\mathbb{Z}[X]/\phi_n(X)$, where $\phi_n(X)$ is the $n^{th}$ cyclotomic polynomial, the action of $\sigma$ being given by multiplication by $X$ (in other words, the character group of $T$ is isomorphic to the ring of integers of the $n^{th}$ cyclotomic extension of $\mathbb{Q}$, with the action of $\sigma$ being given by multiplication by a primitive $n^{th}$ root of unity). Then $T$ is stably rational over $k$. 


Proof. For \(i = 1, \ldots, r\), let \(X_i\) be the unique quotient of \(G\) isomorphic to \(\mathbb{Z}/p_i\). With the notations of the preceding theorem, the \(\Gamma_k\)-module \(J\) is isomorphic to the character module of \(T\) (this is just the fact that the ring of integers of the \(n^\text{th}\) cyclotomic extension of \(\mathbb{Q}\) is naturally isomorphic to the tensor product of the rings of integers of the \(p_i^\text{th}\) cyclotomic extensions of \(\mathbb{Q}\)), whence the claim. \(\square\)

We are now able to give a simple proof of the following theorem.

**Theorem 2.4** (Klyachko) Let \(k\) be a field, and \(X, Y\) two finite \(\Gamma_k\)-sets, of coprime orders \(p\) and \(q\), respectively. Consider the two basic exact sequences

\[
0 \rightarrow J_X \rightarrow \mathbb{Z}^X \rightarrow \mathbb{Z} \rightarrow 0,
\]

\[
0 \rightarrow J_Y \rightarrow \mathbb{Z}^Y \rightarrow \mathbb{Z} \rightarrow 0.
\]

Then, a \(k\)-torus \(T\) with character module isomorphic to \(J := J_X \otimes J_Y\) is rational over \(k\).

Proof. Select integers \(u, v\) such that \(up - vq = 1\). Theorem 2.3 gives the following presentation of \(J\):

\[
0 \rightarrow J \rightarrow \mathbb{Z}^{X \times Y} \oplus \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}^X \oplus \mathbb{Z}^Y \rightarrow 0,
\]

where \(\pi(x \otimes y, 0) = (x, y)\) and \(\pi(0, 1) = (u \sum_{x \in X} x, v \sum_{y \in Y} y)\). Let \(E/k\) (resp. \(F/k\)) be the etale extension of \(k\) corresponding to \(X\) (resp. to \(Y\)). Then, in terms of tori, this exact sequence reads as

\[
1 \rightarrow R_{E/k}(\mathbb{G}_m) \times R_{F/k}(\mathbb{G}_m) \xrightarrow{i} R_{E \otimes_k F/k}(\mathbb{G}_m) \times \mathbb{G}_m \rightarrow T \rightarrow 1,
\]

where \(R\) denotes Weil scalar restriction. The map \(i\) is given on the \(k\)-points of the considered tori by the following formula:

\[
i(x, y) = (x \otimes y, N_{E/k}(x)^u N_{F/k}(y)^v), x \in E^*, y \in F^*.
\]

Thus, we have a generically free action of the algebraic \(k\)-group \(H := R_{E/k}(\mathbb{G}_m) \times R_{F/k}(\mathbb{G}_m)\) on the \(k\)-vector space \(V := (E \otimes_k F) \oplus k\), such that \(T\) is birational to the quotient \(V/H\) (of course, such a quotient is defined up to birational equivalence only).

Assume that \(p < q\). Let \(G/k\) be the algebraic \(k\)-group \(\text{GL}_k(E) \times R_{F/k}(\mathbb{G}_m)\) (\(E\) being viewed as a \(k\)-vector space). I claim that the action of \(H\) on \(V\) can be naturally extended to an action of \(G\) on \(V\) (\(H\) being viewed as a
subgroup of $G$ the obvious way). Indeed, this new action is given on the $k$-points by the formula, for $g = (\phi, y) \in G(k), v = (e \otimes f, \lambda) \in V$:

$$g.v = (\phi(e) \otimes yf, \det(\phi)^u N_{F/k}(y)^v \lambda).$$

This action is generically free. Indeed, this is an easy consequence of the equality $up - vq = 1$ and of the following lemma.

**Lemma 2.5** Let $G$ act on $E \otimes_k F$ the obvious way. Then the stabilizer of a generic element is the subgroup $\mathbb{G}_m$ of $G$ given, on the level of $k$-points, by elements of the form $(x, x^{-1}) \in \text{GL}_k(E) \times F^*$, for $x \in k^*$.

We postpone the proof until the end of this section. Assuming this lemma, we have a birational $G$-equivariant isomorphism $V \simeq (V/G) \times G$, where the action of $G$ on the right is given by translation. Indeed, this is a direct consequence of Hilbert’s theorem 90, asserting that $H^1(l, G) = 1$ for any field extension $l$ of $k$. Hence we have birational isomorphisms

$$T \simeq V/H \simeq V/G \times G/H.$$

It is clear that the $k$-variety $G/H = \text{GL}_k(E)/R_{E/k}(\mathbb{G}_m)$ is $k$-rational. As in Klyachko’s original proof, the key point is here that the $k$-variety (defined up to birational equivalence) $V/G$ is independent of $E$ (seen as an etale $k$-algebra). Hence, the birational equivalence class of $T$ is independent of $E$; we may therefore assume that $E$ is split, i.e. that the action of $\Gamma_k$ on $X$ is trivial. But then $J$ is isomorphic to $J_{p}^{p-1}$, hence $T$ is birational to $(R_{F/k}(\mathbb{G}_m)/\mathbb{G}_m)^{p-1}$, which is a rational variety (it is an open subvariety of $(\mathbb{P}_k^{q-1})^{p-1}$).

**Proof of lemma**. We may assume that $F$ is split, i.e. $F = k^q$ as an etale $k$-algebra. Let $f_i, i = 1, ..., q$ denote the canonical $k$-basis of $F$. Consider an element $w = \sum_i e_i \otimes f_i \in E \otimes_k F$ in general position. Let $g = (\phi, (\lambda_1, ..., \lambda_q)) \in \text{GL}_k E \times F^*$ be such that $g.w = w$. This amounts to saying that $\phi(e_i) = \lambda_i^{-1} e_i$ for all $i$. Since $p < q$ and since $w$ is in general position, $e_1, ..., e_p$ form a basis of $E$ with respect to which the $i$’th component of $e_{p+1}$ is non zero for all $i = 1, ..., p$. This readily implies that the $\lambda_i$ are all equal to some scalar $\lambda$ and that $\phi = \lambda^{-1} Id$, thus proving the claim.
References
