ALGEBRAIC TORI — THIRTY YEARS AFTER

BORIS KUNYAVSKIĬ

To my teacher Valentin Evgenyevich Voskresenskiĭ, with gratitude and admiration

This article is an expanded version of my talk given at the International Conference "Algebra and Number Theory" dedicated to the 80th anniversary of V. E. Voskresenskiĭ, which was held at the Samara State University in May 2007. The goal is to give an overview of results of V. E. Voskresenskiĭ on arithmetic and birational properties of algebraic tori which culminated in his monograph [Vo77] published 30 years ago. I shall try to put these results and ideas into somehow broader context and also to give a brief digest of the relevant activity related to the period after the English version of the monograph [Vo98] appeared.

1. Rationality and nonrationality problems

A classical problem, going back to Pythagorean triples, of describing the set of solutions of a given system of polynomial equations by rational functions in a certain number of parameters (*rationality problem*) has been an attraction for many generations. Although a lot of various techniques have been used, one can notice that after all, to establish rationality, one usually has to exhibit some explicit parameterization such as that obtained by stereographic projection in the Pythagoras problem. The situation is drastically different if one wants to establish non-existence of such a parameterization (*nonrationality problem*): here one usually has to use some known (or even invent some new) *birational invariant* allowing one to detect nonrationality by comparing its value for the object under consideration with some "standard" one known to be zero; if the computation gives a nonzero value, we are done. Evidently, to be useful, such an invariant must be (relatively) easily computable. Note that the above mentioned subdivision to rationality and nonrationality problems is far from being absolute: given a class of objects, an ultimate goal could be to introduce some computable birational invariant giving *necessary and sufficient* conditions for rationality. Such a task may be not so hopeless, and some examples will be given below.

In this section, we discuss several rationality and nonrationality problems related to *algebraic tori*. Since this is the main object of our consideration, for the reader's convenience we shall recall the definition.

Definition 1.1. Let k be a field. An algebraic k-torus T is an algebraic k-group such that over a (fixed) separable closure $\bar{k}$ of k it becomes isomorphic to a direct product of d copies of the multiplicative group:

$$T \times_k \bar{k} \cong \mathbb{G}^d_{\mathrm{m},\bar{k}}$$

(here d is the dimension of T).

We shall repeatedly use the duality of categories of algebraic k-tori and finite-dimensional torsion-free $\mathbb{Z}$-modules viewed together with the action of the Galois group $\mathfrak{g} := \mathrm{Gal}(\bar{k}/k)$ which is given by associating to a torus T its $\mathfrak{g}$-module of characters $\hat{T} := \mathrm{Hom}(T \times \bar{k}, \mathbb{G}_{\mathrm{m},\bar{k}})$. Together with the fact that T splits over a finite extension of k (we shall denote by L the smallest of such extensions and call it the *minimal splitting field* of T), this allows us to reduce many problems to considering (conjugacy classes of) finite subgroups of $GL(d, \mathbb{Z})$ corresponding to $\hat{T}$.

1.1. **Tori of small dimension.** There are only two subgroups in $GL(1, \mathbb{Z})$: $\{(1)\}$ and $\{(1), (-1)\}$, both corresponding to k-rational tori: $\mathbb{G}_{\mathrm{m},k}$ and $R_{L/k}\mathbb{G}_{\mathrm{m},L}/\mathbb{G}_{\mathrm{m},k}$, respectively (here L is a separable quadratic extension of k and $R_{L/k}$ stands for the Weil functor of restriction of scalars).

For $d = 2$ the situation was unclear until the breakthrough obtained by Voskresenskiĭ [Vo67] who proved

Theorem 1.2. *All two-dimensional tori are k-rational.*

For $d = 3$ there exist nonrational tori, see [Ku87] for birational classification.

For $d = 4$ there is no classification, some birational invariants were computed in [Po].

Remark 1.3. The original proof of rationality of the two-dimensional tori in [Vo67] is based on the classification of finite subgroups in $GL(2, \mathbb{Z})$ and case-by-case analysis. In the monographs [Vo77] and [Vo98] a simplified proof is given, though using the classification of *maximal* finite subgroups in $GL(2, \mathbb{Z})$. Merkurjev posed a question about the existence of a classification-free proof. (Note that one of his recent results on 3-dimensional tori [Me] (see Section 3 below) was obtained without referring to the birational classification given in [Ku87].) During discussions in Samara, Iskovskikh and Prokhorov showed me a proof only relying on an "easy" part of the classification theorem for rational surfaces.

Remark 1.4. One should also note a recent application of Theorem 1.2 to the problem of classification of elements of prime order in the Cremona group $Cr(2, \mathbb{Q})$ of birational transformations of plane (see [Se, 6.9]). The problem was recently solved by Dolgachev and Iskovskikh [DI]. See the above cited papers for more details.

1.2. **Invariants arising from resolutions.** Starting from the pioneering works of Swan and Voskresenskiĭ on Noether's problem (see Section 1.4), it became clear that certain resolutions of the Galois module $\hat{T}$ play an important role in understanding birational properties of T. These ideas were further developed by Lenstra, Endo and Miyata, Colliot-Thélène and Sansuc (see [Vo77], [Vo98] for an account of that period); they were pursued through several decades, and some far-reaching generalizations were obtained in more recent works (see the remarks at the end of this and the next sections).

For further explanations we need to recall some definitions. Further on "module" means a finitely generated $\mathbb{Z}$-free $\mathfrak{g}$-module.

Definition 1.5. We say that M is a *permutation* module if it has a $\mathbb{Z}$-basis permuted by $\mathfrak{g}$. We say that modules M_1 and M_2 are similar if there exist permutation modules S_1 and S_2 such that $M_1 \oplus S_1 \cong M_2 \oplus S_2$. We denote the similarity class of M by $[M]$. We say that M is a *coflasque* module if $H^1(\mathfrak{h}, M) = 0$ for all closed subgroups $\mathfrak{h}$ of $\mathfrak{g}$. We say that M is a *flasque* module if its dual module $M^\circ := \mathrm{Hom}(M, \mathbb{Z})$ is coflasque.

The following fact was first established in the case when k is a field of characteristic zero by Voskresenskiĭ [Vo69] by a geometric construction (see below) and then in [EM], [CTS77] in a purely algebraic way (the uniqueness of $[F]$ was established independently by all above authors).

Theorem 1.6. *Any module M admits a resolution of the form*

$$0 \to M \to S \to F \to 0, \tag{1.1}$$

where S is a permutation module and F is a flasque module. The similarity class $[F]$ is determined uniquely.

We denote $[F]$ by $p(M)$. We call (1.1) the flasque resolution of M. If T is a k-torus with character module M, the sequence of tori dual to (1.1) is called the flasque resolution of T.

Seeming strange at the first glance, the notion of flasque module (and the corresponding flasque torus) turned out to be very useful. Its meaning is clear from the following theorem due to Voskresenskiĭ [Vo77, 4.60]:

Theorem 1.7. *If tori T_1 and T_2 are birationally equivalent, then $p(\hat{T}_1) = p(\hat{T}_2)$. Conversely, if $p(\hat{T}_1) = p(\hat{T}_2)$, then T_1 and T_2 are stably equivalent, i.e. $T_1 \times \mathbb{G}_{\mathrm{m},k}^{d_1}$ is birationally equivalent to $T_2 \times \mathbb{G}_{\mathrm{m},k}^{d_2}$ for some integers d_1, d_2.*

Theorem 1.7 provides a birational invariant of a torus which can be computed in a purely algebraic way. Moreover, it yields other invariants of cohomological nature which are even easier to compute. The most important among them is $H^1(\mathfrak{g}, F)$. One should note that it is well-defined in light of Shapiro's lemma (because $H^1(\mathfrak{g}, S) = 0$ for any permutation module S) and, in view of the inflation-restriction sequence, can be computed at a finite level: if L/k is the minimal splitting field of T and $\Gamma = \mathrm{Gal}(L/k)$, we have $H^1(\mathfrak{g}, F) = H^1(\Gamma, F)$. The finite abelian group $H^1(\Gamma, F)$ is extremely important for birational geometry and arithmetic, see below.

Remark 1.8. Recently Colliot-Thélène [CT07] discovered a beautiful generalization of the flasque resolution in a much more general context, namely, for an arbitrary connected linear algebraic group G.

1.3. **Geometric interpretation of the flasque resolution.** As mentioned above, the flasque resolution (1.1) was originally constructed in a geometric way. Namely, assuming k is of characteristic zero, one can use Hironaka's resolution of singularities to embed a given k-torus T into a smooth complete k-variety V as an open subset and consider the exact sequence of $\mathfrak{g}$-modules

$$0 \to \hat{T} \to S \to \mathrm{Pic}\, \overline{V} \to 0, \tag{1.2}$$

where $\overline{V} = V \times_k \bar{k}$, Pic $\overline{V}$ is the Picard module, and S is a permutation module (it is generated by the components of the divisors of $\overline{V}$ whose support is outside $\overline{T}$). With another choice of an embedding $T \to V'$ we are led to an isomorphism $\mathrm{Pic}\, \overline{V} \oplus S_1 \cong \mathrm{Pic}\, \overline{V}' \oplus S_2$, so the similarity class $[\mathrm{Pic}\, \overline{V}]$ is well defined. Voskresenskiĭ established the following property of the Picard module (see [Vo77, 4.48]) which is of utmost importance for the whole theory:

Theorem 1.9. *The module* Pic $\overline{V}$ *is flasque.*

As mentioned above, this result gave rise to a purely algebraic way of constructing the flasque resolutions, as well as other types of resolutions; flasque tori and torsors under such tori were objects of further thorough investigation [CTS87a], [CTS87b].

Remark 1.10. The geometric method of constructing flasque resolutions described above can be extended to arbitrary characteristic. This can be done in the most natural way after the gap in Brylinski's proof [Br] of the existence of a smooth complete model of any torus have been filled in [CTHS].

Remark 1.11. Recently Theorem 1.9 was extended to the Picard module of a smooth compactification of an arbitrary connected linear algebraic group [BK04] and, even more generally, of a homogeneous space of such a group with connected geometric stablizer [CTK06]. In each case, there is a reduction to the case of tori (although that in [CTK06] is involved enough).

1.4. **Noether's problem.** One of the most striking applications of the birational invariant described above is a construction of counter-examples to a problem of E. Noether on rationality of the field of rational functions invariant under a finite group G of permutations. Such an example first appeared in a paper by Swan [Sw] where tori were not mentioned but a resolution of type (1.1) played a crucial role; at the same time Voskresenskiĭ [Vo69] considered the same resolution to prove that a certain torus is nonrational. In a later paper [Vo70] he formulated in an explicit way that the field of invariants under consideration is isomorphic to the function field of an algebraic torus. This discovery yielded a series of subsequent papers (Endo–Miyata, Lenstra, and Voskresenskiĭ himself) which led to almost complete understanding of the case where the finite group G acting on the function field is abelian; see [Vo77, Ch. VII] for a detailed account. Moreover, the idea of realizing some field of invariants as the function field of a certain torus proved useful in many other problems of the theory of invariants, see works of Beneish, Hajja, Kang, Lemire, Lorenz, Saltman, and others; an extensive bibliography can be found in the monograph [Lo], see [Ka] and references therein for some more recent development; note also an alternative approach to Noether's problem based on cohomological invariants (Serre, in [GMS]).

Note a significant difference in the proofs of nonrationality for the cases $G = \mathbb{Z}_{47}$ (the smallest counter-example for a cyclic group of prime order) and $G = \mathbb{Z}_8$ (the smallest counter-example for an arbitrary cyclic group). If G is a cyclic group of order $q = p^n$, and k is a field of characteristic different from p, the corresponding k-torus splits over the cyclotomic extension $k(\zeta_q)$. If $p > 2$, the extension $k(\zeta_q)/k$ is cyclic. According to [EM], if a k-torus T splits over an extension L such that all Sylow subgroups of $\mathrm{Gal}(L/k)$ are cyclic, then the Γ-module F in the flasque resolution for T is a direct summand of a permutation module. Thus to prove that it is not a permutation module, one has to use subtle arguments. If $p = 2$ and $n \geq 3$, the Galois group Γ of $k(\zeta_q)/k$ may be noncyclic and contain a subgroup Γ' such that $H^1(\Gamma', F) \neq 0$ which guarantees that F is not a permutation module and hence T is not rational. This important observation was made in [Vo73]. Another remark should be done here: for the tori appearing in Noether's problem over a field k with cyclic G such that $\mathrm{char}(k)$ is prime to the exponent of G, triviality of the similarity class $[F]$ is necessary and *sufficient* condition for rationality of T (and hence of the corresponding field of invariants). This is an important instance of the following phenomenon: in a certain class of tori any stably rational torus is rational. The question whether this principle holds in general is known as Zariski's problem for tori and is left out of the scope of the present survey.

The group $H^1(\Gamma, \mathrm{Pic}\,\overline{X})$, where X is a smooth compactification of a k-torus T, admits another interpretation: it is isomorphic to $\mathrm{Br}\ X/\mathrm{Br}\ k$, where $\mathrm{Br}\ X$ stands for the Brauer–Grothendieck group of X. This birational invariant, later named the unramified Brauer group, played an important role in various problems, as well as its generalization for higher unramified cohomology (see [CT96a], [Sa96] for details). Let us only note that the main idea here is to avoid explicit construction of a smooth compactification of an affine variety V under consideration, trying to express $\mathrm{Br}\ X/\mathrm{Br}\ k$ in terms of V itself. In the toric case this corresponds to the formula [CTS87b]

$$\mathrm{Br}\ X/\mathrm{Br}\ k = \ker[H^2(\Gamma, \hat{T}) \to \prod_C H^2(C, \hat{T})], \tag{1.3}$$

where the product is taken over all cyclic subgroups of Γ. Formulas of similar flavour were obtained for the cases where $V = G$, an arbitrary connected linear algebraic group [CTK98], [BK00], and $V = G/H$, a homogeneous space of a simply connected group G with connected stabilizer H [CTK06]; the latter formula was used in [CTKPR] for proving nonrationality of the field extensions of the form $k(V)/k(V)^G$, where k is an algebraically closed field of characteristic zero, G is a simple

k-group of any type except for A_n, C_n, G_2, and V is either the representation of G on itself by conjugation or the adjoint representation on its Lie algebra.

It is also interesting to note that the same invariant, the unramified Brauer group of the quotient space V/G, where G is a finite group and V its faithful complex representation, was used by Saltman [Sa84] to produce the first counter-example to Noether's problem over $\mathbb{C}$. In the same spirit as in formula (1.3) above, this invariant can be expressed solely in terms of G: it equals

$$B_0(G) := \ker[H^2(G, \mathbb{Q}/\mathbb{Z}) \to \prod_A H^2(A, \mathbb{Q}/\mathbb{Z})], \tag{1.4}$$

where the product is taken over all abelian subgroups of G (and, in fact, may be taken over all bicyclic subgroups of G) [Bo87]. This explicit formula yielded many new counter-examples (all arising for nilpotent groups G, particularly from p-groups of nilpotency class 2). The reader interested in historical perspective and geometric context is referred to [Sh], [CTS07], [Bo07]. We only mention here some recent work [BMP], [Ku07] showing that such counter-examples cannot occur if G is a simple group; this confirms a conjecture stated in [Bo92].

1.5. **Generic tori.** Having at our disposal examples of tori with “good” and “bad” birational properties, it is natural to ask what type of behaviour is typical. Questions of such “nonbinary” type, which do not admit an answer of the form “yes-no”, have been considered by many mathematicians, from Poincaré to Arnold, as the most interesting ones. In the toric context, the starting point was the famous Chevalley–Grothendieck theorem stating that the variety of maximal tori in a connected linear algebraic group G is rational. If G is defined over an algebraically closed field, its underlying variety is rational. However, if k is not algebraically closed, k-rationality (or nonrationality) of G is a hard problem. The Chevalley–Grothendieck theorem gives a motivation for studying generic tori in G: if this torus is rational, it gives the k-rationality of G. The notion of generic torus can be expressed in Galois-theoretic terms: these are tori whose minimal splitting field has “maximal possible” Galois group Γ (i.e. Γ lies between $W(R)$ and $\mathrm{Aut}(R)$ where R stands for the root system of G). This result, going back to E. Cartan, was proved in [Vo88]. In this way, Voskresenskiĭ and Klyachko [VoKl] proved the rationality of all adjoint groups of type A_{2n}. The rationality was earlier known for the adjoint groups of type B_n, the simply connected groups of type C_n, the inner forms of the adjoint groups of type A_n, and (after Theorem 1.2) for all groups of rank at most two. It turned out that for the adjoint and simply connected groups of all remaining types the generic torus is not even stably rational [CK]; in most cases this was proved by computing the birational invariant $H^1(\Gamma', F)$ for certain subgroups $\Gamma' \subset \Gamma$. In the case of inner forms of simply connected groups of type A_n, corresponding to generic norm one tori, this confirms a conjecture by Le Bruyn [LB] (independently proved later in [LL]). The above theorem was extended to groups which are neither simply connected nor adjoint and heavily used in the classification of linear algebraic groups admitting a rational parameterization of Cayley type [LPR].

The above mentioned results may give an impression that except for certain types of groups the behaviour of generic tori is "bad" from birational point of view. However, there is also a positive result: if T is a generic torus in G, then $H^1(\Gamma, F) = 0$, This was first proved in [VoKu] for generic tori in the classical simply connected (type A_n) and adjoint groups, and in [Kl89] in the general case. (An independent proof for the simply connected case was communicated to the author by M. Borovoi.) This result has several number-theoretic applications, see Section 2.

Remark 1.12. Yet another approach to the notion of generic torus was developed in [Gr05b] where the author, with an eye towards arithmetic applications, considered maximal tori in semisimple simply connected groups arising as the centralizers of regular semisimple stable conjugacy classes.

2. Relationship with arithmetic

2.1. **Global fields: Hasse principle and weak approximation.** According to a general principle formulated in [Ma], the influence of (birational) geometry of a variety on its arithmetic (diophantine) properties may often be revealed via some algebraic (Galois-cohomological) invariants. In the toric case such a relationship was discovered by Voskresenskiĭ and stated as the exact sequence (see [Vo77, 6.38])

$$0 \to A(T) \to H^1(k, \operatorname{Pic} \overline{V})^{\tilde{}} \to Ш(T) \to 0, \tag{2.1}$$

where k is a number field, T is a k-torus, V is a smooth compactification of T, $A(T)$ is the defect of weak approximation, $Ш(T)$ is the Shafarevich–Tate group, and $\tilde{}$ stands for the Pontrjagin duality of abelian groups. The cohomological invariant in the middle, being a purely algebraic object, governs arithmetic properties of T.

On specializing T to be the norm one torus corresponding to a finite field extension K/k, we get a convenient algebraic condition sufficient for the Hasse norm principle to hold for K/k. In particular, together with results described in Section 1.5, this shows that the Hasse norm principle holds "generically", i.e. for any field extension K/k of degree n such that the Galois group of the normal closure is the symmetric group S_n [VoKu]. (Another proof was independently found for $n > 7$ by Yu. A. Drakokhrust.) Another application was found in [KS]: combining the above mentioned theorem of Klyachko with the Chevalley–Grothendieck theorem and Hilbert's irreducibility theorem, one can produce a uniform proof of weak approximation property for all simply connected, adjoint and absolutely almost simple groups. (Another uniform proof was found by Harari [Ha] as a consequence of a stronger result on the uniqueness of the Brauer–Manin obstruction, see the next paragraph.) Yet another interesting application of sequence (2.1) refers to counting points of bounded height on smooth compactifications of tori [BT95], [BT98]: the constant appearing in the asymptotic formula of Peyre [Pe] must be corrected by a factor equal to the order of $H^1(k, \operatorname{Pic} \overline{V})$ and arising on the proof as the product of the orders of $A(T)$ and $\text{Ш}(T)$ (I thank J.-L. Colliot-Thélène for this remark).

The sequence (2.1) was extended by Sansuc [San] to the case of arbitrary linear algebraic groups. On identifying the invariant in the middle with $\operatorname{Br} V/\operatorname{Br} k$, as in Section 1.4, one can put this result into more general context of the so-called Brauer–Manin obstruction to the Hasse principle and weak approximation (which is thus the only one for principal homogeneous spaces of linear algebraic groups). This research, started in [Ma], gave many impressive results. It is beyond the scope of the present survey.

Remark 2.1. Other types of approximation properties for tori have been considered in [CTSu] (weaker than weak approximation), [Ra], [PR] (strong approximation with respect to certain infinite sets of primes with infinite complements — so-called generalized arithmetic progressions). In the latter paper generic tori described above also played an important role. They were also used in [CU] in a quite different arithmetic context.

2.2. **Arithmetic of tori over more general fields.** Approximation properties and local-global principles were studied for some function fields. In [An] the exact sequence (2.1) has been extended to the case where the ground field k is pseudoglobal, i.e. k is a function field in one variable whose field of constants κ is pseudofinite (this means that

κ has exactly one extension of degree n for every n and every absolutely irreducible affine κ-variety has a κ-rational point). In [CT96b] weak approximation and the Hasse principle were established for any torus defined over $\mathbb{R}(X)$ where X is an irreducible real curve. This allows one to establish these properties for arbitrary groups over such fields, and, more generally, over the fields of virtual cohomological dimension 1 [Sch]. The same properties for tori defined over some geometric fields of dimension 2 (such as a function field in two variables over an algebraically closed field of characteristic zero, or the fraction field of a two-dimensional. exce;;ent, Henselian, local domain with algebraically closed residue field, or the field of Laurent series in one variable over a field of characteristic zero and cohomological dimension one) were considered in [CTGP]. Here one can note an interesting phenomenon: there are counter-examples to weak approximation but no counter-example to the Hasse principle is known. One can ask whether there exists some Galois-cohomological invariant of tori defined over more general fields whose vanishing would guarantee weak approximation property for the torus under consideration. Apart from the geometric fields considered in [CTGP], another interesting case could be $k = \mathbb{Q}_p(X)$, where X is an irreducible $\mathbb{Q}_p$-curve; here some useful cohomological machinery has been developed in [SvH].

2.3. **Integral models and class numbers of tori.** The theory of integral models of tori, started by Raynaud who constructed an analogue of the Néron smooth model [BLR], has been extensively studied during the past years, and some interesting applications were found using both Néron–Raynaud models and Voskresenskiĭ's "standard" models. The interested reader is referred to the bibliography in [VKM]. Some more recent works include standard integral models of toric varieties [KM] and formal models for some classes of tori [DGX].

Main results on class numbers of algebraic tori are summarized in [Vo98]. One can only add that the toric analogue of Dirichlet's class number formula established in [Shyr] suggests that a toric analogue of the Brauer–Siegel theorem may also exist. A conjectural formula of the Brauer–Siegel type for constant tori defined over a global function field can be found in a recent paper [KT].

3. R-equivalence and zero-cycles

R-equivalence on the set of rational points of an algebraic variety introduced in [Ma] turned out to be an extremely powerful birational invariant. Its study in the context of algebraic groups, initiated in [CTS77], yielded many striking achievements. We shall only recall here that the first example of a simply connected group whose underlying variety is not k-rational is a consequence of an isomorphism, established by Voskresenskiĭ, between $G(k)/R$, where $G = SL(1, D)$, the group of norm 1 elements in a division algebra over k, with the reduced Whitehead group $SK_1(D)$; as the latter group may be nonzero because of a theorem by Platonov [Pl], this gives the needed nonrationality of G. This breakthrough gave rise to dozens of papers on the topic certainly deserving a separate survey. For the lack of such, the interested reader is referred to [Vo98, Ch. 6], [Gi07a, Sections 24–33], [Gi07b].

As to R-equivalence on tori, the most intriguing question concerns relationship between $T(k)/R$ and the group $A_0(X)$ of classes of 0-cycles of degree 0 on a smooth compactification X of T. In a recent paper [Me] Merkurjev proved that these two abelian groups are isomorphic if T is of dimension 3 (for tori of dimension at most 2 both groups are zero because of their birational invariance and Theorem 1.2). For such tori he also obtained a beautiful formula expressing $T(k)/R$ in "intrinsic" terms, which does not require constructing X as above nor a flasque resolution of $\hat{T}$ as in [CTS77]: $T(k)/R \cong H^1(k, T^\circ)/R$, where T° denotes the dual torus (i.e. $\hat{T^\circ} = \mathrm{Hom}(\hat{T}, \mathbb{Z})$). (In the general case, it is not even known whether the map $X(k)/R \to A_0(X)$ is surjective, see [CT05, §4] for more details.) As a consequence, Merkurjev obtained an explicit formula for the Chow group $CH_0(T)$ of classes of 0-cycles on a torus T of dimension at most 3: $CH_0(T) \cong T(k)/R \oplus \mathbb{Z}_{i_T}$ where i_T denotes the greatest common divisor of the degrees of all field extensions L/k such that the torus T_L is isotropic. The proofs, among other things, use earlier results [Kl82], [MP] on the K-theory of toric varieties. As mentioned above, they do not rely on the classification of 3-dimensional tori.

To conclude this section, one can also add the same references [An], [CTGP] as in Section 2.2 for R-equivalence on tori over more general fields.

4. Applications in information theory

4.1. **Primality testing.** One should mention here several recent papers [Gr05a], [Ki] trying to interpret in toric terms some known methods for checking whether a given integer n is a prime. In fact, this approach goes back to a much older paper [CC] where the authors noticed symmetries in the sequences of Lucas type used in such tests (though algebraic tori do not explicitly show up in [CC]).

4.2. **Public-key cryptography.** A new cryptosystem based on the discrete logarithm problem in the group of rational points of an algebraic torus T defined over a finite field was recently invented by Rubin and Silverberg [RS03], [RS04a], [RS04b]. Since this cryptosystem possesses a compression property, i.e. allows one to use less memory at the same security level, it drew serious attention of applied cryptographers and yielded a series of papers devoted to implementation issues [DGPRSSW], [DW], [GV], [Ko] (in the latter paper another interesting approach is suggested based on representing a given torus as a quotient of the generalized jacobian of a singular hyperelliptic curve). In [GPS] the authors propose to use a similar idea of compression for using tori in an even more recent cryptographic protocol (so-called pairing-based cryptography). It is interesting to note that the efficiency (compression factor) of the above mentioned cryptosystems heavily depends on *rationality* of tori under consideration (more precisely, on an explicit rational parameterization of the underlying variety). As the tori used by Rubin and Silverberg are known to be stably rational, the seemingly abstract question on rationality of a given stably rational torus is moving to the area of applied mathematics. The first challenging problem here is to obtain an explicit rational parameterization of the 8-dimensional torus T_{30}, defined over a finite field k and splitting over its cyclic extension L of degree 30, whose character module $\hat{T}_{30}$ is isomorphic to $\mathbb{Z}[\zeta_{30}]$, where $\mathbb{Z}[\zeta_{30}]$ stands for a primitive 30th root of unity. (Here is an alternative description of T_{30}: it is a maximal torus in E_8 such that $\mathrm{Gal}(L/k)$ acts on $\hat{T}_{30}$ as the Coxeter element of $W(E_8)$; this can be checked by a direct computation or using [BF].)

This is a particular case of a problem posed by Voskresenskiĭ [Vo77, Problem 5.12] 30 years ago. Let us hope that we will not have to wait another 30 years for answering this question on a degree 30 extension.

Acknowledgements. The author was supported in part by the Russia–Israel Scientific Research Cooperation Project 3-3578 and by the Minerva Foundation through the Emmy Noether Research Institute of Mathematics. This paper was written during the visit to the MPIM (Bonn) in August–September 2007. The support of these institutions is highly appreciated. I thank J.-L. Colliot-Thélène for many helpful remarks.

References

[An] V. I. Andriychuk, *On the R-equivalence on algebraic tori over pseudoglobal fields*, Mat. Stud. **22** (2004) 176–183.

[BT95] V. V. Batyrev, Yu. Tschinkel, *Rational points of bounded height on compactifications of anisotropic tori*, Internat. Math. Res. Notices **1995** 591–635.

[BT98] V. V. Batyrev, Yu. Tschinkel, *Manin's conjecture for toric varieties*, J. Algebraic Geom. **7** (1998) 15–53.

[BF] E. Bayer-Fluckiger, *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comment. Math. Helv. **59** (1984) 509–538.

[Bo87] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Izv. Akad. Nauk. SSSR Ser. Mat. **51** (1987) 485–516; English transl. in Math. USSR Izv. **30** (1988) 455–485.

[Bo92] F. A. Bogomolov, *Stable cohomology of groups and algebraic varieties*, Mat. Sb. **183** (1992) 1–28; English transl. in Sb. Math. **76** (1993) 1–21.

[Bo07] F. Bogomolov, *Stable cohomology of finite and profinite groups*, "Algebraic Groups" (Y. Tschinkel, ed.), Universitätsverlag Göttingen, 2007, pp. 19–49.

[BMP] F. Bogomolov, J. Maciel, T. Petrov, *Unramified Brauer groups of finite simple groups of Lie type A_ℓ*, Amer. J. Math. **126** (2004) 935–949.

[BK00] M. Borovoi, B. Kunyavskiĭ, *Formulas for the unramified Brauer group of a principal homogeneous space of a linear algebraic group*, J. Algebra **225** (2000) 804–821.

[BK04] M. Borovoi, B. Kunyavskiĭ (with an appendix by P. Gille), *Arithmetical birational invariants of linear algebraic groups over two-dimensional geometric fields*, J. Algebra **276** (2004) 292–339.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer-Verlag, Berlin, 1990.

[Br] J.-L. Brylinski, *Décomposition simpliciale d'un réseau, invariante par un groupe fini d'automorphismes*, C. R. Acad. Sci. Paris Sér. A-B **288** (1979) 137–139.

[CC] D. Chudnovsky, G. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. Appl. Math. **7** (1986) 385–434.

[CU] L. Clozel, E. Ullmo, *Equidistribution adélique des tores et équidistribution des points CM*, Doc. Math. **Extra Vol.** (2006) 233–260.

[CT96a] J.-L. Colliot-Thélène, *Birational invariants, purity and the Gersten conjecture*, "K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras (Santa Barbara, CA, 1992) (B. Jacob, A. Rosenberg, eds.)", Proc. Symp. Pure Math., vol. 58, Part 1, Amer. Math. Soc., Providence, RI, 1995, pp. 1–64.

[CT96b] J.-L. Colliot-Thélène, *Groupes linéaires sur les corps de fonctions de courbes réelles*, J. reine angew. Math. **474** (1996) 139–167.

[CT05] J.-L. Colliot-Thélène, *Un théorème de finitude pour le groupe de Chow des zéro-cycles d'un groupe algébrique linéaire sur un corps p-adique*, Invent. Math. **159** (2005) 589–606.

[CT07] J.-L. Colliot-Thélène, *Résolutions flasques des groupes linéaires connexes*, J. reine angew. Math., to appear.

[CTGP] J.-L. Colliot-Thélène, P. Gille, R. Parimala, *Arithmetic of linear algebraic groups over two-dimensional fields*, Duke Math. J. **121** (2004) 285–341.

[CTHS] J.-L. Colliot-Thélène, D. Harari, A. N. Skorobogatov, *Compactification équivariante d'un tore (d'après Brylinski et Künnemann)*, Expo. Math. **23** (2005) 161–170.

[CTK98] J.-L. Colliot-Thélène, B. Kunyavskiĭ, *Groupe de Brauer non ramifié des espaces principaux homogènes de groupes linéaires*, J. Ramanujan Math. Soc. **13** (1998) 37–49.

[CTK06] J.-L. Colliot-Thélène, B. Kunyavskiĭ, *Groupe de Picard et groupe de Brauer des compactifications lisses d'espaces homogènes,* J. Algebraic Geom. **15** (2006) 733–752.

[CTKPR] J.-L. Colliot-Thélène, B. Kunyavskiĭ, V. L. Popov, Z. Reichstein, *Rationality problems for the adjoint action of a simple group*, in preparation.

[CTS77] J.-L. Colliot-Thélène, J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. Ec. Norm. Sup. (4) **10** (1977) 175–229.

[CTS87a] J.-L. Colliot-Thélène, J.-J. Sansuc, *La descente sur les variétés rationnelles*, II, Duke Math. J. **54** (1987) 375–492.

[CTS87b] J.-L. Colliot-Thélène, J.-J. Sansuc, *Principal homogeneous spaces under flasque tori, applications*, J. Algebra **106** (1987) 148–205.

[CTS07] J.-L. Colliot-Thélène, J.-J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group)*, Proc. Intern. Colloquium on Algebraic Groups and Homogeneous Spaces (Mumbai 2004) (V. Mehta, ed.), TIFR Mumbai, Narosa Publishing House, 2007, pp. 113–186.

[CTSu] J.-L. Colliot-Thélène, V. Suresh, *Quelques questions d'approximation faible pour les tores algébriques*, Ann. Inst. Fourier **57** (2007) 273–288.

[CK] A. Cortella, B. Kunyavskiĭ, *Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000) 771–793.

[DGX] O. Demchenko, A. Gurevich, X. Xarles, *Formal completions of Néron models for algebraic tori*, preprint arXiv:0704.2578.

[DGPRSSW] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, D. P. Woodruff, *Practical cryptography in high dimensional tori*, "Advances in Cryptology — EUROCRYPT 2005 (R. Cramer, ed.)", Lecture Notes Comp. Sci. **3494** (2005) 234–250.

[DW] M. van Dijk, D. P. Woodruff, *Asymptotically optimal communication for torus-based cryptography*, "Advances in Cryptology — CRYPTO 2004 (M. K. Franklin, ed.)", Lecture Notes Comp. Sci. **3152** (2004) 157–178.

[DI] I. V. Dolgachev, V. A. Iskovskikh, *On elements of prime order in* $Cr_2(\mathbb{Q})$, preprint arxiv:0707.4305.

[EM] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85–104; *ibid.* **79** (1980), 187–190.

[GMS] S. Garibaldi, A. Merkurjev, J-P. Serre, *Cohomological Invariants in Galois Cohomology*, Univ. Lecture Ser. **28**, Amer. Math. Soc., Providence, RI, 2003.

[Gi07a] P. Gille, *Rationality properties of linear algebraic groups and Galois cohomology*, lecture notes available at http://www.dma.ens.fr/~gille

[Gi07b] P. Gille, *Le problème de Kneser–Tits*, preprint, 2007.

[GPS] R. Granger, D. Page, M. Stam, *On small characteristic algebraic tori in pairing-based cryptography*, London Math. Soc. J. Comput. Math. **9** (2006) 64–85.

[GV] R. Granger, F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, "Advances in Cryptology — CRYPTO 2005 (V. Shoup, ed.)", Lecture Notes Comp. Sci. **3621** (2005) 66–85.

[Gr05a] B. Gross, *An elliptic curve test for Mersenne primes*, J. Number Theory **110** (2005) 114–119.

[Gr05b] B. Gross, *On the centralizer of a regular, semi-simple, stable conjugacy class*, Represent. Theory **9** (2005) 287–296.

[Ha] D. Harari, *Méthode des fibrations et obstruction de Manin*, Duke Math. J. **75** (1994) 221–260.

[Ka] M.-c. Kang, *Some group actions on* $K(x_1, x_2, x_3)$, Israel J. Math. **146** (2005) 77–92.

[Ki] M. Kida, *Primality tests using algebraic groups*, Experim. Math. **13** (2004) 421–427.

[Kl82] A. A. Klyachko, *K-theory of Demazure models*, "Investigations in Number Theory", Saratov. Gos. Univ., Saratov, 1982, pp. 61–72; English transl. in "Selected Papers in K-Theory", Amer. Math. Soc. Transl. (2) **154** (1992), pp. 37–46.

[Kl89] A. A. Klyachko, *Tori without affect in semisimple groups*, "Arithmetic and Geometry of Varieties", Kuĭbyshev State Univ., Kuĭbyshev, 1989, pp. 67–78. (Russian)

[Ko] D. Kohel, *Constructive and destructive facets of torus-based cryptography*, preprint, 2004.

[Ku87] B. È. Kunyavskiĭ, *Three-dimensional algebraic tori*, "Investigations in Number Theory", vol. 9, Saratov, 1987, pp. 90–111; English transl. in Selecta Math. Sov. **21** (1990) 1–21.

[Ku07] B. È. Kunyavskiĭ, *The Bogomolov multiplier of finite simple groups*, preprint, 2007.

[KM] B. È. Kunyavskiĭ, B. Z. Moroz, *On integral models of algebraic tori and affine toric varieties*, Trudy SPMO **13** (2007) 97–119; English transl. to appear in Proc. St. Petersburg Math. Soc.

[KS] B. È. Kunyavskiĭ, A. N. Skorobogatov, *A criterion for weak approximation on linear algebraic groups*, appendix to A. N. Skorobogatov, *On the fibration method for proving the Hasse principle and weak approximation*, Sém. de Théorie des Nombres, Paris 1988–1989, Progr. Math. **91**, Birkhäuser, Boston, MA, 1990, pp. 215–219.

[KT] B. È. Kunyavskiĭ, M. A. Tsfasman, *Brauer–Siegel theorem for elliptic surfaces*, Internat. Math. Res. Notices, to appear.

[LB] L. Le Bruyn, *Generic norm one tori*, Nieuw Arch. Wisk. (4) **13** (1995) 401–407.

[LL] N. Lemire, M. Lorenz, *On certain lattices associated with generic division algebras*, J. Group Theory **3** (2000) 385–405.

[LPR] N. Lemire, V. L. Popov, Z. Reichstein, *Cayley groups*, J. Amer. Math. Soc. **19** (2006) 921–967.

[Lo] M. Lorenz, *Multiplicative Invariant Theory*, Encycl. Math. Sci., vol. 135, Invariant Theory and Algebraic Transformation Groups, VI, Springer-Verlag, Berlin et al., 2005.

[Ma] Yu. I. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic*, Nauka, Moscow, 1972; English transl. of the 2nd ed., North-Holland, Amsterdam, 1986.

[Me] A. S. Merkurjev, *R-equivalence on 3-dimensional tori and zero-cycles*, preprint, 2007.

[MP] A. S. Merkurjev, I. A. Panin, *K-theory of algebraic tori and toric varieties*, K-Theory **12** (1997) 101–143.

[Pe] E. Peyre, *Hauteurs et nombres de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995) 101–218.

[Pl] V. P. Platonov, *On the Tannaka–Artin problem*, Dokl. Akad. Nauk SSSR **221** (1975) 1038–1041; English transl. in Soviet Math. Dokl. **16** (1975) 468–473.

[Po] S. Yu. Popov, *Galois lattices and their birational invariants*, Vestn. Samar. Gos. Univ. Mat. Mekh. Fiz. Khim. Biol. 1998, no. 4, 71–83. (Russian).

[PR] G. Prasad, A. S. Rapinchuk, *Irreducible tori in semisimple groups*, Internat. Math. Res. Notices **2001** 1229–1242; **2002** 919–921.

[Ra] M. S. Raghunathan, *On the group of norm 1 elements in a division algebra*, Math. Ann. **279** (1988) 457–484.

[RS03] K. Rubin, A. Silverberg, *Torus-based cryptography*, "Advances in Cryptology — CRYPTO 2003" (D. Boneh, ed.), Lecture Notes Comp. Sci. **2729** (2003) 349–365.

[RS04a] K. Rubin, A. Silverberg, *Algebraic tori in cryptography*, "High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams" (A. van der Poorten, A. Stein, eds.), Fields Inst. Communications Ser. **41**, Amer. Math. Soc., Providence, RI, 2004, pp. 317–326.

[RS04b] K. Rubin, A. Silverberg, *Using primitive subgroups to do more with fewer bits*, "Algorithmic Number Theory (ANTS VI) (D. A. Buell, ed.)", Lecture Notes Comp. Sci. **3076** (2004) 18–41.

[Sa84] D. J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984) 71–84.

[Sa96] D. J. Saltman, *Brauer groups of invariant fields, geometrically negligible classes, an equivariant Chow group, and unramified H^3*, "K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras (Santa Barbara, CA, 1992) (B. Jacob,

A. Rosenberg, eds.)", Proc. Symp. Pure Math., vol. 58, Part 1, Amer. Math. Soc., Providence, RI, 1995, pp. 189–246.

[San] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. reine angew. Math. **327** (1981) 12–80.

[Sch] C. Scheiderer, *Hasse principles and approximation theorems for homogeneous spaces over fields of virtual cohomological dimension one*, Invent. Math. **125** (1996) 307–365.

[SvH] C. Scheiderer, J. van Hamel, *Cohomology of tori over p-adic curves*, Math. Ann. **326** (2003) 155–183.

[Se] J-P. Serre, *Bounds for the orders of finite subgroups of $G(k)$*, "Group Representations Theory" (M. Geck, D. Testerman, J. Thévenaz, eds.), EPFL Press, Lausanne, 2007.

[Sh] I. R. Shafarevich, *The Lüroth problem*, Trudy Mat. Inst. Steklov **183** (1990) 199–204; English transl. Proc. Steklov Inst. Math. **183** (1991) 241–246.

[Shyr] J.-M. Shyr, *On some class number relations of algebraic tori*, Michigan Math. J. **24** (1977) 365–377.

[Sw] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969) 148–158.

[Vo67] V. E. Voskresenskiĭ, *On two-dimensional algebraic tori*, II, Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967) 711–716; English transl. in Izv. Math. **1** (1967) 691–696.

[Vo69] V. E. Voskresenskiĭ, *The birational equivalence of linear algebraic groups*, Dokl. Akad. Nauk SSSR **188** (1969) 978–981; English transl. in Soviet Math. Dokl. **10** (1969) 1212–1215.

[Vo70] V. E. Voskresenskiĭ, *On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $Q(x_1, \dots, x_n)$*, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970) 366–375; English transl. in Math. USSR Izv. **4** (1970) 371–380.

[Vo73] V. E. Voskresenskiĭ, *The geometry of linear algebraic groups*, Trudy Mat. Inst. Steklov. **132** (1973) 151–161; English transl. in Proc. Steklov Inst. Math. **132** (1973) 173–183.

[Vo88] V. E. Voskresenskiĭ, *Maximal tori without affect in semisimple algebraic groups*, Mat. Zametki **44** (1988) 309–318; English transl. in Math. Notes **44** (1989) 651–655.

[Vo77] V. E. Voskresenskiĭ, *Algebraic Tori*, Nauka, Moscow, 1977. (Russian)

[Vo98] V. E. Voskresenskiĭ, *Algebraic Groups and Their Birational Invariants*, Amer. Math. Soc., Providence, RI, 1998.

[VoKl] V. E. Voskresenskiĭ, A. A. Klyachko, *Toric Fano varieties and systems of roots*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984) 237–263; English transl. in Math. USSR Izv. **24** (1984) 221–244.

[VoKu] V. E. Voskresenskiĭ, B. È. Kunyavskiĭ, *Maximal tori in semisimple algebraic groups*, Manuscript deposited at VINITI 15.03.84, no. 1269-84, 28pp. (Russian)

[VKM] V. E. Voskresenskiĭ, B. È. Kunyavskiĭ, B. Z. Moroz, *On integral models of algebraic tori*, Algebra i Analiz **14** (2002) 46–70; English transl. in St. Petersburg Math. J. **14** (2003) 35–52.

Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, ISRAEL

E-mail address: `kunyav@macs.biu.ac.il`