ON THE INTEGER POINTS OF AN AFFINE TORIC VARIETY (GENERAL CASE)

B.Z. Moroz

1. Given an algebraic variety X defined over $\mathbb{Z}$, the study of the distribution of integer points $X(\mathbb{Z})$ in the real locus $X(\mathbb{R})$ is a classical subject in Diophantine Geometry. Our purpose here is to address this problem for a class of (integral models of) affine toric varieties. To be specific, let T be an algebraic torus defined over $\mathbb{Q}$, and let X be an affine toric variety associated with T. In other words, we are given an integral representation

$$\rho : \mathfrak{G} \to \mathrm{GL}(d, \mathbb{Z}), d := \dim T, \mathfrak{G} := \mathrm{Gal}(K \mid \mathbb{Q}),$$

of the Galois group $\mathrm{Gal}(K \mid \mathbb{Q})$ of the splitting field K of T, and a $\mathfrak{G}$ -invariant strongly convex rational polyhedral cone $\sigma_{\mathbb{Q}}$ in the $\mathbb{Q}$ -vector space $V = M \otimes \mathbb{Q}$, where M is the $\mathbb{Z}[\mathfrak{G}]$ -module defined by ρ. In this situation, one defines a group $I(\sigma)$ of "fractional ideals", and a class of varieties $\{X_{\mathfrak{B}} \mid \mathfrak{B} \in I(\sigma)\}$ defined over $\mathbb{Z}$, for each of which $X_{\mathfrak{B}} \times_{\mathbb{Z}} \mathbb{Q} \cong X$ (see $n°2$). Let Y be the (Zariski-) open subset of X isomorphic to T, the so-called "big" orbit (or "embedded torus"). Although our variety X may be singular, Y is certainly smooth. In n° 5, we construct a homomorphism

$$\xi : Y(\mathbb{R}) \to (\mathbb{R}_+^*)^{\nu} \times \mathbb{C}_1^{d_1} \times (\mathbb{Z}/2\mathbb{Z})^{\nu} \tag{1}$$

with $d_1 + \nu = d, \nu = \mu + r$, where r is equal to the free rank of the group of units $T(\mathbb{Z}), \mu \geq 1$, and $\mathbb{C}_1 := \{z \mid z \in \mathbb{C}, \mid z \mid = 1\}$. The map ξ allows one to define a "height" $\| \cdot \|: Y(\mathbb{R}) \to \mathbb{R}_+$ in such a way that the set

$$U(w) = \{a \mid a \in Y(\mathbb{R}), \| a \| < w\}, w \in \mathbb{R}_+$$

contains at most finitely many integer points. Indeed, the following theorem holds true. Let $Y_{\mathfrak{B}}(\mathbb{Z}) := X_{\mathfrak{B}}(\mathbb{Z}) \cap Y(\mathbb{Q})$. Given a "conductor" $\mathfrak{f} = (\mathfrak{f}_0, \mathfrak{f}_1)$ with $\mathfrak{f}_0 \in \mathbb{Z}, \mathfrak{f}_0 \geq 1, \mathfrak{f}_1 \subseteq (\mathbb{Z}/2\mathbb{Z})^{\nu}$, one can define the "ray"

$$Z_{\mathfrak{f}} = \{a \mid a \in Y_{\mathfrak{B}}(\mathbb{Z}), a = 1 (\mathrm{mod}\, \mathfrak{f})\}$$

in such a way that $Z_{\mathfrak{f}} = Y_{\mathfrak{B}}(\mathbb{Z})$ for $\mathfrak{f} = (1, (\mathbb{Z}/2\mathbb{Z})^{\nu})$ (see n° 5).

Theorem 1. *If* $\sigma_{\mathbb{Q}} \cap M \neq \{0\}$, *then*

$$card(Z_{\mathfrak{f}} \cap U(w)) = c\, w (\log w)^{\beta} (1 + O(1/\log w)), \tag{2}$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX *where $c \geq 0, 0 \leq \beta < B + r, \beta \in \mathbb{Z}$; moreover, if $Z_f \neq \phi$ then $c > 0$. Here B is a non-negative integer, to be defined in Lemma 3.*

This paper is a sequel to [8], where theorem 1 has been proved for the subclass of "maximal" toric varieties (cf. also [7, 9]). In n° 4, the general problem considered here is essentially reduced to the leading special case studied in [8]; theorem 1 is proved in n° 5. In the next section, we set up our notation and make a few comments on the nature of the objects defined there; our concluding remarks are collected in n° 6.

2. Throughout this paper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}$ denote, respectively, the fields of rational, real, complex numbers, and the ring of rational integers; $\mathbb{R}_+^*$ is the multiplicative group of positive real numbers; in general, R^* stands for the group of units of a (commutative) ring R; $\mathbb{C}_1 := \{a \mid a \in \mathbb{C}, \mid a \mid = 1\}$ is the unit circle in $\mathbb{C}$. A number field is, by definition, a finite extension of $\mathbb{Q}$; given a number field L, let $I(L), I_0(L)$, and $S(L)$ be the group of fractional ideals of L, the monoid of integral ideals, and the set of prime ideals of L respectively. Given a (finite) group $\mathfrak{G}$ and a $\mathbb{Z}[\mathfrak{G}]$-module M, let $M(\mathfrak{G}) := \{a \mid a \in M, ga = a \text{ for } g \in \mathfrak{G}\}$ denote the submodule of the $\mathfrak{G}$-invariants of M.

Let T be an algebraic torus defined over a number field k; it splits over a finite normal extension $K \mid k$, so that $T \times_k K \cong G^d_{m,K}$, where $d := \dim T$ is the dimension of T. Let $n := [K : k]$, and denote by $\mathfrak{O}$ and v the rings of integers of K and k, respectively; let $\mathfrak{G}$ be the Galois group of the normal extension $K \mid k$. The torus T is uniquely determined by the integral representation $\rho : \mathfrak{G} \to \mathrm{GL}(d, \mathbb{Z})$ acting on a $\mathbb{Z}[\mathfrak{G}]$ -module M (of rank d over $\mathbb{Z}$); let $\check{M}$ be the dual $\mathbb{Z}[\mathfrak{G}]$-module, corresponding to the contragredient representation $\check{\rho}$. Let $V = M \otimes \mathbb{Q}$ and $\check{V} = \check{M} \otimes \mathbb{Q}$ be the corresponding $\mathbb{Q}[\mathfrak{G}]$ -modules; write, for brevity, $gv := \check{\rho}(g)v, gv' := \rho(g)v'$ for $v \in \check{V}, v' \in V, g \in \mathfrak{G}$, so that $(gv \mid gv') = (v \mid v')$. Let $\sigma_{\mathbb{Q}}$ be a $\mathfrak{G}$-invariant strongly convex rational polyhedral cone in the $\mathbb{Q}$-vector space V, and $\check{\sigma}_{\mathbb{Q}} := \{v \mid v \in \check{V}, (v \mid u) \geq 0 \text{ for } u \in \sigma_{\mathbb{Q}}\}$ be the dual cone in $\check{V}$; let $\sigma := \sigma_{\mathbb{Q}} \cap M$, and $\check{\sigma} := \check{\sigma}_{\mathbb{Q}} \cap \check{M}$. Then $\check{\sigma} = \{\sum_{i=1}^{l} m_i u_i \mid m_i \geq 0, m_i \in \mathbb{Z}\}$, where $\{u_i \mid 1 \leq i \leq l\}$ is the minimal set of generators of $\check{\sigma}$ (cf. [4, § 1.3]). Let us fix a $\mathbb{Z}$-basis $\{e_i \mid 1 \leq i \leq d\}$ of M. Since $\check{\sigma} + (-\check{\sigma}) = \check{M}$, there are two matrices

$$c = (c_{ij})_{\substack{1 \leq i \leq d \\ 1 \leq j \leq l}} \qquad \text{and}$$

$$\tilde{c} = (\tilde{c}_{ij})_{\substack{1 \leq i \leq l \\ 1 \leq j \leq d}}$$

with $c_{ij} \in \mathbb{Z}, \tilde{c}_{ij} \in \mathbb{Z}$ for all i, j, and such that $u_i = \sum\limits_{1 \leq j \leq d} e_j c_{ji}$, and $e_j = \sum\limits_{1 \leq i \leq l} u_i \tilde{c}_{ij}$. Let $C := \tilde{c} \cdot c$; since $c \cdot \tilde{c} = 1$, it follows that $C^2 = C, c \cdot C = c$ and $C \cdot \tilde{c} = \tilde{c}$. Note also that $u_i = \sum_{j=1}^{l} C_{ij} u_j$ with $C = (C_{ij})_{1 \leq i,j \leq l}$. On writing $ge_i = \sum_{j=1}^{d} e_j r_{ji}(g)$, it follows that $gu_i = \sum_{j=1}^{l} u_j \tilde{r}_{ji}(g)$ with $\tilde{r}(g) := \tilde{c} r(g) c$.

Definition 1. *Given an Abelian group R, we let $a_i^g = \prod_{j=1}^{d} a_j^{r_{ji}(g)}$ for $a \in R^d$, and $b_i^g = \prod_{j=1}^{l} b_j^{\tilde{r}_{ji}(g)}$ for $b \in R^l; g \in \mathfrak{G}$.*

Definition 2. *For an Abelian group R, let $f : R^l \to R^d$ be given by the equations $f(b) = a, a_i = \prod_{j=1}^{l} b_j^{\tilde{c}_{ji}}, 1 \le i \le d,$ with $a \in R^d, b \in R^l$.*

Lemma 1. *The map $f : R^l \to R^d$ is a surjective $\mathfrak{G}$ -homomorphism.*

Proof. It follows from Definition 1 that $f(b^g) = f(b)^g$ for $b \in R^l, g \in \mathfrak{G}$. Equation $c \cdot \tilde{c} = 1$ shows that f is surjective.

To define the affine toric variety X over k corresponding to $\sigma_{\mathbb{Q}}$, let us choose a set $x = \{x_{ij} \mid 1 \le i \le l, 1 \le j \le n\}$ of $l \cdot n$ independent variables, and a basis $\{\omega_i \mid 1 \le i \le n\}$ of $K \mid k$. Write, for brevity, $gy_i := \sum_{j=1}^{n} x_{ij} g\omega_j, g \in \mathfrak{G}, 1 \le i \le l.$ The toric variety X is defined by the system of equations

$$gy = y^g, g \in \mathfrak{G}. \tag{3}$$

Each of the equations $gy_i = \prod_{j=1}^{l} y_\nu^{\tilde{r}_{\nu i}(g)}$ is equivalent to a system of n polynomial equations

$$P_j^{(i,g)}(x) = 0, 1 \le j \le n,$$

with $P_j^{(i,g)}(x) \in k[x]$. Let $\mathfrak{C}(\sigma)$ be the ideal of $k[x]$ generated by the polynomials $\{P_j^{(i,g)}(x) \mid 1 \le j \le n, 1 \le i \le l, g \in \mathfrak{G}\}$, then $X = \operatorname{Spec}(k[x]/\mathfrak{C}(\sigma))$. The torus T corresponds to the cone $\sigma_{\mathbb{Q}}^{(0)} = \{0\}$, and it may be defined by the system of equations

$$gt = t^g, g \in \mathfrak{G}, \prod_{i=0}^{d} t_i = 1, t := (t_1, \dots, t_d),$$

where again we introduce the independent variables $z = \{z_{ij} \mid 0 \le i \le d, 0 \le j \le n\}$, and let $gt_i := \sum_{j=1}^{n} z_{ij} g\omega_j, t_i^g = \prod_{j=1}^{d} t_j^{r_{ji}(g)}, 1 \le i \le d, g \in \mathfrak{G}, t_0 := \sum_{j=1}^{n} z_{0j}\omega_j$; thus $T = \operatorname{Spec}(k[z]/\mathfrak{C}_T)$, the ideal $\mathfrak{C}_T$ being generated by the polynomials $\{P_j^{(i,g)}, P_j^{(0)} \mid 1 \le j \le n, 1 \le i \le d, g \in \mathfrak{G}\}$ arising from the defining equations (cf. [7-9]). Let Y be the open subset of X defined by the condition $\prod_{i=1}^{l} y_i \ne 0$, where $y_i := \sum_{j=1}^{n} x_{ij}\omega_j, 1 \le i \le n$. The variety Y is easily seen to be isomorphic to T (it is the "big" orbit alluded to in n° 1), the isomorphism $\varphi : Y \to T$ being defined by the equations $\varphi(y)_i = \prod_{j=1}^{l} y_j^{\tilde{c}_{ji}}, 1 \le i \le d, \prod_{i=0}^{d} \varphi(y)_i = 1$.

Let now $I(\sigma) = \{\mathfrak{B} \mid \mathfrak{B} \in I(K)^l, g\mathfrak{B} = \mathfrak{B}^g \text{ for } g \in \mathfrak{G}\}$, and let $I_0(\sigma) := I(\sigma) \cap I_0(K)^l$. Choose $\mathfrak{B}$ in $I(K)$, and suppose, for simplicity, that

$$\mathfrak{B}_i \qquad \text{is an } v\text{-free module}, \qquad 1 \le i \le l. \tag{4}$$

Let $\{\omega_j^{(i)} \mid 1 \le j \le n\}$ be an v-basis of $\mathfrak{B}_i$, and let $gy_i := \sum_{j=1}^{n} x_{ij} g\omega_j^{(i)}, 1 \le i \le l$. Now the system of equations (3) defines a variety $X_{\mathfrak{B}} = \operatorname{Spec}(v[x]/J(\mathfrak{B}))$ over the ring of integers v, the ideal $J(\mathfrak{B})$ being generated by the polynomials

$$\{P_j^{(i,g)}(x) \mid P_j^{(i,g)}(x) \in v[x], 1 \le j \le n, 1 \le i \le l, g \in \mathfrak{G}\},$$

where each of the equations $gy_i = \prod_{\nu=1}^{l} y_\nu^{\tilde{r}_{\nu i}(g)}$ is equivalent to the system of n equations $P_j^{(i,g)}(x) = 0, 1 \le j \le n$. By construction, $X_{\mathfrak{B}} \times_v k \cong X$. Let $\mathcal{A}(v)$ be the category of commutative v-algebras. Clearly,

$$X_{\mathfrak{B}}(A) = \{\alpha \mid \alpha \in B, g\alpha = \alpha^g \qquad \text{for} \qquad g \in \mathfrak{G}\}, A \in \mathcal{A}(v), \tag{5}$$

where $B_i := A \otimes_v \mathfrak{B}_i, B := (B_1, \dots, B_l), 1 \le i \le l$. Let, by definition, $Y_{\mathfrak{B}}(v) := X_{\mathfrak{B}}(v) \cap Y(k)$.

If $k = \mathbb{Q}$, then $v = \mathbb{Z}$ and therefore condition (4) holds automatically. On the other hand, making use of the Weil restriction of scalars $\mathrm{Res}_{k/\mathbb{Q}}$, [11], [5, p. 245-246], we note that X may be regarded as a toric variety for the algebraic torus $\mathrm{Res}_{k/\mathbb{Q}}T$ defined over $\mathbb{Q}$. Therefore, when investigating the distribution of integer points $Y_{\mathfrak{B}}(v)$ in the real locus $Y(\mathbb{R})$ in n° 5, we may (and shall) assume that $k = \mathbb{Q}$. This assumption would not, however, simplify the matters in n° 3 and n° 4, where k is subject to no restrictions.

Remark 1. Let Sgr be the category of commutative semigroups. Consider the functor $\mathfrak{F}_{\mathfrak{B}} : \mathcal{A}(v) \to Sgr$ defined by

$$\mathfrak{F}_{\mathfrak{B}} : A \mapsto \{\alpha \mid \alpha \in B, g\alpha = \alpha^g \qquad \text{for} \qquad g \in \mathfrak{G}\}, A \in \mathcal{A}(v),$$

where $B := (\dots, A \otimes_v \mathfrak{B}_i, \dots)$ as above. Under supposition (4), the scheme $X_{\mathfrak{B}}$ represents the functor $\mathfrak{F}_{\mathfrak{B}}$ in view of (5). If (4) does not hold, the v-scheme representing $\mathfrak{F}_{\mathfrak{B}}$ still gives an integral model of the toric variety X; this model may be of interest for its own sake.

Example 1. Clearly, $T(A) = \{\alpha \mid \alpha \in (B^*)^d, g\alpha = \alpha^g \text{ for } g \in \mathfrak{G}\}$ with $B := A \otimes_v \mathcal{O}, A \in \mathcal{A}(v)$. In particular, $T(v) = \{\alpha \mid \alpha \in (\mathcal{O}^*)^d, g\alpha = \alpha^g \text{ for } g \in \mathfrak{G}\}$.

Example 2. Let $T = \mathrm{Res}_{K/\mathbb{Q}} G_{m,K}, k = \mathbb{Q}, \mathfrak{B}_i = \mathcal{O}$ for $1 \le i \le d, d = l = n, \sigma_{\mathbb{Q}} = \{a \mid a \in V, g \cdot a \ge 0 \text{ for } g \in \mathfrak{G}\}$ (here $a \ge 0$ means $a_i \ge 0$ for $1 \le i \le d$). Then $T(\mathbb{Z}) \cong \mathcal{O}^*, Y_{\mathfrak{B}}(\mathbb{Z}) = \mathcal{O} \setminus \{0\}$; in particular, taking $K = \mathbb{Q}, d = 1$ one obtains $T(\mathbb{Z}) = \{1, -1\}$, and $Y_{\mathfrak{B}}(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$.

Remark 2. Let $I^{pr}(\sigma) = \{(\alpha) \mid \alpha \in K^{*l}, g\alpha = \alpha^g \text{ for } g \in \mathfrak{G}\}$. If $\mathfrak{B}' = (\alpha)\mathfrak{B}$ with $(\alpha) \in I^{pr}(\sigma)$, then the varieties $X_{\mathfrak{B}}$ and $X_{\mathfrak{B}'}$ are v-isomorphic. Since $I(\sigma)/I^{pr}(\sigma)$ is a finite group (cf. n° 4), it follows that there are only finitely many pairwise non-isomorphic schemes $X_{\mathfrak{B}}$ for a given X.

3. In this section, we study the structure of the group of fractional ideals $I(\sigma)$, and establish the first properties of the L-functions associated to homomorphisms of the monoid $I_0(\sigma)$ of integral ideals. For $\mathfrak{p} \in S(K)$, let $\mathfrak{G}_{\mathfrak{p}} = \{g \mid g \in \mathfrak{G}, g\mathfrak{p} = \mathfrak{p}\}$ be the decomposition group at $\mathfrak{p}$, and let $\mathfrak{G}^{(\mathfrak{p})} = \{g\mathfrak{G}_{\mathfrak{p}} \mid g \in \mathfrak{G}\}$ denote the set of the right cosets of $\mathfrak{G}$ modulo $\mathfrak{G}_{\mathfrak{p}}$. Let $p \in S(k)$, and $\mathfrak{p} \mid p, \mathfrak{p} \in S(K)$; then $p = \prod_{h \in \mathfrak{G}^{(\mathfrak{p})}} (h\mathfrak{p})^{e(p)}$. One defines the group

$$I^{(p)}(\sigma) = \{\mathfrak{A}_a \mid \mathfrak{A}_a = (\dots, \prod_{h \in \mathfrak{G}^{(\mathfrak{p})}} (h\mathfrak{p})^{(u_i|ha)}, \dots), a \in M(\mathfrak{G}_{\mathfrak{p}})\}$$

of the p-primary ideals, and the semigroup

$$I_p(\sigma) = \{\mathfrak{A}_a \mid \mathfrak{A}_a \in I^{(p)}(\sigma), a \in \sigma\}$$

of the p-primary integral ideals (here $M(\mathfrak{G}_\mathfrak{p})$ denotes the submodule of $G_\mathfrak{p}$ -invariants in M). A straightforward calculation shows that

$$I(\sigma) = \prod_{p \in S(k)} I^{(p)}(\sigma), \qquad \text{and} \qquad I_0(\sigma) = \prod_{p \in S(k)} I_p(\sigma). \tag{6}$$

For $\mathfrak{B} \in I(\sigma)$, let $N_{K/k}\mathfrak{B} := \prod_{j=1}^{l} N_{K/k}\mathfrak{B}_j$, and $N\mathfrak{B} := \prod_{j=1}^{l} N\mathfrak{B}_j$ (where, as usual, $N := N_{K/\mathbb{Q}}$). It follows that

$$N_{K/k}\mathfrak{A}_a = p^{(z|a)/e(p)} \quad \text{with} \quad z := (\sum_{g \in \mathfrak{G}} g) \cdot (\sum_{1 \le i \le l} u_i) \tag{7}$$

for $\mathfrak{A}_a \in I^{(p)}(\sigma)$. Let $\sigma(m) = \{a \mid a \in \sigma, (z \mid a) = m\}$, and let

$$\kappa = \min\{m \mid m \in \mathbb{Z}, m \ge 1, \sigma(m) \ne \phi\}.$$

Given a homomorphism $\chi : I_0(\sigma) \to \mathbb{C}_1 \cup \{0\}$ such that $\chi^{-1}(\{0\}) = \prod_{p | \mathfrak{f}_0(\chi)} I_p(\sigma)$ for some $\mathfrak{f}_0(\chi)$ in $I_0(k)$, one defines a Dirichlet series

$$L(\sigma; \chi, s) = \sum_{\mathfrak{A} \in I_0(\sigma)} \chi(\mathfrak{A}) N\mathfrak{A}^{-s/\kappa}. \tag{8}$$

Let

$$L_p(\sigma; \chi, s) = \sum_{\mathfrak{A} \in I_p(\sigma)} \chi(\mathfrak{A}) N\mathfrak{A}^{-s/\kappa} = \sum_{a \in \sigma_\mathfrak{p}} \chi(\mathfrak{A}_a) N p^{-s(z|a)/\kappa e(p)}, \tag{9}$$

where $\sigma_\mathfrak{p} := M(\mathfrak{G}_\mathfrak{p}) \cap \sigma$. Since the set $\sigma(m)$ contains no more than $(m+1)^{l_1}$ elements, where l_1 is the minimal number of generators of the semigroup σ, the power series (9) converges absolutely for $Re\, s > 0$. We have

$$L(\sigma; \chi, s) = \prod_{p \in S(k)} L_p(\sigma; \chi, s), \tag{10}$$

and both the Dirichlet series (8) and the Euler product (10) are easily seen to converge absolutely for $Re\, s > 1$ (cf. [7-9]).

Let $\mathfrak{P} \in I_0(\sigma)$. We say that $\mathfrak{P}$ is prime if $\mathfrak{A} \mid \mathfrak{P} \Leftrightarrow (\mathfrak{A} = 1 \text{ or } \mathfrak{A} = \mathfrak{P})$, and $\mathfrak{P}$ is said to be a strict prime if $\mathfrak{A} \mid \mathfrak{P}^m \Rightarrow (\mathfrak{A} = \mathfrak{P}^n$ for some $n)$ for $\mathfrak{A} \in I_0(\sigma)$ and m, n ranging over the non-negative integers. Each prime $\mathfrak{P}$ lies in $I_p(\sigma)$ for some p in $S(k)$, and every ideal $\mathfrak{A}$ in $I_0(\sigma)$ can be factorised into primes: $\mathfrak{A} = \mathfrak{P}_1^{n_1} \ldots \mathfrak{P}_s^{n_s}, \mathfrak{P}_i \ne \mathfrak{P}_j$ for $i \ne j$, $\mathfrak{P}_i$ is prime, $n_i > 0, 1 \le i \le s$ (assuming $\mathfrak{A} \ne 1$), although such a decomposition does not need to be unique. It follows from a combinatorial theorem in the theory of linear Diophantine equations [10, theorem 2.5] that

$$L(\sigma; \chi, s) = \prod_{\mathfrak{P} \in \mathcal{P}(\sigma)} (1 - \chi(\mathfrak{P}) N\mathfrak{P}^{-s/\kappa})^{-1} \prod_{p \in S(k)} Q_p(Np^{-s/e(p)\kappa}),$$

where $Q_p(t) \in \mathbb{C}[t], Q_p(t) = 1 (mod\, t^\kappa)$, and $\mathcal{P}(\sigma)$ denotes the set of strict primes (cf. [7-9]). If σ generates M then the primes generate $I(\sigma)$; on the other hand, if $\sigma = \{0\}$ then $I_0(\sigma) = \{1\}$ (and consequently $L(\sigma;\chi,s) = 1$ for all χ and s). Henceforth, it will therefore be assumed that

$$\sigma \neq \{0\}. \tag{11}$$

Let μ denote the $\mathbb{Z}$-rank of $M(\mathfrak{G})$, the submodule of $\mathfrak{G}$-invariants. The torus T is said to be *isotropic* if $\mu \geq 1$ (and *anisotropic* if $\mu = 0$). Assumption (11) implies, in particular, that T is isotropic. For let $b \in \sigma \backslash \{0\}$, and let $a = \sum_{g\in\mathfrak{G}} g\cdot b$; it follows from the definition that $a \in M(\mathfrak{G})$. Moreover, since σ is $\mathfrak{G}$-invariant, $a \in \sigma$; therefore $a \neq 0$ (because $\sigma_{\mathbb{Q}}$ is a strongly convex cone).

4. Let us investigate the properties of the map $f : R^l \to R^d$ described in Definition 2, for $R = I(K)$ and for $R = K^*$. Let $\sigma(k) := \{\alpha \mid \alpha \in K^{*l}, g\alpha = \alpha^g \text{ for } g \in \mathfrak{G}\}$, and let $I(T) = \{\mathfrak{A} \mid \mathfrak{A} \in I(K)^d, g\mathfrak{A} = \mathfrak{A}^g \text{ for } g \in \mathfrak{G}\}$. It follows from (6) that $I(T) = \prod_{p\in S(k)} I^{(p)}(T)$, where

$$I^{(p)}(T) := \{\mathfrak{C}_a \mid a \in M(\mathfrak{G}_\mathfrak{p}), \mathfrak{C}_\alpha = \prod_{h\in\mathfrak{G}^{(\mathfrak{p})}} (h\mathfrak{p})^{ha}\}$$

with $\mathfrak{q}^a := (\mathfrak{q}^{a_1}, \ldots, \mathfrak{q}^{a_d}), a_i := (e_i \mid a), 1 \leq i \leq d$, for $a \in M, \mathfrak{q} \in S(K)$ (cf. [7-9]). By Lemma 1, f is a surjective $\mathfrak{G}$-homomorphism.

Lemma 2. *(i) When restricted to $I(\sigma)$, the map f is an isomorphism, $f : I(\sigma) \xrightarrow{\cong} I(T)$; moreover, $f(\mathfrak{A}_a) = \mathfrak{C}_a$ for $\mathfrak{A}_a \in I^{(p)}(\sigma), \mathfrak{C}_a \in I^{(p)}(T), a \in M(\mathfrak{G}_\mathfrak{p}), p \in S(k)$. In particular, $f(I^{(p)}(\sigma)) = I^{(p)}(T)$.*
(ii) When restricted to $\sigma(k)$, the map f is an isomorphism, $f : \sigma(k) \xrightarrow{\cong} T(k)$.

Proof. It follows from the definitions by a straightforward calculation (let us note that $T(k) = \{\alpha \mid \alpha \in K^{*d}, g\alpha = \alpha^g \text{ for } g \in \mathfrak{G}\}$).

As in the cited papers [7-9], we write $T(v) \cong \mathbb{Z}^r \times A$ with finite A, and let $T_\infty(k) = \prod_{p|\infty} T(k_p)$, where $p \mid \infty$ means that p ranges over all the infinite places of k. There is an isomorphism

$$\eta : T_\infty(k) \to (\mathbb{R}_+^*)^\mu \times T_\infty^1(k),$$

with

$$T_\infty^1(k) := (\mathbb{R}_+^*)^r \times \mathbb{C}_1^{d_1} \times (\mathbb{Z}/2\mathbb{Z})^\nu, \nu \leq \mu + r;$$

moreover, if k is a totally real field then $\nu = \mu + r, \nu + d_1 = d$ (see, for instance, [8, lemma 2]). Let $\mathfrak{f} = (\mathfrak{f}_0, \mathfrak{f}_1)$ with $\mathfrak{f}_0 \in I_0(k), \mathfrak{f}_1 \subseteq (\mathbb{Z}/2\mathbb{Z})^\nu$. By composing η with the diagonal embedding $T(k) \hookrightarrow T_\infty(k)$ and then projecting on $(\mathbb{Z}/2\mathbb{Z})^\nu$, one obtains a homomorphism

$$\iota : T(k) \to (\mathbb{Z}/2\mathbb{Z})^\nu.$$

Write $\mathfrak{f}_0 = \prod_{p\in S(k)} p^{m_p}, m_p \geq 0$, and let $\alpha \in T(k)$. We say that $\alpha = 1(\operatorname{mod} \mathfrak{f})$ if $\iota(\alpha) \in \mathfrak{f}_1$ and $\alpha_i = 1(\operatorname{mod} \mathfrak{p}^{m_p})$ for $\mathfrak{p} \mid p, \mathfrak{p} \in S(K), 1 \leq i \leq d$; further, one writes

$\alpha = 1(\mathrm{mod}\,\mathfrak{f})$ for $\alpha \in \sigma(k)$ if $\iota(f(\alpha)) \in \mathfrak{f}_1$ and $\alpha_i = 1(\mathrm{mod}\,\mathfrak{p}^{m_\mathfrak{p}})$ for $\mathfrak{p} \mid p, \mathfrak{p} \in S(K), 1 \leq i \leq l$. By construction,

$$(\alpha = 1(\mathrm{mod}\,\mathfrak{f}) \quad \text{for} \quad \alpha \in \sigma(k)) \Leftrightarrow f(\alpha) = 1(\mathrm{mod}\,\mathfrak{f}).$$

Write, for brevity, $(\alpha) := (\dots, (\alpha_i), \dots)$ for $\alpha \in K^{*m}, 1 \leq i \leq m$. Let

$$I_\mathfrak{f}^{pr}(\sigma) = \{(\alpha) \mid \alpha \in \sigma(k), \alpha = 1(\mathrm{mod}\,\mathfrak{f})\},$$

and $I_\mathfrak{f}^{pr}(T) = \{(\alpha) \mid \alpha \in T(k), \alpha = 1(\mathrm{mod}\,\mathfrak{f})\}$. One notes that (cf. (14))

$$f(I_\mathfrak{f}^{pr}(\sigma)) = I_\mathfrak{f}^{pr}(T), \quad \text{and} \quad (f(\alpha)) = f((\alpha)) \quad \text{for} \quad \alpha \in K^{*l}. \tag{15}$$

Let $I_\Phi(\sigma) = \prod\limits_{p\in\Phi} I^{(p)}(\sigma)$, and $I_\Phi(T) = \prod\limits_{p\in\Phi} I^{(p)}(T)$ for $\Phi \subseteq S(k)$. By lemma 2, we have

$$f(I_\Phi(\sigma)) = I_\Phi(T). \tag{16}$$

Let, in particular, $\Phi = \{p \mid p \in S(k), p \nmid \mathfrak{f}_0\}$, and let

$$H_\mathfrak{f}(\sigma) = I_\Phi(\sigma)/I_\mathfrak{f}^{pr}(\sigma), H_\mathfrak{f}(T) = I_\Phi(T)/I_\mathfrak{f}^{pr}(T).$$

It follows from (15) and (16) that the map $f : I(\sigma) \to I(T)$ induces an isomorphism

$$f_1 : H_\mathfrak{f}(\sigma) \xrightarrow{\cong} H_\mathfrak{f}(T).$$

Furthermore, we have [8, relation (11)]:

$$T_\infty^1(k)/T_\mathfrak{f}(v) \cong \mathcal{T}_\mathfrak{f} \quad \text{with} \quad \mathcal{T}_\mathfrak{f} := \mathbb{C}_1^{d_1+r} \times (\mathbb{Z}/2\mathbb{Z})^{\nu_0}, \nu_0 \leq \nu,$$

where $T_\mathfrak{f}(v) := \{\alpha \mid \alpha \in T(v), \alpha = 1(\mathrm{mod}\,\mathfrak{f})\}$. There is a homomorphism $g(\mathfrak{f}) : I_\Phi(T) \to \mathcal{H}(\mathfrak{f})$, where $\mathcal{H}(\mathfrak{f}) := \mathcal{T}_\mathfrak{f} \times H_\mathfrak{f}(T) \times \mathcal{B}_\mathfrak{f}$, the group $\mathcal{B}_\mathfrak{f}$ being defined by the relation (14) in [8]. By composing the maps f and $g(\mathfrak{f})$ one obtains a homomorphism

$$f(\mathfrak{f}) : I_0(\sigma) \cap I_\Phi(\sigma) \to \mathcal{H}(\mathfrak{f}).$$

As before [8, n^0 4], one writes $Gr(T) := \bigcup\limits_\mathfrak{f} Gr_\mathfrak{f}(T)$ for the group of normalised grossencharacters and notes that the group $Gr_\mathfrak{f}(T)$ of grossencharacters modulo $\mathfrak{f}$ is isomorphic to $\mathcal{H}^\vee(\mathfrak{f})$, the group of characters of $\mathcal{H}(\mathfrak{f})$. We set $Gr(\sigma) = \{\chi \circ f \mid \chi \in Gr\,T\}$, and write $\mathfrak{f}(\chi) = \mathfrak{f}(\chi \circ f^{-1})$ for $\chi \in Gr(\sigma)$. A character χ in $Gr(\sigma)$ may be regarded [loc. cit] as a homomorphism $\chi : I_0(\sigma) \to \mathbb{C}_1 \cup \{0\}$ with $\chi^{-1}(\{0\}) = \prod\limits_{p \mid \mathfrak{f}_0(\chi)} I_p(\sigma)$.

Lemma 3. *Let $\chi \in Gr(\sigma)$, and let B be the number of different $\mathfrak{G}$ -orbits in $\sigma(\kappa)$. There are number fields $k_j, 1 \leq j \leq B$, such that $k \subseteq k_j \subseteq K$ for every j and*

$$L(\sigma; \chi, s) = \prod_{j=1}^{B} L(\chi_j, s) L_1(\sigma; \chi, s), \tag{17}$$

where $L(\chi_j, s)$ is a Hecke L-function with a (normalised) grossencharacter χ_j of k_j, the function $s \mapsto L_1(\sigma; \chi, s)$ being holomorphic for $Re\, s > \kappa/\kappa + 1$.

Proof. It follows from a theorem of Draxl's [3, Satz 1] (see [7,8] for an elementary recast of Draxl's argument).

In the course of the proof of lemma 3 [loc. cit.] one observes that the set

$$\mathcal{E}(\sigma) = \{\chi \mid \chi \in Gr(\sigma), \chi_j = 1 \quad \text{for} \quad 1 \leq j \leq B\}$$

of those characters χ in $Gr(\sigma)$ which give rise to trivial χ_j for all j in (17) is a subgroup of $Gr(\sigma)$.

Lemma 4. *If the set $\sigma(\kappa)$ generates M (as an Abelian group) then the group $\mathcal{E}(\sigma)$ is finite.*

Proof. See [3, Satz 1].
We have essentially reduced our problem to the theory of "maximal" toric varieties of [7-9], corresponding to the cone

$$\sigma_0 = \{a \mid a \in M, g \cdot a \geq 0 \quad \text{for} \quad g \in \mathfrak{G}\}.$$

All the results and comments in [8] concerning the distribution of integral and prime ideals are valid mutatis mutandis in the present more general situation, in particular, Theorem 1, Corollaries 1-3, and Remarks 5, 6. There is a natural homomorphism

$$f_2(\mathfrak{f}) : I_0(\sigma) \cap I_\Phi(\sigma) \to H_\mathfrak{f}(\sigma).$$

For $C \in H_\mathfrak{f}(\sigma)$, let

$$\mathcal{N}(C, w) = \text{card}\, \{\mathfrak{A} \mid \mathfrak{A} \in f_2(\mathfrak{f})^{-1}(C), N\mathfrak{A} < w\}.$$

Proposition 1. *If $f_2(\mathfrak{f})^{-1}(C) \neq \phi$ then*

$$\mathcal{N}(C, w) = w\, P_C(log\, w) + O(w^{1-\gamma}), \gamma > 0,$$

with $P_C(t) \in \mathbb{R}[t], P_C(t) \neq 0$, and the degree of the polynomial $P_C(t)$ is lower than B.

Proof. It corresponds to (a weaker form of) Corollary 2 in [8] and can be proved in exactly the same way as this Corollary.

5. Let now $k = \mathbb{Q}$. In this case, $T_\infty(\mathbb{Q}) = T(\mathbb{R})$; therefore (12) and (13) give an isomorphism

$$\eta : T(\mathbb{R}) \to (\mathbb{R}_+^*)^\nu \times \mathbb{C}_1^{d_1} \times (\mathbb{Z}/2\mathbb{Z})^\nu \tag{18}$$

with $\nu = \mu + r, \nu + d_1 = d$. Since T is isomorphic to Y, the manifold $Y(\mathbb{R})$ is homeomorphic to $T(\mathbb{R})$, and the isomorphism η defined by (18) gives rise to the homeomorphism

$$\xi : Y(R) \to (\mathbb{R}_+^*)^\nu \times \mathbb{C}_1^{d_1} \times (\mathbb{Z}/2\mathbb{Z})^\nu. \tag{1}$$

We write $\xi(a) := (\xi_1(a), \ldots, \xi_{\nu+d}(a))$ for $a \in Y(\mathbb{R})$, where $\xi_i(a) \in \mathbb{R}_+^*$ for $i \le \nu$, $\xi_{\nu+i}(a) \in \mathbb{C}_1$ for $i \le d_1$, and $\xi_i(a) \in \mathbb{Z}/2\mathbb{Z}$ for $i > d$. For $a \in Y(\mathbb{R})$, let

$$y_i(a) := \sum_{1 \le j \le n} a_{ij}\omega_j^{(i)}, gy_i(a) := \sum_{1 \le j \le n} a_{ij} g\omega_j^{(i)}, g \in \mathfrak{G}, 1 \le i \le l,$$

and let $Ny(a) := \prod_{\substack{g \in \mathfrak{G} \\ 1 \le i \le l}} gy_i(a), \| a \| := \max\{| Ny(a) |^{1/\kappa}, \xi_j(a), \xi_j(a)^{-1} \mid \mu < j \le \nu\}$.

It follows from the definitions that $y(a) \in \sigma(\mathbb{Q})$ for $a \in Y_{\mathfrak{B}}(\mathbb{Z})$; by a slight abuse of notation, we write $a = 1(\operatorname{mod} \mathfrak{f})$ if $y(a) = 1(\operatorname{mod} \mathfrak{f})$ for $a \in Y_{\mathfrak{B}}(\mathbb{Z})$. By definition (see n° 1),

$$U(w) = \{a \mid a \in Y(\mathbb{R}), \| a \| < w\}, w > 0,$$

and

$$Z_{\mathfrak{f}} = \{a \mid a \in Y_{\mathfrak{B}}(\mathbb{Z}), a = 1(\operatorname{mod} \mathfrak{f})\}$$

for $\mathfrak{f} = (\mathfrak{f}_0, \mathfrak{f}_1), \mathfrak{f}_0 \in \mathbb{Z}, \mathfrak{f}_0 \ge 1, \mathfrak{f}_1 \subseteq (\mathbb{Z}/2\mathbb{Z})^\nu$.

Proof of Theorem 1. By definition,

$$Y_{\mathfrak{B}}(\mathbb{Z}) = \{a \mid a \in \mathbb{Z}^{nl}, g \cdot y(a) = y(a)^g \quad \text{for} \quad g \in \mathfrak{G}, \prod_{1 \le i \le l} y_i(a) \ne 0\}.$$

The map $\varphi : a \mapsto y(a)$ may be regarded as an embedding

$$\varphi : Y_{\mathfrak{B}}(\mathbb{Z}) \hookrightarrow \mathfrak{B} \cap \sigma(\mathbb{Q}).$$

Clearly,

$$\varphi(Z_{\mathfrak{f}}) = \{\alpha \mid \alpha \in \sigma(\mathbb{Q}), \alpha = 1(\operatorname{mod} \mathfrak{f}), (\alpha) = \mathfrak{B}\mathfrak{A}, \mathfrak{A} \in I_0(\sigma)\}. \tag{19}$$

Let, for brevity, $C := f_2(\mathfrak{f})^{-1}(\mathfrak{B}^{-1})$, and let

$$e(\mathfrak{A}, w) = \operatorname{card}\{\alpha \mid \alpha \in \varphi(Z_{\mathfrak{f}}), w^{-1} < \eta_j(f(\alpha)) < w \quad \text{for} \quad \mu < j \le \nu\}.$$

Since the map φ is injective, it follows from (19) that

$$\operatorname{card}(Z_{\mathfrak{f}} \cap U(w)) = \sum_{N\mathfrak{A} < w_1} \psi(\mathfrak{A}) e(\mathfrak{A}, w), w_1 := w^\kappa N\mathfrak{B}^{-1}, \tag{20}$$

where $\psi(\mathfrak{A}) = 1$ if $f_2(\mathfrak{f})(\mathfrak{A}) = C$ and $\psi(\mathfrak{A}) = 0$ otherwise. Suppose that $f_2(\mathfrak{f})(\mathfrak{A}) = C$, then $\mathfrak{A}\mathfrak{B} = (\alpha_0)$ for some α_0 in $\sigma(\mathbb{Q})$ with $\alpha_0 = 1(\operatorname{mod} \mathfrak{f})$. Therefore by lemma 1, (ii)

$$e(\mathfrak{A}, w) = \operatorname{card}\{\epsilon \mid \epsilon \in T_{\mathfrak{f}}(\mathbb{Z}), 1/w < \eta_j(\epsilon f(\alpha_0)) < w \quad \text{for} \quad \mu < j \le \nu\},$$

and, since $T_{\mathfrak{f}}(\mathbb{Z}) \cong \mathbb{Z}^r \times A_{\mathfrak{f}}$ with finite $A_{\mathfrak{f}}$ we have:

$$e(\mathfrak{A}, w) = c_1(\log w)^r(1 + O(1/\log w)), c_1 > 0, \tag{21}$$

with c_1 independent of $\mathfrak{A}$. The assertion of the theorem follows now from (21), (20), and Proposition 1.

Remark 3. Suppose now that $B = 1$ and that $\mathcal{E}(\sigma)$ is a torsion subgroup of $Gr\,(\sigma)$. Then it follows from Lemma 3 (cf. [7-9]) that

$$\sum_{\substack{\mathfrak{A}\in I_0(\sigma)\\ N\mathfrak{A}<w^\kappa}} \chi(\mathfrak{A}) = g(\chi)c_2 w + O(w^{1-\gamma}), \gamma > 0, c_2 > 0,$$

with $g(\chi) = 0$ if $\chi \notin \mathcal{E}(\sigma), g(\chi) = L_1(\sigma; \chi, 1)$ for $\chi \in \mathcal{E}(\sigma)$. In particular,

$$\sum_{\substack{N\mathfrak{A}<w^\kappa\\ \mathfrak{A}\in I_0(\sigma)}} \chi(\mathfrak{A}) = O(w^{1-\gamma}), \gamma > 0, \quad \text{if} \quad \chi \quad \text{is of infinite order.}$$

In this situation, one can prove an equidistribution theorem on the number of integer points $Y_{\mathfrak{B}}(\mathbb{Z}) \cap U$ in a smooth subset U of the real locus $Y(\mathbb{R})$; it turns out that card $(Y_{\mathfrak{B}}(\mathbb{Z}) \cap U)$ is asymptotically proportional to the (appropriately defined) Borel measure of U. Since all the tools, necessary to carry out this proof, have been described elsewhere (see [6] and references therein), we leave the details of this argument to the reader.

6. Recently, in a series of interesting papers (see, for instance, [1] and references therein), V.V. Batyrev and Yu. Tschinkel have obtained an asymptotic formula for the number of rational points of bounded height on a projective toric variety. Several authors study the distribution of integer points in the real locus of an affine homogeneous space of a semisimple group (cf. [2] and references therein). It is instructive to compare the results and methods of the cited papers with the approach adopted here; let us note, in particular, the important role played by Draxl L-functions in [1], and refer to the Introduction of [2] for a discussion of the general problem of counting the number of integer solutions of Diophantine equations (cf. also [6], n° 1).

Acknowledgement. This paper was written during my stay at the Max-Planck-Institut für Mathematik in Bonn. It is a pleasure to thank the Institute for its unfailing hospitality and financial support.

References

[1] V.V. Batyrev, Yu. Tschinkel, *Manin's conjecture for toric varieties*, Journal of Algebraic Geometry, **7** (1998), 15-53.

[2] M. Borovoi, Z. Rudnik, *Hardy-Littlewood varieties and semisimple groups*, Inventiones mathematicae, **119** (1995), 37-66.

[3] P.K.J. Draxl, *L-Funktionen algebraischer Tori*, Journal of Number Theory, **3** (1971), 444-467.

[4] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, **131** (1993), Princeton University Press.

[5] S. Lang, *Number Theory III*, Springer-Verlag, 1991.

[6] B.Z. Moroz, *On the distribution of integral points on an algebraic torus defined by a system of norm-form equations*, Quarterly Journal of Mathematics Oxford (2), **45** (1994), 243-253.

[7] B.Z. Moroz, *Exercises in analytic arithmetic on an algebraic torus*, The F. Hirzebruch Festband, Israel Mathematical Conferences Proceedings, **9** (1995), 347-359.
[8] B.Z. Moroz, *On the integer points of some toric varieties*, Quarterly Journal of Mathematics Oxford (2), **48** (1997), 67-82.
[9] B.Z. Moroz, *On the distribution of integer points in the real locus of an affine toric variety*, Proceedings of the Symposium on sieve methods, exponential sums, and their applications in number theory, LMS Lecture Notes, 237 (1996), 283-291.
[10] R.P. Stanley, *Linear homogeneous Diophantine equations and magic labelings of graphs*, Duke Mathematical Journal, **40** (1973), 607-632.
[11] A. Weil, *Adeles and algebraic groups*, Birkhäuser (1982).

Max-Planck-Institut für Mathematik, Gottfried-Claren-Str. 26, D-53225 Bonn, Germany