Exercises in Analytic Arithmetic on an Algebraic Torus

B.Z. Moroz

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
53225 Bonn
Germany

submitted for publication to the Proceedings of the workshop in algebraic geometry on the occasion of F. Hirzebruch's 65th birthday

MPI / 93-82

Exercises in Analytic Arithmetic on an Algebraic Torus

B.Z. Moroz

Dedicated to Professor F. Hirzebruch
with deep respect and gratitude

1. The multidimensional arithmetic of E. Hecke, [4], [5], [7], may be regarded as a study in analytic number theory on the torus $Res_{k/\mathbb{Q}}G_{m,k}$ for a number field k of finite degree over the field $\mathbb{Q}$ of rational numbers. Here we shall try to generalise these considerations to an arbitrary algebraic torus defined over a number field. After applying Weil's restriction of scalars, if necessary, we may suppose that our torus T is defined over $\mathbb{Q}$; it splits over a finite normal extension $K|\mathbb{Q}$. Let $G = Gal(K|\mathbb{Q})$ be the Galois group of K, let $[K:\mathbb{Q}] = n$ be its degree, and let $d = \dim T$ denote the dimension of T. Such a torus is uniquely defined by an integral representation

$$\rho : G \longrightarrow GL(d, \mathbb{Z}) ,$$

where $\mathbb{Z}$ is the ring of rational integers, [12] (cf. also [15]). Consider a G-module $K[x]$, $x := \{x_{ij} | 1 \leq i \leq d, 1 \leq j \leq n\}$, choose an integral basis $\{\omega_i | 1 \leq i \leq n\}$ of $K|\mathbb{Q}$, and let

$$t_i = \sum_{j=1}^{n} x_{ij}\omega_j \quad , \quad 1 \leq i \leq d .$$

Equations

$$\sigma t_i = t_i^\sigma \quad ; \quad \sigma \in G \ ; \ 1 \leq i \leq d ,$$

where

$$\sigma t_i := \sum_{j=1}^{n} x_{ij}\,\sigma\omega_j \ , \ t_i^\sigma := \prod_{j=1}^{d} t_j^{r_{ji}(\sigma)} \ , \ \rho(\sigma) = \big(r_{ij}(\sigma)\big) \ , \ 1 \leq i, j \leq d ,$$

define an algebraic variety, say

$$X = Spec\ \mathbb{Q}[x]/J \quad ,$$

J being the defining ideal of X; the torus T may be regarded as a Zariski open subset of X given by the condition $\prod_{1\le i\le d} t_i \neq 0$. We view $X(\mathbb{Z})$ as a generalisation of the ring of integers of an algebraic number field (if $T = Res_{k/\mathbb{Q}} G_{m,k}$ one may identify $X(\mathbb{Z})$ with the ring of integers of k), and intend to play the usual game of analytic number theory on this set.

2. On choosing a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ we shall regard the field $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, as a subfield of the field $\mathbb{C}$ of complex numbers. For a k-algebra A, $k \subseteq \mathbb{C}$, let $A_K = A \otimes_{k_0} K$, where $k_0 = K \cap k$ (the fields k and K are linearly disjoint over k_0 since $K|\mathbb{Q}$ is normal). If one defines an embedding

$$t:\ T(A) \longrightarrow A_K^{*^d}$$

in a natural way, $T(A)$ may be viewed as a subset of G_0-invariants, where $G_0 := Gal(K|k_0)$, that is to say

$$T(A) = \{t(a)|\ a \in A^{nd},\ \sigma t(a) = t^\sigma(a) \quad \text{for} \quad \sigma \in G_0\}$$

(a word about notation, $t(a) := (t_1(a), \ldots, t_d(a))$, $t_i(a) = \sum_{j=1}^{n} a_{ij}\omega_j$, $a = \{a_{ij}|\ 1 \le i \le d,\ 1 \le j \le n\}$, $t^\sigma := (t_1^\sigma, \ldots, t_d^\sigma)$, etc.). Since

$$X(\mathbb{Q})\backslash T(\mathbb{Q}) \subseteq \bigcup_{i=1}^{d} \ell_i \ ,\quad \ell_i := \{x|\ x \in \mathbb{Q}^{nd},\ x_{ij} = 0 \text{ for } 1 \le j \le d\} \quad ,$$

we may often replace $X(A)$ by $T(A)$ causing no damage to the type of problems discussed here.

Before proceeding any further let us introduce the G-module of characters

$$\hat{T} = \{x|\ x \in \mathbb{Z}^d,\ \sigma x = \rho(\sigma)x \text{ for } \sigma \in G\} \quad ,$$

and its dual

$$\hat{T}^* = \{y|\ y^t \in \mathbb{Z}^d,\ \sigma y = y\rho(\sigma^{-1})^t \text{ for } \sigma \in G\} \quad ,$$

where the upper affix ^{t} denotes matrix transposition. The G–module

$$M = \left\{ t^x \mid x \in \hat{T},\ \sigma t^x = t^{\sigma x} \text{ for } \sigma \in G \right\} \ ;$$

and its submonoid

$$M_0 = \left\{ t^x \mid x \in \hat{T},\ x \geq 0 \right\}$$

furnish us with a convenient parametrization of $T(A)$. Here $t^x := \prod_{i=1}^{d} t_i^{x_i}$, and $x \geq 0$ means $x_i \geq 0$ for $1 \leq i \leq d$.

3. Let $I(K)$ and $I_0(K)$ denote the group of fractional ideals of K and the monoid of integral ideals of K respectively, and let

$$\begin{aligned} I(T) &= \left\{ \mathfrak{A} \mid \mathfrak{A} \in I(K)^d,\ \sigma \mathfrak{A}_j = \prod_{i=1}^{d} \mathfrak{A}_i^{r_{ij}(\sigma)} \quad \text{for} \quad \sigma \in G,\ 1 \leq j \leq d \right\} \ , \\ I_0(T) &= I(T) \cap I_0(T)^d \ . \end{aligned}$$

One defines the norm homomorphism $N:\ I(T) \to \mathbb{Q}_+^*$ by letting $N\mathfrak{A} = \prod_{1 \leq j \leq d} N\mathfrak{A}_j$ for $\mathfrak{A} \in I(T)$. We say that $\mathfrak{A}$ is a *primary* ideal if $\mathfrak{A} \in I_0(T)$ and $N\mathfrak{A}$ is a prime power in $\mathbb{Q}$. For a rational prime p, let

$$I_p(T)(:= I_p) = \left\{ \mathfrak{A} \mid \mathfrak{A} \in I_0(T),\ N\mathfrak{A} = p^n \text{ for some } n \right\}$$

be the submonoid of p–primary ideals. To analyze the structure of I_p let us introduce the G–module of one–parameter subgroups

$$M_u = \left\{ u^y \mid y \in \hat{T}^*,\ \sigma u^y = u^{\sigma^{-1} y} \right\} \ ,$$

where $u^y := \left(u^{y_1}, \ldots, u^{y_d} \right)$. Clearly, $(\sigma x)(\sigma u^y) = x(u^y)$ if we let $x(u^y) := (u^y)^x = u^{y \cdot x}$ for $x \in \hat{T}$, $u^y \in M_u$.

Let us choose a prime $\mathfrak{p}$ in $I(K)$ dividing p, and let

$$G_{\mathfrak{p}} = \left\{ \sigma \mid \sigma \mathfrak{p} = \mathfrak{p},\ \sigma \in G \right\}$$

be the decomposition group of $\mathfrak{p}$, so that

$$p = \prod_{\tau \bmod G_{\mathfrak{p}}} (\tau \mathfrak{p})^{e(p)} \qquad \text{in} \qquad I(K) \ ,$$

where τ ranges over G. Let $\mathfrak{A} \in I_p$, then

$$\mathfrak{A}_j = \prod_{\tau \bmod G_\mathfrak{p}} (\tau\mathfrak{p})^{a_j(\tau)} \qquad \text{with} \qquad a_j(\tau) \in \mathbb{Z},\ \ a_j(\tau) \geq 0\ ,$$

and

(1) $$\sigma\mathfrak{A}_j = \prod_{i=1}^{d} \mathfrak{A}_i^{r_{ij}(\sigma)} = \prod_{\tau \bmod G_\mathfrak{p}} (\tau\mathfrak{p})^{(a(\tau)\cdot\rho(\sigma)^t)_j}\ .$$

On the other hand,

$$\sigma\mathfrak{A}_j = \prod_{\tau \bmod G_\mathfrak{p}} (\sigma\tau\mathfrak{p})^{a_j(\tau)}\ ,$$

and in particular

$$\tau^{-1}\mathfrak{A}_j = \mathfrak{p}^{a_j(\tau)}\mathfrak{A}'_j \qquad \text{with} \qquad \mathfrak{p} \nmid \mathfrak{A}'_j\ .$$

But

$$\tau^{-1}\mathfrak{A}_j = \mathfrak{p}^{(a(e)\rho(\tau^{-1})^t)_j}\,\mathfrak{A}'_j \qquad \text{with} \qquad \mathfrak{p} \nmid \mathfrak{A}'_j\ ,$$

in view of (1). Therefore

$$a(\tau) = a \cdot \rho(\tau^{-1})^t\ ;$$

and, moreover,

$$a \cdot \rho(\sigma)^t = a \qquad \text{for} \qquad \sigma \in G_\mathfrak{p}\ ,$$

where we write $a(e) = a$ and denote by e the unit element of G. Thus (cf. [1])

(2) $$I_p = I_p(T) = \left\{\mathfrak{A}_a \,\middle|\, \mathfrak{A}_a = \prod_{\tau \bmod G_\mathfrak{p}} (\tau\mathfrak{p})^{\tau\cdot a},\ a \in C^*_\mathfrak{p}\right\}\ ;$$

where

$$C^* = \left\{a \,\middle|\, a \in \hat{T}^*,\ \sigma \cdot a \geq 0 \text{ for } \sigma \in G\right\}\ ,$$

and

$$C^*_\mathfrak{p} = C^* \cap (\hat{T}^*)^{G_\mathfrak{p}}\ .$$

If $C^* \neq \{0\}$ let $a \in C^*\backslash\{0\}$; clearly

$$\sum_{\sigma \in G} \sigma a \in (\hat{T}^*)^G \backslash \{0\}\ ,$$

so that $\hat{T}^G \neq \{0\}$, and T is not anisotropic. Therefore $I_0(T) = \{1\}$, and consequently $T(\mathbb{Z}) = X(\mathbb{Z})$ for an anisotropic torus T. Suppose now that T is not anisotropic (that is $\hat{T}^G \neq \{0\}$), then after a possible change of basis in T it may be assumed that $C^* \cap (\hat{T}^*)^G \neq \{0\}$, and in particular $C^*_\mathfrak{p} \neq \{0\}$.

Let

$$\chi : \; I_0(T) \longrightarrow \mathbb{C}_1 \cup \{0\}$$

be such a homomorphism that

$$\chi^{-1}(\{0\}) = \bigcup_{p \in S} I_p \qquad \text{with} \qquad \#S < \infty \ ;$$

here $\mathbb{C}_1 := \{z \mid z \in \mathbb{C}, \ |z| = 1\}$. Let

(3)
$$L(\chi, s) = \sum_{\mathfrak{A} \in I_0(T)} \chi(\mathfrak{A}) N\mathfrak{A}^{-s} \ ;$$

clearly

(4)
$$L(\chi, s) = \prod_p L_p(\chi, s) \ ,$$

where p ranges over all the rational primes, and

$$L_p(\chi, s) = \sum_{\mathfrak{A} \in I_p} \chi(\mathfrak{A}) N\mathfrak{A}^{-s} \ .$$

Both the Dirichlet series (3) and the Euler product (4) converge absolutely for $Re\, s > 1$. By a well-known theorem (going back to D. Hilbert), the cone C^* and therefore the monoid I_p are finitely generated. The generators of I_p are the *prime ideals* of T; it can be shown that the theorem on the uniqueness decomposition of the primary ideals into primes does **not** hold in this generality. Let $\mathcal{P}(T)$ be the set of all the prime ideals in $I_0(T)$, and let $\mathfrak{P} \in \mathcal{P}(T)$; we say that $\mathfrak{P}$ is a *strict prime* if

$$\mathfrak{A} | \, \mathfrak{P}^n \Longrightarrow (\mathfrak{A} = \mathfrak{P}^m \quad \text{for some} \quad m) \ .$$

Let $\mathcal{P}_s(T)$ be the subset of the strict primes. From a theorem in combinatories, [14, theorem 2.5], one concludes that

(5)
$$L(\chi, s) = \prod_{\mathfrak{P} \in \mathcal{P}_s(T)} \left(1 - \chi(\mathfrak{P}) N\mathfrak{P}^{-s}\right)^{-1} \prod_p Q_p(p^{-s}) \ ,$$

with $Q_p(x) \in \mathbb{C}[x]$, $Q_p(0) = 1$.

Lemma 1. For $\mathfrak{A}_a \in I_p$ one has

(6)
$$N\mathfrak{A}_a = p^{b(a)} \qquad , \qquad b(a)e(p) = a \cdot z \ ,$$

with $z_i = \sum_{\sigma \in G, 1 \leq j \leq d} r_{ij}(\sigma)$; moreover, $z \in \hat{T}^G$.

Proof. Let $N\mathfrak{p} = p^{f(p)}$. It follows from (2) that

$$N\mathfrak{A}_a = p^{f(p)b_1} \qquad \text{with} \qquad b_1 = \sum_{\tau \bmod G_{\mathfrak{p}}} |\tau a| \ ,$$

where $|a| := \sum_{j=1}^{d} a_j$ for $a \in \hat{T}^*$. Since $C^*_{\mathfrak{p}} \subseteq (\hat{T}^*)^{G_{\mathfrak{p}}}$ we have

$$b_1 = \frac{1}{|G_{\mathfrak{p}}|} \sum_{\sigma \in G} |\sigma a| = \frac{1}{|G_{\mathfrak{p}}|} \sum_{\sigma \in G} \sum_{1 \leq i,j \leq d} a_i r_{ij}(\sigma^{-1}) \ .$$

Relation (6) follows now from the equation $|G_{\mathfrak{p}}| = e(p)f(p)$; the last assertion is obvious.

Write now

$$L_p(\chi, s) = \sum_{n=0}^{\infty} p^{-ns} \sum_{\substack{(a|z)e(p)=n \\ \mathfrak{A}_a \in I_p}} \chi(\mathfrak{A}_a) \ . \tag{7}$$

For $H \subseteq G$, let $C^*_H = C^* \cap (\hat{T}^*)^H$, and let

$$\beta(H) := \min \left\{ a \cdot z | \ a \neq 0, \ a \in C^*_H \right\} \ .$$

By construction,

$$\beta(H) = \left(\min \left\{ \sum_{\tau \bmod H} |\tau a| \Big| a \neq 0, \ a \in C^*_H \right\} \right) \cdot |H| \ ,$$

and therefore

$$|H| \leq \beta(H) < \infty \ . \tag{8}$$

Clearly $\beta(H_1) \leq \beta(H_2)$ if $H_1 \subseteq H_2$, so that

$$\min_{H \subseteq G} \beta(H) = \beta_0 \quad , \quad \beta_0 = \beta(\{e\}) \ . \tag{9}$$

By (7)–(9),

$$L_p(\chi, s) = 1 + \sum_{n \geq \beta_0} p^{-ns} \sum_{\substack{(a|z)e(p)=n \\ \mathfrak{A}_a \in I_p}} \chi(\mathfrak{A}_a) \ . \tag{10}$$

Lemma 2. Both the Dirichlet series (3) and the Euler product (4) converge absolutely for $Re\, s > \frac{1}{\beta_0}$.

Proof. It follows from (10) and the definitions (3), (4).

Clearly

$$\mathfrak{A}_a \in I_p \quad , \quad a \cdot z = \beta(G_p) \Longrightarrow \mathfrak{A}_a \quad \text{is prime} \ .$$

Let

$$\mathcal{P}_m(T) = \{\mathfrak{A}_a |\ a \in C^*,\ a \cdot z = \beta_0\}$$

be the set of the *minimal primes.* It follows from (5) that

$$L(\chi, s) = \prod_{\mathfrak{P} \in \mathcal{P}_m(T)} \left(1 - \chi(\mathfrak{P}) N\mathfrak{P}^{-s}\right)^{-1} L^{(1)}(\chi, s) \ , \tag{11}$$

where

$$L^{(1)}(\chi, s) = \prod_{\mathfrak{P} \in \mathcal{P}_s(T) \setminus \mathcal{P}_m(T)} \left(1 - \chi(\mathfrak{P}) N\mathfrak{P}^{-s}\right)^{-1} \prod_p Q_p^{(1)}(s) \tag{12}$$

with $Q_p^{(1)}(x) \in \mathbb{C}[x]$, $Q_p^{(1)}(0) = 1$, and the Euler product (12) converges absolutely for $Re\, s > \frac{1}{\beta_0 + 1}$.

Corollary 1. The set

$$D(\beta) = \{a |\ a \in C^*,\ a \cdot z = \beta\} \quad , \quad \beta > 0 \ ,$$

is a finite G–invariant set.

Proof. It follows from Lemma 1 that $D(\beta)$ is G–invariant since $z \in \hat{T}^G$; moreover, $a \cdot z = \sum_{\sigma \in G} |\sigma a| \geq |a|$ for $a \in C^*$, and therefore

$$|D(\beta)| \leq card\{a |\ a \in \mathbb{Z}^d,\ a \geq 0,\ |a| = \beta\} < \infty \ .$$

Let

$$D(\beta_0) = \bigcup_{i=1}^{B} D_i$$

be the decomposition of the set $D(\beta_0)$ into G–orbits

$$D_i = G \cdot a^{(i)} \quad , \quad 1 \leq i \leq B \ ,$$

and let

$$\overline{D}_i(p) = \{\mathfrak{A}_a |\ \mathfrak{A}_a \in I_p(T),\ a \in D_i\} \ .$$

We have

$$(13) \qquad \prod_{\mathfrak{P}\in\mathcal{P}_m(T)} \left(1-\chi(\mathfrak{P})N\mathfrak{P}^{-s}\right)^{-1} = f(s) \prod_{1\le i\le B}^{p} \ell_p^{(i)}(s)$$

with

$$(14) \qquad \ell_p^{(i)}(s) = \prod_{\mathfrak{P}\in\overline{D}_i(p)} \left(1+\chi(\mathfrak{P})p^{-\beta_0 s/e(p)}\right) \ ,$$

where $f(s)$ is equal to an Euler product absolutely convergent for $Re\, s > \frac{1}{2\beta_0} \ge \frac{1}{\beta_0+1}$.

Let

$$H_i = \left\{\sigma \mid \sigma \in G,\ \sigma a^{(i)} = a^{(i)}\right\}$$

be the stabiliser of $a^{(i)}$, and let

$$k_i = \left\{x \mid x \in K,\ \sigma x = x \text{ for } \sigma \in H_i\right\}$$

be the subfield of K corresponding to H_i; let

$$T_i = Res_{k_i/\mathbb{Q}} G_{m,k_i} \quad , \quad 1 \le i \le B \ ,$$

so that

$$\hat{T}_i^* = \left\{ \sum_{\sigma \bmod H_i} \alpha(\sigma)\sigma \mid \sigma \in G,\ \alpha(\sigma) \in \mathbb{Z} \right\} \ .$$

There is a surjective homomorphism $f_i : \hat{T}_i^* \to \hat{T}^*$, uniquely defined by the condition $f_i(\sigma) = \sigma \cdot a^{(i)}$; clearly $f_i(\hat{T}_i^*)$ coincides with the submodule $[D_i]$ generated in $\hat{T}^*$ by D_i. By construction,

$$I(T_i) = \left\{\mathfrak{A} \mid \mathfrak{A}_1 \in I(k_i),\ \mathfrak{A}_j = \mathfrak{A}_1^{\sigma_j},\ 1 \le j \le d_i\right\} \ ,$$

where $G = \bigcup_{1\le j\le d_i} H_i\sigma_j$, $d_i = |D_i| = [k_i : \mathbb{Q}]$. Therefore we can define a homomorphism

$$\chi_i :\ I_0(k_i) \longrightarrow \mathbb{C}_1 \cup \{0\}$$

as follows: let $\mathfrak{B}_1 \in I_0(k_i)$ with $N\mathfrak{B}_1 = p^\ell$ for a rational prime p, and let $\mathfrak{B}_j = \mathfrak{B}_1^{\sigma_j}$, $1 \le j \le d_i$; then $\mathfrak{B} \in I_p(T_i)$, say $\mathfrak{B} = \mathfrak{A}_a$ with $a \in \hat{T}_i^*$, and we may set $\chi_i(\mathfrak{B}_1) = \chi(\mathfrak{A}_{f_i(a)})$ for the uniquely defined ideal $\mathfrak{A}_{f_i(a)}$ in $I_p(T)$. Let

$$(15) \qquad L(\chi_i, s) = \prod_{\mathfrak{p}\in I(k_i)} \left(1-\chi_i(\mathfrak{p})N\mathfrak{p}^{-s}\right)^{-1} \ .$$

Proposition 1. We have

$$L(\chi, s) = \prod_{i=1}^{B} L(\chi_i, \beta_0 s) L^{(2)}(\chi, s) \quad , \tag{16}$$

where $L^{(2)}(\chi, s)$ is represented by an Euler product absolutely convergent for $Re\ s > \frac{1}{\beta_0+1}$; moreover,

$$\chi_i = 1 \quad \text{for} \quad 1 \leq i \leq B \Longleftrightarrow \chi\big|_{\mathcal{P}_m(T)} = 1 \quad . \tag{17}$$

Proof. In view of (11) - (15), it suffices to note that

$$\overline{D}_i(p) = \left\{\mathfrak{A}_{f_i(a)} |\, \mathfrak{A}_a = \mathfrak{B} \text{ with } N\mathfrak{B}_1 = p,\ \mathfrak{B} \in I_p(T_i)\right\} \quad .$$

Proposition 1 may be regarded as a formal counterpart of a theorem of Draxl's (cf. [1], equation (2.1)).

4. Now we are ready to proceed to the main part of this investigation and to comment on the structure of $X(\mathbb{Z})$ as a discrete subset of $X(\mathbb{R})$. To begin with let

$$G_2 = Gal(K|\ K \cap \mathbb{R}) \quad ,$$

so that

$$|G_2| = \begin{cases} 1 & \text{if } K \subseteq \mathbb{R} \\ 2 & \text{otherwise} \end{cases} \quad .$$

Since both $\hat{T}/\hat{T}^{G_2}$ and $\hat{T}^{G_2}/\hat{T}^{G}$ are torsion-free there is a $\mathbb{Z}$-basis $\{u_j | 1 \leq j \leq d\}$ of $\hat{T}$ such that $\{u_j |\ 1 \leq j \leq \mu\}$ is a basis of T^G, while $\{u_j |\ 1 \leq j \leq \mu + r\}$ is a basis of T^{G_2}. Clearly

$$T(\mathbb{R}) = \left\{a |\ a \in \mathbb{R}^{nd},\ u^{\tau}(a) = \tau u(a) \text{ for } \tau \in G_2\right\} \quad ,$$

and we can define a surjective map

$$\begin{aligned} f : T(\mathbb{R}) &\longrightarrow \mathbb{R}^{*\mu+r} \times (S^1)^{d_1} \quad , \\ a &\longmapsto \left(u_1(a), \ldots, u_{\mu+r}(a), \ldots, \frac{u_i(a)}{|u_i(a)|}, \ldots\right) \quad , \end{aligned}$$

where $\mu + r + d_1 = d$, $d_1 \geq 0$, $i > \mu + r$. By a generalisation of the Dirichlet unit theorem, [12], [13],

$$T(\mathbb{Z}) \cong \mathbb{Z}^r \times \mathfrak{A} \quad \text{with} \quad |\mathfrak{A}| < \infty \quad ;$$

therefore $T(\mathbb{R})/T(\mathbb{Z}) \cong \mathbb{R}_+^{*\mu} \times \mathcal{T}$, where

$$\mathcal{T} = (S^1)^{d-\mu} \times (\mathbb{Z}/2\mathbb{Z})^{r_0}$$

and $r_0 \leq \mu + r$.

Given a set

$$S = \{\infty\} \cup S_0 \quad , \quad S_0 \subseteq \{p | \; p \text{ is a rational prime}\} \ ,$$

let

$$T_A(S) = \prod_{p \in S} T(\mathbb{Q}_p) \times \prod_{p \notin S} T(\mathbb{Z}_p) \ ,$$

and let

$$T_A = \bigcup_{|S|<\infty} T_A(S) \ .$$

Clearly $T_A = T(A_{\mathbb{Q}})$, where $A_{\mathbb{Q}}$ is the adèle–algebra over $\mathbb{Q}$. Let

$$T_A^1 = \left\{ a | \; a \in T_A, \; |x(a)| = 1 \text{ for } x \in \hat{T}^G \right\} \ ;$$

clearly $T(\mathbb{Q}) \subseteq T_A^1$ (if one identifies $T(\mathbb{Q})$ with its image under the diagonal embedding into T_A). By a well-known theorem, [12], [15], $T_A^1/T(\mathbb{Q})$ is a compact group. We have

$$T(\mathbb{Q}_p) = \left\{ \mathfrak{p}^a | \; a \in (\hat{T}^*)^{G_\mathfrak{p}} \right\} \ ,$$

where $\mathfrak{p}$ is a fixed prime in $I(K)$ with $\mathfrak{p}|p$. Therefore there is a natural embedding $g : I_p \hookrightarrow T_A(S)$ with $S = \{\infty, p\}$ such that $g(I_p)_q = 1$ for $q \notin S$, and $g(\mathfrak{A}_a)_p = \mathfrak{p}^a$ for $\mathfrak{A}_a \in I_p$; moreover, it may be assumed that $g(I_p) \subseteq T_A^1$ if one adjusts $g(I_p)_\infty$ properly. One extends g to an embedding

$$g : \; I_0(T) \hookrightarrow T_A^1 \ .$$

Given a character

$$\tilde{\chi} : \; T_A^1/T(k) \longrightarrow \mathbb{C}_1 \ ,$$

the set $S_0 = \left\{ p | \; \tilde{\chi}_p(\mathbb{Z}_p) \neq 1 \right\}$ is finite; for $p \notin S_0$ we let $\chi_p = \tilde{\chi}_p \circ g$, if $p \in S_0$ let $\chi_p(I_p) = 0$. This procedure gives rise to the group $Gr(T)$ of *Hecke characters*

$$\chi : \; I_o(T) \longrightarrow \mathbb{C}_1 \cup \{0\} \ .$$

If $\chi \in Gr(T)$ then $\chi_i \in Gr(k_i)$, $1 \leq i \leq B$, where $Gr(k)$ denotes the group of all the Grössencharakteren of a number field k. The following result may be regarded as a corollary of Satz 1 in [1].

Corollary 2. Suppose that $\chi \in Gr(T)$. Then equation (16) defines $L(\chi, s)$ as a meromorphic function of s in the halfplane $\left\{s \mid s \in \mathbb{C},\ Re\, s > \frac{1}{\beta_0+1}\right\}$, with the only possible pole at $s = 1/\beta_0$.

Proof. It is an immediate consequence of Proposition 1 since $L(\chi_i, s)$, $1 \leq i \leq B$, is a Hecke L–function of k_i in this case.

The usual machinery of analytic number theory (see, for instance, [9] and references therein) yields now the following results:

$$(18) \qquad card\left\{\mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}(T),\ N\mathfrak{p} < y^{1/\beta_0}\right\} = B\int_2^y \frac{du}{\log u} + O\left(ye^{-c\sqrt{\log y}}\right) \ ,$$

$$\text{with} \quad c > 0 \ ,$$

and

$$(19) \qquad card\left\{\mathfrak{A} \mid \mathfrak{A} \in I_0(T),\ N\mathfrak{A} < y^{1/\beta_0}\right\} = yp(\log y) + O(y^{1-c_1}) \ ,$$

$$\text{with} \quad c_1 > 0 \ ,$$

where $p(x) \in \mathbb{C}[x]$, $\deg p = B - 1$.

The infinite component $\tilde{\chi}_\infty$ in the decomposition $\tilde{\chi} = \tilde{\chi}_\infty \cdot \prod_p \chi_p$ may be regarded as a character of $T(\mathbb{R})/T(\mathbb{Z})$, say

$$\tilde{\chi}_\infty : \ \mathbb{R}_+^{*\mu} \times \mathcal{T} \longrightarrow \mathbb{C}_1 \ .$$

The grossencharacter χ obtained from $\tilde{\chi}$ is said to be *normalised* if $\tilde{\chi}_\infty\big|_{\mathbb{R}_+^{*\mu}} = 1$. Write

$$\mathfrak{f}_\infty(\chi) = \{\alpha \mid \alpha \in (\mathbb{Z}/2\mathbb{Z})^{r_0},\ \tilde{\chi}_\infty(\alpha) \neq 1\} \ ,$$

and let $\mathfrak{f}_0(\chi) = \prod_p p^{m_p}$, where

$$m_p = \min\left\{m \mid \alpha \in \mathbb{Z}_p,\ \alpha = 1(\mathrm{mod}\ p^m) \Longrightarrow \tilde{\chi}_p(\alpha) = 1\right\} \ .$$

The pair $\mathfrak{f}(\chi) = \left(\mathfrak{f}_\infty(\chi), \mathfrak{f}_0(\chi)\right)$ is said to be the conductor of χ. The group $Gr_0(T, \mathfrak{f})$ of all the normalised grossencharacters having a given conductor $\mathfrak{f}$ is isomorphic to $\mathbb{Z}^{d-\mu} \times \mathfrak{B}(\mathfrak{f})$, where $\mathfrak{B}(\mathfrak{f})$ is a finite Abelian group. Moreover, $\mathfrak{B}(\mathfrak{f})$ may be chosen to coincide with the subgroup of all the characters of finite order in $Gr_0(T, \mathfrak{f})$. Let

$$\mathfrak{B}(\mathfrak{f})^\perp = \left\{\mathfrak{A} \mid \mathfrak{A} \in I_0(T),\ \chi(\mathfrak{A}) = 1 \text{ for } \chi \in \mathfrak{B}(\mathfrak{f})\right\} \ ,$$

and let

$$I_0^{\mathfrak{f}}(T) = \{\mathfrak{A} | \ \chi(\mathfrak{A}) \neq 0 \text{ for } \chi \in Gr_0(T, \mathfrak{f})\} \ .$$

The ray class group $H(\mathfrak{f}) := I_0^{\mathfrak{f}}(T)/\mathfrak{B}(\mathfrak{f})^{\perp}$ is finite, [12] (cf. also [15]), and $\mathfrak{B}(\mathfrak{f})$ may be regarded as the group of characters of $H(\mathfrak{f})$. In a usual way one obtains the following asymptotic formulae for the number of integral ideals and for the number of the prime ideals in a given ideal class. Let $A \in H(\mathfrak{f})$, we have

$$(20) \qquad card\{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(T) \cap A, \ N\mathfrak{p} < y^{1/\beta_0}\}$$

$$= \left(\sum_{\chi \in \mathfrak{B}(\mathfrak{f})}{}^{*} \ \overline{\chi(A)} g(\chi) \right) \int_2^y \frac{du}{\log u} + O\left(y e^{-c_2 \sqrt{\log y}} \right) \ ;$$

and

$$(21) \qquad card\{\mathfrak{A} | \mathfrak{A} \in A, \ N\mathfrak{A} < y^{1/\beta_0}\} = y \sum_{\chi \in \mathfrak{B}(\mathfrak{f})}{}^{*} \ \overline{\chi(A)} p_\chi(\log y) + O(y^{1-c_3}) \ ,$$

where $c_2 > 0$, $c_3 > 0$, $\sum^{*} := \frac{1}{|H(\mathfrak{f})|} \sum$, p_χ is a polynomial of degree $g(\chi) - 1$ whose coefficients may depend on χ, $g(\chi) := card\{i | \ 1 \leq i \leq B, \ \chi_i = 1\}$ (if $g(\chi) = 0$ we let $p_\chi = 0$).

Although our ultimate purpose is to investigate the distribution of integer points on X in the real locus $X(\mathbb{R})$, the methods for this paper fall short of such a goal, and we should be content with somewhat weaker results on the integer points of the variety Y defined as follows. For $a \in K^{*d}$ let $\epsilon(a, \sigma) = (\sigma a)(a^{\sigma})^{-1}$, and write $\epsilon(a) : \ \sigma \mapsto \epsilon(a, \sigma)$, $\sigma \in G$; define an equivalence relation $\sim$:

$$\epsilon(a) \sim \epsilon(a') \Longleftrightarrow \epsilon(a) = \epsilon(a')\epsilon(b) \text{ for some } b \text{ in } E_K^d \ ,$$

where E_K denotes the group of units of K, and let

$$A = \{\epsilon(a) | \ a \in K^{*d}, \ \epsilon(a, \sigma) \in E_K^d \text{ for } \sigma \in G\} \ .$$

Let B be a set of representatives for $A/\sim$ containing the identity $\epsilon^{(0)}$ (here $\epsilon^{(0)} := \epsilon(1)$, $\epsilon_i(1, \sigma) = 1$ for $1 \leq i \leq d$). We set

$$Y = \bigcup_{\epsilon \in B} V_\epsilon \ ,$$

the variety V_ϵ being defined by the equations

$$\sigma t = \epsilon(\sigma) t^{\sigma} \qquad , \qquad \sigma \in G \ ;$$

clearly $V_{\epsilon(0)} = X$, so that $X \subseteq Y$. The open subset $\tilde{V}_\epsilon$ of V_ϵ defined by the condition $\prod_{i=1}^{d} t_i \neq 0$ is a T-homogeneous space, and we identify $\tilde{V}_\epsilon(\mathbb{R})$ with $T(\mathbb{R})$. Moreover,

$$\big(t(a)\big) \in I_0(T) \Longleftrightarrow a \in \tilde{Y}(\mathbb{Z}) \ ,$$

with $\tilde{Y} := \bigcup_{\epsilon \in B} \tilde{V}_\epsilon$. Making use of the theory developed here we obtain now an estimate for the number of integer points on Y in the "rectangular" compact domain $U(y)$ in $T(\mathbb{R})$ given as follows:

$$U(y) = \big\{a \mid a \in T(\mathbb{R}),\ |Nt(a)| < y^{1/\beta_0},\ \ y^{-1} \leq u_j(a) \leq y \text{ for } \mu+1 \leq j \leq \mu+r\big\} \ ,$$

where $Nt(a) := \prod_{i=1}^{d} \prod_{\sigma \in G} (\sigma t_i)(a)$.

Corollary 3. Let $\mathfrak{A}_0 \in I_0^{\mathfrak{f}}(T)$, and let

$$M(\mathfrak{A}_0) = \big\{a \mid a \in Y(\mathbb{Z}),\ \big(t(a)\big) \subseteq \mathfrak{A}_0,\ \big(t(a)\big) \in \mathfrak{B}_0(\mathfrak{f})^{\perp}\big\} \ .$$

We have

$$card\big(U(y) \cap M(\mathfrak{A}_0)\big) = c_1(\mathfrak{A}_0) y (\log y)^{b+r} \left(1 + O\Big(\frac{1}{\log y}\Big)\right) \ , \tag{22}$$

with $0 \leq b \leq B - 1$.

Proof. Clearly

$$a \in M(\mathfrak{A}_0) \Longleftrightarrow \big(t(a)\big) = \mathfrak{A}\mathfrak{A}_0 \ \text{ with } \ \mathfrak{A} \in A \ ,$$

where $A \in H(\mathfrak{f})$, $\mathfrak{A}_0 \in A^{-1}$. By the unit theorem,

$$card\big\{a \mid \big(t(a)\big) = \big(t(a_0)\big),\ a \in M(\mathfrak{A}_0) \cap U(y)\big\} = c_2 (\log y)^r \left(1 + O\Big(\frac{1}{\log y}\Big)\right) \ .$$

Relation (22) follows from this estimate when combined with (21).

Proposition 2. If T is anisotropic then

$$card\big(X(\mathbb{Z}) \cap U(y)\big) = c_3 (\log y)^r \left(1 + O\Big(\frac{1}{\log y}\Big)\right) \ . \tag{23}$$

Proof. In this case $I_0(T) = \{1\}$, so that $X(\mathbb{Z}) \cap U(y)$ coincides with $T(\mathbb{Z}) \cap U(y)$. Therefore (23) follows from the unit theorem.

Remark 1. The constants $c_1(\mathfrak{A}_0)$ and c_3 can be explicitly evaluated; if $M(\mathfrak{A}_0) \neq \{0\}$ (resp. $X(\mathbb{Z}) \neq \{0\}$) then $c_1(\mathfrak{A}_0) > 0$ (resp. $c_3 > 0$).

5. Proposition 2 provides a complete solution of the problem of counting integer points on an anisotropic torus, although further refinements in the spirit of [3] may be probably obtained. Thus henceforth we assume again that the torus T under consideration is not anisotropic. The deeper results on the spatial ("multidimensional") distribution of the integer points as well as of the integral (or of the prime) ideals depend on the following condition

$$\chi_i = 1 \quad \text{for} \quad 1 \leq i \leq B \Longrightarrow \chi \in B(\mathfrak{f}) \quad \text{for some } \mathfrak{f} \tag{24}$$

to be satisfied. If (24) holds and $B = 1$ then a complete analysis in the spirit of [8], [9], [11] is possible. If (24) holds but $B \neq 1$ we can still prove a spatial equidistribution theorem for integral ideals gaining, however, only a power of logarithm of the main term in the error term (this being insufficient for finer applications to an equidistribution theorem for integer points, as exhibited in [11]).

In view of (17), condition (24) holds true (with an even stronger conclusion) if the set $\mathcal{P}_m(T)$ of minimal primes generates the monoid $I_0(T)$ of integral ideals. The following observation [1, Satz 1] lies deeper, and it is more useful.

Lemma 3. If $\mathcal{P}_m(T)$ generates the group $I(T)$ then (24) holds true.

Proof. It is an immediate consequence of the last assertion in [1, Satz 1].

Example 1. The norm–form (or Vinogradov) torus T can be defined as follows. Let k be a field of algebraic numbers of finite degree over $\mathbb{Q}$; let $k_i|k$, $1 \leq i \leq \nu$, be a finite extension. The torus T_k is defined by the following condition (cf. [1]):

$$T_k(B) = \left\{ b \mid b \in \prod_{i=1}^{\nu} \left(B \otimes_k k_i\right)^*, \ N_{B\otimes_k k_1/B} b_1 = N_{B\otimes k_i/B} b_i, \ 1 \leq i \leq \nu \right\}$$

for any k–algebra B; we let $T = Res_{k/\mathbb{Q}} T_k$. It follows from Lemma 3 that the torus T satisfies (24), and therefore one can prove a theorem on the equidistribution of integral ideals having equal norms (cf. [8], where $k = \mathbb{Q}$ and the fields k_i are assumed to be linearly disjoint over k). Moreover, if the fields k_i, $1 \leq i \leq \nu$, are linearly disjoint over k then $B = 1$; therefore a complete theory in the spirit of [8], [9], [11] (where we have assumed $k = \mathbb{Q}$) can be developed in this case.

An open question. A Draxl L–function $L(s, \chi)$ of an algebraic torus is known to be meromorphic in the half–plane $\{s | \ s \in \mathbb{C}, \ Re\, s > 0\}$, [1]. Moreover, if T is a norm–form torus considered in Example 1, then $L(s, \chi)$ has the line $\{s | \ s \in \mathbb{C}, \ Re\, s = 0\}$ as its natural boundary for analytic continuation, unless either $\#\{i | \ k_i \neq k\} \leq 1$, or $\#\{i | \ k_i \neq k\} = 2$ and $[k_i : k] \leq 2$ for each i in which cases $L(s, \chi)$ is meromorphic on the whole complex plane, [6], [10]. Therefore we may ask under what conditions on T the function $s \mapsto L(x, \chi)$ can be analytically continued to a meromorphic function on $\mathbb{C}$.

Acknowledgement. My intellectual debt to the work of the late Professor P.K.J. Draxl, [1], [2], is quite apparent. I wish to acknowledge also a few inspiring and useful conversations with Professor Yu. I. Manin and Professor V.V. Batyrev. Last but not least I am grateful to the Max–Planck–Gesellschaft for their financial support at the A.G. "Algebraische Geometrie und Zahlentheorie" in Berlin and at the Max–Planck–Institut für Mathematik (Bonn).

Literatur

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

[2] P.K.J. Draxl, *Zeta–Funktionen Algebraischer Tori und Skalarprodukte Hecke-scher L–Reihen*, Diplomarbeit, Göttingen, 1968.

[3] G.R. Everest, *On the canonical height for the algebraic unit group*, Journal für die reine und angewandte Mathematik, 432 (1992), 57–68.

[4] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen (Zweite Mitteilung)*, Mathematische Zeitschrift, 6 (1920), 11–51.

[5] J. Kubilius, *On some problems in geometry of prime numbers (in Russian)*, Matematičeskii Sbornik, 31 (1952), No. 3, 507–542.

[6] N. Kurokawa, *On the meromorphy of Euler products (I, II)*, Proceedings of the London Mathematical Society, 53 (1986), 1–47, 209–236.

[7] T. Mitsui, *Generalised prime number theorem*, Japanese Journal of Mathematics, 26 (1956), 1–42.

[8] B.Z. Moroz, *On the distribution of integral and prime divisors with equal norms*, Annales de l'Institut Fourier (Grenoble), 34 (1984), fasc. 4, 1–17.

[9] B.Z. Moroz, *Analytic arithmetic in algebraic number fields*, Springer Lecture Notes in Mathematics, 1205 (1986), Springer–Verlag.

[10] B.Z. Moroz, *On a class of Dirichlet series associated to the ring of representations of a Weil group*, Proceedings of the London Mathematical Society, 56 (1988), 209–228.

[11] B.Z. Moroz, *On the distribution of integral points on an algebraic torus defined by a system of norm-form equations*, The Quarterly Journal of Mathematics, 45 (1994), to appear.

[12] T. Ono, *Arithmetic of algebraic tori*, Annals of Mathematics, 74 (1961), 101–139.

[13] J.-M. Shyr, *A generalization of Dirichlet's unit theorem*, Journal of Number Theory, 9 (1977), 213– 217.

[14] R.P. Stanley, *Linear homogeneous Diophantine equations and magic labeling of graphs*, Duke Mathematical Journal, 40 (1973), 607–632.

[15] V.E. Voskresenskii, *Algebraic tori (in Russian)*, Nauka, Moscow, 1977.

Correction

p. 3, line 10, read : $I_0(T) = I(T) \cap I_0(K)^d$

p. 5, line 4, read: $\prod\limits_{p \in S}$ (instead of $\coprod\limits_{p \in S}$)

p. 6, formulae (7) and (10), read : $(\alpha/z) = n \cdot e(p)$ (instead of $(\alpha/z)e(p) = n$)

p. 7, line 7 from below, read: $|a| \leq \beta$ (instead of $|a| = \beta$)

p. 9, lines 8, 9 from below, read: $\hat{T}^G, \hat{T}^{G_2}$ (instead of T^G, T^{G_2})

p. 14, in (24) read: $\mathfrak{B}(\mathfrak{f})$ (instead of $B(\mathfrak{f})$)

p. 14, lemma 3 should read: If $C^*(\beta_0)$ generates the group $\hat{T}^*$ then (24) holds true. Here

$$C^*(m) := \{a | a \in C^*, a.z = m\}, m \in \mathbf{Z}, m \geq 1.$$

p. 15, line 7 from below, read: Literature cited