H. K. Kim
Nagoya Math. J.
Vol. 112 (1988), 117-124

UNIT THEOREMS ON ALGEBRAIC TORI

HYUN KWANG KIM

Let k be a p-adic field (a finite extension of $\boldsymbol{Q}_p$) or an algebraic number field (a finite extension of $\boldsymbol{Q}$). Let T be an algebraic torus defined over k. We denote by $\hat{T}$ the character module of T (i.e. $\hat{T} = \mathrm{Hom}(T, G_m)$), where G_m is the multiplicative group.

As is well-known (cf. [7]), T is split by a finite galois extension K/k. We denote by G the galois group of K/k. Then $\hat{T}$ becomes naturally a G-module. Since the map $T \to \hat{T}$ yields a canonical isomorphism between the category of tori defined over k and split by K and the dual category of finitely generated $\boldsymbol{Z}$-free G-modules, it is natural to use $\mathrm{Hom}_G(\hat{T}, M_K)$ as a definition of an object relative to T over k when M_K is a G-module of arithmetical interest related to K.

In this paper, we will determine the structure of $\mathrm{Hom}_G(\hat{T}, O_K^\times)$ where $O_K^\times$ is the group of units of K and will discuss the meaning of this group.

§ 1. Local unit theorem

Let k be a p-adic field. First we recall the structure of $O_k^\times$. Let π be a prime element of k and let U_1 be the group of one units of k i.e. $U_1 = 1 + \pi O_k$. $\boldsymbol{Z}_p$ acts on U_1 as follows:

Let $a = a_0 + a_1 p + \cdots + a_n p^n + \cdots \in \boldsymbol{Z}_p$ and $u \in U_1$. Set $a_n = \sum_{i=0}^n a_i p^i$. Then $\{u^{a_n}\}$ is a Cauchy sequence in U_1. Since U_1 is compact, the limit exists and denoted by u^a.

So we can view U_1 as $\boldsymbol{Z}_p$-module. We have the following proposition (cf. [5]).

(1.1) PROPOSITION. *$U_1 \approx W(U_1) \times \boldsymbol{Z}_p^{[k \cdot \boldsymbol{Q}_p]}$, where $W(U_1)$ is the group of roots of unity in U_1.* □

Now $O_k/(\pi)$ has $q = p^s$ elements. Let η be a primitive $(q-1)$th root of unity in O_k. Then

Received April 27, 1987.

$$O_k^\times = \langle\eta\rangle \times U_1 \approx \langle\eta\rangle \times W(U_1) \times Z_p^{[k:Q_p]}.$$

We have proved

(1.2) PROPOSITION. *Let k be a p-adic field. Up to finite torsions, $O_k^\times$ is a free Z_p-module of rank $[k: Q_p]$.* □

Let k be a p-adic field and T be a torus defined over k split by K, where K is a finite galois extension of k with galois group G. We can think $\mathrm{Hom}(\hat{T}, O_K^\times)$ as a G-module. Let $\mathrm{Hom}_G(\hat{T}, O_K^\times)$ denote the G-invariant submodule of this module.

(1.3) DEFINITION. $T(O_k) = \mathrm{Hom}_G(\hat{T}, O_K^\times)$

We have the following main theorem for local theory.

(1.4) THEOREM. *Up to finite torsions, $T(O_k)$ is a free Z_p-module of rank $r(T) = [k: Q_p]\cdot(\dim T)$.*

Proof. By Proposition 1.2,

$$O_K^\times = W \times U_1, \text{ where } W \text{ is a finite group.}$$

Therefore,

$$T(O_k) = \mathrm{Hom}_G(\hat{T}, W) \times \mathrm{Hom}_G(\hat{T}, U_1).$$

Since $\mathrm{Hom}_G(\hat{T}, W)$ is a finite group, it suffices to determine the Z_p-module structure of $\mathrm{Hom}_G(\hat{T}, U_1)$. For each $m \geq 1$, set $U_m = 1 + \langle\pi^m\rangle$.

It is well-known that (cf. [5]):

(i) U_m is a Z_p-submodule of U_1 of finite index.

(ii) U_m is free if $m > \dfrac{e}{p-1}$, where e is the ramification index of p over K.

We will determine the Z_p-rank of $\mathrm{Hom}_G(\hat{T}, U_m)$ for sufficiently large m.

Now we need lemmas.

(1.5) LEMMA. *Let R be a commutative ring and M, N be R-modules. We have an isomorphism*

$$\mathrm{Hom}_R(M, N) \approx M^* \otimes_R N,$$

where $M^* = \mathrm{Hom}_R(M, R)$ denote the dual module of M. Assume further that a finite group G acts on M and N. Then the isomorphism induces an isomorphism of G-invariant parts.

$$\mathrm{Hom}_{R[G]}(M, N) \approx (M^* \otimes_R N)^G$$

Proof. See Proposition 10.30 in [2]. □

(1.6) LEMMA. *Let R be a principal ideal domain and let K be its quotient field. Let X be a finitely generated R-free module. Assume that a group G acts on X. Then*

$$\mathrm{rank}_R X^G = \dim_K (X \otimes_R K)^G .$$

Proof. It sufficies to show $X^G \otimes_R K = (X \otimes_R K)^G$. Clearly $X^G \otimes_R K \subset (X \otimes_R K)^G$. To do converse, choose a basis $\{x_1, \cdots, x_n\}$ of X over R such that $\{a_1x_1, \cdots, a_lx_l\}$ is a basis of X^G, $a_1, \cdots, a_l \in R$. Assume $x = x_1k_1 + \cdots + x_nk_n$, $k_i \in K$, be an element of $(X \otimes_R K)^G$. We can choose $r \in R$ such that $k_ir \in R$ for all $i = 1, \cdots, n$. Hence $xr = x_1k_1r + \cdots x_nk_nr \in X^G$. By the choice of our basis, we have $k_ir = 0$ if $i > l$. This proves that $x \in X^G \otimes_R K$. □

(1.7) LEMMA. *Let V be a vector space over a field K,* $\mathrm{char}\, K = 0$. Let $\varphi\colon G \to GL(V)$ *be a representation of G in V. Then*

$$\dim_K V^G = \frac{1}{|G|} \sum_{g \in G} \chi(g) ,$$

where χ is the character of φ.

Proof. First assume that φ is irreducible. Then $V^G = 0$ or G.
(i) $V^G = V$. Then $\varphi(g) = \mathrm{id}_V$ for all $g \in G$.
Hence

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \frac{1}{|G|} \sum_{g \in G} (\dim V) = \dim V.$$

(ii) $V^G = 0$.
Let $\{v_1, \cdots, v_n\}$ be a basis of V over K and let $(a_{ij}(g))$ be the matrix of $\varphi(g)$ with respect to this basis. For each i,

$$\sum_{g \in G} \varphi(g) v_i \in V^G = 0 .$$

On the other hand,

$$\sum_{g \in G} \varphi(g) v_i = \sum_{g \in G} (\sum_j a_{ij}(g) v_j) = \sum_j (\sum_{g \in G} a_{ji}(g)) v_j .$$

By linearly independence,

$$\sum_{g\in G} a_{ji}(g) = 0 \qquad \text{for all } i, j = 1, \cdots, n.$$

Hence

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} (\sum_i a_{ii}(g)) = \sum_i (\sum_{g\in G} a_{ii}(g)) = 0.$$

For general case, let $V = V_1 \oplus \cdots \oplus V_k$ be a decomposition of V into irreducible subspaces. So we have $V^G = V_1^G \oplus \cdots \oplus V_k^G$. Let χ_i be the character of the subrepresentation $\varphi_i\colon G \to GL(V_i)$. By the first case,

$$\dim V_i^G = \frac{1}{|G|} \sum_{g\in G} \chi_i(g).$$

Hence

$$\dim V^G = \sum_i \dim V_i^G = \sum_i \left(\frac{1}{|G|} \sum_{g\in G} \chi_i(g)\right) = \frac{1}{|G|} \sum_{g\in G} \chi(g). \qquad \square$$

To apply Lemma 1.5 to our problem we need:

SUBLEMMA. *There is a natural isomorphism*

$$\mathrm{Hom}_Z(\hat{T}, U_m) \approx \mathrm{Hom}_{Z_p}(\hat{T} \otimes Z_p, U_m).$$

Furthermore,

$$\mathrm{Hom}_{Z[G]}(\hat{T}, U_m) \approx \mathrm{Hom}_{Z_p[G]}(\hat{T} \otimes Z_p, U_m).$$

Proof. Straightforward. $\square$

By abuse of notation, we will write $\hat{T}$ instead of $\hat{T} \otimes Z_p$. Assume that $m > \frac{e}{p-1}$. Then U_m is Z_p-free.

By Lemma 1.5,

$$\mathrm{Hom}_G(\hat{T}, U_m) = (\hat{T}^* \otimes U_m)^G.$$

By Lemma 1.6,

$$r(T) = \mathrm{rank}_{Z_p}(\hat{T}^* \otimes U_m)^G = \dim_{Q_p}(\hat{T}^* \otimes U_m)^G.$$

Assume that G acts on $\hat{T}$ and U_m with characters χ_1 and χ_2, respectively. Let χ be the character comes from the action of G on $\hat{T}^* \otimes U_m$. Then

$$\chi(\sigma) = \chi_1(\sigma^{-1}) \cdot \chi_2(\sigma) \qquad \text{for all } \sigma \in G.$$

By Lemma 1.7,

$$r(T) = \frac{1}{|G|} \sum_{\sigma \in G} \chi_1(\sigma^{-1}) \cdot \chi_2(\sigma) = \langle \chi_1, \chi_2 \rangle .$$

Now we will describe the action of G on U_m.

SUBLEMMA. *Let* $|G| = n$. *There exists* π' *in* $\pi^n O_K$ *such that* $\sigma(\pi') = \pi'$ *for all* $\sigma \in G$.

Proof. Put $\pi' = \prod_{\sigma \in G} \sigma(\pi)$. □

Assume that $m > \dfrac{e}{p-1}$ and $|G| = n/m$. By the above sublemma, we may assume that $\sigma(\pi^m) = \pi^m$ for all $\sigma \in G$. We have the following commutative diagram:

$$\begin{array}{ccccc} U_m & \xrightarrow[\log]{\approx} & \pi^m O_K & \xrightarrow[\times \pi^{-m}]{\approx} & O_K \\ \downarrow \sigma & & \downarrow \sigma & & \downarrow \sigma \\ U_m & \xrightarrow[\log]{\approx} & \pi^m O_K & \xrightarrow[\times \pi^{-m}]{\approx} & O_K \end{array}$$

Choose a normal basis $\{x^\sigma\}_{\sigma \in G}$ of K over k, and let $\{\alpha_1, \cdots, \alpha_m\}$ be a basis of k over $\boldsymbol{Q}_p$. Then $\{\alpha_i x^\sigma\}_{\substack{i=1,\cdots,m \\ \sigma \in G}}$ forms a basis of K over $\boldsymbol{Q}_p$. By multiplying some power of π which is invariant under the action of G, we may assume that $\alpha_i x^\sigma \in O_K$ for all $\sigma \in G$ and $i = 1, \cdots, m$. By the above diagram $\{\exp(\pi^m \alpha_i x^\sigma)\}_{\substack{i=1,\cdots,m \\ \sigma \in G}}$ forms a basis of U_m over $\boldsymbol{Z}_p$. So we have

$$\chi_2(\sigma) = \begin{cases} m \cdot |G| & \text{if } \sigma = \text{identity}, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned} r(T) &= \frac{1}{|G|} \sum_{\sigma \in G} \chi_1(\sigma^{-1}) \chi_2(\sigma) = \frac{1}{|G|} \chi_1(\mathrm{id}) \cdot m |G| \\ &= m \cdot (\dim T) = [k : \boldsymbol{Q}_p] \cdot (\dim T) . \end{aligned}$$

(1.8) *Remark.* Take $T = G_m$ the multiplicative group. If we think T is defined over k and split by k, then Theorem 1.4 reduced to Proposition 1.2.

§ 2. Global unit theorem

Let k be a number field, and T, K, G be as in Section 1. As in Section 1, we define the O_k point of T as follows:

(2.1) DEFINITION. $T(O_k) = \mathrm{Hom}_G(\hat{T}, O_K^\times)$.

Then $T(O_k)$ becomes a $\boldsymbol{Z}$-module. Let $r(T)$ denote its rank. By the arguments in Section 1, we have

$$r(T) = \frac{1}{|G|}\sum_{\sigma\in G}\chi_1(\sigma^{-1})\chi_2(\sigma) = \langle\chi_1, \chi_2\rangle,$$

where χ_1 is the character comes from the action of G on $\hat{T}$ and χ_2 is the character comes from the action of G on $O_K^\times$.

Now we will describe the action of G on $O_K^\times$. Let $m = [k: \boldsymbol{Q}]$ and $n = [K: k]$. Let $k_1, \cdots, k_{\rho_1+\rho_2}, k'_{\rho_1+\rho_2+1}, \cdots, k'_{\rho_1+\rho_2+r_2}, k''_{\rho_1+\rho_2+1}, \cdots, k''_{\rho_1+\rho_2+r_2}$ be the distinct conjugates of k $(\rho_1 + \rho_2 + 2r_2 = m)$. To each of them, we can correspond a conjugate of K to which we will give the same index. The indices are chosen in the way that:

(i) For $1 \leq i \leq \rho_1$, k_i and K_i are real,

(ii) for $\rho_1 < i \leq \rho_1 + \rho_2$, k_i is real and K_i is imaginary,

(iii) for $\rho_1 + \rho_2 < i$, k'_i and k''_i are complex conjugates and the same for K'_i and K''_i.

Note that K_i is galois over k_i whose galois group is isomorphic to G. So we may identify its galois group with G. Suppose that $\rho_2 \neq 0$. Then n is even. For $\rho_1 < i \leq \rho_1 + \rho_2$, K_i is of degree 2 over the maximal real subfield of K_i/k_i. Let H_i be the subgroup of G corresponding to this field. We have the following proposition (cf. [3], [4]).

(2.2) PROPOSITION. *Let H be the representation of G on $O_K^\times$, C be the trivial representation of G, A be the regular representation of G and B_i be the induced representation of G induced by the trivial representation of H_i, $\rho_1 + 1 \leq i \leq \rho_1 + \rho_2$. Then we have*

$$H + C = (\rho_1 + r_2)A + \sum_{i=\rho_1+1}^{\rho_1+\rho_2} B_i. \qquad \square$$

Proposition 2.2 says that

$$\chi_2 = (\rho_1 + r_2)\chi_A + \sum_{i=\rho_1+1}^{\rho_1+\rho_2}\chi_{B_i} - \chi_C.$$

Hence

$$\langle\chi_1, \chi_2\rangle = (\rho_1 + r_2)\langle\chi_1, \chi_A\rangle + \sum_{i=\rho_1+1}^{\rho_1+\rho_2}\langle\chi_1, \chi_{B_i}\rangle - \langle\chi_1, \chi_C\rangle.$$

On the other hand,

$$\langle\chi_1, \chi_A\rangle = \frac{1}{|G|}(\dim T)\cdot|G| = \dim T$$

$$\langle \chi_1, \chi_C \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \chi_1(\sigma^{-1})\chi_C(\sigma) = \frac{1}{|G|} \sum_{\sigma \in G} \chi_1(\sigma) = \operatorname{rank} \hat{T}^G \quad \text{(by Lemma 1.7)}$$

$$\begin{aligned} \langle \chi_1, \chi_{B_i} \rangle &= \langle \chi_1|_{H_i}, \chi_{B_i}|_{H_i} \rangle_{H_i} \quad \text{(by Frobenius reciprocity law)} \\ &= \operatorname{rank} \hat{T}^{H_i} \quad \text{(by Lemma 1.7)}. \end{aligned}$$

So we have proved

(2.3) THEOREM. *Let T be a torus defined over a number field k. Up to finite torsions, $T(O_k)$ is a free Z-module of rank $r(T)$, where*

$$r(T) = (\rho_1 + r_2)\cdot \dim T + \sum_{i=\rho_1+1}^{\rho_1+\rho_2} \operatorname{rank} \hat{T}^{H_i} - \operatorname{rank} \hat{T}^G. \qquad \square$$

(2.4) *Remark.* T. Ono showed the following generalization of Dirichlet unit theorem (cf. [6]):

Let T be a torus defined over $\boldsymbol{Q}$. Then $\boldsymbol{Z}$-rank of $T(\boldsymbol{Z})$ is $r_\infty - r_{\boldsymbol{Q}}$, where $r_\infty = \operatorname{rank} \hat{T}(\boldsymbol{R})$ and $r_{\boldsymbol{Q}} = \operatorname{rank} \hat{T}(\boldsymbol{Q})$.

We can deduce this result from Theorem 2.3. Let K be a splitting field of T over $\boldsymbol{Q}$. Note first that $r_{\boldsymbol{Q}} = \operatorname{rank} \hat{T}(\boldsymbol{Q}) = \operatorname{rank} \hat{T}^G$.

(i) K is real, i.e. $\rho_1 = 1$, $\rho_2 = r_2 = 0$.
Since $\hat{T}(\boldsymbol{R}) = \hat{T}$, $r_\infty = \dim T$. Therefore,

$$r(T) = \dim T - \operatorname{rank} \hat{T}^G = r_\infty - r_{\boldsymbol{Q}}.$$

(ii) K is imaginary, i.e. $\rho_1 = 0$, $\rho_2 = 1$, $r_2 = 0$.
Since $\hat{T}(\boldsymbol{R}) = \hat{T}^H$, $r(T) = \operatorname{rank} \hat{T}^H - \operatorname{rank} \hat{T}^G = r_\infty - r_{\boldsymbol{Q}}$. $\square$

(2.5) *Remark.* Definition 1.3 and Definition 2.1 are independent of the choice of a splitting field.

Proof. Since the compositum of splitting fields of T is again a splitting field of T, it suffices to prove the following:

Let E be an another splitting field of T containing K with galois group L, then

$$\operatorname{Hom}_L(\hat{T}, O_E^\times) \approx \operatorname{Hom}_G(\hat{T}, O_K^\times).$$

Key point: Assume $\xi \in \operatorname{Hom}_L(\hat{T}, O_E^\times)$ such that $\xi^\sigma = \xi$ for all $\sigma \in L = \operatorname{Gal}(E/k)$. Then $\xi^\sigma = \xi$ for all $\sigma \in \operatorname{Gal}(E/K)$. Hence $\xi(\hat{T}) \subset O_K^\times$. $\square$

(2.6) *Remark.* Let k be a number field and $T = R_{k/\boldsymbol{Q}}(G_m)$, where R is the Weil functor (cf. [9] Chapter 1)

Let $\mathscr{C}(K/k)$ be the category of tori defined over k split by K and $\hat{\mathscr{C}}(K/k)$ be the dual category of finitely generated $\boldsymbol{Z}$-free $\mathrm{Gal}(K/k)$-modules.

We have the following commutative diagram (cf. [7]):

$$\begin{array}{ccc} \mathscr{C}(K/k) & \xrightarrow{\ \wedge\ } & \hat{\mathscr{C}}(K/k) \\ {\scriptstyle R_{k/\boldsymbol{Q}}}\downarrow & & \downarrow{\scriptstyle \mathrm{Ind}(G,\, G'\ :\ )} \\ \mathscr{C}(K/\boldsymbol{Q}) & \xrightarrow{\ \wedge\ } & \hat{\mathscr{C}}(K/\boldsymbol{Q}) \end{array}$$

where $G = \mathrm{Gal}(K/\boldsymbol{Q})$ and $G' = \mathrm{Gal}(K/k)$. So

$$\hat{T} = \widehat{R_{k/\boldsymbol{Q}(G_m)}} = \hat{G}_m \otimes_{\boldsymbol{Z}[G']} \boldsymbol{Z}[G] = \boldsymbol{Z} \otimes_{\boldsymbol{Z}[G']} \boldsymbol{Z}[G]$$

Therefore,

$$\begin{aligned} \mathrm{Hom}_G(\hat{T}, O_K^\times) &= \mathrm{Hom}_G(\boldsymbol{Z} \otimes_{\boldsymbol{Z}[G']} \boldsymbol{Z}[G], O_K^\times) \\ &= (\boldsymbol{Z} \otimes_{\boldsymbol{Z}[G']} \boldsymbol{Z}[G]) \otimes_{\boldsymbol{Z}[G]} (O_K^\times)^* \\ &= \boldsymbol{Z} \otimes_{\boldsymbol{Z}[G']} (\boldsymbol{Z}[G] \otimes_{\boldsymbol{Z}[G]} (O_K^\times)^*) \\ &= \boldsymbol{Z} \otimes_{\boldsymbol{Z}[G']} (O_K^\times) = \mathrm{Hom}_{G'}(\boldsymbol{Z}, O_K^\times) \\ &= (O_K^\times)^{G'} = O_k^\times . \end{aligned}$$

We have the following conclusion.

If $T = R_{k/\boldsymbol{Q}}(G_m)$, then $T(\boldsymbol{Z}) = O_k^\times$ the group of units of k.

Note that similar conclusion also holds true for p-adic field case.

References

[1] E. Artin, Über Einheiten relativ galoisscher Zählkörper, Crelle Journal, **167** (1932), 153–156.

[2] C. W. Curtis and I. Reiner, Methods of representation theory with application to finite groups and orders, **1**, John Wiley & Sons Inc., 1981.

[3] M. J. Herbrand, Nouvelle démonstration et généralisation d'un théoreme de Minkowski, Comptes rendus, **191** (1930), 1282–1285.

[4] ——, Sur les unités d'un corps algébrique, Comptes rendus, **192** (1931), 24–27.

[5] R. L. Long, Algebraic number theory, Marcel Dekker Inc., 1977, pp. 57–65.

[6] T. Ono, On some arithmetic properties of linear algebraic groups, Ann. of Math., **70**, no. 2 (1959), 266–290.

[7] ——, Arithmetic of algebraic tori, Ann. of Math., v. 74, no. 1 (1961), 101–119.

[8] ——, Arithmetic of algebraic groups and its applications, Lecture Notes, Rikkyo 1986.

[9] A. Weil, Adeles and algebraic groups, Birkhäuser, 1982.

Department of Mathematics
Pohang Institute of Science and Technology
P.O. Box 125 POHANG 790, KOREA