Progress in Mathematics
Vol. 23

Edited by
J. Coates and
S. Helgason

Birkhäuser
Boston · Basel · Stuttgart

A. Weil

Adeles and Algebraic Groups

1982

Birkhäuser
Boston • Basel • Stuttgart

Author:

A. Weil
The Institute for Advanced Study
Princeton, New Jersey 08540

Library of Congress Cataloging in Publication Data

Weil, André, 1906-
Adeles and algebraic groups.

(Progress in mathematics ; v. 23)
"Notes are based on lectures, given at the Institute for Advanced Study in 1959-1960"--Foreword.
Bibliography: p.
1. Forms, Quadratic. 2. Linear algebraic groups. 3. Adeles. I. Title. II. Series: Progress in mathematics (Cambridge, Mass.) ; v. 23.
QA243.W44 1982 512.9'44 82-12767
ISBN 3-7643-3092-9

CIP - Kurztitelauf der Deutschen Bibliothek

Weil, Andre:

Adeles and algebraic groups / Andre Weil. -
Boston; Basel; Stuttgart : Birkhäuser, 1982.
(Progress in mathematics; 23)
ISBN 3-7643-3092-9

NE: GT

ISBN 3-7643-3092-9

Printed in USA

FOREWORD

The present notes are based on lectures, given at the Institute for Advanced Study in 1959-1960, which, in a sense, were nothing but a commentary on various aspects of Siegel's work-chiefly his classical papers on quadratic forms, but also the later papers where the volumes of various fundamental domains are computed.

The very fruitful idea of applying the adele method to such problems comes from Tamagawa, whose work on this subject is not yet published; I was able to make use of a manuscript of his, where that idea was applied to the restatement and proof of Siegel's theorem on quadratic forms.

If the reader is able to derive some profit from these notes, he will owe it, to a large extent, to M. Demazure and T. Ono, who have greatly improved upon the oral presentation of this material as given in my lectures. At many points they have acted as collaborators rather than as note-takers. If the final product is not as pleasing to the eye as one could wish, this is not their fault; it indicates that much work remains to be done before this very promising topic reaches some degree of completion.

Princeton, January 15, 1961

A. WEIL

TABLE OF CONTENTS

CHAPTER I

PRELIMINARIES ON ADELE-GEOMETRY

1.1. Adeles.

We always denote by k a field of algebraic numbers or a field of algebraic functions of one variable over a finite constant field. We denote by k_v the completion of k with respect to a valuation v of k; if v is discrete, we use often the notation p and denote by $\underline{o}_p$ the ring of p-adic integers in k_p. We denote by S any finite set of valuations which contains all the non discrete valuations (infinite places).

By an adele, we mean an element $a = (a_v)$ of the product $\prod_v k_v$ such that $a \in A_S = \prod_{v \in S} k_v \times \prod_{p \notin S} \underline{o}_p$ for some S. The adeles of k form a ring A_k, addition and multiplication being defined componentwise. Each A_S has its natural product topology and $A_k = \bigcup_S A_S$ is topologized as the inductive limit with respect to S. There is an obvious embedding of k in A_k, by means of which we identify k with a subring of A_k; k is discrete in A_k and A_k/k is compact.

1.2. Adele-spaces attached to algebraic varieties.

Let V be an algebraic variety defined over k and let K be a field containing k. We denote by V_K the set of points of V rational over K. We know that V admits a finite covering by Zariski-open sets each of which is isomorphic to an affine variety V_i defined over k; $V = \bigcup_i f_i(V_i), f_i$ being defined over k. We have $V_K = \bigcup_i f_i(V_{i,K})$. In particular, $V_{k_v} = \bigcup_i f_i(V_{i,k_v})$ is locally compact with respect to the v-topology. We put

$$[V,f_i,V_i]_{\underline{o}_p} = \bigcup_i f_i(V_{i,\underline{o}_p}) ,$$

where $V_{i,\underline{o}_p}$ means the (compact) subset of V_{i,k_p} formed by points with coordinates in $\underline{o}_p$. Hence $[V,f_i,V_i]_{\underline{o}_p}$ is a compact subset of V_{k_p}. Now we put

$$V_S = \prod_{v\in S} V_{k_v} \times \prod_{p\notin S} [V,f_i,V_i]_{\underline{o}_p}$$

and $V_{A_k} = \bigcup_S V_S$. The union V_{A_k} with its inductive limit topology with respect to S will be called the adele-space attached to V over k. If there is no confusion, we write simply V_A instead of V_{A_k}.

Remark. If V is complete, one can prove that V_{k_v} and V_A are compact and that $[V,f_i,V_i]_{\underline{o}_p} = V_{k_p}$ for almost all p, which gives $V_A = \prod_v V_{k_v}$.

Theorem 1.2.1. Let $V = \bigcup_i f_i(V_i), W = \bigcup_j g_j(W_j)$ be varieties defined over k and let $F: V \to W$ be a morphism defined over k. Then there exists an S such that F maps $[V,f_i,V_i]_{\underline{o}_p}$ into $[W,g_j,W_j]_{\underline{o}_p}$ for all $p\notin S$.

To prove this, it is sufficient to consider the case of only one V_i, i.e. the case where V is affine. For each j, we set $F_j = g_j^{-1} \circ F: V \to W_j$; if S^{n_j} is the ambient space for W_j, F_j is represented by rational functions $R_{j\lambda}$ on $V (1 \leqslant \lambda \leqslant n_j)$. Let $\mathfrak{A}_j$ be the ideal in $k[X]$ consisting of all A such that $A(x)R_{j\lambda}(x) = Q_\lambda(x), Q_\lambda \in k[X]$, for all λ, x being a generic point of V over k. It is then clear that F_j is defined at $x_1 \in V$ if and only if x_1 is not a zero of $\mathfrak{A}_j$. Since F is everywhere defined, at least one F_j is defined at any x_1, which means that there is no common zero of $\Sigma_j \mathfrak{A}_j$, i.e.

$\Sigma_j \mathfrak{A}_j = (1)$. We write $1 = \Sigma_j A_j$, $A_j \in \mathfrak{A}_j$ and take $Q_{j\lambda} \in k[X]$ such that $A_j(x)R_{j\lambda}(x) = Q_{j\lambda}(x)$. Let S contain all p's at which some coefficients of $A_j, Q_{j\lambda}$ are not p-integral. For any $x_1 \in V_{\underline{o}_p}$, $p \notin S$, $A_j(x_1)$ is a p-unit for some $j = j_1$ and $R_{j_1\lambda}(x_1) = Q_{j_1\lambda}(x_1)/A_{j_1}(x_1)$ is in $\underline{o}_p$ for all λ; this proves the theorem.

Corollary. If F is an isomorphism: $V \cong W$, then $F([V,f_i,V_i]_{\underline{o}_p}) = [W,g_j,W_j]_{\underline{o}_p}$ for almost all p.

The definition of $[V,f_i,V_i]_{\underline{o}_p}$ is thus "almost intrinsic" and applying this Corollary to the identity map of V to itself, we see that V_{A_k} is defined independently of the choice of affine coverings. Theorem 1.2.1 also shows that F determines a continuous $F_A: V_A \to W_A$. If V is a subvariety of W, and if this is applied to the injection map, one sees that V_A can be embedded as a closed subset in W_A. V_A has the "functorial" property: if $V \overset{F}{\to} W \overset{G}{\to} U$, then $(G \circ F)_A = G_A \circ F_A$. For the product, we have $(V \times W)_A = V_A \times W_A$.

Now, we shall find a convenient criterion for the map $F_A: V_A \to W_A$ to be surjective.

Theorem 1.2.2. Let $F: V \to W$ be a morphism defined over k. If for each $P \in W$ there exists a map $\phi_P: W \to V$ defined at P, rational over k, such that $F \circ \phi_P = \text{identity}$ ("local cross-section" in the sense of algebraic geometry), then $F_A: V_A \to W_A$ is surjective.

For every P, choose ϕ_P as above; call $D(\phi_P)$ the k-open set where ϕ_P is defined; this has a covering by k-open subsets, isomorphic to affine varieties; let Ω_P be one such subset containing P. Then the Ω_P, for all P, are a k-open covering of W, over each one of which there is a global cross-section ϕ_P. By the "compactoid" property of the k-topology, we can now write $W = \bigcup_j g_j(W_j)$, with affine W_j, such that there is a global cross-section ϕ_j over each $g_j(W_j)$. Then $G_j = \phi_j \circ g_j$ is a morphism $W_j \to V$ with $F \circ G_j = g_j$. By Theorem 1.2.1, there is an S_o such that

$$G_j(W_{j,\underline{o}_p}) \subset [V,f_i,V_i]_{\underline{o}_p}$$

for all j, if $p \notin S_o$. Take an element $P = (P_v) \in W_A$ with $P_v \in g_{j(v)}(W_{j(v)})$. By definition of W_A, there is an $S \supset S_o$ such that $P_p \in g_{j(p)}(W_{j(p),\underline{o}_p})$ for $p \notin S$. Put $Q_v = \phi_{j(v)}(P_v)$. Then, if $p \notin S$, $Q_p \in G_{j(P)}(W_{j(P),\underline{o}_p}) \subset [V,f_i,V_i]_{\underline{o}_p}$. Thus $Q = (Q_v)$ is well defined, and we get $F(Q_v) = P_v$, i.e. $F_A(Q) = P$.

Remark. Theorem 1.2.2 is mostly applied to the group theoretic situation. Let $H = G/g$ be a homogeneous space with G connected, everything being defined over k. Then the condition of Theorem 1.2.2 is satisfied, and consequently we have $H_A = G_A/g_A$, if there exists one "generic section" (a map $\phi : H \to G$, defined over k, such that $p \circ \phi = 1_H$, p being the canonical map $G \to H$) and if G_k is Zariski-dense in G. The latter condition will be fulfilled by all groups in these lectures. As to the first condition, take for example G orthogonal, g a subgroup leaving one vector invariant. Then H is a sphere, and Witt's theorem guarantees the existence of a generic section.

1.3. Restriction of the basic field. Let K/k be a separable algebraic extension of degree d and let A_k, A_K be their adele rings. Every valuation w of K induces a valuation v on k (we write this as w/v) and there are at most d w's such that w/v; k_v will be identified with the closure of k in K_w; for discrete valuations P/p, we have $\underline{o}_p = k_p \cap \underline{O}_P$. The mapping $a = (a_v) \to b = (b_w)$, with $b_w = a_v$ for w/v, is an injection of A_k into A_K; we identify A_k with its image by this mapping, which is a closed subset of A_K.

Suppose K/k normal with Galois group Γ; Γ acts on K continuously under the v-topology. Since K is everywhere dense in

$\prod_{i=1}^m K_{w_i}, w_i/v$, by the approximation theorem, the operation of Γ can be extended to this product and then to A_K. Emphasizing the order with respect to K/k, we may write

$$A_K = \bigcup_S \Big(\prod_{v \in S} \big(\prod_{w/v} K_w \big) \times \prod_{p \notin S} \big(\prod_{P/p} \underline{O}_P \big) \Big)$$

where S runs over the finite sets of v's in k. It is easily seen that A_k is the set of invariant elements of A_K under Γ.

If a variety V is defined over k, it is so over K, and V_{A_k} is canonically embedded in V_{A_K}. If K is normal over k, its Galois group Γ operates in an obvious manner on V_{A_K}, and V_{A_k} is the set of invariant elements of A_K by Γ.

It will now be our purpose to find a variety W over k, for a given V over K, such that $V_{A_K} \cong W_{A_k}$ canonically. To do this we need an algebraic-geometric construction.

Let V, W be varieties defined over K, k respectively (K/k not necessarily normal). Let $p : W \to V$ be a map defined over K. Let $\Sigma = \{\sigma_1, \dots, \sigma_d\}$ be the set of all distinct isomorphisms of K into $\bar{k}$. We can then define $p^\sigma : W \to V^\sigma$, and also

$$(p^{\sigma_1}, \dots p^{\sigma_d}) : W \to V^{\sigma_1} \times \dots \times V^{\sigma_d}$$

this being the mapping $w \to (p^\sigma(w))_{\sigma \in \Sigma}$. If the latter map gives an isomorphism, we call W (actually the pair $\{W,p\}$) the variety obtained from V by the restriction of the field of definition from K to k and write $\{W,p\} = R_{K/k}(V)$, or, by abuse of language, $W = R_{K/k}(V)$.

The uniqueness is a special case of the following universal mapping property :

$$\begin{array}{ccc} X & \xrightarrow{f} & V \\ \phi \downarrow & \nearrow_{p} & \\ W & & \end{array}$$

let X be a variety defined over k and let $f : X \to V$ be defined over K. Then there is a unique $\phi : X \to W$, defined over k, such that $f = p \circ \phi$. In fact, put

$$\phi = (p^{\sigma_1}, \dots, p^{\sigma_d})^{-1} \circ (f^{\sigma_1}, \dots, f^{\sigma_d});$$

then ϕ is obviously defined over k and unique. As for the existence we first note the following :

Proposition 1.3.1. Let V, $\{W,p\}$ be as above and let V' be defined over K. If V' is either a Zariski-open subset of V or a subvariety of V, then there exists $\{W',p'\}$ for V'. If $\{W_i,p_i\}$, $i = 1,2$, exist for V_i, then $\{W_1 \times W_2, p_1 \times p_2\} = R_{K/k}(V_1 \times V_2)$.

The proof will be left to the reader.

For $V = \underline{\underline{P}}^n$ (projective space), an explicit construction is given in "the field of definition of a variety" (Am. J., 78 (1956), pp. 509-524). For an affine straight line $V = S^1$, let $K = \Sigma_{i=1}^{d} k\alpha_i$. Take $W = S^d$ and put

$$p^{\sigma}(u_1, \dots, u_d) = \sum_i \alpha_i^{\sigma} u_i = v_{\sigma}$$

Since K/k is separable, one has $\det\left(\| \alpha_i^{\sigma} \| \right) \neq 0$, i.e. $W \cong \prod V^{\sigma}$. By Proposition 1, the existence is settled for V affinely or projectively imbeddable; this covers all cases to be considered in these lectures.

If we apply the universal mapping property to the case where X is reduced to a point, we see that every point of V_K is an image of a point of W_k under the projection p; actually p induces on W_k a 1-1 correspondence of W_k with V_K.

If V has additional structures (group variety, algebra variety, etc.), then the morphism p should have the corresponding property (homomorphism, etc.); and the result W has the same structures as is easily seen. E.g. let $V = G_m$ (the 1-dimensional multiplicative group), considered as defined over K. Then W is a group of dimension $d = [K : k]$, defined over k; the multiplication is defined by that of K^* considered as a k-linear transformation on K; $W_k = K^*$ (regular representation!). We will consider later the "algebra varieties".

Let us return to general varieties. Let K/k be separably algebraic; let $\Sigma = \{\sigma_1, \dots, \sigma_d\}$ be the set of distinct isomorphisms of K into $\bar{k}$. Let k' be any extension of k. Let us consider any automorphism ω of $\bar{k}'/k'$ as acting on Σ to the right, according to the formula $\xi^{\sigma\omega} = (\xi^{\sigma})^{\omega}$, $\sigma \in \Sigma$, $\xi \in K$. Then $\sigma' = \sigma\omega (\sigma, \sigma' \in \Sigma)$ defines an equivalence relation, and this determines a partition of Σ into disjoint parts Σ_i. We choose representatives for the Σ_i, and assume that $\sigma_1 =$ identity of K.

Let V, $\{W,p\} = R_{K/k}(V)$ be as above, with respect to K/k. As Kk' is also a field of definition for V, we can form $\{W_1,p_1\} = R_{Kk'/k'}(V)$. By the universal mapping property for W_1, there is a unique map q_1, defined over k', such that $p = p_1 \circ q_1$. If we identify

$$\begin{array}{ccc} W_1 & \xrightarrow{p_1} & V \\ q_1 \uparrow & \nearrow_{p} & \\ W & & \end{array}$$

(over $\bar{k}'$) W with $\prod_{\sigma \in \Sigma} V^{\sigma}$ by the map $(p^{\sigma})_{\sigma \in \Sigma}$, W_1 with $\prod_{\sigma \in \Sigma_1} V^{\sigma}$ by the map $(p_1^{\sigma})_{\sigma \in \Sigma_1}$, then, by the unicity (over k') of q_1, we see that q_1 is identified with the projection on the partial product for Σ_1. Now, if we replace K, V by K^{σ} and V^{σ}, then W is not changed (up to a canonical isomorphism), but Σ_1 is replaced by Σ_i with $\sigma \in \Sigma_i$. we set

$$\{W_i, p_i\} = R_{K^{\sigma_i}k'/k'}(V^{\sigma_i}), \; p = p_i \circ q_i.$$

Then, by the same argument applied on q_i, we see that $(q_1, q_2, \dots)$ gives a canonical isomorphism over $k' : W \cong \prod_i W_i$.

Theorem 1.3.1. Let K/k be separable, k'/k any extension. Let $\Sigma = \{\sigma\}$ be the set of isomorphisms of K into $\bar{k}$, let σ_i be a system of representatives of Σ with respect to the equivalence relation defined by the action on Σ of automorphisms of $\bar{k}'/k'$. Let V be a variety defined over K. Then,

$$R_{K/k}(V) \cong \prod_i R_{K^{\sigma_i}k'/k'}(V^{\sigma_i})$$

Let us apply the above to V = affine straight line S^1 with its algebra structure over K; then $W = S^d$ with the structure of algebra over k; $V_K = K$, $W_k = K$, $W_{k'} = K \otimes_k k'$. Since

$$(R_{K^{\sigma_i} \cdot k'/k'}(V^{\sigma_i}))_{k'} = (V^{\sigma_i})_{K^{\sigma_i}k'} = K^{\sigma_i} \cdot k',$$

by Theorem 1.3.1, we have

$$K \otimes_k k' \cong \sum_i K^{\sigma_i} \cdot k'$$

which is well known. Let now K_i be the simple components of $K \otimes_k k'$. Then, $\sigma_i : K \otimes_k k' \to K^{\sigma_i}k'$ induces an isomorphism $\tau_i : K_i \cong K^{\sigma_i}k'$, i.e. $\tau_i(\xi \cdot 1_i \cdot \lambda) = \xi^{\sigma_i} \cdot \lambda$, $\xi \in K$, $\lambda \in k'$, 1_i being the identity of K_i. Let again V be any variety over K; τ_i^{-1} transforms V^{σ_i} to a variety defined over K_i. If we identify K, k' with their images in K_i by $\xi \to \xi \cdot 1_i, \lambda \to 1_i \cdot \lambda$, K_i can be considered as an extension of K, the image of V^{σ_i} by τ_i^{-1} is identified with V, and the image of $R_{K^{\sigma_i}k'/k'}(V^{\sigma_i})$ is identified with $R_{K_i/k'}(V) : W \cong \prod_i R_{K_i/k'}(V)$. In particular, this means that

$$W_{k'} = \prod_i [R_{K_i/k'}(V)]_{k'} = \prod_i V_{K_i}.$$

Theorem 1.3.2. Let K/k, k'/k be as in Theorem 1.3.1, and let $K \otimes_k k' = \oplus_i K_i$ (direct sum). Let V be a variety defined over K, let $W = R_{K/k}(V)$. Then $W_{k'}$ is identified canonically with $\prod_i V_{K_i}$.

Applying this to the case $k' = k_v$, $K \otimes_k k_v = \oplus_{w/v} K_w$, we get $W_{k_v} = \prod_{w/v} V_{K_w}$. Going up to adele-spaces, one gets the following

Theorem 1.3.3. Let K/k be separable, V a variety over K, $W = R_{K/k}(V)$. Then W_{A_k} can be canonically identified with $V_{A_K} : W_{A_k} = V_{A_K}$.

In what follows we give an independent proof for th. 1.3.3. and describe more explicitly the identification in it. Let K' be the Galois extension of k generated by the K^{σ}, let Γ be the Galois group of K'/k. By the map $(p^{\sigma_1}, \ldots, p^{\sigma_d})$, W is identified with $\prod V^{\sigma}$ over K', and W_{A_k} is identified with the part of $\prod_{\sigma}(V^{\sigma})_{A_{K'}}$ which is invariant by Γ, where the action of Γ on this product is defined by that of Γ on $W_{A_{K'}}$ by means of that identification. Namely, let $y \in W_{A_{K'}}$, y^{ω} its transform by $\omega \in \Gamma$, and let $x = (x_{\sigma})$, $x' = (x'_{\sigma})$ be the images of y, y^{ω} in $\prod(V^{\sigma})_{A_{K'}}$; $x_{\sigma} = p^{\sigma}(y)$, $x'_{\sigma} = p^{\sigma}(y^{\omega})$. If we transform $x_{\sigma} = p^{\sigma}(y)$ by ω, we easily see that $x_{\sigma}^{\omega} = p^{\sigma\omega}(y^{\omega}) = x'_{\sigma\omega}$, which shows that Γ acts on $\prod(V^{\sigma})_{A_{K'}}$ by $(x_{\sigma})^{\omega} = (x^{\omega}_{\sigma\omega^{-1}})$. It is easily seen that the projection of $\prod(V^{\sigma})_{A_{K'}}$ on the first factor $V_{A_{K'}}$ induces, on the set of invariant elements by Γ, a 1-1 mapping onto $V_{A_K} : W_{A_k} \rightleftharpoons V_{A_K}$.

CHAPTER II

TAMAGAWA MEASURES

2.1. Preliminaries.

2.1.1. We normalize the Haar measure dx_v of the complete field k_v in the following way :

$$k_v = \mathbb{R} \qquad dx_v = dx$$

$$k_v = \mathbb{C} \qquad dx_v = i \cdot dx \cdot d\bar{x}$$

$$k_p \qquad \int_{\mathfrak{o}_p} dx_p = 1$$

In general if G is a locally compact group with left Haar measure dx and if $\rho : G \to G$ is an automorphism of G, then $d(\rho(x))$ is also a left Haar measure. We define the module of ρ, denoted $|\rho|$, by $d(\rho(x)) = |\rho| dx$.

In the above case, for $a \in k_v^*$, $x \to ax$ is an automorphism of k_v, and the module of a, denoted $|a|_v$, is defined by $d(ax)_v = |a|_v dx_v$. We put $|0|_v = 0$. If $k_v = \mathbb{R}$ (resp. $\mathbb{C}$) then $|a|_v$ is the usual absolute value of a (resp. its square). In the p-adic case, $|a|_p = (Np)^{-v_p(a)}$.

2.1.2. The canonical measure of A_k. The idele-module.

The canonical Haar measure ω_A on A_k is defined as the measure which induces in each $\prod_{v \in S} k_v \times \prod_{p \notin S} \mathfrak{o}_p$ the (convergent) product measure $\prod_v dx_v$.

If I_k (ideles of k) denotes the group of invertible elements of A_k, then, for $a \in I_k$, $x \to ax$ is an automorphism of A_k, and the idele-module of a is defined : $d(ax) = |a| dx$. An alternative definition is $|a| = \prod_v |a_v|_v$. In particular if $a \in k^*$ is a principal idele, then $x \to ax$ induces an automorphism of the compact group A_k/k; this must preserve the Haar measure; hence, if a is a principal idele, $|a| = \prod_v |a_v|_v = 1$ (Artin-Whaples product-formula).

Theorem 2.1.1. There is on A_k a character χ such that, if we put $\chi(xy) = \chi_x(y)$, the mapping $x \to \chi_x$ is an isomorphism of A_k onto its dual group, and k is orthogonal to itself in this isomorphism.

Here, by a character, we understand a continuous homomorphism into the group $\{z \in \mathbb{C} \mid |z| = 1\}$. The last assertion means that $y \in k$ if and only if $\chi(xy) = 1$ for all $x \in k$. In the number-theoretic case, we define a character χ_o on $A_{\mathbb{Q}}$ by putting, for $x = (x_v) \in A_{\mathbb{Q}}$:

$$\chi_o(x) = \exp\left(2\pi i\left(\sum_p \langle x_p \rangle - x_\infty\right)\right)$$

where $\langle x_p \rangle$ denotes the rational number of the form $p^{-n}a$, $n \geq 0$, $0 \leq a < p^n$, such that $x_p - \langle x_p \rangle \in \mathfrak{o}_p$; for $k = \mathbb{Q}$, this has the property asserted in our theorem. For an arbitrary k, we can identify A_k with $k \otimes_{\mathbb{Q}} A_{\mathbb{Q}}$; denote by tr the trace in k over $\mathbb{Q}$, which we extend in the obvious manner to a linear mapping of A_k into $A_{\mathbb{Q}}$; then we take $\chi(x) = \chi_o(\text{tr } x)$. In the function-theoretic case, we proceed similarly, replacing $\mathbb{Q}$ by $k_o = F_q(t)$, where F_q is the field of constants in k, and t is so chosen in k that k is separably algebraic over k_o; thus it is enough to consider k_o. For a valuation v of degree n of k_o, and for $x_v \in k_{o/v}$, call $\rho_v(x_v)$ the trace of $\text{Res}(x_v dt)$, taken in F_{q^n} over the prime field. Then, for $x = (x_v) \in A_{k_o}$, we take $\chi_o(x) = \Psi(\Sigma_v \rho_v(x_v))$, where Ψ is a non-trivial character of the additive group of the prime field.

2.1.3. The constant μ_k.

Let us compute $\mu_k = \int_{A_k/k} \omega_A$, where ω_A is the measure introduced above. Denote again by S a finite non-empty set of places, containing all the places at infinity; put $A_S = \prod_{v \in S} k_v \times \prod_{p \notin S} \underline{o}_p$, and $\underline{o}(S) = A_S \cap k$; also $\underline{o}'(S)$ the projection of $\underline{o}(S)$ on the first factor $k_S = \prod_{v \in S} k_v$ of A_S. By the approximation theorem, every coset of A_S in A_k contains an element of k, so that A_k/k is isomorphic to $A_S/\underline{o}(S)$. Let M be a measurable set of representatives of $k_S/\underline{o}'(S)$ in k_S; then $M' = M \times \prod_{p \notin S} \underline{o}_p$ is a measurable set representatives of $A_S/\underline{o}(S)$ in A_S, so that we have $\mu_k = \int_{M'} \omega_A$. In view of the definition of ω_A, this gives

$$\mu_k = \int_M \prod_{v \in S} dx_v = \int_{k_S/\underline{o}'(S)} \prod_{v \in S} dx_v .$$

We now distinguish two cases :

a) k is an algebraic number-field.

Then we take for S the set of all infinite places (r_1 real, r_2 imaginary); $k_S = k \otimes_{\underline{Q}} \underline{R} = \prod_\rho k_\rho \times \prod_\iota k_\iota$ (with $k_\rho = \underline{R}$, $1 \leq \rho \leq r_1$, and $k_\iota = \underline{C}$, $r_1 + 1 \leq \iota \leq r_1 + r_2$); $\underline{o}(S)$ is the ring of integers in k; $\underline{o}'(S)$ is a lattice in the real vector-space k_S. More precisely, if (a_α), for $1 \leq \alpha \leq n = [k : \underline{Q}]$, is a basis for $\underline{o}(S)$, and if the σ_λ, for $1 \leq \lambda \leq r_1 + r_2$, are the embeddings $\sigma_\lambda : k \to k_\lambda$ of k into $\underline{C}$, the vectors $A_\alpha = (\sigma_\lambda(a_\alpha))$ are a basis for $\underline{o}'(S)$; as the set of representatives M, we can take the set of all points $\Sigma_\alpha t_\alpha A_\alpha$ in k_S with $0 \leq t_\alpha < 1$ for $1 \leq \alpha \leq n$; then we have

$$\mu_k = \int_M \prod_\rho dx_\rho \times \prod_\iota i dx_\iota d\bar{x}_\iota = i^{r_2} D \int_M dt_1 \ldots dt_n = i^{r_2} D ,$$

where D is the determinant of the matrix

$$\| \sigma_\rho(a_\alpha) \; \sigma_\iota(a_\alpha) \; \overline{\sigma_\iota(a_\alpha)} \|$$

By definition, D^2 is the discriminant Δ_k of the field k; this gives

$$\mu_k = |\Delta_k|^{\frac{1}{2}}$$

b) k is a function field over the finite field F_q.

Then we take S reduced to one place p; if d is the degree of p, we have $N(p) = q^d$; and, if π is a prime element in $\underline{o}_p$ (i.e. such that $(\pi) = \pi \underline{o}_p$ is the maximal ideal in $\underline{o}_p$), we have $\int_{(\pi)} dx_p = q^{-d}$. We have $k_S = k_p$, and $\underline{o}'(S) \cap (\pi) = \{0\}$, so that we can take for M a set consisting of cosets of (π) in k_p, and μ_k is $q^{-d} \times$ the number of such cosets. The Riemann-Roch theorem shows at once that the latter number is q^{g+d-1}, where g is the genus of k. Therefore $\mu_k = q^{g-1}$.

2.2. The case of an algebraic variety : the local measure.

2.2.1. Let V be a variety defined over k, and ω an algebraic differential form, defined over k, of degree $n = \dim V$.

Let x^o be a simple point of V and $x_1, \ldots x_n$ a system of local coordinates at x^o (not necessarily 0 at x^o). Suppose furthermore that ω is holomorphic and not zero at x^o.

In a neighborhood of x^o, ω can be expressed as

$$\omega = f(x) dx_1 \ldots dx_n$$

where $f(x)$ is a rational function defined at x^o, which can be written as a formal power-series :

$$(1) \qquad f(x) = \Sigma a_{(i)} (x_1 - x_1^o)^{i_1} \ldots (x_n - x_n^o)^{i_n}$$

Now, we take a completion k_v of k and assume the x_i^o to be in k_v;

then f is a power series with coefficients in k_v. By the implicit functions theorem, (1) converges in some neighborhood of the origin in k_v^n. If the x_i^o are in A_k, the $a_{(i)}$'s are integers for almost all p and, by a suitable linear change of coordinates, we can make them integers for all p; then for each p, (1) converges for $x_i \equiv x_i^o\ (p)$.

In any case, there is, for each v, a neighborhood U of x^o in V_{k_v} such that

(1) $\psi : x \to (x_1 - x_1^o, \dots, x_n - x_n^o)$ is a homeomorphism of U onto a neighborhood of the origin in k_v^n,

(2) the power-series expansion (1) converges in $\psi(U)$.

In $\psi(U)$ we have the positive measure $|f(x)|_v (dx_1)_v \dots (dx_n)_v$. We can pull it back to U by ψ^{-1} and we get a positive measure ω_v on U.

A priori, this measure depends on the choice of the system of local coordinates. We shall prove now that it is actually independent of this choice. In order to prove this, it is enough to change one coordinate at a time. Consider e.g. a change of the form $(x_1, x_2 \dots x_n) \to (y_1, x_2, \dots x_n)$; by Fubini's theorem we are reduced to the case $n = 1$, i.e. to proving :

$$\frac{(dy)_v}{(dx)_v} = \left|\frac{dy}{dx}\right|_v \quad .$$

This formula is well known in the classical case. In the p-adic case the proof is as follows : we can by linearity suppose $y = x + a_2 x^2 + \dots a_n x^n + \dots \quad a_i \in \mathfrak{o}_p$ Then $\left|\frac{dy}{dx}\right|_p = 1$, and one has to verify that $(dy)_p = (dx)_p$ in some neighborhood of 0. This follows from the fact that, for $x \equiv x' \equiv 0(p)$, or for $y \equiv y' \equiv 0(p)$, the relations $x \equiv x'(p^n)$, $y \equiv y'(p^n)$ are equivalent.

In this way, we have defined a measure ω_v on the open subset of V_{k_v} consisting of the simple points where ω is holomorphic and not zero.

2.2.2. From now on, V will be a non-singular variety subject to the following condition : there exists on V an algebraic differential form of degree n, everywhere holomorphic and not zero. Such a form will be called a gauge-form.

If ω and ω' are two gauge-forms on V, then $\omega' = \phi(x)\omega$, where ϕ is a rational function defined over k without poles or zeros, that is a morphism of the variety V into the multiplicative group in one variable, $G_m = GL(1)$.

Theorem 2.2.2 (Rosenlicht). Let V be a non-singular variety. The multiplicative group of morphisms $\phi : V \to G_m$ is the product of the group of non-zero constants and of a finitely generated group. If V is an algebraic group, any such ϕ such that $\phi(e) = 1$ is a character (i.e. a homomorphism $V \to G_m$).

For the first part, we remark that it is sufficient to prove it for an affine piece of V; it will then be true a fortiori for V. Hence we can suppose V affine. We take the normalized variety of the projective closure of V. It is a complete variety $\bar{V}$, without singularities in codimension one. The variety V is open in $\bar{V}$, the complement $\bar{V} - V$ having finitely many irreducible components of maximum dimension. The morphisms $\phi : V \to G_m$ are exactly the rational functions on $\bar{V}$ whose divisors have their support contained in $\bar{V} - V$. Up to a constant factor, such a function is uniquely determined by its divisor; and the divisors of such functions, being a subgroup of the group of all divisors with support contained in $\bar{V} - V$, make up a finitely generated group. This proves our first assertion.

If now V is an algebraic group, and x, y two independent generic points of V, then $\frac{\phi(xy)}{\phi(y)}$ as a function of x is a morphism of V into G_m. If $\phi_1, \dots \phi_r$ is a set of generators of the above group then $\frac{\phi(xy)}{\phi(y)} = \lambda\prod_i \phi_i(x)^{a_i}$, hence is independent of y. Taking $y = e$, we find $\frac{\phi(xy)}{\phi(y)} = \phi(x)$, which proves the second part.

Corollary. Let G be an algebraic group, and ω a translation-invariant gauge-form on G. Any gauge-form on G can then be written as $\lambda\chi(x)\omega$, where χ is a character of G and λ a non-zero constant.

We begin by recalling a few facts about abstract varieties. Let V be such a variety, given, as usual, as a finite union of isomorphic images of affine varieties, $V = \bigcup_\alpha f_\alpha(V_\alpha)$; V being defined over k, take corresponding generic points $x_\alpha = f_\alpha^{-1}(M)$ of the affine varieties V_α, where M is a generic point of V over k. We may always assume that the covering of V by the $f_\alpha(V_\alpha)$ has been taken so fine that there is, on each V_α, an everywhere valid system of local coordinates. Then, if V_α is defined in the affine space of dimension N_α by the equations $F_\mu(X_{\alpha 1},\dots,X_{\alpha N_\alpha}) = 0$, and if $x_{\alpha 1},\dots,x_{\alpha n}$ are local coordinates on V_α, we can reorder the F_μ in such a way that the determinant

$$\Delta_\alpha(X_\alpha) = \det(\partial F_\mu / \partial X_{\alpha j}) \quad (1 \leq \mu \leq N_\alpha - n, n+1 \leq j \leq N_\alpha)$$

is everywhere finite and non-zero on V_α; this means that $\Delta_\alpha(x_\alpha)$ and $\Delta_\alpha(x_\alpha)^{-1}$ can be expressed as polynomials in $x_{\alpha 1},\dots,x_{\alpha N_\alpha}$.

Let $\mathfrak{p}_{\alpha\beta}$ be the ideal in $k[X_\alpha,X_\beta]$ which defines the graph of the birational correspondence $f_{\beta\alpha} = f_\beta^{-1} \circ f_\alpha$ between V_α and V_β; let $\mathfrak{D}_{\alpha\beta}$ be the ideal of those polyonomials D in $k[X_\alpha]$ such that, for each j, $D(X_\alpha)\cdot X_{\beta j} \in k[X_\alpha] + \mathfrak{p}_{\alpha\beta}$. As the correspondence $f_{\beta\alpha}$ is biregular at every pair of points (x'_α,x'_β) of its graph, $\mathfrak{p}_{\alpha\beta}$ and $\mathfrak{D}_{\alpha\beta}$ have no common zero. By Hilbert's Nullstellensatz, we can find polynomials $D_\nu^{(\alpha,\beta)} \in \mathfrak{D}_{\alpha\beta}$ and $P_\nu^{(\alpha,\beta)} \in k[X_\beta]$ such that

$$(1) \qquad 1 - \sum_\nu D_\nu^{(\alpha,\beta)}(X_\alpha)P_\nu^{(\alpha,\beta)}(X_\beta) \in \mathfrak{p}_{\alpha\beta};$$

At the same time, by the definition of $\mathfrak{D}_{\alpha\beta}$, there are, for all ν and j, polynomials $F_{\nu j}^{(\alpha,\beta)}$ in $k[X_\alpha]$ such that

$$(2) \qquad D_\nu^{(\alpha,\beta)}(X_\alpha)X_{\beta j} - F_{\nu j}^{(\alpha,\beta)}(X_\alpha) \in \mathfrak{p}_{\alpha\beta}.$$

Let A be the set of all α's and for $B \subset A$ let $\mathfrak{p}_B \subset k[(X_\alpha), \alpha \in B]$ be the ideal of relations between the coordinates of the x_α's $(\alpha \in B)$ where the x_α are, as above, corresponding generic points of the V_α over k.

Then $\mathfrak{p}_B \cap k[(X_\alpha)_{\alpha\in B'}] = \mathfrak{p}_{B'}$, $B' \subset B$.

$\mathfrak{p}_{\{\beta,\alpha\}} = \mathfrak{p}_{\beta\alpha}$

$\mathfrak{p}_{\{\alpha\}}$ = ideal in $k[X_\alpha]$ defining V_α.

That being so, the conjunction of (1) and (2) is equivalent to

$$(3) \qquad \begin{cases} 1 - \sum_\nu D_\nu^{(\alpha,\beta)}(X_\alpha)P_\nu^{(\alpha,\beta)}(X_\beta) \in \mathfrak{p}_A & \text{for all } \alpha,\beta \\ D_\nu^{(\alpha,\beta)}(X_\alpha)X_{\beta j} - F_{\nu,j}^{(\alpha,\beta)}(X_\alpha) \in \mathfrak{p}_A & \text{for all } \alpha,\beta,\nu,j \end{cases},$$

where $\mathfrak{p}_A$ is the absolutely prime ideal of $k[(X_\alpha), \alpha\in A]$ defining the locus of $(x_\alpha)_{\alpha\in A}$ over k.

Conversely, whenever an absolutely prime ideal $\mathfrak{p}_A$ is given in $k[(X_\alpha), \alpha\in A]$ such that there exist polynomials D,F,P satisfying the above relations, this defines an abstract variety defined over k.

Let there be given, now, a gauge-form ω on V; on V_α, ω can be written $\omega = \phi_\alpha(x_\alpha)dx_{\alpha 1}\dots dx_{\alpha n}$, where $\phi_\alpha(x_\alpha)$ and $\phi_\alpha(x_\alpha)^{-1}$ are everywhere defined rational functions, hence polynomials.

We recall the definition of reduction of an ideal modulo p. Let $\mathfrak{p}$ be an absolutely prime ideal in $k[Y], Y = (Y_1,\dots,Y_n)$. Let us take a finite set of generators $P_\mu(Y)$ of $\mathfrak{p}$. For a finite place p where all the coefficients of the P_μ's are integral, the reduction $\bar{P}_\mu^{(p)}$ of P_μ modulo p is defined and we define $\bar{\mathfrak{p}}^{(p)}$ as the ideal generated by the $\bar{P}_\mu^{(p)}$ in $(\underline{o}_p/p)[Y]$. If we take another set of generators, then for almost all p, the reduction $\bar{\mathfrak{p}}^{(p)}$ will be the same as above ($\bar{\mathfrak{p}}^{(p)}$ is "almost intrinsic"). A well known theorem of E. Noether (Math. Annalen 1923) asserts :

Theorem 2.2.2. For almost all p, $\bar{\mathfrak{p}}^{(p)}$ is absolutely prime.

Let now S be a finite set of primes such that for all p not in S :-

(I) all the $\bar{\mathfrak{p}}_B^{(p)}$ $(B \subset A)$ are absolutely prime

(II) all the polynomials $D_\nu^{(\alpha,\beta)}$, $P_\nu^{(\alpha,\beta)}$, $F_{\nu,j}^{(\alpha,\beta)}$, $\Delta_\alpha, \Delta_\alpha^{-1}, \phi_\alpha, \phi_\alpha^{-1}$ have integral coefficients.

Then for all p not in S we shall define a non-singular variety $\bar{V}^{(p)}$ defined over the field $\underline{o}_p/p = F_q$ (finite field with $q = Np$ elements) called the reduction of V modulo p.

Let $\bar{V}_\alpha^{(p)}$ be the variety defined by $\bar{\mathfrak{p}}_\alpha^{(p)} \in F_q[X_\alpha]$. Let $\bar{f}_{\beta\alpha}^{(p)}$ be the birational correspondence between $\bar{V}_\alpha^{(p)}$ and $\bar{V}_\beta^{(p)}$ defined by $\bar{\mathfrak{p}}_{\{\alpha,\beta\}}^{(p)}$. By the hypothesis (II), the polynomials D,P,F can be reduced modulo p, and the equations (1), (2), (3) remain true. Hence we can glue together the varieties $\bar{V}_\alpha^{(p)}$ by the correspondences $\bar{f}_{\beta\alpha}^{(p)}$, and find an abstract variety $\bar{V}^{(p)}$ defined over F_q.

Moreover the Δ_α are p-adic units and the n first coordinates are uniformizing parameters on $\bar{V}_\alpha^{(p)}$ which is therefore non-singular.

2.2.3. We want now to interpret the rational points of $\bar{V}^{(p)}$ over F_q. We have already defined $[V; f_\alpha, V_\alpha]_{\underline{o}_p} = \bigcup_\alpha f_\alpha(V_{\alpha/\underline{o}_p})$; we denote it here by $V_{\underline{o}_p}$ (though it is only "almost intrinsic"), and we introduce an equivalence relation on $V_{\underline{o}_p}$. Let μ be a fixed integer > 0.

We say that $a \equiv a'(p^\mu)$ $a, a' \in V_{\underline{o}_p}$ if one can find an $\alpha \in A$ such that $a = f_\alpha(a_\alpha), a' = f_\alpha(a'_\alpha)$, $a_\alpha, a'_\alpha \in V_{\alpha/\underline{o}_p}$, $a_\alpha \equiv a'_\alpha(p^\mu)$.

To justify this definition we have to prove

Lemma 2.2.1. If $a = f_\alpha(a_\alpha) = f_\beta(a_\beta)$, $a_\alpha \in V_{\alpha/\underline{o}_p}$, $a_\beta \in V_{\beta/\underline{o}_p}$, and if $a' = f_\alpha(a'_\alpha)$ with $a'_\alpha \equiv a_\alpha(p^\mu)$ then one can find $a'_\beta \in V_{\beta/\underline{o}_p}$ such that $a' = f_\beta(a'_\beta)$ and $a'_\beta \equiv a_\beta(p^\mu)$.

As (a_α, a_β) is in the graph of $f_{\beta,\alpha}$, we have

$$1 = \Sigma\, D_\nu^{(\alpha,\beta)}(a_\alpha) P_\nu^{(\alpha,\beta)}(a_\beta).$$

In view of (II), at least one of the $D_\nu^{(\alpha,\beta)}(a_\alpha)$ must be a p-adic unit; then, by (2), we have, for this value of ν :

$$a_{\beta,j} = \frac{F_{\nu,j}^{(\alpha,\beta)}(a_\alpha)}{D_\nu^{(\alpha,\beta)}(a_\alpha)} .$$

But, if we replace a_α by a'_α and define $a'_{\beta,j} = \dfrac{F_{\nu,j}^{(\alpha,\beta)}(a'_\alpha)}{D_\nu^{(\alpha,\beta)}(a'_\alpha)}$, then $D_\nu^{(\alpha,\beta)}(a'_\alpha)$ is still a p-adic unit, $a'_\beta \equiv a_\beta(p^\mu)$ and a'_β is in $V_{\beta/\underline{o}_p}$.

We are now ready to prove :

Theorem 2.2.3. The reduction modulo p gives a one-to-one-correspondence between the equivalence classes modulo p of $V_{\underline{o}_p}$ and the rational points of $\bar{V}^{(p)}$ over F_q.

Two equivalent points lie on the same affine V_α by definition, hence it is sufficient to prove the theorem for an affine V. In this case, V is given by an absolutely prime ideal $\mathfrak{p}$. Obviously a zero of $\mathfrak{p}$ in $(\underline{o}_p)^N$ reduces modulo p to a zero of $\bar{\mathfrak{p}}^{(p)}$. The equivalent points modulo p reduce to the same zero. It remains only to prove the following generalization of Hensel's lemma :

Lemma 2.2.4. *Let* k_p *be a* p*-adic field and* V *an affine variety of dimension* n *defined over* k_p *by an ideal* $\mathfrak{p} \in k_p[X_1, \ldots X_N]$. *Let* $\bar{a}$ *be a zero in* $F_q^N (q = N(p))$ *of the reduction* $\bar{\mathfrak{p}}^{(p)}$. *Suppose that there exists* $F_1, \ldots F_{N-n}$ *in* $\mathfrak{p} \cap \underline{o}_p|X|$ *such that the matrix* $\|\partial \bar{F}_\mu / \partial \bar{a}_\nu\|$ *is of rank* $N - n$. *Then there exists a zero* a *of* $\mathfrak{p}$ *in* $(\underline{o}_p)^N$ *reducing modulo* p *to* $\bar{a}$.

(It is not necessary, for the lemma to be valid, that $\bar{\mathfrak{p}}^{(p)}$ should be an absolutely prime ideal). For a proof, see P. Samuel, Int. Congress Amsterdam 1954, vol. 2, p. 63.

Let us now compute

$$\int_{V_{\underline{o}_p}} \omega_p \quad .$$

We decompose $V_{\underline{o}_p}$ into equivalence classes :

$$\int_{V_{\underline{o}_p}} \omega_p = \sum_{\bar{a} \in \bar{V}^{(p)}} \int_{x \equiv a(p)} \omega_p$$

But $\{x | x \equiv a(p)\}$ is by definition in the image of one affine V_α; on V_α, ω can be written as $\phi_\alpha(x) dx_{\alpha 1} \ldots dx_{\alpha n}$. But ϕ_α is a p-adic unit; therefore, for a in $V_{\alpha/\underline{o}_p}$:

$$\int_{x \equiv a(p)} \omega_p = \int_{x \equiv a(p)} dx_{\alpha 1} \ldots dx_{\alpha n} \quad .$$

The projection of V_α on the space $(x_{\alpha 1}, \ldots x_{\alpha n})$ is an isomorphism on the subset $x \equiv a(p)$; therefore

$$\int_{x \equiv a(p)} dx_{\alpha 1} \ldots dx_{\alpha n} = q^{-n}$$

This completes the proof of

Theorem 2.2.5. *If* V *is non-singular and* ω *is a gauge-form on* V, *then, for almost all* p, V *reduces modulo* p *to a non-singular variety which has* $q^n \int_{V_{\underline{o}_p}} \omega_p$ *rational points over* F_q, *where* $q = N(p)$.

2.3. The global measure and the convergence factors

A set (λ_v) of strictly positive real numbers indexed by the valuations v of k is called a *set of factors* for k. Let V be a non-singular variety, defined over k, and ω a gauge-form on V, rational over k. For each place v of k, we have defined the positive measure ω_v on V_{k_v}. For every p, we put $\mu_p(V) = \int_{V_{\underline{o}_p}} \omega_p$.

Definition. *A set of factors* (λ_v) *is called a set of convergence factors for* V *if the product* $\prod_p (\lambda_p^{-1} \mu_p)$ *is absolutely convergent.*

This definition is valid because

(1) $V_{\underline{o}_p}$ is almost intrinsic

(2) If ω' is another form, $\int_{V_{\underline{o}_p}} \omega_p = \int_{V_{\underline{o}_p}} \omega'_p$ for almost all p.

(This follows from Theorem 2.2.5. Alternative proof : $\omega' = f\omega$ where f is a morphism of V into G_m. For almost all p, $f(V_{\underline{o}_p}) \subset (G_m)_{\underline{o}_p} = U_p$ and $|f|_p = 1$).

Definition. *If* (λ_v) *is a set of convergence factors for* V, *the Tamagawa measure* $\Omega = (\omega, (\lambda_v))$ *on* V_{A_k} *derived from* ω *by means of* (λ_v) *is defined as the measure on* V_{A_k} *inducing in each product* $\prod_{v \in S} V_{k_v} \times \prod_{p \notin S} V_{\underline{o}_p}$ *the product measure* $\mu_k^{-\dim V} \prod_v (\lambda_v^{-1} \omega_v)$ (μ_k is the constant introduced in 2.1.3).

Theorem 2.3.1. *If* $c \in k^*$, $(\omega, (\lambda_v)) = (c\omega, (\lambda_v))$.

In fact, $(c\omega)_v = |c|_v \omega_v$ and $\prod_v |c|_v = 1$.

Let now K/k be a finite and separable algebraic extension. Let V be a variety defined over K and $(W,p) = R_{K/k}(V)$ (1.3). If ω is a differential form on V defined over K, we define the differential form $p^*(\omega)$ on W as follows. Let θ be such that $K = k(\theta)$. Let (σ_i) be the isomorphisms of K into $\bar{k}$ and let $\sqrt{\Delta} = \prod_{i<j}(\theta^{\sigma_i} - \theta^{\sigma_j})$. Then we define $p^*(\omega) = (\sqrt{\Delta})^{\dim V} \bigwedge_\sigma (p^\sigma)^* \omega^\sigma$. We see easily that $p^*(\omega)$ is defined over k. Then one has

Theorem 2.3.2. *Let K/k be finite and separable and $(W,p) = R_{K/k}(V)$. Let (λ_w) be a set of factors for K and $\mu_v = \prod_{w/v} \lambda_w$. Then*

(1) *(μ_v) is a set of convergence factors for W if and only if (λ_w) is a set of convergence factors for V.*

(2) *If (1) is satisfied, $(\omega,(\lambda_w))$ corresponds to $(p^*(\omega),(\mu_v))$ in the canonical isomorphism $V_{A_K} \cong W_{A_k}$* (Theorem 1.3.3).

This follows at once from Theorems 1.3.2 and 1.3.3 and from the definition of W.

This theorem gives the reason for the introduction of the factor μ_k in the definition of the Tamagawa measures.

2.4. Algebraic groups and Tamagawa numbers

By an algebraic group, we shall always mean in this course an algebraic group isomorphic to a subgroup of a linear group.

If G is an algebraic group defined over k, the product morphism $G \times G \to G$ induces a group law on G_{A_k} which makes G_{A_k} a topological locally compact group : the *adele-group* of G.

If ω is a gauge-form on G, ivariant by left-translations on G and if (λ_v) is a set of convergence factor for G, then the Tamagawa measure $\Omega = (\omega,(\lambda_v))$ is a *left Haar measure* on G_{A_k}. This measure is independent of the choice of ω (Theorem 2.3.1) and will be called *the Tamagawa measure for* G *derived from the convergence factors* (λ_v). If (1) is a set of convergence factors, then $(\omega,(1))$ will be called *the Tamagawa measure for* G.

The group G_k is a discrete subgroup of G_{A_k} and we consider the left homogeneous space G_{A_k}/G_k. We shall be interested in the following questions :

(I) *Is* G_{A_k}/G_k *compact* ?

(II) *Is* G_{A_k}/G_k *of finite measure for any left Haar measure on* G_{A_k} ?

(III) *If* G *is unimodular, if* (II) *is true, and if* (1) *a set of convergence factors for* G, *then what is the number*

$\tau(G) = \int_{G_{A_k}/G_k} (\omega,(1))$?

Under the assumptions in (III), $\tau(G)$ will be called the *Tamagawa number of* G.

For instance, if $G = G_a^n$ (additive group in n variables), then (I) is true (a fortiori (II)), and, by definition of μ_k, $\tau(G) = 1$.

If G is an algebraic group and ω a left-invariant algebraic gauge-form, $\omega(xs)$ is also left-invariant for all $s \in G$, hence must be of the form $\omega(xs) = \Delta(s)\omega(x)$ where Δ is a character of G, called the *module* of G. As in the topological case, $\omega(x^{-1}) = \Delta(x^{-1})\omega(x)$. If $\Delta = 1$, G is said to be *unimodular* (example : all reductive groups).

If G is defined over k, then we may take ω defined over k; therefore the module Δ also is defined over k and extends to a homomorphism $\Delta_{A_k} : G_{A_k} \to I_k = (G_m)_{A_k}$. Then $|\Delta_{A_k}|$ where $| \, |$ denotes the idele-module is a homomorphism of G_{A_k} into R_+^* which coincides obviously with the (topological) module of G_{A_k}. Hence, if G *is unimodular*, G_{A_k} *is unimodular*.

Let now $H = G/g$ be an algebraic homogeneous space of G. A gauge-form ω on H is called a relatively invariant form belonging to the character χ of G if

$$\omega(s\cdot P) = \chi(s)\cdot\omega(P) \qquad s\in G,\ P\in H$$

We have, as in the topological case, the theorem :

Theorem 2.4.1. Denote by Δ and δ the modules of G and g. There exists a relatively invariant form on G/g belonging to the character χ of G, if and only if the character $\delta(\sigma)\Delta(\sigma^{-1})$ of g coincides with χ on g.

Corollary. If G and g are unimodular, there exists on G/g a gauge-form invariant by G.

Let dx, $d\sigma$, dP be respectively a left-invariant gauge-form on G, a left-invariant gauge-form on g, and a relatively invariant gauge-form on G/g belonging to the character χ of G; let ϕ be the canonical mapping of G onto G/g, and put $P = \phi(x) = xg$ for $x\in G$. Then $\phi^*(dP)$ is a differential form on G. Put $\alpha(x) = \phi^*(dP)$, and let $\beta(x)$ be any differential form on G such that, for every $s\in G$, $\beta(s\sigma) = d\sigma$ for $\sigma\in g$, i.e. such that $\beta(sx)$ induces on g the form $d\sigma$. It is easily seen that the form $\alpha(x)\wedge\beta(x)$ on G is a gauge-form which does not depend upon the choice of β; this will be denoted symbolically by $dP\cdot d\sigma$. We have $dP\cdot d\sigma = \lambda\chi(x)dx$, where λ is a constant. If $\lambda = 1$, we say that dx, $d\sigma$, dP match together algebraicallay.

Let G' be a locally compact group, g' a closed subgroup; if dx', $d\sigma'$, dP' are respectively a Haar measure on G', a Haar measure on g', and a relatively invariant measure on G'/g' belonging to the character χ' of G', we will say that dx', $d\sigma'$, dP' match together topologically if the integral formula

$$\int_{G'/g'} dP' \int_{g'} f(x'\sigma')d\sigma' = \int_{G'} f(x')\chi'(x')dx'$$

holds for every f in $L^1(G',dx')$; in this formula, P' means the image $x'g'$ of x' in G'/g'. This formula will be abbreviated symbolically by $dP'\cdot d\sigma' = \chi'(x')dx'$.

Theorem 2.4.2. Let G and $g\subset G$ be algebraic groups defined over k. Suppose that the map $G\to G/g = H$ admits local cross-sections (in the sense of Theorem 1.2.2), and that the density condition of Theorem 1.2.2 is fulfilled. Then $G_A/g_A = H_A$.

Straightforward application of Theorem 1.2.2. We note that the density condition of Theorem 1.2.2 is automatically verified if k is a number-field (Rosenlicht). For the function fields it is easily verified in each of the particular cases treated in Chapters III and IV.

Theorem 2.4.3. Let G, g be as in Theorem 2.4.2. Let dx, $d\sigma$, dP be gauge-forms defined over k on $G,g,G/g$, matching together algebraically. Let (λ_v), (μ_v), (ν_v) be three sets of factors for k with $\lambda_v = \mu_v\cdot\nu_v$. Then :

(1) If two of three sets (λ_v), (μ_v), (ν_v) are sets of convergence factors (for G, g, G/g respectively), so is the third one.

(2) If (1) is satisfied, denoting $d_Ax = (dx, (\lambda_v))$, $d_A\sigma = (d\sigma,(\mu_v))$, $d_AP = (dP, (\nu_v))$, then d_Ax, $d_A\sigma$, d_AP match together topologically. Moreover if $dP\cdot d\sigma = \chi(x)dx$, then $d_AP\cdot d_A\sigma = |\chi_A(x)|d_Ax$ where $|\ |$ is the idele-module and $\chi_A : G_A\to I_k$ the adele extension of $\chi : G\to G_m$.

The proof is straightforward and is left to the reader.

Lemma 2.4.1. Let G be a locally compact unimodular group, g a unimodular subgroup of G, γ a discrete subgroup of g. Let d_Gx, d_gu, $d_{G/g}x$ be Haar measures of G, g, G/g such that $d_Gx = d_{G/g}x\cdot d_gu$. Let $d_{g/\gamma}u$ and $d_{G/\gamma}x$ be the measures induced by d_gu and d_Gx in the local isomorphism $g\to g/\gamma$, $G\to G/\gamma$. Then we have $d_{G/\gamma}x = d_{G/g}x\cdot d_{g/\gamma}u$ in the sense that

(1) $$\int_{G/\gamma} f(x)d_{G/\gamma}x = \int_{G/g} d_{G/g}x \int_{g/\gamma} f(xu)d_{g/\gamma}u \quad \text{for} \quad f \in L^1(G/\gamma).$$

Slight modification of Fubini's theorem.

Lemma 2.4.2. Let furthermore Γ be a discrete subgroup such that $G \supset \Gamma \supset \gamma$ and let $d_{G/\Gamma}x$ be the Haar measure on G/Γ locally isomorphic to $d_G x$. Let $\mu_g = \int_{g/\gamma} d_{g/\gamma}u \leq +\infty$. Then for $f \in L^+(G/g)$ (positive integrable continuous functions), we have :

(2) $$\mu_g \cdot \int_{G/g} f(x)d_{G/g}x = \int_{G/\Gamma} \Big[\sum_{\xi \in \Gamma/\gamma} f(x\xi)\Big] d_{G/\Gamma}x$$

where the two sides of (2) are both infinite or both finite and equal (as usual $\infty \cdot 0 = 0$).

From (1) $\int_{G/\gamma} f(x)d_{G/\gamma}x = \int_{G/g} d_{G/g}x \int_{g/\gamma} f(xu)d_{g/\gamma}u = \mu_g \cdot \int_{G/g} f(x) \cdot d_{G/g}x$; on the other hand :

$$\int_{G/\gamma} f(x)d_{G/\gamma}x = \int_{G/\Gamma} d_{G/\Gamma}x \Big[\sum_{\xi \in \Gamma/\gamma} f(x\xi)\Big] d_{G/\gamma}x.$$

Lemma 2.4.3. With the same notations, suppose g normal and $\Gamma \cap g = \gamma$. Put $H = G/g$, $\Gamma_H = \Gamma g/g \approx \Gamma/\gamma$. Assume furthermore that $d_G x = d_H y \cdot d_g u$, where $y \in H$ is the image of $x \in G$ by the canonical map $p : G \to H$. Then for $f \in L^+(H/\Gamma_H)$,

(3) $$\mu_g \cdot \int_{H/\Gamma_H} f(y)d_{H/\Gamma_H}y = \int_{G/\Gamma} f(p(x))d_{G/\Gamma}x.$$

In particular, if $\mu_H = \int_{H/\Gamma_H} d_{H/\Gamma_H}y$, $\mu_G = \int_{G/\Gamma} d_{G/\Gamma}x$, then : if two of the three numbers μ_g, μ_H, μ_G are finite, so is the third one, and $\mu_g \cdot \mu_H = \mu_G$.

By assumption we have $d_H y = d_{G/g}y$. Then by formula (2),

$$\mu_g \cdot \int_H h(y)d_H y = \int_{G/\Gamma} \sum_{\xi \in \Gamma/\gamma} h(p(x\xi))d_{G/\Gamma}x$$

$$= \int_{G/\Gamma} \sum_{\xi \in \Gamma_H} h(p(x)\cdot\xi)d_{G/\Gamma}x, \text{ for } h \in L^+(H, d_H y) .$$

But by Fubini,

$$\int_H h(y)d_H y = \int_{H/\Gamma_H} d_{H/\Gamma_H}y \sum_{\xi \in \Gamma_H} h(y\cdot\xi).$$

If we put $f(y) = \sum_{\xi \in \Gamma_H} h(y\xi)$, then we have :

$$\mu_g \int_{H/\Gamma_H} f(y)d_{H/\Gamma_H}y = \int_{G/\Gamma} f(p(x))d_{G/\Gamma}x \quad .$$

But there are "sufficiently many" functions $\sum_{\xi \in \Gamma_H} h(y\xi)$ in $L^+(H/\Gamma_H)$. This proves (3). Putting $f = 1$ in (3), we get the second part.

Theorem 2.4.4. Let G and $g \subset G$ be unimodular algebraic groups defined over k; assume that g is normal; call ϕ the canonical mapping of G onto $H = G/g$. Put $H'_A = \phi_A(G_A)$, $H'_k = \phi(G_k)$; assume that H'_A is an open subgroup of H_A; also assume that (1) is a set of convergence factors for g. Then every set (λ_v) of convergence factors for G is such a set for H; and, if $d_A x$, $d_A y$ are the corresponding Tamagawa measures for G_A, H_A, we have, for $f \in L^+(H'_A/H'_k)$:

(4) $$\tau(g) \int_{H'_A/H'_k} f(y)d_A y = \int_{G_A/G_k} f(\phi(x))d_A x.$$

($\tau(g)$ = Tamagawa number of g, if it is defined; otherwise $+\infty$).

As the kernel of the mapping ϕ_A of G_A onto H'_A is g_A, we can identify H'_A with G_A/g_A. As H'_A is open in H_A, the image of G_{k_v} by ϕ is open in H_{k_v} for every v, and the image of $G_{\underline{o}_p}$ by ϕ is $H_{\underline{o}_p}$ for almost all p. Let dx, dy, du be gauge-forms for G, H and g, matching together algebraically. By the theory of analytic groups over complete valued fields, there are, locally, analytic cross-sections for g_{k_v} in G_{k_v} for each v; this is enough to guarantee (just as in Theorem 2.4.3) that $(dx)_v$, $(dy)_v$, $(du)_v$ match together topologically for every v, with the same conclusion as in Theorem 2.4.3 about sets of convergence factors; in particular, if (1) is such a set for g, the sets of convergence factors for G and H are the same. Then $d_A x$, $d_A y$ and the Tamagawa measure for g match together topologically on G_A, H'_A and g_A; (4) follows now from Lemma 2.4.3.

Corollary. *If at the same time G and g satisfy the conditions of Theorem* 2.4.2 (existence of a cross-section and the density condition), *then* (4) *holds with* $H'_A = H_A$, $H'_k = H_k$; *and, if* (1) *is a set of convergence factors for* G (*or for* H), $\tau(G) = \tau(g)\tau(H)$.

Remark 1. If, instead of assuming that (1) is a set of convergence factors for g, we merely denote by (λ_v), (μ_v), (ν_v) sets of convergence factors for G, g and H satisfying $\lambda_v = \mu_v \nu_v$ for all v (as we may by Theorem 2.4.3), then the proof of Theorem 2.4.4 remains valid and shows that (4) holds when we take for $d_A x$, $d_A y$ the Tamagawa measures for G_A and H_A corresponding to the sets (λ_v), (ν_v), provided we replace $\tau(g)$ by the "modified Tamagawa number"

$$\tau'(g) = \int_{g_A/g_k} d_A u$$

where $d_A u$ is the Tamagawa measure for g_A corresponding to the set (μ_v).

Remark 2. In the proofs of Theorems 2.4.2 (identification of H_A with G_A/g_A) and 2.4.4 (identification of H'_A with G_A/g_A), we have made implicit use of the fact that, whenever a group such as G_A acts on a locally compact space, then the mapping of G_A onto any locally

closed orbit in that space is open, so that the orbit can be identified with the quotient of G_A by the stability group of any one of its points. This is a special case of a known theorem (cf. Montgomery-Zippin, Top. Transf.-Groups, p. 65), proved by an elementary category argument. The same theorem will be used occasionally, sometimes without reference, in the next chapters.

CHAPTER III

THE LINEAR, PROJECTIVE AND SYMPLECTIC GROUPS

3.1. The zeta-function of a central division algebra

As formerly, whenever V is a variety, defined over a field k, we denote by V_k the set of points of V, rational over k; a vector-space of dimension d over k can always be denoted by R_k, where R is an affine space of dimension d in the sense of algebraic geometry. In particular, any algebra over k can be so written; the obvious extension to R of the multiplication-law on the algebra R_k makes R into an algebra-variety, defined over k (which means that the multiplication-law on R is defined over k). The given algebra R_k over k is absolutely semisimple if and only if R is so, i.e. if and only if R is isomorphic (over the universal domain) to a direct sum of matrix algebras.

Let D_k be a central division algebra of dimension n^2 over k. This algebra defines an algebra-variety D of center $Z(Z_k = k)$. Over $\bar{k}$, D is isomorphic to $M_n(\Omega)$ (total matrix algebra over the universal domain Ω).

The reduced norm is a multiplicative mapping $N : D \to Z$; it is a homogeneous polynomial function of degree n.

Let $D^{(1)}$ be the subvariety of dimension $n^2 - 1$ defined in D by the equation $N(x) = 1$. This is an algebraic group defined over k, the special linear group of D.

In the projective space $\underline{P}(D)$ derived from D considered as an affine space, the multiplication on D induces on the Zariski-open subset defined by the homogeneous relation $N(x) \neq 0$, a structure of algebraic group defined over k, the projective group of D. We can describe it alternatively in this manner : denote by D^* the multiplicative (algebraic) group of the elements of D with non-zero norm. Then $G = D^*/Z^*$ is isomorphic to the projective group of D. Furthermore, the restriction to $D^{(1)}$ of the canonical mapping $D^* \to G$ identifies $D^{(1)}/$(center of $D^{(1)}$) with G.

Let α_i, $1 \le i \le n^2$, be a basis of D_k over k, and let $x = \Sigma_i \alpha_i x_i$ be a generic point of D. The set $D_{\underline{o}_p} = \Sigma_i \alpha_i \underline{o}_p$ forms a ring for almost every p. Furtermore if p does not divide the discriminant of D then $D_{\underline{o}_p}$ is a maximal order of D_{k_p}, and one has $D_{k_p} = M_n(k_p)$. Since every maximal order of $M_n(k_p)$ is conjugate to $M_n(\underline{o}_p)$, there is a ring isomorphism $D_{\underline{o}_p} \cong M_n(\underline{o}_p)$ if $p \notin S$, S being suitably chosen.

As an invariant measure on D^*, we can take

$$\omega = N(x)^{-n}\, dx_1 \ldots dx_{n^2}$$

and if $p \notin S$, we have

$$\mu_p = \int_{D^*_{\underline{o}_p}} \omega_p = \int_{GL_n(\underline{o}_p)} |\det X|_p^{-n} (dX)_p = \int_{GL_n(\underline{o}_p)} (dX)_p$$

$$= q^{-n^2}(q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) = (1 - q^{-n})(1 - q^{-(n-1)})\ldots(1 - q^{-1})$$

$$X = (x_{ij}),\ dX = \prod_{i,j} dx_{ij},\ q = N(p)\ .$$

From this formula follows that the $\lambda_p = 1 - N(p)^{-1}$ are a set of convergence factors for D^*. The Tamagawa measure $(\omega, (\lambda_p))$ will be called ω'_A :

$$\omega'_A = \mu_k^{-n^2} \prod_{\lambda \text{ infinite}} \omega_\lambda \prod_p \omega'_p, \text{ where } \omega'_p = (1-N(p)^{-1})^{-1}\omega_p .$$

The mapping $N : D^* \to Z^* \cong G_m$ can be extended to $N : D_A^* \to (G_m)_A = I_k$. We denote by $|\ |$ the idele-module (2.1.1).

We take on D_A the Tamagawa measure $dx_A = dx_S \times \prod_{p\notin S} dx_p$, where $dx_S = \mu_K^{-n^2} \prod_{v\in S} dx_v$. Then $\int_{D_A/D_k} dx_A = 1$.

Lemma 3.1.1 (Fujisaki). *If $0 < m \leq M$, the image in D_A^*/D_k^* of the subset of D_A^* determined by $m \leq |N(x)| \leq M$ is compact.*

Let X be that subset. Take a compact subset C of D_A whose measure (for the measure dx_A) is $> M^n$ and $> m^{-n}$; put $C' = C + (-C) = \{c_1 - c_2 | c_1, c_2 \in C\}$. If $a \in D^*_A$, $x \to ax$ and $x \to xa$ are automorphisms of D_A whose module is $|N(a)|^n$ (idele-module of the regular norm $N(a)^n$); therefore, if $a \in X$, the images $a^{-1}C$, Ca of C under the automorphisms $x \to a^{-1}x$, $x \to xa$ of D_A have a measure > 1 and are not mapped in a one-to-one manner onto their images in D_A/D_k by the canonical homorphism of D_A onto D_A/D_k, since the measure of D_A/D_k is 1. This is the same as to say that $a^{-1}C' \cap D_k^*$ and $C'a \cap D_k^*$ are not empty, i.e. that there are $\alpha, \beta \in D_k^*$ such that $c' = a\alpha \in C'$, $c'' = \beta a^{-1} \in C'$. Then $c''c' = \beta\alpha$ is in $C'^2 \cap D_k^*$, which is a finite set $\{\xi_1, \ldots, \xi_h\}$ since D_k is discrete in D_A and C'^2 is compact. Assume that $\beta\alpha = \xi_i$; as $c' = a\alpha$, this gives $c'^{-1} = \xi_i^{-1}c''$. As D^* can be identified with its image in $D \times D$ under the mapping $x \to (x, x^{-1})$ (since that image is closed in $D \times D$), D_A^* can be identified with its image in $D_A \times D_A$ under the corresponding adele-mapping; so the set Y_i of the points $x \in D_A^*$ such that $(x, x^{-1}) \in C' \times (\xi_i^{-1}C')$ is compact. We have thus proved that, whenever $a \in X$, there is $\alpha \in D_k^*$ such that $a\alpha$ is in the union of the compact sets Y_i. This proves the lemma.

Remark. Lemma 3.1.1 shows that Problem (I) of 2.4 ("is G_A/G_k compact?") has an affirmative answer for the group $D^{(1)}$.

Lemma 3.1.2. *There is a constant $c > 0$ such that, in the number-field case*

$$\int_{D_A^*/D_k^*} F(|N(x)|)\omega'_A = c \int_0^{+\infty} F(t)dt/t ,$$

resp., in the function-field case

$$\int_{D_A^*/D_k^*} F(|N(x)|)\omega'_A = c \sum_{\nu=-\infty}^{+\infty} F(q^\nu) ,$$

whenever F is a function on $\underline{\underline{R}}_+$ (resp. on the group $\{q^\nu | \nu \in \underline{\underline{Z}}\}$) such that the integral (resp. the sum) in the right-hand side converges absolutely. (N.B. In the function-field case, q denotes the number of elements of the field of constants of k).

Let first F be a continuous function with compact support on the multiplicative group $\underline{\underline{R}}_+$ (resp. on the group $\{q^\nu\}$); then lemma 3.1.1 shows that $F(|N(x)|)$ has compact support in D_A^*/D_k^*, so that the integral in the left-hand side is convergent. For any $t_o \in \underline{\underline{R}}_+$ (resp. for any $t_o = q^\nu$) there is $x_o \in D_A^*$ such that $|N(x_o)| = t_o$; replacing then, in the left-hand side, x by $x_o x$, we see that it does not change if $F(t)$ is replaced by $F(t_o t)$; in other words, as a function of F, it is translation-invariant in the group $\underline{\underline{R}}_+$ (resp. $\{q^\nu\}$). This proves the lemma, for F continuous with compact support; the general case follows from this in the usual manner. (For the value of c, cf. Theorem 3.1.1.)

Now denote by Tr the reduced trace in D_k over k, which we extend in the usual manner to a linear function on D, and also to a linear mapping of $D_A = D_k \otimes_k A_k$ into A_k; $Tr(xy)$ is then a non-degenerate bilinear form on $D \times D$. If χ is the character of A_k defined in Theorem 2.1.1, we put $\chi_D(x) = \chi(\operatorname{Tr} x)$ for $x \in D_A$; then χ_D has the properties corresponding to those stated for χ in Theorem 2.1.1: $\chi_D(xy)$ determines an isomorphism of D_A onto its dual group, and D_k is self-orthogonal for this isomorphism. As a consequence, if we define the Fourier transform $\Psi(y)$ of a function $\Phi(x)$ on D_A by the formula

$$\Psi(y) = \int_{D_A} \Phi(x)\chi_D(xy)dx_A ,$$

we have the inversion formula

$$\Phi(x) = \int_{D_A} \Psi(y)\, \overline{\chi_D(xy)}dy_A$$

and the Poisson summation formula

$$\sum_{\alpha \in D_k} \Phi(\alpha) = \sum_{\beta \in D_k} \Psi(\beta)$$

under suitable conditions for Φ and Ψ. For instance, these formulas are valid if both Φ and Ψ are continuous, absolutely integrable, and such that the series $\Sigma_\alpha \Phi(x+\alpha)$, $\Sigma_\beta \Psi(y+\beta)$ are absolutely and uniformly convergent; when that is so, we say that Φ, Ψ are "of Poisson type". If, in the definition for Φ, we substitute xa, $a^{-1}y$ for x, y, where $a \in D_A^*$, we see that the Fourier transform of $\Phi(xa)$ is $|N(a)|^{-n}\Psi(a^{-1}y)$; similarly (and in view of the fact that $\chi_D(axa^{-1}) = \chi_D(x)$, by the definition of χ_D) the Fourier transform of $\Phi(ax)$ is $|N(a)|^{-n}\Psi(ya^{-1})$.

Now we say that Φ is of <u>standard type</u> if, for every $a \in D_A^*$, $\Phi(ax)$ and $\Phi(xa)$ are of Poisson type and if the following conditions are satisfied :

(a) There is an S (i.e. a finite set of valuations of k, including all the infinite places) such that, for $x = (x_v) \in D_A$, $x_S = (x_v)_{v \in S}$:

$$\Phi(x) = \Phi_S(x_S) \prod_{p \notin S} \phi_p(x_p)$$

where ϕ_p is the characteristic function of $D_{\underline{o}_p}$, and Φ_S is continuous and absolutely integrable in $D_S = \prod_{v \in S} D_{k_v}$. If this condition is satisfied for some S, it is clearly also satisfied for every $S' \supset S$. Also, it implies that the Fourier transform Ψ of Φ satisfies a similar condition (but possibly with another S).

(b) The integral

(1) $$\int_{D_S} \prod_{v \in S} |N(x_v)|_v^s \Phi_S(x_S)dx_S$$

and the similar integral for Ψ, converge absolutely and uniformly for $s \geq 0$.

One special method for constructing functions of standard type is as follows. In the function-theoretic case, take any set S as in (i), and take for Φ_S the characteristic function of any compact open subset of D_S, or a finite linear combination of such functions. In the number-theoretic case, let S_o be the set of the infinite places of k, so that $D_{S_o} = D_k \otimes_k \underline{\underline{R}}$; on D_{S_o}, considered as a vector-space over $\underline{\underline{R}}$, let P be a polynomial function and F a positive-definite quadratic form; for $x_o \in D_{S_o}$, take $\Phi_o(x_o) = P(x_o)e^{-F(x_o)}$; on the other hand, let S' be any finite set of valuations of k, disjoint from S_o, and let Φ' be the characteristic function of a compact open subset of $D_{S'}$, or a finite linear combination of such functions; take $S = S_o \cup S'$, so that $D_S = D_{S_o} \times D_{S'}$, and, for $x_o \in D_{S_o}$, $x' \in D_{S'}$, take $\Phi_S(x_o, x') = \Phi_o(x_o)\Phi'(x')$; then define Φ as in (i). It is easily seen that, in both cases, Φ is of standard type, and that its Fourier transform is another function of the same nature.

<u>Definition</u>. <u>Let</u> Φ <u>be a function of standard type on</u> D_A; <u>the</u>

function

(2) $$Z^{\Phi}(s) = \int_{D_A^*} |N(x)|^s \Phi(x)\omega'_A$$

will be called the zeta-function of D with respect to Φ.

This definition will be justified by proving, firstly, by a multiplicative calculation, that the integral for $Z^{\Phi}(s)$ is absolutely convergent for $\mathrm{Re}(s) > n$ (and uniformly so for $\mathrm{Re}(s) \geq n+\varepsilon$ for every $\varepsilon > 0$), and, secondly, by an additive calculation, that it can be continued analytically in the whole s-plane. For the multiplicative calculation, take S as in (a) and put, for every $S' \supset S$:

$$D^*_{S'} = \prod_{v \in S'} D^*_{k_v}, \quad D^*_{(S')} = D^*_{S'} \times \prod_{p \notin S'} D^*_{\underline{o}_p} .$$

Then, by definition of the adele-space, we have

$$Z^{\Phi}(s) = \lim_{S'} \int_{D^*_{(S')}} |N(x)|^s \Phi(x)\omega'_A ,$$

where the limit is taken over the filter of the sets S', ordered by inclusion. Now call $Z^{\Phi}_S(s)$ the integral (1); this is the same as the same integral taken over D^*_S, since $\prod_{v \in S} |N(x_v)|_v$ is 0 on $D_S - D^*_S$. Also, put, for $p \notin S$

$$Z_p(s) = \int_{D^*_{k_p}} |N(x_p)|_p^s \phi_p(x_p)\omega'_p ,$$

and denote by $Z^o_p(s)$ the same integral taken over $D^*_{\underline{o}_p}$; then:

$$Z^{\Phi}(s) = (\prod_{v \in S} \lambda_v^{-1}) Z^{\Phi}_S(s-n) \lim_{S'} (\prod_{p \in S'-S} Z_p(s) \prod_{p \notin S'} Z^o_p(s))$$

where, as before, $\lambda_p = 1 - N(p)^{-1}$ for a p-adic valuation, and $\lambda_v = 1$ for

an infinite place. Now, on $D^*_{\underline{o}_p}$, we have $|N(x_p)|_p = 1$ (provided S has been taken large enough) and $\phi_p(x_p) = 1$, so that $Z^o_p(s)$ is the ω'_p-measure of $D^*_{\underline{o}_p}$; by the definition of convergence factors, this implies that $\prod_p Z^o_p(s)$ is absolutely convergent. Therefore

$$Z^{\Phi}(s) = (\prod_{v \in S} \lambda_v^{-1}) Z^{\Phi}_S(s-n) \prod_{p \notin S} Z_p(s) .$$

As we have seen, we can identify $D_{\underline{o}_p}$ with $M_n(\underline{o}_p)$ for $p \notin S$ provided S has been taken large enough. Write $M_n(\underline{o}_p)^*$ for the set of the matrices in $M_n(\underline{o}_p)$ with a non-zero determinant, and $U_{n,p}$ for the set of the invertible matrices in $M_n(\underline{o}_p)$, i.e. those whose determinant is a unit in $\underline{o}_p$; we have, for $p \in S$ and $q = N(p)$:

$$Z_p(s) = \int_{M_n(\underline{o}_p)^*} |\det X|_p^s (1-q^{-1})^{-1} |\det X|_p^{-n} (dX)_p .$$

For a given p, call π a prime element in $\underline{o}_p$ (this means that $\pi\underline{o}_p$ is the maximal prime ideal in $\underline{o}_p$). It is well-known that $M_n(\underline{o}_p)$ is the disjoint union of the sets $U_{n,p}A$ when one takes for A the following matrices:

$$A = \begin{pmatrix} \pi^{d_1} & & & \\ & \pi^{d_2} & & \alpha_{ij} \\ & & \ddots & \\ 0 & & & \pi^{d_n} \end{pmatrix}$$

where $(d_1, \ldots, d_n)$ run through all n-tuples of integers ≥ 0, and, for each choice of the d_i, each α_{ij} runs through a complete set of representatives of $\underline{o}_p \bmod \pi^{d_j}$. This gives:

$$(1-q^{-1}) Z_p(s) = \sum_A |\det A|_p^s \int_{U_{n,p}A} |\det X|_p^{-n} (dX)_p .$$

As the integrand in the right-hand side is (by construction) invariant under translations in $M_n(k_p)$, the integral is independent of A, taking $A = 1_n$ (the unit-matrix), we see that its value is the measure of $U_{n,p}$ for the measure $(dX)_p$, in the space $M_n(k_p)$; this is $q^{-n^2}\nu$ if ν is the number of matrices of non-zero determinant in the ring $M_n(F_q)$, where F_q is the finite field with q elements; this gives

$$\int_{U_{n,p}} (dX)_p = (1-q^{-n})(1-q^{-n+1})\dots(1-q^{-1}) .$$

On the other hand, for given values of $d_1,\dots,d_n$, there are

$$q^{d_2+2d_3+\dots+(n-1)d_n}$$

matrices A. Therefore :

$$Z_p(s) = (1-q^{-n})\dots(1-q^{-2}) \sum_{(d_i)} q^{\Sigma_i(i-1-s)d_i}$$

$$= \prod_{i=2}^{n}(1-q^{-i}) \prod_{i=1}^{n}(1-q^{i-1-s})^{-1} .$$

From the elementary theory of the zeta-function for k, we borrow the fact that the product $\zeta_k(s) = \prod_p (1-q^{-s})^{-1}$ is absolutely convergent for s real and >1, and that $(s-1)\zeta_k(s)$ tends to a finite limit ρ_k for $s \to 1$; this implies that $\prod_{p \notin S} Z_p(s)$ converges absolutely for $Re(s) > n$ and is $\sim\rho(s-n)^{-1}$, with ρ a constant, for $s \to n$. This proves that, as asserted, the integral which defines $Z^{\Phi}(s)$ is absolutely convergent for $Re(s) > n$. Also, we have

(3) $$\lim_{s\to n}(s-n)Z^{\Phi}(s) = \rho_k Z_s^{\Phi}(0) = \rho_k \int_{D_A} \Phi(x)dx_A ,$$

where ρ_k depends only upon the field k.

For the <u>additive</u> calculation, introduce on $\underline{\mathbb{R}}_+$ the function $\lambda(t)$ defined by $\lambda(t) = 1$ for $0 < t < 1$, $\lambda(t) = 0$ for $1 < t$, and $\lambda(1) = \frac{1}{2}$. For $x \in D_A^*$, put :

$$f_+(x) = \lambda(|N(x)|^{-1}),\ f_-(x) = \lambda(|N(x)|) ,$$

so that we have $f_+ + f_- = 1$; and write

$$Z_+^{\Phi}(s) = \int_{D_A^*} f_+(x)|N(x)|^s\Phi(x)\omega_A' ,$$

$$Z_-^{\Phi}(s) = \int_{D_A^*} f_-(x)|N(x)|^s\Phi(x)\omega_A' ,$$

so that $Z^{\Phi} = Z_+^{\Phi} + Z_-^{\Phi}$. Clearly, if the integral for Z_+^{Φ} converges absolutely for some s_o, it converges absolutely and uniformly for $Re(s) \leq Re(s_o)$; as the multiplicative calculation has shown that the integral for Z^{Φ}, hence also the integral for Z_+^{Φ}, converges absolutely for $Re(s) > n$, we conclude that $Z_+^{\Phi}(s)$ is an entire function of s. On the other hand, we have, for $Re(s) > n$

$$Z_-^{\Phi}(s) = \int_{D_A^*/D_k^*} f_-(x)|N(x)|^s\Big(\sum_{\alpha\in D_k^*}\Phi(x\alpha)\Big)\omega'_A$$

$$= \int_{D_A^*/D_k^*} f_-(x)|N(x)|^s\Big(\sum_{\alpha\in D_k}\Phi(x\alpha) - \Phi(0)\Big)\omega'_A$$

(D_A^*/D_k^* is the space of <u>right</u> cosets xD_k^* of D_k^* in D_A^*). By Poisson summation, we have

$$\sum_{\alpha\in D_k}\Phi(x\alpha) = |N(x)|^{-n}\sum_{\beta\in D_k}\Psi(\beta x^{-1}) ,$$

where Ψ is as before the Fourier transform of Φ; hence

$$Z_-^{\Phi}(s) = \int_{D_A^*/D_k^*} f_-(x)|N(x)|^s\Big(|N(x)|^{-n}\sum_{\beta\in D_k}\Psi(\beta x^{-1}) - \Phi(0)\Big)\omega_A' ,$$

this still being absolutely convergent for $\mathrm{Re}(s) > n$. Now, in the integral defining $Z_+(s)$, which converges absolutely for all s, substitute $n-s$ for s and x^{-1} for x; as the latter substitution does not affect the Haar measure, and as $f_+(x^{-1}) = f_-(x)$, we get :

$$Z_+^{\Psi}(n-s) = \int_{D_A^*} f_-(x)|N(x)|^{s-n}\Psi(x^{-1})\,\omega_A'$$

$$= \int_{D_A^*/D_k^*} f_-(x)|N(x)|^{s-n}\Big(\sum_{\beta\in D_k^*}\Psi(\beta x^{-1})\Big)\,\omega_A' .$$

Combining our two last formulas, we get

$$Z^{\Phi}(s) - Z_+^{\Phi}(n-s) = \int_{D_A^*/D_k^*} \mu(|N(x)|)\omega_A'$$

where $\mu(t)$ is the function defined on $\underline{\underline{R}}_+$ by

$$\mu(t) = [\Psi(0)t^{s-n} - \Phi(0)t^s]\lambda(t) .$$

By lemma 3.1.2, this gives

$$Z_-^{\Phi}(s) - Z_+^{\Psi}(n-s) = \begin{cases} c\,\Big(\dfrac{\Psi(0)}{s-n} - \dfrac{\Phi(0)}{s}\Big) \\ \dfrac{c}{2}\Big(\Psi(0)\,\dfrac{q^{s-n}+1}{q^{s-n}-1} - \Phi(0)\,\dfrac{q^s+1}{q^s-1}\Big) \end{cases}$$

(c is the constant in Lemma 3.1.2). This shows that Z_-^{Φ} and Z^{Φ} are meromorphic in the whole plane, with a residue at $s = n$ equal to $c\Psi(0)$ (resp. $c\Psi(0)/\log q$). As we have $\Psi(0) = \int_{D_A}\Phi(x)dx_A$, a comparison with (3) gives $c = \rho_k$ (resp. $c = \rho_k \log q$). This proves :

Theorem 3.1.1. (i) $Z(s)$ *is the sum of an entire function of* s *and of*

$$\rho_k\Big(\frac{\Psi(0)}{s-n} - \frac{\Phi(0)}{s}\Big) \text{ resp. } \rho_k \log q\,\Big(\frac{\Psi(0)}{q^{s-n}-1} - \frac{\Phi(0)}{q^s-1}\Big)$$

where $\rho_k = [(s-1)\zeta_k(s)]_{s=1}$, *and* Ψ *is the Fourier transform of* Φ.

(ii) $Z^{\Phi}(s) = Z^{\Psi}(n-s)$.

(iii) *We have the formula*

$$\int_{D_A^*/D_k^*} F(|N(x)|)\omega_A' = \begin{cases} \rho_k \displaystyle\int_0^{+\infty} F(t)dt/t \\ \text{resp. } \rho_k \log q \displaystyle\sum_{\nu=-\infty}^{+\infty} F(q^{\nu}) \end{cases}$$

provided F *is such that the right-hand side is absolutely convergent* (N.B. *In the function-field case,* q *is the number of elements of the field of constants of* k).

3.2. *The projective group of a central division algebra.*

Lemma 3.2.1. *Let* G *be a locally compact unimodular group,* g *a closed subgroup of the center of* G; *put* $G' = G/g$, *and let* dx, $d'x'$, $d_g z$ *be Haar measures matching together topologically on* G, G', g. *Let* Δ *be a discrete subgroup of* G; *put* $H = G/\Delta$, $\delta = \Delta\cap g$, $\Delta' = g\Delta/g = \Delta/\delta$, $H' = G'/\Delta' = G/g\Delta$, $\gamma = g/\delta = g\Delta/\Delta$. *Then* γ *is a commutative group operating continuously on* H; *the quotient* H/γ *is canonically isomorphic to* H'; *and we have, for* $f \in L^+(H)$

$$\int_H f(u)du = \int_{H'} d'u' \int_{\gamma} f(tu)d_g t$$

where tu, *for* $u\in H$, $t\in\gamma$, *is the transform of* u *by* t *acting on* H *as we have said, and* u' *is the image* γu *of* u *in the canonical mapping of* H *onto* $H' = H/\gamma$.

The first assertion follows algebraically from the fact that g is in the center, and topologically from the fact that Δ is discrete in G. Now we have, under obvious assumptions on ϕ, ϕ', ϕ'' :

$$\int_G \phi(x)dx = \int_{G'} d'x' \int_g \phi(xz)d_g z \qquad (x' = xg),$$

$$\int_{G'} \phi'(x')d'x' = \int_{H'} \Big(\sum_{\xi' \in \Delta'} \phi'(x'\xi')\Big)d'x'' \qquad (x'' = x'\Delta'),$$

$$\int_g \phi''(z)d_g z = \int_\gamma \Big(\sum_{\zeta \in \delta} \phi''(z\zeta)\Big)d_g z' \qquad (z' = z\delta).$$

Combining these, and using the fact that g and δ are in the center, we get

(1) $$\int_G \phi(x)dx = \int_{H'} d'u' \int_\gamma \Big(\sum_{\xi \in \Delta} \phi(xz\xi)\Big)d_g z' \qquad (z' = z\delta,\ u' = xg\Delta).$$

On the other hand, we have

(2) $$\int_G \phi(x)dx = \int_H \Big(\sum_{\xi \in \Delta} \phi(x\xi)\Big)du \qquad (u = x\Delta).$$

The comparison of (1) and (2) concludes the proof, since there are "sufficiently many" functions $\Sigma_{\xi\in\Delta}\,\phi(x\xi)$ on H.

Now, in Lemma 3.2.1, we replace G, Δ, g by D^*_A, D^*_k, Z^*_A, respectively, where Z is, as before , the center of the algebra variety D. As in 3.1, we write G for the algebraic group D^*/Z^*, i.e. for the projective group of D; Z^* may be identified with G_m; as it is well known that every fibering by G_m has local cross-sections, we can apply Theorem 2.4.2 to D^* and Z^*, and therefore identify D^*_A/Z^*_A with G_A; also, if we identify Z^* with G_m, Z^*_A gets identified with $(G_m)_A = I_k$, the idele-group of k. On D^*_A and D^*_A/D^*_k, we take the measure denoted above by ω'_A. The proof in 3.1, applied to the case $n = 1$, shows that the set of convergence factors (λ_p) which was used to define ω'_A is also a set of convergence factors for $Z^* = G_m$; we denote by ω'_Z the Tamagawa measure determined by this set on $Z^*_A = I_k$, and also on $Z^*_A/Z^*_k = I_k/k^*$. Then, by Theorem 2.4.3, (1) is a set of convergence factors for $G = D^*/Z^*$; we denote by ω_G the Tamagawa measure on G_A, and

the corresponding measure on G_A/G_k. In view of Theorem 2.4.3, we can now apply to this situation our Lemma 3.2.1, and get

$$\int_{D^*_A/D^*_k} F(|N(x)|)\omega'_A = \int_{G_A/G_k} \omega_G \int_{Z^*_A/Z^*_k} F(|N(xz)|\cdot\omega'_Z(z),$$

where F is any function such that the left-hand side converges absolutely. The left-hand side can be expressed by means of Theorem 3.1.1 (iii); on the other hand, the second integral in the right-hand side can be written as

$$\int_{Z^*_A/Z^*_k} F(|N(x)|\cdot|z|^n)\omega'_Z(z)\ ,$$

which can be expressed by Theorem 3.1.1 (iii) applied to Z instead of D and is thus seen to have the value

$$\rho_k \int_0^{+\infty} F(|N(x)|t^n)dt/t = \frac{\rho_k}{n}\int_0^{+\infty} F(t)dt/t$$

in the number-field case, and

$$\rho_k \log q \sum_{\nu=-\infty}^{+\infty} F(|N(x)|q^{\nu n})$$

in the function-field case. Comparing both results, we see at once, in the former case, that $\tau(G) = \int_{G_A/G_k}\omega_G$ has the value n; we get the same conclusion in the latter case by taking, for instance, F such that $F(q^\nu) = 1$ for $0 \le \nu \le n-1$, and $= 0$ otherwise. Thus :

<u>Theorem</u> 3.2.1. <u>The Tamagawa number of the projective group of a division algebra of dimension</u> n^2 <u>over its center is</u> n.

3.3 <u>Isogenies</u>.

We recall that an isogeny is a homomorphism of an algebraic group onto another of the same dimension; two groups G, G' are called isogenous if G'' can be found so that there are isogenies of G'' onto G and onto G'. In this section, we consider Tamagawa numbers of groups isogenous to projective groups of simple algebras, and products of such groups; this, combined with Theorem 3.2.1, will give for instance the Tamagawa number of the special linear group of a division algebra.

Lemma 3.3.1. *If two groups G, G' are isogenous over k, every set of convergence factors for G is a set of convergence factors for G'.*

Assume that there is an isogeny f of G onto G' over k; by means of representations of G, G' into special linear groups, we can consider them as affine varieties; then, if $x' = f(x)$, the coordinates of x' can be written as polynomials in those of x. As in 2.2, we see that G, G' and f can be reduced modulo p for almost all p. Our lemma is now an immediate consequence of Theorem 2.2.5 and of Lang's theorem, according to which two isogenous groups over a finite field have the same number of rational points (Am. J. of Math. 78 : see last five lines of p. 561).

Any simple algebra R can be written as $M_m(D)$, where D, as in 3.1, is a division algebra. The same calculation as in 3.1 shows that the $\lambda_p = 1 - N(p)^{-1}$ is a set of convergence factors for R^*; as it is also a set of convergence factors for Z^*, where Z is the center of R, Theorem 2.4.3 shows that (1) is such a set for R^*/Z^*, hence also for every group isogenous to R^*/Z^* (in particular, for $R^{(1)}$) and that (λ_p) is such a set for every group isogenous to $(R^*/Z^*) \times G_m$. In what follows, we shall use these facts freely. Tamagawa measures in the strict sense (derived from the set (1) of convergence factors) will be denoted by ω, ω_A, dx, etc.; by ω', ω'_A, $d'x$, etc., we denote Tamagawa measures derived from the set of convergence factors $(1-N(p)^{-1})$; for instance, on I_k, we use the Tamagawa measure $(dt/t)'$.

As in 3.1, let D_k be a division algebra of dimension n^2 over its center $Z_k = k$; D being the algebra variety defined by D, with the center Z, take $R = M_m(D)$; call N the reduced norm in R over its center. Take any divisor ν of mn $(1 \leq \nu \leq mn)$. Let Γ be the group

$$\Gamma = \{(x,v) \in R^* \times G_m \mid v^\nu = N(x)\} ,$$

i.e. the algebraic subgroup of $R^* \times G_m$ determined by $v^\nu = N(x)$; it is connected and defined over k. The connected component of the identity in its center is

$$\Gamma_o = \{(t \cdot 1_R,\ t^{mn/\nu}) \mid t \in G_m\}$$

and is obviously isomorphic to G_m; here 1_R is the unit-element in R. Put $G = \Gamma/\Gamma_o$; this is an algebraic group, defined over k; for $\nu = 1$, Γ is isomorphic to R^* and G can be identified with R^*/Z^*, the projective group of R; for $\nu = mn$, the mapping $(x,v) \to v^{-1}x$ determines a homomorphism of Γ onto $R^{(1)}$ with the kernel Γ_o, so that G can be identified with $R^{(1)}$. For any ν, there are obvious isogenies $R^{(1)} \to G \to R^*/Z^*$ such that the composite isogeny $R^{(1)} \to R^*/Z^*$ is the canonical one.

Theorem 3.3.1. *We have* $\tau(G) = mn/\nu$.

Consider the homomorphism ϕ of Γ onto G_m given by $\phi(x,v) = v$; its kernel is

$$\Gamma' = \{(x,1) \in R^{(1)} \times G_m\}$$

and is isomorphic to $R^{(1)}$; by means of ϕ, we can identify Γ/Γ' with G_m; as usual, we extend ϕ to a homomorphism of Γ_A into $(G_m)_A = I_k$.

Lemma 3.3.2 $\phi(\Gamma_A)/\phi(\Gamma_k) = I_k/k^*$.

It is known (Eichler, Math. Zeitschr. 1938) that an element λ

of k^* is the norm of an element of R_k if and only if it is the norm of an element of R_{k_v} for every v; the latter condition is equivalent to saying that λ must be the norm of an element of R_A. Now, for $\alpha \in k^*$, we have $\alpha \in \phi(\Gamma_A)$ if and only if α^ν is the norm of an element of R_A; then, by Eichler's theorem, α^ν is the norm of an element of R_k. This proves that $k^* \cap \phi(\Gamma_A) = \phi(\Gamma_k)$. Now we show that $I_k = k^*.\phi(\Gamma_A)$. In fact, if $x = (x_v) \in I_k$, it is known that x_p is the norm of an element of R_{k_p} for every p, and that x_v is the norm of an element of R_{k_v} whenever v is a complex place (i.e. $k_v = \underline{\underline{C}}$), and also whenever v is a real place (i.e. $k_v = \underline{\underline{R}}$) and $x_v > 0$. Moreover, for almost all p, $R_{\underline{o}_p} = M_{mn}(\underline{o}_p)$, so that the image of $\Gamma_{\underline{o}_p}$ by ϕ is $(G_m)_{\underline{o}_p} = U_p$ (the unit-group of $\underline{o}_p$). Algebraically, our conclusion follows at once from these facts; the same holds topologically (so that we may identify $\phi(\Gamma_A)/\phi(\Gamma_k)$ with I_k/k^*) in view of the final remark of Chapter II.

As $(x,v) \to x$ is an isogeny of Γ onto R^*, $(1-N(p)^{-1})$ is a set of convergence factors for Γ; let $d'(x,v)$ be the corresponding measure. We shall discuss the number-field case; the function-field case can be treated quite similarly. We compute in two ways the integral

$$\int_{\Gamma_A/\Gamma_k} F(|v|)d'(x,v)$$

where F is an arbitrary function (say, continuous with compact support) on the group $\underline{\underline{R}}_+$. We first use the decomposition $G = \Gamma/\Gamma_o$; as $\Gamma_o \cong G_m$, it has cross-sections in Γ, so that we can apply Theorem 2.4.3. Then, by Lemma 3.2.1, we have

$$\int_{\Gamma_A/\Gamma_k} F(|v|)d'(x,v) = \int_{G_A/G_k} \omega_G \int_{I_k/k^*} F(|t^{mn/\nu}v|)(dt/t)' ;$$

the second integral in the right-hand side can be computed by Theorem

3.1.1 (iii) applied to G_m, which shows that it is independent of v (this would have to be modified in the function-field case, just as in the last part of the proof of Theorem 3.2.1), and gives

$$\int_{\Gamma_A/\Gamma_k} F(|v|)d'(x,v) = \tau(G)\,\frac{\rho_k \nu}{mn} \int_0^\infty F(t)dt/t .$$

On the other hand, applying Theorem 2.4.4 and Lemma 3.3.2 to the decomposition $G_m = \Gamma/\Gamma'$, we get :

$$\int_{\Gamma_A/\Gamma_k} F(|v|)d'(x,v) = \tau(\Gamma') \int_{I_k/k^*} F(|v|)(dv/v)' ,$$

where the right-hand side can again be computed as above. This shows that, if one of the numbers $\tau(G)$, $\tau(\Gamma')$ is finite, the other is so, and that $\tau(\Gamma') = \nu\tau(G)/mn$.

Take $m = \nu = 1$; then $\Gamma' = D^{(1)}$, G is the projective group of D, and $\tau(G) = n$ by Theorem 3.2.1; therefore $\tau(D^{(1)}) = 1$. Take $m = 1$, and take for ν any divisor of n; then $\Gamma' = D^{(1)}$, $\tau(\Gamma') = 1$; this gives $\tau(G) = n/\nu$, and proves Theorem 3.3.1 in the case $n = 1$.

In the general case, we have $\tau(G) = mn\tau(\Gamma')/\nu$, with $\Gamma' \cong R^{(1)}$. Thus, in order to complete the proof of Theorem 3.3.1, it only remains to show that $\tau(R^{(1)}) = 1$ for $R = M_m(D)$; as we know that this is so for $m = 1$, we shall proceed by induction on m.

3.4. <u>End of proof of Theorem</u> 3.3.1 : <u>central simple algebras</u>.

We change our notations slightly. From now on, D will be as before; we write $R_m = M_m(D)$. We denote by D^m the space of $(m,1)$-matrices (i.e., column-vectors of order m) over D, and let R_m act on D^m by $(X,x) \to Xx$ for $X \in R_m$, $x \in D^m$. Put

$$e = \begin{pmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

(we write 1 for the unit-element of D). Call H the orbit of e under the action of R_m^* in D^m; as Xe is generic over k in D^m if X is so in R_m, H is a Zariski-open subset of D^m over k. More precisely, if K is any field containing k, H_K can be determined as follows. As $D_K = D_k \otimes K$ is a simple central algebra over K, there is an isomorphism ρ of D_K onto a matrix algebra $M_r(D')$ over a central division algebra D' over K; then H_K consists of the column-vectors $x = (x_i)_{1 \leq i \leq m}$, $x_i \in D_K$, such that the (mr,r)-matrix

$$\rho(x) = \begin{pmatrix} \rho(x_1) \\ \rho(x_2) \\ \cdot \\ \cdot \\ \cdot \\ \rho(x_m) \end{pmatrix}$$

over D' has the rank r.

From now on, we assume that $m \geq 2$, and we put $G = R_m^{(1)}$, $G' = R_{m-1}^{(1)}$; it is easily seen that H is also the orbit of e under G. Call g the subgroup of G leaving e fixed; it consists of the matrices

$$X = \begin{pmatrix} 1 & {}^t u \\ 0 & X' \end{pmatrix} \qquad (u \in D^{m-1},\ X' \in G')$$

(${}^t u$ is the transpose of u). If $x = (x_i)_{1 \leq i \leq m}$ is a generic point of D^m over k, it is the image $M(x)e$ of e under the element

$$M(x) = \begin{pmatrix} x_1 & 0 & 0 & 0 \dots 0 \\ x_2 & x_1^{-1} & 0 & 0 \dots 0 \\ x_3 & 0 & & \\ \cdot & \cdot & & 1_{m-2} \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ x_m & 0 & & \end{pmatrix}$$

of G, where 1_{m-2} is the unit element of R_{m-2}. This is a "generic cross-section" (in the sense of Theorem 1.2.2) for the mapping $X \to Xe$ of G into $H = G/g$; also, G_k is obviously Zariski-dense in G. We can therefore apply Theorem 2.4.2 (cf. Remark 2 at the end of Chapter II), and therefore identify G_A/g_A, and, for every v, G_{k_v}/g_{k_v}, with the orbits H_A, H_{k_v} of e under G_A and under G_{k_v}, respectively; also, for almost every p, we can identify $G_{\underline{o}_p}/g_{\underline{o}_p}$ with the orbit $H_{\underline{o}_p}$ of e under $G_{\underline{o}_p}$. For every v, there is an isomorphism ρ_v of D_{k_v} onto a matrix algebra $M_{r_v}(D'_v)$ over a division algebra D'_v with the center k_v; this can be extended to an isomorphism which we also call ρ_v, of $R_{k_v} = M_m(D_{k_v})$ onto $M_{mr_v}(D'_v)$, and also to an isomorphism of $(D_{k_v})^m$ onto the space of (mr_v, r_v)-matrices over D'_v; as we have seen, H_{k_v} consists of the elements $x \in (D_{k_v})^m$ such that $\rho_v(x)$ has the rank r_v. For almost all p, we have $r_p = n$, $D'_p = k_p$, and, for $x \in (D_{\underline{o}_p})^m$, $\rho_p(x)$ is an (mn,n)-matrix over $\underline{o}_p$; this matrix, by reduction modulo p, determines an (mn,n)-matrix $\bar{\rho}_p(x)$ over the finite field F_q with $q = N(p)$ elements; it is easily seen that we can choose S such that this is so for $p \notin S$, and also that, for $p \notin S$, $H_{\underline{o}_p}$ consists of the elements x of $(D_{\underline{o}_p})^m$ such that $\bar{\rho}_p(x)$ is of rank n.

The additive group D_A^m is isomorphic to $(A_k)^{mn^2}$; it will now be shown that $D_A^m - H_A$ is of measure 0. This is a special case of the following :

Lemma 3.4.1. *Let* ω *be a gauge-form on a non-singular variety* V, *defined over* k; *let* V' *be a k-open subset of* V; *assume that there is a common set* (λ_v) *of convergence factors for* V *and for* V'. *Then the measure* $(\omega,(\lambda_v))$ *for* V'_A *is the measure induced on* V'_A *by the measure* $(\omega,(\lambda_v))$ *for* V_A; *and, for that measure,* $V_A - V'_A$ *has the measure* 0.

Let j be the injection mapping of V' into V; then j_A is an injective mapping of V'_A into V_A, which we use to identify V'_A with a subset of V_A (note that the topology of V'_A is in general not that induced by V_A, as shown by the case of G_m considered as the complement of $\{0\}$ in G_a, which corresponds to the "natural" embedding of I_k in A_k; in that case the two varieties have no common set of convergence factors, and I_k, not $A_k - I_k$, is of measure 0 in A_k). The first assertion follows from the definition of $(\omega,(\lambda_v))$. Now define $V_{\underline{o}_p}$, $V'_{\underline{o}_p}$ ("almost intrinsically", cf. 2.2.3 and 2.3) by means of suitable converings of V and V'; by Theorem 1.2.1, there is S such that $V'_{\underline{o}_p} \subset V_{\underline{o}_p}$ for $p \notin S$; let μ_p, μ'_p be the measures of $V_{\underline{o}_p}$, $V'_{\underline{o}_p}$ for the "local measure" ω_p; by assumptions, $\prod_p \lambda_p^{-1}\mu_p$ and $\prod_p \lambda_p^{-1}\mu'_p$ are absolutely convergent. For each v, put $X_v = V_{k_v} - V'_{k_v}$; this is an analytic subset of V_{k_v} and is therefore of measure 0 for the local measure ω_v (by the theory of analytic varieties over complete valued fields). Take $S'' \supset S' \supset S$; put $V_{S'} = \prod_{v\in S'} V_{k_v}$, $P_{S'} = \prod_{p\notin S'} V_{\underline{o}_p}$, and

$$P_{S'}(S'') = \prod_{p\in S''-S'} V_{\underline{o}_p} \times \prod_{p\notin S''} V'_{\underline{o}_p} .$$

Then, for the product-measure $\prod_p(\lambda_p^{-1}\omega_p)$ on $P_{S'}$, $P_{S'}(S'')$ has the measure

$$\prod_{p\in S''-S'}(\lambda_p^{-1}\mu_p)\cdot\prod_{p\notin S''}(\lambda_p^{-1}\mu'_p) .$$

Therefore, if we put $Q_{S'} = \bigcup_{S''} P_{S'}(S'')$, $P_{S'} - Q_{S'}$ has the measure 0. We have thus shown that, in the product $V_{S'} \times P_{S'}$, the set of the points $x = (x_v)$ such that either $x_v \in X_v$ for some v or $(x_p)_{p\in S'} \notin Q_{S'}$ is of measure 0; since the complement of that set is contained in V'_A, this proves the lemma.

In order to apply this to D^m and H, all we need show is that (1) is a set of convergence factors for $H = G/g$, or (in view of Theorem 2.4.3) that this is so for g. In fact, g is the semi-direct product of the groups consisting respectively of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & X' \end{pmatrix} \quad (X' \in G'), \qquad \begin{pmatrix} 1 & {}^t u \\ 0 & 1_{m-1} \end{pmatrix} \quad (u \in D^{m-1}) ,$$

these groups being respectively isomorphic to G' and to D^{m-1}; our assertion follows now from Theorem 2.4.3 applied to g, D^{m-1} and $G' = g/D^{m-1}$. Also, this shows that g is unimodular; and, in view of the fact that $\tau(D^{m-1}) = 1$ (since $\tau(G_a) = 1$), and that $\tau(G') = 1$ by the induction assumption, Theorems 2.4.3 and 2.4.4 show that $\tau(g) = 1$. Now, applying Lemma 2.4.2 to the groups G_A, g_A, G_k, g_k, we get

$$\int_{H_A} f(x)dx = \int_{G_A/G_k} \Big(\sum_{\xi\in H_k} f(X\xi)\Big)dX$$

where dx and dX are Tamagawa measures in H_A and G_A respectively; as $D_A^m - H_A$ is of measure 0, we may, in the left-hand side, replace the integral on H_A by the integral on D_A^m, dx being then (in view of Lemma 3.4.1) the Tamagawa measure on D_A^m. On the other hand, since D_k is a division algebra, we have $H_k = D_k^m - \{0\}$; therefore

$$(1) \qquad \int_{D_A^m} f(x)dx = \int_{G_A/G_k} \Big(\sum_{\xi\in D_k^m} f(X\xi) - f(0)\Big)dX .$$

Here f may be taken as any function in D_A^m such that the left-hand side is absolutely convergent. If at the same time we assume f to be such that $f(Xx)$, for every $X \in G_A$, is of Poisson type (one can select such a function by a procedure similar to that described in 3.1), the right-hand side can be transformed by Poisson's formula. Let g be the Fourier transform of f:

$$g(y) = \int_{D_A^m} f(x)\chi_D({}^t y \cdot x)dx$$

(as before, ${}^t y$ is the transpose of the column-vector y); replacing x, y by Xx, ${}^t X^{-1} y$, with $X \in G_A$, we see that the Fourier transform of $f(Xx)$ is $g({}^t X^{-1} y)$ since $\det X = 1$; (1) gives now :

$$\int_{D_A^m} f(x)dx = \int_{G_A/G_k} \Big(\sum_{\eta \in D_k^m} g({}^t X^{-1} \eta) - f(0)\Big)dX .$$

If in (1) we substitute g for f and ${}^t X^{-1}$ for X (which does not change dX), and combine the two formulas, we get

$$\int_{D_A^m} [f(x) - g(x)]dx = \int_{G_A/G_k} [g(0) - f(0)]dX .$$

Here the left-hand side has the value $g(0) - f(0)$, and all integrals are absolutely convergent; choosing f so that $g(0) \neq f(0)$, we see that $\tau(G) = 1$. This completes the proof of Theorem 3.3.1.

3.5. The symplectic group.

Using the same method as in 3.4, we prove :

Theorem 3.5.1. $\tau(Sp(2n)) = 1$.

As usual, $Sp(2n)$ is the symplectic group in $2n$ variables, i.e. the subgroup of $GL(2n)$ which leaves invariant the exterior form

$$x_1 \wedge x_2 + \dots + x_{2n-1} \wedge x_{2n}.$$

We have $Sp(2) = SL(2)$, so that $\tau(Sp(2)) = 1$ is a special case of Theorem 3.3.1. Now we proceed by induction on n. Take $n \geq 2$; put $G = Sp(2n)$, $G' = Sp(2n-2)$; call g the subgroup of G leaving the column-vector $e = (1,0,\dots,0)$ invariant. An easy calculation shows that g consists of the matrices

$$X = \begin{pmatrix} 1 & x & {}^t u \cdot J'X' \\ 0 & 1 & 0 \\ 0 & u & X' \end{pmatrix}$$

where $X' \in G'$, u is a column-vector of order $2n-2$, x is arbitrary, and J' is the alternating matrix invariant under G'. The subgroup g' of g, consisting of the matrices X for which $X' = 1_{2n-2}$, is normal; more precisely, g is the semidirect product of g' and of $g/g' \cong G'$; moreover, the subgroup g'' of g', consisting of the matrices X for which $X' = 1_{2n-2}$ and $u = 0$, is normal, and g' is the semidirect product of $g'' \cong G_a$ and of $g'/g'' \cong (G_a)^{2n-2}$. From these facts and from the induction assumption $\tau(G') = 1$, one concludes, by applying twice Theorem 2.4.3, that (1) is a set of convergence factors, first for g', and then for g, that $\tau(g') = 1$, and that $\tau(g) = 1$. Now the orbit of e under G is $H = S^{2n} - \{0\}$, where S^{2n} is the affine space of all column-vectors of order $2n$; just as in 3.4, we see that we can identify H with G/g, H_A with G_A/g_A, etc.; also, $H_{\underline{o}_p}$ consists of the vectors in $\underline{o}_p^{2n}$ which are not $\equiv 0 \bmod p$; an easy calculation shows then that (1) is a set of convergence factors for H as well as for S^{2n}, so that we can apply Lemma 3.4.1; also, by Theorem 2.4.3, (1) is a set of convergence factors for G. Now we can apply Lemma 2.4.2 to G_A, g_A, G_k, g_k; this gives

$$\int_{H_A} f(x)dx = \int_{G_A/G_k} \Big(\sum_{\xi \in H_k} f(X\xi) \Big) dX .$$

In the left-hand side, we can replace H_A by $(A_k)^{2n}$; also, H_k is the same as $k^{2n} - \{0\}$. Proceeding now exactly as in 3.4, we get $\tau(G) = 1$.

3.6. Isogenies for products of linear groups.

The method of 3.3 can be applied to a more general situation. Let R be any absolutely semisimple algebra-variety over k; this is the same as to say that R_k is absolutely semisimple, or also that R, over the universal domain, is isomorphic to a direct sum of matrix-algebras. We can write $R = \oplus R_i$, where the R_i, for $1 \leq i \leq r$, are the simple components of R; for each i, we have $R_i = M_{m_i}(D_i)$, where D_i is such that $(D_i)_k$ is a division-algebra. If Z_i is the center of D_i, which we identify in an obvious manner with the center of R_i, $(Z_i)_k = k_i$ is a finite, separably algebraic extension of k, and $(D_i)_k$ may be considered as a central division algebra over k_i, which can be written as $(D'_i)_{k_i}$, where D'_i is an algebra-variety over k_i; then we have, with the notations of 1.3, $D_i = R_{k_i/k}(D'_i)$, hence $R_i = R_{k_i/k}(R'_i)$ with $R'_i = M_{m_i}(D'_i)$; also, if Z'_i is the center of D'_i and R'_i, we have $Z_i = R_{k_i/k}(Z'_i)$; and the reduced norm N'_i, taken in R'_i over its center, determines (by applying to its graph the operation $R_{k_i/k}$) a norm mapping N_i of R_i into Z_i. We write $R_i^{(1)}$ for the special linear group of R_i, i.e. the algebraic subgroup of R_i^* determined by $N_i(x) = 1$; this is the same as $R_{k_i/k}(R_i'^{(1)})$, and we have, by Theorems 1.3.2, 1.3.3

$$(R_i'^{(1)})_{k_i} = (R_i^{(1)})_k \ , \ (R_i'^{(1)})_{A_{k_i}} = (R_i^{(1)})_{A_k} \ ,$$

which, in view of Theorem 2.3.2, implies $\tau(R_i'^{(1)}) = 1$. By the definition of the operation $R_{k_i/k}$, the algebraic group $R_i^{(1)}$, over the universal

domain, is isomorphic to $(SL(m_i n_i))^{d_i}$, where $d_i = [k_i : k]$ and n_i^2 is the dimension of D'_i.

Write N for the mapping

$$x = (x_1, \dots, x_r) \to N(x) = (N_1(x_1), \dots, N_r(x_r))$$

of R into its center $Z = \oplus_i Z_i$. This determines a homomorphism of the multiplicative group R^* of the invertible elements of R into the corresponding group Z^* for Z; we have $Z^* = \prod_i Z_i^*$, with $Z_i^* = R_{k_i/k}(Z_i'^*) \cong R_{k_i/k}(G_m)$; this is a torus of dimension $d = \Sigma_i d_i$; we have $(Z^*)_k \cong \prod_i k_i^*$; and the mapping N induces on Z^* an isogeny of Z^* onto itself, given by

$$z = (z_1, \dots, z_r) \to N(z) = (z_1^{m_1 n_1}, \dots, z_r^{m_r n_r}) .$$

In the special case treated in 3.3, the norm mapping $N : z \to z^{mn}$ of Z^* into itself was factored into $z \to z^{mn/\nu} \to z^{mn}$. Similarly, we assume now that we have factored N as follows :

$$\begin{array}{ccc} Z^* & \xrightarrow{\quad N \quad} & Z^* \\ & {\scriptstyle \mu} \searrow \quad \nearrow {\scriptstyle \nu} & \\ & T & \end{array}$$

where T is a commutative group-variety, defined over k, and μ, ν are isogenies of Z^* onto T and of T onto Z^*, also defined over k; then T is a torus, isogenous to Z^*. We introduce the algebraic groups :

$$\Gamma \equiv \{(x,t) \in R^* \times T \,|\, \nu(t) = N(x)\}$$

$$\Gamma_o \equiv \{(z, \mu(z)) \,|\, z \in Z^*\}$$

As in 3.3, Γ_o is the connected component of the identity in the center of Γ; it is isomorphic to Z^*; the group $G = \Gamma/\Gamma_o$ is isogenous to $R^{(1)}$ (it is <u>perhaps</u> the most general group isogenous to $R^{(1)}$ over k, but this will not be discussed here), and we investigate $\tau(G)$.

Call ϕ the homomorphism of Γ into T given by $\phi(x,t) = t$; its kernel is the group $\Gamma' = \{(x,e) | x \in R^{(1)}\}$, where e is the neutral element in T, and is isomorphic to $R^{(1)}$. Lemma 3.3.2 can be generalized as follows :

<u>Lemma</u> 3.6.1. $\phi(\Gamma_A)/\phi(\Gamma_k)$ <u>is canonically isomorphic to an open subgroup of</u> T_A/T_k <u>of finite index</u> 2^i.

Just as in the proof of Lemma 3.3.2, one sees, by using Eichler's theorem, that $\phi(\Gamma_A) \cap T_k$ is the same as $\phi(\Gamma_k)$, and also that any $t \in T_A$ is in $\phi(\Gamma_A)$ whenever $t_v \in \phi(\Gamma_{k_v})$, i.e. whenever $\nu(t_v) \in N(R^*_{k_v})$, for every infinite place v of k. This proves the lemma, with $i = 0$, in the function-field case. In the number-field case, call S the set of the infinite places of k; put $Z^*_S = \prod_{v \in S} Z^*_{k_v}$; call $Z^*_{S,o}$ the connected component of the identity in Z^*_S, and put

$$Z^o_A = Z^*_{S,o} \times \prod_{p \notin S} Z^*_{k_p} \ ;$$

as Z^*_S is a product of factors $\underline{R}^*$, $\underline{C}^*$, the group $\gamma = Z^*_A/Z^o_A$ is a finite abelian group of type $(2,2,\dots,2)$; call σ the canonical homomorphism of Z^*_A onto γ. From the remarks made above and in the proof of Lemma 3.3.2, it follows that, if $t \in T_A$ is such that $\nu(t) \in Z^o_A$, t is in $\phi(\Gamma_A)$; therefore $\phi(\Gamma_A)$ contains the kernel of the homomorphism $\sigma \circ \nu$ of T_A into γ; as the index in our lemma is equal to the index of $\phi(\Gamma_A)T_k$ in T_A, this completes the proof.

(N.B. It has been shown by Serre and Tate that, if T is any torus over $\underline{Q}$ (the rational numbers), and $T^o_{\underline{R}}$ is the connected component of the identity in $T_{\underline{R}}$, then $T_{\underline{R}} = T^o_{\underline{R}} \cdot T_{\underline{Q}}$; from this one easily concludes, firstly (using the operation $R_{k/\underline{Q}}$) that, if T is a torus over a number-field k, and T^o_A is defined from T as Z^o_A was defined above from Z^*, $T_A = T^o_A \cdot T_k$, and, secondly, that the index 2^i in Lemma 3.6.1 has <u>always</u> the value 1).

Now we apply to the groups Γ, Γ', Γ_o the method used in 3.3. For each i, let ν_i be the norm in $(Z_i)_k = k_i$ over k (this is both the reduced norm and the regular norm in the sense of the theory of algebras); this can be extended to a norm mapping ν_i in Z_i (which is a polynomial function of degree $d_i = [k_i : k]$), which induces on Z^*_i a character, i.e. a representation of Z^*_i into G_m, rational over k; moreover, the group of all such characters of Z^*_i is generated by ν_i, and the group of all characters of $Z^* = \prod_i Z^*_i$, rational over k, is generated by the characters

$$z = (z_1, \dots, z_r) \to \nu_i(z_i) \ .$$

As μ is an isogeny of Z^* into T, one concludes from this (by well-known elementary arguments in the theory of algebraic toruses) that the group of the characters of T, rational over k, is generated by r characters χ_i, and that the characters $\chi_i \circ \mu$ of Z^* generate a subgroup of finite index of the similar group for Z^*. In other words, if we write

$$\chi_i(\mu(z)) = \prod_j \nu_j(z_j)^{a_{ij}} \ ,$$

with integers a_{ij}, we have $\det(a_{ij}) \neq 0$.

Now we need a Tamagawa measure for Γ_A. As Γ is isogenous to $R^* = \prod_i R^*_i$, we can use for Γ any set of convergence factors $(\lambda_v) = (\prod_i \lambda_v^{(i)})$, where $(\lambda_v^{(i)})$ is a set of convergence factors for $R^*_i = R_{k_i/k}(R'^*_i)$; such a set can be chosen at once, by Theorem 2.3.2 and the results of 3.3, by putting $\lambda_v^{(i)} = 1$ whenever v is an infinite place of k, and otherwise :

$$\lambda_p^{(i)} = \prod_{P/p} (1 - N(P)^{-1})$$

where the product is extended to all the prime divisors P of p in k_i, and the norm $N(P)$ is the absolute norm (equal to $N(p)^f$ if P is of relative degree f over p). For the same reasons, this same set of convergence factors can also be used for Z^*, hence also for Γ_o, and (by Lemma 3.3.1) for the torus T. On the other hand, the same argument shows that (1) is a set of convergence factors for $R^{(1)}$, hence for Γ', and also for G which is isogenous to $R^{(1)}$. We denote by $d''(x,t)$ the Tamagawa measure for Γ_A, with the set of convergence factors (λ_v), and use similar notations for Z^* and T.

Now we compute in two different ways the integral

$$I = \int_{\Gamma_A/\Gamma_k} F(|\chi_1(t)|,\dots,|\chi_r(t)|)d''(x,t) ;$$

here $| \ |$ denotes as usual the idele-module, and F is an arbitrary function (say, continuous with compact support) on the group $(\underline{\underline{R}}_+)^r$; we do this by using the two decompositions $G = \Gamma/\Gamma_o$ and $T = \Gamma/\Gamma'$; this will be carried out in the number-field case (the function-field case can be treated similarly, mutatis mutandis). The first decomposition gives :

(1) $$I = \tau(G) \int_{Z_A^*/Z_k^*} F((\prod_j |\nu_j(z_j)|^{a_{ij}})_{1\leq i\leq r})d''z$$

while the second one gives, since $\tau(\Gamma') = 1$:

(2) $$I = \int_{\phi(\Gamma_A)/\phi(\Gamma_k)} F(|\chi_1(t)|,\dots,|\chi_r(t)|)d''t .$$

For each i, we can identify $(Z_i^*)_A = (R_{k_i/k}(G_m))_A$ with $(G_m)_{A_{k_i}} = I_{k_i}$; therefore Z_A^* is the same as $\prod_i I_{k_i}$, while Z_k^* is the same as $\prod_i k_i^*$; and the idele-module $|\nu_i(z_i)|$, taken in I_k, is the same as the idele-module $|z_i|_i$ taken in I_{k_i}. From these facts, and from Theorem 3.1.1 (iii), we conclude that we have

$$\int_{Z_A^*/Z_k^*} f(|\nu_1(z_1)|,\dots,|\nu_r(z_r)|)d''z = (\prod_{i=1}^r \rho_{k_i}) \int_{(\underline{\underline{R}}_+)^r} f(\theta_1,\dots,\theta_r)d\theta_1\dots d\theta_r/\theta_1\dots\theta_r$$

whenever f is such that the right-hand side is absolutely convergent. This gives for (1) the value :

(3) $$I = \tau(G)|\det(a_{ij})|^{-1}(\prod_i \rho_{k_i}) \int_{(\underline{\underline{R}}_+)^r} F(\theta_1,\dots,\theta_r)d\theta_1\dots d\theta_r/\theta_1\dots\theta_r .$$

As to (2), we apply Lemma 3.6.1, together with the following remark : for every $t\in T_A$, there is $(x',t')\in\Gamma_A$ such that $|\chi_i(t^{-1}t')| = 1$ for $1\leq i\leq r$ (in fact, it is easily seen that we can take $x' = z$, $t' = \mu(z)$, for a suitable $z\in Z_A^*$); therefore, we can choose, as representatives of the 2^i cosets of $\phi(\Gamma_A)T_k$ in T_A, elements t such that $|\chi_i(t)| = 1$ for all i. From this, one concludes that the integral in the right-hand side of (2), taken over every one of the 2^i cosets of $\phi(\Gamma_A)/\phi(\Gamma_k)$ in T_A/T_k, has always the same value. Therefore :

(4) $$I = 2^{-i} \int_{T_A/T_k} F(|\chi_1(t)|,\dots,|\chi_r(t)|)d''t .$$

The comparison between (3) and (4) shows that (apart from the determination of the index 2^i, which is effected by the result of Serre and Tate) the computation of $\tau(G)$ has been reduced to a purely commutative problem concerning the torus T, viz. the computation of the integral in (4).

This problem has been studied by Ono (Ann. of Math. 1961) but is not yet completely solved. Before making some applications of the results obtained above to the orthogonal groups, we insert a few general remarks about toruses.

Let T be any torus over k; by Theorem 2.2.2, its characters (i.e., its representations into G_m over the universal domain) make up a finitely generated free abelian group (free, because T is here assumed to be algebraically connected), on which the Galois group $\mathfrak{G}$ of $\bar{k}/k$ ($\bar{k}$ = algebraic closure of k) operates in an obvious manner (actually, every character of T is defined over a separably algebraic extension of k). This group, written additively and considered as a representation-module for $\mathfrak{G}$, is denoted by $\hat{T}$ and is known as the dual module of T; Tate has shown that there is a duality of the usual type between such modules and toruses over k. We write $\hat{T}_k$ for the group of the elements of $\hat{T}$ which are invariant under $\mathfrak{G}$ (these correspond to the characters of T which are defined over k). Let Ψ be the trace of the representation of $\mathfrak{G}$ (with coefficients in $\mathbb{Q}$) given by the operation of $\mathfrak{G}$ on the vector-space $\hat{T}\otimes\mathbb{Q}$ over $\mathbb{Q}$; according to Artin, there belongs to the "character" Ψ of $\mathfrak{G}$ an L-function $L(s,\Psi)$, which has at $s=1$ a pole of order r if r is the number of generators for $\hat{T}_k$; this L-function is given by an infinite product

$$L(s,\Psi)=\prod_p L_p(s,\Psi)$$

taken over all the p-adic valuations of k. Now, combining Theorems 2.3.2 and 2.4.3 with a theorem of Artin on rational representations of finite groups, we see that, by putting $\lambda_v=1$ for $v\in S$, $\lambda_p=L_p(1,\Psi)$ for $p\notin S$ (as usual, S is a finite set of valuations of k containing all the infinite places), we define a set of convergence factors for T. If

$\tilde{d}t$ is the Tamagawa measure constructed by means of that set, we have a formula

$$\int_{T_A/T_k} F(|\chi_1(t)|,\dots,|\chi_r(t)|)\tilde{d}t = c\int_{(\mathbb{R}_+)^r} F(\theta_1,\dots,\theta_r)d\theta_1\dots d\theta_r/\theta_1\dots\theta_r$$

in the number-field case (the integral in the right-hand side is to be replaced by a series, in the usual manner, in the function-field case); here $\chi_1,\dots,\chi_r$ are generators for the group of characters of T, defined over k; moreover, if we put

$$\rho = \left[(s-1)^r\prod_{p\notin S} L_p(s,\Psi)\right]_{s=1}$$

the constant $r(T)=c/\rho$ is independent of the choice of S and of the generators χ_i and is invariantly attached to the torus T; it has obvious "functorial" properties such as $r(T_1\times T_2) = r(T_1)r(T_2)$, and $r(R_{k'/k}T')=r(T')$ if T' is a torus over k'.

If now notations are again as in (3) and (4), our results (taking into account the theorem of Serre and Tate) give $\tau(G) = r(T)|\det(a_{ij})|$. This raises the question whether, at least for toruses isogenous to Z^*, the number $r(T)$ is always an integer.

3.7. Application to some orthogonal and hermitian groups.

In view of the well-known "canonical isomorphisms" between classical groups, the Tamagawa numbers for the orthogonal groups in 3 and 4 variables and for the hermitian groups in 2 variables can be calculated by means of the above results; this will provide the starting point for the consideration of the orthogonal groups, by induction on the number of variables, in Chapter IV. We avoid complications by excluding once for all the case of characteristic 2 (there is, however, no reason for thinking that our main results do not remain true even in that case). A quadratic form F, with coefficients in k, is said to be of index 0 if it "does not represent" 0, i.e. if $F(x) = 0$ has no solution in k, other than 0.

(a) <u>Orthogonal group in 3 variables</u> : Let F be a quadratic form in 3 variables, and G the "special" orthogonal group of F ("special" = determinant 1): then G is isomorphic to the projective group of a simple central algebra of dimension 4. viz. a quaternion algebra if F is of index 0, and the matrix algebra M_2 otherwise; by Theorem 3.2.1 in the former case, and by Theorem 3.3.1 in the latter case, we have $\tau(G) = 2$.

(b) <u>Hermitian group in 2 variables</u> : let k' be a quadratic extension of k; take Z' over k', such that $Z'_{k'} = k'$; take $D' = Z'$, $R' = M_2(Z')$, $Z = R_{k'/k}(Z')$, $R = R_{k'/k}(R') = M_2(Z)$, so that $R_k = (M_2)_{k'}$. The non-trivial automorphism $z \to \bar{z}$ of k' over k can be extended in an obvious manner to an automorphism of the algebra variety Z, defined over k, which we also denote by $z \to \bar{z}$, and then to an automorphism $X \to \bar{X}$ of R, defined over k. We can identify G_m with the subgroup of Z^* defined by $z = \bar{z}$: the norm mapping of Z^* into G_m can then be written as $z \to z\bar{z}$. and its kernel is the subgroup U of Z^* defined by $z\bar{z} = 1$. Now let S be an invertible hermitian matrix over k'. i.e. an element of $R^*_k = (M_2)_{k'}$ such that ${}^t\bar{S} = S$: this determines the hermitian form $F(x) = {}^t\bar{x} \cdot S \cdot x$ on the space Z^2 of vectors $x = \binom{x_1}{x_2}$ over Z; F is said to be of index 0 if $F(x) = 0$ has no solution in $Z^2_k = k'^2$, other than 0. The hermitian (or "unitary") group attached to S, or to $F(x)$, is the subgroup G of R^* given by :

$$G = \{X \in R^* \mid {}^t\bar{X} \cdot S \cdot X = S,\ N(X) = 1\}$$

where $N(X) = \det(X)$ is the reduced norm taken in R over Z.

It is known that G is isomorphic to the special linear group

$R_1^{(1)}$ of a simple central algebra R_1 of dimension 4 over k. viz. a quaternion algebra if F is of index 0, and the matrix algebra M_2 otherwise. Therefore $\tau(G) = 1$.

(c) <u>Orthogonal group in 4 variables</u> : let F be a quadratic form over k, in 4 variables, Δ its discriminant, G the "special" orthogonal group for F. If $\Delta^{\frac{1}{2}} \in k$, there is an algebra R_1 of dimension 4 (a quaternion algebra if F is of index 0, otherwise the matrix algebra M_2) such that $G = (R_1^{(1)} \times R_1^{(1)})/\gamma$, where γ is the subgroup of order 2 consisting of the elements $(1,1)$, $(-1,-1)$. With the notations used in 3.6, this can be written as $G = \Gamma/\Gamma_0$ when we take $R_1 = R_2$, $R = R_1 \oplus R_2$, hence $Z^* = G_m \times G_m$, $N(z) = z^2$, $T = G_m \times G_m$, $\mu(z) = (z_1 z_2, z_1^{-1} z_2)$ for $z = (z_1, z_2) \in Z^*$, and $\nu(t) = (t_1 t_2^{-1}, t_1 t_2)$ for $t = (t_1, t_2) \in T$. The integral in (4) can be calculated by Theorem 3.1.1 (iii) and has the value

$$\rho_k^2 \int_{(\underline{R}_+)^2} F(\theta_1, \theta_2) d\theta_1 d\theta_2 / \theta_1 \theta_2 \ ;$$

also, one finds at once that $2^i = 1$, $|\det(a_{ij})| = 2$. This gives $\tau(G) = 2$.

Now assume that $k' = k(\Delta^{\frac{1}{2}})$ is a quadratic extension of k. Then G is isogenous to $R_{k'/k}(R'^{(1)})$, where R' is a central simple algebra of dimension 4 over k' (again a quaternion algebra or M_2 according as F is of index 0 or not); over k', it becomes isomorphic to $(R'^{(1)} \times R'^{(1)})/\gamma$, with γ as above. Let Z', Z, U and the mapping $z \to \bar{z}$ be defined as in (b). Then we can write G, with the notations of 3.6, as $G = \Gamma/\Gamma_0$ for $r = 1$, $k_1 = k'$, $R'_1 = R'$, $R_1 = R$, $N(z) = z^2$, $T = G_m \times U$, $\mu(z) = (z\bar{z}, z^{-1}\bar{z})$ for $z \in Z^*$, $\nu(t) = (t_1 t_2^{-1}, t_1 t_2)$ for $t = (t_1, t_2)$, $t_1 \in G_m$, $t_2 \in U$. We have now $a_{11} = 1$, $2^i = 1$. Now we have to calculate (4) for $T = G_m \times U$. As we take our Tamagawa measure for G_m by means of the factors $\lambda_p = 1 - N(p)^{-1}$, and for Z^* and T by means of the factors

$$\lambda'_p = \prod_{p'/p} (1 - N(p')^{-1})$$

where the product is taken over the prime divisors p' of p in k', we have to take the Tamagawa measure on $U = T/G_m$ by means of the factors

$$\lambda''_p = \lambda_p^{-1}\lambda'_p = 1 - \chi(p)N(p)^{-1}$$

where χ is the character associated with the quadratic extension k' of k. Applying now Theorem 2.4.3 and Theorem 2.4.4 (the latter, in the modified form explained in the Remark following it) to the groups Z^*, U, $G_m = Z^*/U$ and to the norm mapping $z \to z\bar{z}$ of Z^* onto G_m, we get

$$(5) \qquad \tau'(U) \cdot \int_{H'_A/H'_k} F(|y|)d'_A y = \int_{Z^*_A/Z^*_k} F(|z\bar{z}|)d'_A z$$

where H'_A, H'_k are the images of Z^*_A, Z^*_k under the norm mapping, $\tau'(U) = \int_{U_A/U_k} d'_A u$, and $d'_A z$, $d'_A y$, $d'_A u$ are the Tamagawa measures for Z^*, G_m, U constructed by means of the sets λ'_p, λ_p, λ''_p defined above. In the right-hand side of (5), Z^*_A, Z^*_k may be identified with $I_{k'}$ and with k'^*; as $|\;|$ is the idele-module taken in I_k, $|z\bar{z}|$ is then the same as the idele-module taken in $I_{k'}$; therefore the right-hand side of (5), computed by Theorem 3.1.1 (iii), is

$$\rho_{k'} \int_0^\infty F(t)dt/t \ .$$

On the other hand, by class-field theory, H'_A/H'_k, in the left-hand side, is nothing else than the open subgroup of I_k/k^* of index 2 determined by $\chi(y) = 1$, where χ is the character of I_k/k^* belonging to the quadratic extension k'/k. Therefore the integral in the left-hand side has

the value

$$\tfrac{1}{2}\rho_k \int_0^\infty F(t)dt/t \ .$$

This gives $\tau'(U) = 2\rho_{k'}/\rho_k$ (which can also be written as $\tau'(U) = 2L(1,\chi)$). As the integral in (4) has the value

$$\tau'(U) \int_{I_k/k^*} F(|x|)(dx/x)' = \tau'(U)\rho_k \int_0^\infty F(t)dt/t \ ,$$

we get, as before, $\tau(G) = 2$:

Theorem 3.7.1. The Tamagawa number of all special orthogonal groups in 3 and 4 variables has the value 2.

3.8. The zeta-function of a central simple algebra.

We have already twice made use of results in class-field theory (in the latter part of 3.8, and implicitly by using Eichler's norm theorem in the proof of Lemmas 3.3.2 and 3.6.1); we shall also use such results freely in our treatment of the classical groups in Chapter IV, both directly and by our use of Hasse's theorem on quadratic forms (which can be derived formally from the norm theorem for quaternion algebras). It is known, on the other hand, that most of these results can be derived from Hasse's theorem according to which "a central simple algebra which splits locally everywhere splits globally". This will now be proved by a more precise calculation of "the" zeta-function of an algebra (independently of our use of class-field theory in 3.3, 3.6, 3.8). It is therefore likely that, by following up this idea, our treatment could be rendered completely self-contained.

The multiplicative calculation of $Z^\Phi(s)$ for a division algebra in 3.1 can be extended to any central simple algebra; this will be done (following Fujisaki) for a special choice of Φ.

Let R be an algebra-variety over k, with the center Z, such that $Z_k = k$ and that R_k is a simple algebra; let n^2 be the dimension of R (equal to the dimension of R_k over k). Take a basis $(\alpha_i)_{1 \leq i \leq n^2}$ of R_k over k. As we have observed before, there is S such that, for $p \notin S$, R_{k_p} is isomorphic to $M_n(k_p)$ and $\underline{O}_p = \Sigma_i \alpha_i \underline{o}_p$ is a maximal order of R_{k_p}, isomorphic to $M_n(\underline{o}_p)$ (this follows from the consideration of the discriminant). For every v, R_{k_v} is isomorphic to a matrix algebra $M_{m_v}(D'_v)$ over a central division algebra D'_v over k_v; we call r_v^2 the dimension of D'_v over k_v, so that $n = m_v r_v$. For each $p \in S$ we select a maximal order $\underline{O}_p$ of R_{k_p}; this is isomorphic to $M_{m_p}(\underline{o}'_p)$, where $\underline{o}'_p$ is the maximal order of D'_p. For every p, we denote by π' a prime element of $\underline{o}'_p$ (a generator of the maximal two-sided ideal in $\underline{o}'_p$); by the theory of p-adic algebras, this can be done in such a way that $\pi = \pi'^{r_p}$ is a prime element of $\underline{o}_p$.

<u>The</u> zeta-function of R is defined as

$$Z(s) = \int_{R_A^*} |N(x)|^s \Phi(x)\omega'_A \tag{1}$$

where ω'_A, as before, is the Tamagawa measure for R^* with the convergence factors $1 - N(p)^{-1}$, and $\Phi(x) = \prod_v \phi_v(x_v)$ for $x = (x_v) \in R_A$, the ϕ_v being defined as follows. For $p \notin S$, ϕ_p is the characteristic function of $\underline{O}_p$. For $p \in S - S_o$, where S_o is the set of the infinite places of k (the empty set in the function-field case), ϕ_p is the characteristic function of $\pi'^{a(p)}\underline{O}_p$, where $a(p)$ is any integer (for $p \notin S$, we put $a(p) = 0$). For $v = v_\lambda \in S_o$, we have $k_\lambda = \underline{R}$ or $\underline{C}$ (we write k_λ instead of k_{v_λ}, etc.), with $k_\rho = \underline{R}$ for $1 \leq \rho \leq r_1$, $D'_\rho \cong \underline{R}$ or $\underline{K}$ ($\underline{K}$ = quaternion algebra over $\underline{R}$), $k_\iota = \underline{C}$ for $r_1 + 1 \leq \iota \leq r_1 + r_2$, $D'_\iota \cong \underline{C}$. Let Tr be the reduced trace in R_k over k, which we extend as usual to R, and to R_{k_v} for each v. For each $v_\lambda \in S_o$, choose a positive involution $x \to \bar{x}$ in R_λ, i.e. an involutory antiautomorphism such that $Tr(\bar{x}x) > 0$ for $x \neq 0$; this can be done by transporting to R_λ, by means of some isomorphism of R_λ with $M_{m_\lambda}(D'_\lambda)$, the involution $X \to {}^t\bar{X}$ (here ${}^tX$ is the transpose, and $z \to \bar{z}$ is the identity in $\underline{R}$, the complex conjugate in $\underline{C}$, the quaternion conjugate in $\underline{K}$). Now we take

$$\phi_\lambda(x) = \exp(-A_\lambda Tr(\bar{x}x)) ,$$

where A_λ is any constant > 0. It will be seen that the choice of S, of the integers $a(p)$, and of the constants A_λ does not affect "the" zeta-function except for an inessential factor.

We have, by definition,

$$\omega'_A = \mu_k^{-n^2} \prod_v \lambda_v^{-1}\omega_v$$

with $\lambda_v = 1$ for $v \in S_o$, $\lambda_p = 1 - q^{-1}$, $q = N(p)$, for $p \notin S_o$, and

$$\omega_v = |N(x_v)|_v^{-n} (\prod_i dt_i)_v$$

for $x_v = \Sigma_i \alpha_i t_i$, $t_i \in k_v$. Just as in 3.1, we find

$$Z(s) = \mu_k^{-n^2} \prod_v Z_v(s) \ , \ Z_v(s) = \lambda_v^{-1} \int_{R_{k_v}^*} |N(x_v)|_v^s \phi_v(x_v)\omega_v . \tag{2}$$

In order to calculate $Z_p(s)$ for a given $p \notin S_o$, write a, r, m instead of $a(p)$, r_p, m_p. Identifying R_{k_p} with $M_m(k_p)$; we have

$$Z_p(s) = (1-q^{-1})^{-1} \int_\Omega |N(x)|_p^s \omega_p \ , \ \Omega = M_m(D'_p)^* \cap \pi'^a M_m(\underline{o}'_p) . \tag{3}$$

Let U be the set of the invertible matrices in the ring $M_m(\underline{o}'_p)$; Ω is the disjoint union of cosets $U \cdot \pi'^a A$, if one takes for A the same matrices as in 3.1, except that π' has now to be substituted for π, and that α_{ij} has now to run through a complete set of representatives of $\underline{o}'_p$ modulo π'^{d_j}. As ω_p is an invariant measure in the multiplicative group $R^*_{k_p}$, the integral in (3), taken over $U\cdot\pi'^{a}A$, has the value $|N(\pi'^{a}A)|_p^s\int_U\omega_p$. Here $|N(\pi'^{a}A)|_p$ is easily computed by remembering that the regular norm in R is $N(x)^n$, and that π'^r is a prime element of $\underline{o}_p$; one finds $|N(\pi'^{a}A)|_p = q^{-N}$ with $N = \Sigma_i d_i + ma$. Also, the number of matrices A for given values of the d_i is q^M with $M = r\Sigma_i(i-1)d_i$. This gives

$$Z_p(s) = (1-q^{-1})^{-1}q^{-mas}\prod_{i=o}^{m-1}(1-q^{ri-s})^{-1}\int_U\omega_p .$$

In order to compute the last integral, we change from the basis (α_i) to a basis (β_i) of $M_m(\underline{o}'_p)$ considered as an $\underline{o}_p$-module; for $x = \Sigma_i\alpha_i t_i = \Sigma_i\beta_i u_i$, $\beta_i = \Sigma_j n_{ij}\alpha_j$, $n_{ij}\in k_p$, we get :

$$\int_U\omega_p = \int_U(\prod_i dt_i)_p = |\det(n_{ij})|_p\int_U(\prod_i du_i)_p .$$

If we put $d = \det(\mathrm{Tr}(\alpha_i\alpha_j))$, $d' = \det(\mathrm{Tr}(\beta_i\beta_j))$, where Tr is as before the reduced trace in $M_m(D'_p)$ over k_p, we have, by the theory of the different in p-adic algebras, $|d'|_p = q^{n(m-n)}$; since $d^{-1}d' = \det(n_{ij})^2$, this gives the value of $|\det(n_{ij})|_p$. Finally, $\underline{o}'_p/\pi'\underline{o}'_p$ is the finite field with q^r elements, and a matrix in $M_m(\underline{o}'_p)$ is in U if and only if its reduction modulo $\pi'\underline{o}'_p$ is a matrix of non-zero determinant over that field; the number of such matrices is

$$\nu = (q^{rm}-1)(q^{rm}-q^r)\dots(q^{rm}-q^{r(m-1)}) ,$$

and $\int_U(\prod_i du_i)_p$ has the value $q^{-rm^2}\nu$. Thus :

$$Z_p(s) = |d|_p^{-\frac{1}{2}}\, q^{-mas-n(n-m)/2}(1-q^{-1})^{-1}\prod_{i=o}^{m-1}\frac{1-q^{ri-n}}{1-q^{ri-s}}$$

For $p\notin S$, we have $a=0$, $m=n$, $r=1$. This shows that $\prod_p Z_p(s)$ is absolutely convergent for $\mathrm{Re}(s)>n$.

Now we calculate the $Z_\lambda(s)$: we identify R_λ with $M_m(D_\lambda)$, writing again m, r for m_λ, r_λ; also, put $\rho = [k_\lambda:\underline{R}]$. As $R_\lambda - R^*_\lambda$ is of measure 0, we have

$$Z_\lambda(s) = \int_{R_\lambda}\exp(-A_\lambda\mathrm{Tr}({}^t\bar{X}\cdot X))|N(X)|_\lambda^s\omega_\lambda ;$$

we recall that N and Tr mean the reduced norm and trace in R_λ over k_λ, and, if $z\in k_\lambda$, $|z|_\lambda$ means $|z|^\rho$ if $|\ |$ is the "usual" absolute value. Use the "Iwasawa decomposition" $X = UDT$, where ${}^t\bar{U}\cdot U = 1_m$, $D = \mathrm{diag}(\delta_1,\dots,\delta_m)$ is the diagonal matrix with the elements $\delta_i>0$, and $T=(t_{ij})$ is triangular ($t_{ij}=0$ for $i>j$, $t_{ii}=1$ for $1\le i\le m$). Then, if dU, dD, dT denote Haar measures on the groups $\{U\}$, $\{D\}$, $\{T\}$ one sees at once that a Haar measure on R_λ must be of the form $f(D)dUdDdT$; here we can take for dT the additive Haar measure in the space of the vectors $(t_{ij})_{i<j}$, i.e. $dT = \prod_{i<j}d^+t_{ij}$ if d^+t is the measure in the additive group D'_λ; and we can take $dD = \prod_i(d\delta_i/\delta_i)$. Expressing now that $f(D)dUdDdT$ is invariant under $X\to XD_o$, i.e. under $(U,D,T)\to(U,DD_o,D_o^{-1}TD_o)$, we see that f, up to a constant factor, must be given by

$$f(D) = \prod_i \delta_i^{r^2\rho(m-2i+1)}$$

Also, we have

$$|N(X)|_\lambda = |N(D)|_\lambda = \prod_i\delta_i^{r\rho}$$

$$\mathrm{Tr}({}^t\bar{X}\cdot X) = r\sum_{i=1}^m\delta_i^2(1+\sum_{j=i+1}^m\bar{t}_{ij}t_{ij}) .$$

As ω_λ is a Haar measure on R_λ^*, one finds now immediately

$$Z_\lambda(s) = C_\lambda A_\lambda^{-\rho ns/2} \prod_{i=0}^{m-1} \Gamma(\tfrac{1}{2}r\rho(s-ri))$$

where C_λ is a constant factor, which can be computed by calculating $Z_\lambda(n)$; this is easily done by changing the basis (α_i) for a basis adapted to the identification $R_\lambda = M_m(D_\lambda')$; one finds

$$Z_\lambda(n) = |d|_\lambda^{-\frac{1}{2}} (A_\lambda/\pi r\rho)^{-\rho n^2/2} .$$

In view of the product formula $\prod_v |d|_v = 1$, the product for $Z(s)$ does not contain d, as was to be expected ($Z(s)$ cannot depend upon the choice of the basis (α_i)).

Now we prove :

Theorem 3.8.1. Let R_k be a central simple algebra over k. If, for every valuation v of k, R_{k_v} is isomorphic to a matrix algebra over k_v, R_k is isomorphic to a matrix algebra over k.

The calculation given above shows that, except for a factor of the form $C_1C_2^s$, with constant C_1, C_2, "the" zeta-function of R depends only upon the "ramification indices" r_v; in particular, if R "splits everywhere", i.e. if $r_v = 1$ for all v, we have

$$Z(s) = C_1C_2^s \prod_{i=0}^{n-1} F(s-i)$$

with

$$F(s) = \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \zeta_k(s) ;$$

in particular, for $n = 1$, we see that $F(s)$ is "the" zeta-function of k itself.

In order to prove our theorem, it is clearly enough to show that a central division algebra over k, other than k, cannot "split

everywhere", i.e. that this $Z(s)$ cannot be the zeta-function of a division algebra unless $n = 1$. In fact, the additive calculation in 3.1 has shown that, for such an algebra, $Z(s)$ has no other poles than $s = 0$ and $s = n$ on the real axis; in particular, $F(s)$ has the poles $s = 0$, $s = 1$. The above formula shows now that $Z(s)$ has simple poles at $s = 0$, $s = n$, and double poles at $s = 1, \ldots, n-1$; therefore $n = 1$.