Journal of the Mathematical Society of Japan Vol. 9, No. 3, July, 1957

L-functions of number fields and zeta functions of abelian varieties.

by Yutaka TANIYAMA

(Received Feb. 20, 1957)

Introduction.

It was found out in several cases that Hasse's zeta functions of algebraic curves or of abelian varieties over an algebraic number field can be expressed by Hecke's L-functions with " Grössencharaktere " of that field.[1] It deserves our attention that these phenomena have always presented themselves in connection with arithmetic of abelian extensions of that number field. However, since the relation of Hasse's functions with abelian extensions was not so direct in the proofs of these results, which have been done from different angles, it would be desirable to clearify the relation between Hasse's functions and abelian extensions attached to abelian varieties in question, treating all cases from a unified point of view. This is the first problem. In pursuing this problem, I have succeeded in obtaining a new interpretation of Hasse's functions in general, and in characterizing under which particular conditions the above phenomena take place.

On the other hand, " Grössencharaktere " can be interpreted as characters of idèle class groups, so it seems natural that they have some connection with abelian varieties related to abelian extensions of the basic fields. However, as class field theory shows, it is not the idèle class group, but the factor group of it by the connected component of the identity, that can be interpreted by the Galois group of the maximally abelian extension. The above phenomena suggest conversely the possibility of an interpretation of characters of idèle class group by something connected with abelian extensions. To find out such an interpretation is a problem, first proposed by A. Weil [4], which seems no less important than the above.

[1] Weil [9], Deuring [1], Taniyama [3]. There are also cases first treated by Eichler, where this does not hold.

I shall solve .this last problem in this paper for a special type of characters, called characters of type (A_0) by A. Weil [4]. The problem of interpretation of characters which are not of type (A_0) has a quite different feature, and will be entirely left open. The characters of type (A_0) correspond to certain representations of the Galois group of the maximally abelian extension of the basic field, and can be characterized by some properties of these representations. On the other hand, we can compute the zeta function of an abelian variety with the help of certain representations of the Galois group of the field obtained by division of periods of this abelian variety. When this variety has sufficiently many complex multiplications, these ıepresentations have the properties characterizing characters of type (A_0). This gives a proof of the conjecture of Hasse in case of complex multiplications, under somewhat weaker conditions than in my former paper [3]. This theory reveals more intimate relation of Hasse's functions, "Grössencharaktere" of type (A_0) and abelian extensions.

Moreover, the above relation between representations of the Galois groups and of the general Hasse's functions gives a new relation between these functions and the zeta functions of infinitely many finite extensions of the basic field. This relation holds for a little more general type of L-functions, including L-functions with characters of type (A_0), and may be considered to express, in a sense, the decomposition law of prime ideals in the infinitely many fields attached to these functions.

All this shows furthermore that Hasse's zeta functions of general abelian varieties are closely connected with the infinite normal, non-abelian extensions obtained by division of periods of these varieties. Hence these functions may have a quite different nature from those in our special cases, and we still stand far from the solutions of Hasse's conjecture in the general case, although these normal extensions have some remarkable properties as expressed in our axioms below.

The main method used in the present paper is due to A. Weil [4], where he has shown that we can associate to every character of type (A_0) a system of local representations (i. e. representations into $\mathfrak{P}$-adic completions of a number field) of the idèle class group. This idea of local representation is a quite adequate one, because, first, we can pass from idèle class group to the Galois group very naturally by its means, and second, the Galois group and $\mathfrak{P}$-adic unit group have similar topologies, while the usual character of the Galois group is necessarily of finite order. Moreover, we can connect these local representations with "l-adic representations" of the ring of endomorphisms of abelian varieties, which is the essential base of the proof of conjecture of Hasse in the present paper.

In § 1, I shall give a characterization of characters of idèle class groups of type (A_0). In § 2, the above mentioned relation of L-functions with characters of type (A_0) and an infinite product of zeta functions of number fields will be given. In § 3, I shall first reformulate the result in § 1 in a form which may be applied directly to the proof of conjecture of Hasse. This reformulation allows moreover a generalization, and an infinite product relation like that in § 2 for the generalized L-function will be obtained. In § 4, it will be shown that this generalization contains the case of Hasse's zeta functions of general abelian varieties. § 4 implies furthermore the proof of the conjecture of Hasse in case of sufficiently many complex multiplications mentioned above.

Notations and terminologies. Basic results assumed to be known.

The following notations and terminologies will be used throughout the paper, often without references. As to the basic concepts discussed here, the reader is referred to Weil's papers [4], [6]. Terminologies and basic notations concerning algebraic geometry used in § 4 will be the same as those of so-called Weil-school in algebraic geometry. As to basic results recalled in § 4, see Weil [7], [8], Shimura [2] and Taniyama [3].

$\boldsymbol{Q}$ denotes the rational number field, $\boldsymbol{R}$ the real number field, $\boldsymbol{C}$ the complex number field and $\boldsymbol{Z}$ the ring of rational integers. $|\alpha|$ denotes the usual absolute value of a complex number α. σ_0 denotes the complex conjugate automorphism of $\boldsymbol{C}$, or of any subfield of $\boldsymbol{C}$: $\sigma_0\alpha=\overline{\alpha}$, $\alpha\in\boldsymbol{C}$.

If M is a square matrix, *detM* denotes the determinant of M. E denotes always a unit matrix. The degree of E will be clear from the context.

All groups treated in this paper are considered as topological groups with their proper topologies, maybe discrete. The words isomorphism, homomorphism, representation of groups are accordingly used in the sense of topological groups. In particuar, ***representation*** means an algebraic homomorphism which is continuons. The word ***character*** is used ***in the wider sense***, i. e. representation into the multiplicative group $\boldsymbol{C}^*$ of $\boldsymbol{C}$.

Let k be a field. Then k^* denotes the multiplicative group of all non-zero elements of k. $\overline{k}$ denotes the algebraic closure of k, and A_k the maximal abelian extension of k in $\overline{k}$. If k' is a Galois extension of k (finite or infinite), then $G(k'/k)$ denotes the Galois group of k' over k, endowed with Krull's topology. In particular, we write $G_k=G(A_k/k)$: the Galois group of the maximal abelian extension of k over k. If k' is a finite extension of k, $N_{k'/k}$ denotes the relative norm from k' to k, and $[k':k]$ the degree of k' over k.

Algebraic number field is always considered as contained in $\boldsymbol{C}$.

Let k be an algebraic number field of finite degree. Then $H(k)$ denotes the set of all isomorphisms of k into $\boldsymbol{C}$. If k' is a finite extension of k, $H(k'/k)$ denotes the set of all isomorphisms of k' into $\boldsymbol{C}$ over k. N denotes always the absolute norm of ideals. For any α in k^*, (α) denotes the principal ideal of α. Let $\mathfrak{m}$ be an integral ideal of k. Then $G(\mathfrak{m})$ denotes the group of all ideals of k, prime to $\mathfrak{m}$. Let K be also an algebraic number field, then the ***Galois closure*** of k and K means the smallest absolutely normal field in $\boldsymbol{C}$, containing k and K. Let k' be any normal extension of k, and ψ^* be a representation of the group $G(k'/k)$ into some group. The kernel of ψ^* being a closed subgroup of $G(k'/k)$, it corresponds to a subfield of k' containing k, by Galois theory. k' being as above, let $\mathfrak{P}$ be a prime divisor in k' of a prime ideal $\mathfrak{p}$ of k. Then the ***decomposition group*** of $\mathfrak{P}$ over k (consisting of all σ in $G(k'/k)$ such that $\sigma\mathfrak{P}=\mathfrak{P}$) is denoted by $G(\mathfrak{P})$. We shall denote by $\sigma_{\mathfrak{P}}$ any one of the ***Frobenius automorphisms*** of $\mathfrak{P}$ over k, i. e. $\sigma_{\mathfrak{P}}$ is an element in $G(\mathfrak{P})$ inducing on the residue field of k' mod. $\mathfrak{P}$ the automorphism $\xi\rightarrow\xi^{\mathrm{N}\mathfrak{p}}$. If $G(k'/k)$ is abelian, we can write $\sigma_{\mathfrak{p}}$ instead of $\sigma_{\mathfrak{P}}$. ***Inertia group*** of $\mathfrak{p}$ over k is the subgroup of $G(\mathfrak{P})$ consisting of all σ in $G(\mathfrak{P})$ which induce the identity antomorphism on the residue field. Then $\mathfrak{p}$ is said to be ***unramified*** in k' if the group $G(\mathfrak{P})$ operates faithfully on the residue field of k' mod. $\mathfrak{P}$, i. e. the inertia group of $\mathfrak{P}$ is the identity. ψ^* being as above, $\mathfrak{p}$ is unramified in the field corresponding to the kernel of ψ^* if and only if $\psi^*(\sigma_{\mathfrak{P}})$ does not depend on the choice of $\sigma_{\mathfrak{P}}$ for any one of $\mathfrak{P}$. Let S be a set of ideals in k. Then the word *density* of prime ideals in S is used in Kronecker's sense, i. e. it means the limit

$$\Delta(S)=\lim_{s\to 1+0}\left(-\sum N\mathfrak{p}^{-s}/\log(s-1)\right),$$

if this limit exists, the sum $\sum N\mathfrak{p}^{-s}$ being taken over all prime ideals $\mathfrak{p}$ in S. The density of the set of all prime ideals of the first degree is 1. Also, the density of prime ideals in each ideal class modulo an integral ideal $\mathfrak{m}$ ("Strahlklasse" mod. $\mathfrak{m}$) is definite, and equal for all classes. Now, Tschebotareff's density theorem asserts that, for any finite normal extension k'' of k, and for any element σ in $G(k''/k)$, the density of the prime ideals $\mathfrak{p}$ of k of the first degree such that σ is a Frobenius automorphism of a prime divisor of $\mathfrak{p}$ in k'', is definite and positive. The word *almost all*, used for a set of ideals in k, means "all but a finite number of". Then *the set of all $\sigma_{\mathfrak{P}}$ for all prime divisors $\mathfrak{P}$ of almost all prime ideals $\mathfrak{p}$ of the first degree in k is everywhere dense in $G(k'/k)$*, as is immediately seen from Tschebotareff's density theorem.

$\mathfrak{p}, \mathfrak{l}, \mathfrak{h}_i$ *denote always prime ideals* in some algebraic number fields, and *corresponding latin letters p, l, h_i denote rational primes divisible respectively by* $\mathfrak{p}, \mathfrak{l}, \mathfrak{h}_i$, unless the other indications are explicitely given.

Let k be as above, and v be a valuation of k. Equivalent valuations will be considered as the same. k_v denotes the completion of k with respect to v, and v is considered to be extended to k_v. If v is discrete, we use $\mathfrak{p}$ to denote either the corresponding prime ideal in k, or valuation ideal in k_v, or equivalence class of v, and write $k_{\mathfrak{p}}$ instead of k_v. In particular, $\boldsymbol{Q}_p$ denotes a p-adic number field. The normalized exponential valuation corresponding to $\mathfrak{p}$ is denoted by $\nu_{\mathfrak{p}}$. Then, an element α in $k_{\mathfrak{p}}$ such that $\nu_{\mathfrak{p}}(\alpha)=0$ is called a *unit* in $k_{\mathfrak{p}}$, or $\mathfrak{p}$-*unit*. All $\mathfrak{p}$-units form a multiplicative group, the $\mathfrak{p}$-unit group, in $k_{\mathfrak{p}}^*$, which is denoted by $U_{\mathfrak{p}}$. Any element α such that $\nu_{\mathfrak{p}}(\alpha)\geqq 0$ is called $\mathfrak{p}$-integral. We define similarly units and integral elements in $\overline{\boldsymbol{Q}_p}$. *All congruences are used in the sense of valuation theory.*

Idèle group of k is denoted by I_k. There is a canonical isomorphism of the multiplicative group k^* into I_k, which is denoted by ι.

The ***principal idèle grovp*** ιk^* is denoted by P_k. The canonical isomorphism of $k_v{}^*$ into I_k is denoted by ι_v, and also by $\iota_{\mathfrak{p}}$ if v corresponds to $\mathfrak{p}$. C_k denotes the ***idèle class group*** I_k/P_k of k. D_k denotes the connected component of 1 in C_k. Then the factor group $C_k'=C_k/D_k$ is compact and totally disconnected. *Class field theory assures now the existence of canonical isomorphism of C_k' onto the Galois group G_k of A_k over k.* By this isomorphism, the image of $\iota_{\mathfrak{p}}(U_{\mathfrak{p}})$ into C_k' (by the natural homomorphism) corresponds to the inertia group of $\mathfrak{p}$, and the image of $\iota_{\mathfrak{p}}(\pi_{\mathfrak{p}}U_{\mathfrak{p}})$ into C_k' corresponds to the set of all the Frobenius automorphisms $\sigma_{\mathfrak{p}}$ of $\mathfrak{p}$, where $\pi_{\mathfrak{p}}$ denotes a $\mathfrak{p}$-prime element in k (i. e. $\nu_{\mathfrak{p}}(\pi_{\mathfrak{p}})=1$).

If an idèle a in I_k is written as $a=(a_v)$, a_v denotes the v-components of a. Let k' be a finite extension of k and $a'=(a'_{v'})$ be in $I_{k'}$. Then the ***norm*** $N_{k'/k}(a')$ of a' is defined by $N_{k'/k}(a')=(a_v)\in I_k$ such that $a_v=\prod N_{(v')}(a'_{v'})$, where the product is taken over all extensions v' of v to k', and $N_{(v')}$ denotes the norm of $k'_{v'}$ into k_v. (a) will denote the ideal of an idèle $a=(a_v)$ defined by $(a)=\prod\limits_{\mathfrak{p}}\mathfrak{p}^{\nu_{\mathfrak{p}}(a_{\mathfrak{p}})}$. Then for any a in I_k, the positive real number

$$||a||=\mathrm{N}((a))^{-1}\prod_{\lambda}|a_{v_\lambda}|^{\eta_\lambda}$$

is called the ***volume*** of a, where v_λ runs over all Archimedean v, and k_{v_λ} is identified with $\boldsymbol{R}$ or $\boldsymbol{C}$ as the case may be, and $\eta_\lambda=[k_{v_\lambda}:\boldsymbol{R}]$. Then we have $||\iota\alpha||=1$ for any α in k^*, so we can speak of volumes of idèle classes. C_k^0 denotes the subgroup of C_k of all elements with volume 1, then C_k is isomorphic to the direct product $\boldsymbol{R}\times C_k^0$ of C_k^0 and the additive group of $\boldsymbol{R}$.

Representation ψ of C_k is identified with representation of I_k induced by ψ, and, if ψ takes the value 1 on D_k, it is also identified with that of $C_k'=C_k/D_k$ induced by ψ. In this latter case, ψ determines also a representation of the Galois group G_k under the identification of C_k' with G_k by class field theory. This representation of G_k is denoted by ψ^*. Now, a representation ψ of C_k is called ***unramified at*** $\mathfrak{p}$ if $\psi(\iota_{\mathfrak{p}}(U_{\mathfrak{p}}))=1$. When $\psi(D_k)=1$, *ψ is unramified at $\mathfrak{p}$ if and only if $\psi^*(\sigma_{\mathfrak{p}})$ does not depend on the choice of* $\sigma_{\mathfrak{p}}$, i. e. $\mathfrak{p}$ is unramified in the field corresponding to the kernel of ψ^*. ψ is called unramified at real Archimedean v if $\psi(\iota_v(-1))=$*the identity element.*

As to the following, special references are made to Weil [4]. For any integral ideal $\mathfrak{m}$ in k, $I(\mathfrak{m})$ denotes the subgroup of I_k consisting of all $a=(a_v)$ such that $a_{\mathfrak{p}}=1$ for all prime factors $\mathfrak{p}$ of $\mathfrak{m}$, and $a_v=1$ for all Archimedean v. Then $I^0(\mathfrak{m})$ denotes the subgroup of $I(\mathfrak{m})$ consisting of all a in $I(\mathfrak{m})$ such that the ideal $(a)=1$. Then the factor group $I(\mathfrak{m})/I^0(\mathfrak{m})$ is canonically isomorphic to the ideal group $G(\mathfrak{m})$. Now let a representation ψ of C_k be unramified at all $\mathfrak{p}$ in $G(\mathfrak{m})$. Then ψ takes the value 1 on $I^0(\mathfrak{m})$, hence ψ induces a representation of $G(\mathfrak{m})$, which is denoted by $\tilde{\psi}$. Notice that the subgroup $I(\mathfrak{m})P_k$ is everywhere dense in I_k (as is seen from approximation theorem for valuations), hence ψ is determined uniquely by $\tilde{\psi}$. Conversely, *a representation $\tilde{\psi}$ of $G(\mathfrak{m})$ into a complete group Γ can be obtained from a representation of C_k into Γ in this manner if and only if the following holds*: Given any neighbourhood V of the identity element of Γ, there is a natural number n and a positive number ε such that $\tilde{\psi}((\alpha))\in V$ for all $\alpha\in k^*$ satisfying $\alpha\equiv 1$ mod. $\mathfrak{m}^n$, and $|\sigma\alpha-1|<\varepsilon$ for all isomorphisms σ in $H(k)$.

All this holds in particular for a character ψ of C_k. Moreover, a character χ of C_k must be of the form $\chi(a)=\chi_1(a)\|a\|^\rho$, where χ_1 is a character with absolute value 1 and ρ is a uniquely determined real number, which is called the *real part* of χ. Any χ is unramified at almost all $\mathfrak{p}$. If we denote by $\mathfrak{h}_1,\cdots,\mathfrak{h}_t$ the exceptional prime ideals where χ is ramified, then, for each $\mathfrak{h}_i$, there is the smallest natural number c_i such a that $\chi(\iota_{\mathfrak{h}_i}(\alpha))=1$ for all α in $k_{\mathfrak{h}_i}$ satisfying $\alpha\equiv 1$ mod. $\mathfrak{h}_i^{ci}$. Then an integral ideal $\mathfrak{f}=\mathfrak{h}_1^{c1}\cdots\mathfrak{h}_t^{ct}$ is called the conductor of χ. Let $\tilde{\chi}$ be, as above, the corresponding character of $G(\mathfrak{f})$. Notice that $|\tilde{\chi}(\mathfrak{a})|=N\mathfrak{a}^{-\rho}$ for any $\mathfrak{a}$ in $G(\mathfrak{f})$. Now, there is a character X of k^* such that $X(\alpha)=\tilde{\chi}((\alpha))$ for any α in k^* satisfying $\alpha\equiv 1$ mod. $\mathfrak{f}$. We shall then say, following A. Weil, that a character χ of C_k is *of type* (A_0) if the corresponding character X of k^* has the following form:

$$(*)\qquad X(\alpha)=\pm\prod_{\sigma\in H(k)}\sigma\alpha^{n(\sigma)}$$

where $n(\sigma)$ are integers, and ± may depend on α. Notice that the real part ρ of such χ is a half integer, i. e. 2ρ is an integer, and also that $n(\sigma)$ must satisfy a certain condition. Conversely, if there is a character $\tilde{\chi}$ of ideal group $G(\mathfrak{m})$ such that $\tilde{\chi}((\alpha))=X(\alpha)$ for any $\alpha\equiv 1$ mod. $\mathfrak{m}^n$ with a suitably fixed n, where $X(\alpha)$ is of the form (*) with integers $n(\sigma)$ independent of α, then $\tilde{\chi}$ *can be obtained from* *a character χ of C_k of type* (A_0) *in the above exposed manner.*

A character χ of C_k is said to be *of finite order* if some power of χ, say χ^n, is the unit character, i. e. $\chi^n(a)=1$ for all $a \in I_k$.

If χ is a character of C_k of type (A_0), the values $\tilde{\chi}(\mathfrak{a})$ of all $\mathfrak{a}$ in $G(\mathfrak{f})$ lie in a certain algebraic number field K of finite degree. Notice that K need not contain k. For any valuation w in K, $\tilde{\chi}$ may also be cosidered as a representation of $G(\mathfrak{m})$ into the completion K_w^*, where $\mathfrak{m}$ is a multiple of $\mathfrak{f}$ to be determined later. Then the above criterion shows that this representation determines a representation χ_w, such that $\tilde{\chi}=\tilde{\chi}_w$ on $G(\mathfrak{m})$, if we take $\mathfrak{m}=\mathfrak{f}$ when w is Archimedean, and $\mathfrak{m}=\mathfrak{f}l$ when w is associated with a prime ideal $\mathfrak{l}$ of K. In the latter case χ_w is written as $\chi_{\mathfrak{l}}$. From the definition, $\chi_{\mathfrak{l}}$ is unramified at each $\mathfrak{p}$ in $G(\mathfrak{f}l)$. Since $K_{\mathfrak{l}}^*$ is totally disconnected, $\chi_{\mathfrak{l}}$ takes the value 1 on the connected component D_k, so that $\chi_{\mathfrak{l}}$ is also a representation of C_k', and it determines the representation $\chi_{\mathfrak{l}}^*$ of the Galois group G_k. Moreover, since C_k' is compact, the image $\chi_{\mathfrak{l}}(C_k')=\chi_{\mathfrak{l}}^*(G_k)$ lies in the unit group $U_{\mathfrak{l}}$ of $K_{\mathfrak{l}}^*$. If w is Archimedean, χ_w is written as χ^τ or as $\chi^{\sigma_0\tau}$ with corresponding isomorphisms τ, $\sigma_0\tau$ in $H(K)$. Notice that χ^τ may also be defined by $\tilde{\chi}^\tau(\mathfrak{a})=\tau\tilde{\chi}(\mathfrak{a})$ for $\mathfrak{a}\in G(\mathfrak{f})$.

§ 1. Characterization of characters of type (A_0).

1. Let k be an algebraic number field of finite degree.

Let χ be a character of C_k of type (A_0), with conductor $\mathfrak{f}$, real part $-\rho$, and associated character $\boldsymbol{X}$ of k^* defined by

$$(1) \qquad \boldsymbol{X}(\alpha)=\pm\prod_{\sigma\in H(k)}\sigma\alpha^{n(\sigma)}\,.$$

We shall denote by K an algebraic number field of finite degree, containing all values $\tilde{\chi}(\mathfrak{a})$ of the associated character $\tilde{\chi}$ of the ideal group $G(\mathfrak{f})$. Then K' will denote the Galois closure of k and of K. Since a suitable power of ideals in k can be represented as principal ideals, the ideal $(\tilde{\chi}(\mathfrak{a}))$ in K' must have the form $(\tilde{\chi}(\mathfrak{a}))=\prod_\sigma \sigma\mathfrak{a}^{n(\sigma)}$ for all ideals $\mathfrak{a}$ in $G(\mathfrak{f})$, where all $\sigma\mathfrak{a}$ are considered as ideals in K'.

For any τ in $H(K')$, χ^τ is also of type (A_0), with the same conductor $\mathfrak{f}$ as χ. Let $-\rho'$ be the real part of χ^τ. Then, since $\tilde{\chi}((r))$ is rational for any rational number r satisfying $r\equiv 1$ mod. $\mathfrak{f}$, we see that $\mathrm{N}((r))^\rho=|\tilde{\chi}((r))|=|\tau\tilde{\chi}((r))|=\mathrm{N}((r))^{\rho'}$, where $\mathrm{N}((r))$ is the norm of

(r) considered as an ideal in k. This shows $\rho=\rho'$, i.e. χ and χ^{τ} have the same real part. In particular, we have $|\tau\tilde{\chi}(\mathfrak{p})|=\mathrm{N}\mathfrak{p}^{\rho}$ for any $\mathfrak{p}$ in $G(\mathfrak{f})$ and any τ in $H(K')$. Observe finally that, if we put $n_0=\mathop{\mathrm{Min}}_{\sigma} n(\sigma)$, $\tilde{\chi}(\mathfrak{p})\,\mathrm{N}\mathfrak{p}^{-n_0}$ is an algebraic integer in K for any $\mathfrak{p}$ in $G(\mathfrak{f})$.

Let $\mathfrak{l}$ be a prime ideal in K and $\chi_{\mathfrak{l}}$ the representation of C_k into the unit group $U_{\mathfrak{l}}$ in $K_{\mathfrak{l}}^*$ associated with χ. Denote by $k(\chi,\mathfrak{l})$ the subfield of A_k corresponding to the kernel of the representation $\chi_{\mathfrak{l}}^*$ of G_k induced by $\chi_{\mathfrak{l}}$. This $k(\chi,\mathfrak{l})$ is nothing but the field attached to χ and $\mathfrak{l}$ by A. Weil [4]. If $\mathfrak{p}$ is in $G(\mathfrak{f}l)$, $\chi_{\mathfrak{l}}$ is unramified at $\mathfrak{p}$, hence $\mathfrak{p}$ is unramified in $k(\chi,\mathfrak{l})$. Moreover, from the definition, we see $\chi_{\mathfrak{l}}^*(\sigma_{\mathfrak{p}})=\chi_{\mathfrak{l}}(\iota_{\mathfrak{p}}\pi_{\mathfrak{p}})=\tilde{\chi}(\mathfrak{p})$ for any $\mathfrak{p}$ in $G(\mathfrak{f}l)$, where $\pi_{\mathfrak{p}}$ denotes a $\mathfrak{p}$-prime element in $k_{\mathfrak{p}}^*$.

2. Let again k and K be algebraic number fields of finite degree, and K' be the Galois closure of k and K. Let S be a set of prime ideals of K with *positive* density δ. We shall consider a system $\{\psi_{\mathfrak{l}}^*\}$ of representations $\psi_{\mathfrak{l}}^*$ of the Galois group G_k into $U_{\mathfrak{l}}\subset K_{\mathfrak{l}}^*$, where $\mathfrak{l}$ runs through all prime ideals in S. We denote by $k(\psi,\mathfrak{l})$ the subfield of A_k corresponding to the kernel of $\psi_{\mathfrak{l}}^*$. Now, we assume that the following four conditions (CA_I)—(CA_{IV}) are satisfied:

(CA_I) There is an integral ideal $\mathfrak{m}$ of k with the property that $\mathfrak{p}$ is unramified in $k(\psi,\mathfrak{l})$ for any $\mathfrak{p}$ in $G(\mathfrak{m})$ and for any $\mathfrak{l}$ in S such that $\mathfrak{p}$ lies in $G(\mathfrak{m}l)$.

This means that the value $\psi_{\mathfrak{l}}^*(\sigma_{\mathfrak{p}})$ is independent of the choice of $\sigma_{\mathfrak{p}}$ for each $\mathfrak{p}$ in $G(\mathfrak{m}l)$.

(CA_{II}) $\psi_{\mathfrak{l}}^*(\sigma_{\mathfrak{p}})$ belongs to K and is independent also of $\mathfrak{l}$ in S such that $\mathfrak{p}$ belongs to $G(\mathfrak{m}l)$.

We shall denote this common value of $\psi_{\mathfrak{l}}^*(\sigma_{\mathfrak{p}})$ by $\tilde{\psi}(\mathfrak{p})$, and also put $\tilde{\psi}(\mathfrak{a})=\prod_{\mathfrak{p}}\tilde{\psi}(\mathfrak{p})^{c_{\mathfrak{p}}}$ for any ideal $\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{c_{\mathfrak{p}}}$ in $G(\mathfrak{m})$.

(CA_{III}) We have

$$|\tau\tilde{\psi}(\mathfrak{p})|=\mathrm{N}\mathfrak{p}^{\rho}$$

for all $\mathfrak{p}$ in $G(\mathfrak{m})$ and for all τ in $H(K)$, where ρ is a fixed half integer independent of $\mathfrak{p}$ and of τ.

(CA_{IV}) There is a natural number n_0 such that $\tilde{\psi}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{n_0}$ are algebraic integers in K for all $\mathfrak{p}$ in $G(\mathfrak{m})$.

Finally we impose one more condition, which is a temporary one:

(A) The principal ideal $(\tilde{\psi}(\mathfrak{p}))$ in K' can be expressed in the form

$$(\tilde{\psi}(\mathfrak{p}))=\prod_{\sigma\in H(k)}\sigma\mathfrak{p}^{n(\sigma,\mathfrak{p})}, \tag{2}$$

for all $\mathfrak{p}$ in $G(\mathfrak{m})$, where $n(\sigma,\mathfrak{p})$ are rational integers, which *may depend on* $\mathfrak{p}$ as well as σ. Notice that $n(\sigma,\mathfrak{p})$ need not be uniquely determined by $\mathfrak{p}$ and σ, unless $\mathfrak{p}$ is of the first degree.

As we have seen in **1**, the system $\{\chi_{\mathfrak{l}}^*\}$ obtained from a character χ of C_k of type (A_0) satisfies these conditions, with $\mathfrak{m}=\mathfrak{f}$, $\tilde{\psi}(\mathfrak{p})=\tilde{\chi}(\mathfrak{p})$ and $S=$ *the set of all prime ideals in K.* Our aim is now to prove the converse, i. e. to show that our conditions (CA_I)—(CA_{IV}) characterize the character of type (A_0), in the language of the Galois group G_k.

If we take the natural number n_0 in the condition (CA_{IV}) and put $\varpi=\tilde{\psi}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{n_0}$ for any $\mathfrak{p}$ in $G(\mathfrak{m})$, then ϖ, and also $\bar{\varpi}$, are algebraic integers in k. From the condition (CA_{III}), we have $\varpi\cdot\bar{\varpi}=|\varpi|^2=\mathrm{N}\mathfrak{p}^{2\rho+2n_0}$, hence any prime factor of ϖ must divide $\mathrm{N}\mathfrak{p}$, so that any prime factor of $\tilde{\psi}(\mathfrak{p})$ (with positive or negative exponent) must divide $\mathrm{N}\mathfrak{p}$. We thus see that, if the conditions (CA_I)—(CA_{IV}) are satisfied, and if k is suitably large, e. g. if $k=K'$, the condition (A) is antomatically satisfied. Moreover, as we shall see later, (A) is logically dependent on (CA_I)—(CA_{IV}) for any field k. We have added this condition (A) for the convenience of the proof.

3. $\psi_{\mathfrak{l}}^*$ determines a representation $\psi_{\mathfrak{l}}$ of $C'_k=C_k/D_k$ into $U_{\mathfrak{l}}$. Then conditions (CA_I), (CA_{II}) are equivalent to the following: $\psi_{\mathfrak{l}}$ is unramified at each $\mathfrak{p}$ in $G(\mathfrak{m}l)$, and $\psi_{\mathfrak{l}}(\iota_{\mathfrak{p}}(\pi_{\mathfrak{p}}))=\tilde{\psi}(\mathfrak{p})$ for any $\mathfrak{p}$-prime element $\pi_{\mathfrak{p}}$ in $k_{\mathfrak{p}}^*$, for each $\mathfrak{p}$ in $G(\mathfrak{m}l)$.

More generally, let $\mathfrak{p}$ be prime to l. From the continuity of the representation $\psi_{\mathfrak{l}}\circ\iota_{\mathfrak{p}}$ of $k_{\mathfrak{p}}^*$, we see that there is a natural number c such that $\alpha\equiv 1 \bmod. \mathfrak{p}^c$ $(\alpha\in k^*)$ implies $\psi_{\mathfrak{l}}\circ\iota_{\mathfrak{p}}(\alpha)\equiv 1 \bmod. \mathfrak{l}$. For such α, α^{p^n} converges to 1 in $k_{\mathfrak{p}}^*$ as $n\to\infty$, so that $\psi_{\mathfrak{l}}\circ\iota_{\mathfrak{p}}(\alpha)^{p^n}$ must converge to 1 in $K_{\mathfrak{l}}^*$ as $n\to\infty$, which is however not the case unless $\psi_{\mathfrak{l}}\circ\iota_{\mathfrak{p}}(\alpha)=1$, because $\mathfrak{l}$ does not divide p. Thus, for any $\mathfrak{p}$ in $G((l))$, there is the smallest non-negative integer $c(\mathfrak{p},\mathfrak{l})$ such that $\alpha\equiv 1 \bmod. \mathfrak{p}^{c(\mathfrak{p},\mathfrak{l})}$ implies $\psi_{\mathfrak{l}}\circ\iota_{\mathfrak{p}}(\alpha)=1$. We have clearly $c(\mathfrak{p},\mathfrak{l})=0$ if $\mathfrak{p}$ is in $G(\mathfrak{m}l)$, where the congruence $\alpha\equiv 1 \bmod. \mathfrak{p}^0$ indicates $\alpha\in U_{\mathfrak{l}}$. Then we put $\mathfrak{f}(\mathfrak{l})=\prod_{\mathfrak{p}\in G((l))}\mathfrak{p}^{c(\mathfrak{p},\mathfrak{l})}$. This $\mathfrak{f}(\mathfrak{l})$ is an integral ideal in k. Since the number of classes of $U_{\mathfrak{l}}$ modulo $\mathfrak{p}^{c(\mathfrak{p},\mathfrak{l})}$ is finite, the images of $\alpha\in U_{\mathfrak{l}}$ by $\psi_{\mathfrak{l}}\circ\iota_{\mathfrak{p}}$ are roots of unity in $K_{\mathfrak{l}}$. Hence we have

$$\psi_{\mathfrak{l}}(a)=\varepsilon\tilde{\psi}((a)) \text{ for } a=(a_{\mathfrak{p}}) \text{ in } I((l)) \text{ such that } (a)\in G(\mathfrak{m}), \tag{3}$$

where ε is a root of unity in $K_{\mathfrak{l}}$ depending only on the classes of $a_{\mathfrak{p}}$ mod. $\mathfrak{p}^{c(\mathfrak{p},\mathfrak{l})}$ for prime factors $\mathfrak{p}$ of $\mathfrak{m}$ prime to l. We shall denote by $W(\mathfrak{l})$ the number of roots of unity ε which appear in (3) for some $a \in I((l))$ such that $(a) \in G(\mathfrak{m})$. We shall now show that $W(\mathfrak{l})$ are bounded for infinitely many $\mathfrak{l}$ in S.

Let $\mathfrak{h}_1, \cdots, \mathfrak{h}_m$ be all the prime factors of $\mathfrak{m}$ in k, and put $h = h_1 \cdots h_m$, $c(\mathfrak{h}_i, \mathfrak{l}) = c_i$. Denote then by $W'(\mathfrak{l})$ the number of ε which appear in (3) for some $a = (a_{\mathfrak{p}}) \in I((l))$ such that $a_{\mathfrak{h}_i} \equiv 1$ mod. $\mathfrak{h}_i (i = 1, \cdots, m)$. Clearly, $W(\mathfrak{l})/W'(\mathfrak{l})$ are bounded for all $\mathfrak{l}$ in S, i. e. $\leqq \prod_{i=1}^{m} \mathrm{N}\mathfrak{h}_i$. If we take t large enough, we have $a_{\mathfrak{h}_i}^{h^t} \equiv 1$ mod. $\mathfrak{h}_i^{c_i}$ for $a \in I((l))$ such that $a_{\mathfrak{h}_i} \equiv 1$ mod. $\mathfrak{h}_i$ $(i = 1, \cdots, m)$. This shows that $\varepsilon^{h^t} = 1$ for any ε corresponding to these a, i. e. $W'(\mathfrak{l})$ divides h^t; here t may depend on $\mathfrak{l}$. Now take a natural number t_0 so large that we have $[K(\zeta) : K] > 2/\delta$ for a primitive h^{t_0}-th root of unity ζ (δ is the density of S). Class field theory shows that the set of prime ideals of the first degree in K, which split completely in the abelian extension $K(\zeta)$, has the definite density $[K(\zeta) : K]^{-1}$. Hence there are infinitely many $\mathfrak{l}$ in S (at least with density $\delta/2$), which split in $K(\zeta)$ into prime ideals of higher degrees, that is to say, there are infinitely many $\mathfrak{l}$ in S such that $K_{\mathfrak{l}}$ do not contain ζ. For such $\mathfrak{l}$, $W'(\mathfrak{l})$ must be smaller than h^{t_0}. Thus we have seen that *the number* $W(\mathfrak{l})$ *are bounded for infinitely many prime ideals* $\mathfrak{l}$ *of the first degree in* S. We shall denote by S' a set of infinitely many prime ideals $\mathfrak{l}$ of the first degree in K such that $W(\mathfrak{l})$ are smaller than a given bound, and moreover such that l are prime to $\mathfrak{m}$ and unramified in K'. We shall then denote by $\mathcal{E}$ the group of roots of unity generated by all roots of unity in K' and by all ε in (3) for all $\mathfrak{l}$ in S'; this $\mathcal{E}$ is clearly a finite group.

4. We want to prove now that $\tilde{\psi}(\mathfrak{a})$ has the form $\prod_{\sigma} \sigma\mathfrak{a}^{n(\sigma)}$ with $n(\sigma)$ independent of $\mathfrak{a}$. For this purpose, observe the integers $n(\sigma, \mathfrak{p})$ in (A). From (CA_{III}), we see $(\tau\tilde{\psi}(\mathfrak{p}) \cdot \sigma_0\tau\tilde{\psi}(\mathfrak{p})) = \mathrm{N}\mathfrak{p}^{2\rho} = \prod_{\sigma \in H(k)} \sigma\mathfrak{p}^{2\rho}$ for any $\mathfrak{p}$ in $G(\mathfrak{m})$ and for any τ in $H(K')$. If $\mathfrak{p} \in G(\mathfrak{m})$ is of the first degree, and unramified over $\boldsymbol{Q}$, then $\sigma\mathfrak{p}$ and $\sigma'\mathfrak{p}$ have no common prime factor in K' if $\sigma \neq \sigma'$, so that the expression for $\tilde{\psi}(\mathfrak{p})$ in (A) is unique, i. e. $n(\sigma, \mathfrak{p})$ are uniquely determined by $\sigma, \mathfrak{p}$. Hence we have

$$n(\sigma, \mathfrak{p}) + n(\tau^{-1}\sigma_0\tau\sigma, \mathfrak{p}) = 2\rho \tag{4}$$

for all σ in $H(k)$, τ in $H(K')$. Moreover, (CA_{IV}) shows that $n(\sigma, \mathfrak{p}) \geqq -n_0$ if $n(\sigma, \mathfrak{p})$ are uniquely determined. Notice that if a set of integers $\{n(\sigma, \mathfrak{p}) \mid \sigma \in H(k)\}$ satisfies the condition (4), then we have $|\tau\alpha'| = |N_{k/Q}\alpha|^{\rho}$, where $\alpha' = \prod \sigma\alpha^{n(\sigma,\mathfrak{p})}$, $\alpha \in k^*$.

For general $\mathfrak{p}$, this last relation maybe does not hold. But in any case, let $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ be all the prime factors of p in K', and K_i the decomposition field of $\mathfrak{p}_i$ over $\boldsymbol{Q}$. Then, a suitable power of $\mathfrak{p}_1$, say $\mathfrak{p}_1^f$, can be represented as principal ideal (π_1) with π_1 in $K_1 : \mathfrak{p}_1^f = (\pi_1)$. Clearly, for any τ in $H(K')$, $\tau\mathfrak{p}_1 = \mathfrak{p}_1$ if and only if $\tau\pi_1 = \pi_1$. It is also clear that, if $\tau\mathfrak{p}_1 = \mathfrak{p}_i$, then $\pi_i = \tau\pi_1 \in K_i$ does not depend on the choice of such τ, and $\mathfrak{p}_i^f = (\pi_i)$. Now, let $\mathfrak{p} = (\mathfrak{p}_1 \cdots \mathfrak{p}_j)^e$ be the prime decomposition of $\mathfrak{p}$ in K'. If we put $\pi = (\pi_1 \cdots \pi_j)^e$ accordingly, π belongs to k, $\mathfrak{p}^f = (\pi)$ and $|\tau\pi'| = \mathrm{N}\mathfrak{p}^{f\rho}$ for any τ in $H(K')$, where $\pi' = \prod_{\sigma} \sigma\pi^{n(\sigma,\mathfrak{p})}$ and $n(\sigma, \mathfrak{p})$ are integers in any expression of $\tilde{\psi}(\mathfrak{p})$ in (A). Thus $\tilde{\psi}(\mathfrak{p}^f)\pi'^{-1} = \eta$ is a unit in K', and we have $|\tau\eta| = 1$ for any τ in $H(K')$, so that η is a root of unity in K', i. e. $\tilde{\psi}(\mathfrak{p}^f) = \eta\pi' = \eta \prod_{\sigma} \sigma\pi^{n(\sigma,\mathfrak{p})}$ with a root of unity η in K'.

Let now $\{n_\nu(\sigma) \mid \sigma \in H(k)\}$ be systems of rational integers $n_\nu(\sigma) \geqq -n_0$, satisfying

$$(5) \qquad n_\nu(\sigma) + n_\nu(\tau^{-1}\sigma_0\tau\sigma) = 2\rho$$

for any $\sigma \in H(k)$ and $\tau \in H(K')$. Since $n_\nu(\sigma)$ must be $\leqq 2\rho + n_0$, the number of these systems is finite. Let then T_ν be the set of all ***principal*** prime ideals $\mathfrak{p}$ of the first degree in $G(\mathfrak{m})$, unramified over $\boldsymbol{Q}$, such that $n(\sigma, \mathfrak{p}) = n_\nu(\sigma)$ for all σ, and put $T = \bigcup_{\nu} T_\nu$. From what we have remarked above, these T_ν are mutually disjoint, and T contatins almost all principal $\mathfrak{p}$ of the first degree in k. We shall denote by $<T_\nu>$ the subgroup of $G(\mathfrak{m})$ generated by $\mathfrak{p}$ in T_ν. Then the finiteness of the number of T_ν brings forth the following result:

For any natural number n, $S((n))$ denotes the subgroup of $G((n))$ consisting of all $\mathfrak{a}$ in $G((n))$ representable as $\mathfrak{a} = (\alpha)$ with α in k^* satisfying $\alpha \equiv 1$ mod. n, then the factor group $\mathfrak{S}(n) = G((n))/S((n))$ is the "Strahlklassengruppe" modulo (n) in k. We denote by $G_0((n))$ the set of all principal ideals is $G((n))$, and put $\mathfrak{S}_0(n) = G_0((n))/S((n))$. Then we denote by $\mathfrak{T}_\nu(n)$ the image of the subgroup $<T_\nu> \cap G((n))$ into $\mathfrak{S}_0(n)$ by the natural homomorphism. We shall denote moreover by $\mathfrak{S}_0'(n)$ the multiplicative group of all the prime residue classes mod. (n) in k. There is a natural homomorphism of $\mathfrak{S}_0'(n)$ onto

$\mathfrak{S}_0(n)$, whose kernel consists of all classes containing a unit in k. We shall then denote by $\mathfrak{T}_\nu'(n)$ the inverse image of $\mathfrak{T}_\nu(n)$ in $\mathfrak{S}_0'(n)$. Assume now for a moment that, for each ν, there are infinitely many prime numbers $l_i^{(\nu)}$ $(i=1,2,\cdots)$ such that $\mathfrak{T}_\nu(l_i^{(\nu)})\neq\mathfrak{S}_0(l_i^{(\nu)})$, i. e. $\mathfrak{T}_\nu'(l_i^{(\nu)})\neq\mathfrak{S}_0'(l_i^{(\nu)})$. Let $m_t^{(\nu)}$ be a product of a finite number t of different $l_i^{(\nu)}$, say, $m_t^{(\nu)}=l_1^{(\nu)}\cdots l_t^{(\nu)}$. Then, since $\mathfrak{S}_0'(m_t^{(\nu)})$ is isomorphic to a direct product $\mathfrak{S}_0'(l_1^{(\nu)})\times\cdots\times\mathfrak{S}_0'(l_t^{(\nu)})$, and since the index $[\mathfrak{S}_0'(l_i^{(\nu)}):\mathfrak{T}_\nu'(l_i^{(\nu)})]\geqq 2$, we have, $[\mathfrak{S}_0(m_t^{(\nu)}):\mathfrak{T}_\nu(m_t^{(\nu)})]=[\mathfrak{S}_0'(m_t^{(\nu)}):\mathfrak{T}_\nu'(m_t^{(\nu)})]\geqq 2^t$. Hence, if we denote by $T_t^{(\nu)}$ the set of prime ideals in the inverse image of $\mathfrak{T}_\nu(m_t^{(\nu)})$ in $G((m_t^{(\nu)}))$, the density of $T_t^{(\nu)}$ is definite and is at most 2^{-t}. Notice that the union $\bigcup_\nu T_t^{(\nu)}$ contains almost all principal prime ideals of the first degree in k, for any $t=1,2,\cdots$, hence it has a non-zero definite density. But the number of sets T_ν being finite, the density of $\bigcup_\nu T_t^{(\nu)}$ must become arbitrarily small if we take t suitably large, which is a contradiction. Thus we have proved that there is at least one ν, for which $\mathfrak{T}_\nu(l)=\mathfrak{S}_0(l)$ hold for all but a finite number of prime number l.

We shall take a fixed one T_ν with this property, and denote this T_ν, $<T_\nu>$, $n_\nu(\sigma)$ by T_0, $<T_0>$, $n(\sigma)$ respectively. With these $n(\sigma)$ we put

$$X(\alpha)=\prod_{\sigma\in H(k)}\sigma\alpha^{n(\sigma)} \tag{6}$$

for $\alpha\in k^*$. Since $n(\sigma)$ satisfiy (5), we have $|\tau X(\alpha)|=|N_{k/Q}\alpha|^\rho$ for any $\tau\in H(K')$. Clearly this X is a representation of k^* with discrete topology into $(K')^*$.

5. We need a new topology of k^*. Let v be a valuation of $\boldsymbol{Q}$ and $v_1,\cdots,v_g$ be all the extensions of v to k. Then the weakest topology of k stronger than each topology of k determined by $v_i(i=1,\cdots,g)$ will be called the v-*topology* of k. This topology is metrisable, and makes k a topological field. Then the completion k_{v} of k with respect to the v-topology is an algebra over $\boldsymbol{Q}_{\mathrm{v}}$, and is isomorphic to the direct sum $k_{v_1}+\cdots+k_{v_g}$ as topological algebras. Hence the canonical isomorphism of $k_{v_1}^*\times\cdots\times k_{v_g}^*$ into I_k determines an imbedding ι_{v} of k^* into I_k. Then ι_{v} is bicontinuous with respect to v-topology of k and the topology of $\iota_{\mathrm{v}}(k^*)$ induced by that of I_k. Let w be an extension of v to K'. Then $\alpha\to\sigma\alpha(\alpha\in k^*)$ is continuous with respect to v-topology of k and the topology of K' determined by w, for any σ in $H(k)$, hence the mapping X defined in (6) is a representation of k^*

into K'^* with respect to these topologies. When v is determined by a prime number l, we speak of l-topology, and write k_l, ι_l instead of k_v, ι_v. Notice that an element α in k^* is near to 1 with respect to l-topology if and only if $\alpha\equiv 1$ mod. l^i with a high power l^i of l. We put finally $(\alpha)_l=(\iota_l\alpha)$ for α in k^*, i.e. $(\alpha)_l=\mathfrak{q}_1^{\nu_1(\alpha)}\cdots\mathfrak{q}_g^{\nu_g(\alpha)}$, where $\mathfrak{q}_1,\cdots,\mathfrak{q}_g$ denotes all the prime divisors of l in k and $\nu_i=\nu_{\mathfrak{q}_i}$.

Now take a prime ideal $\mathfrak{l}$ in K in the set S, such that l is prime to $\mathfrak{m}$. Put then

$$\Psi_{\mathfrak{l}}(\alpha)=\psi_{\mathfrak{l}}(\iota_l(\alpha))\cdot\tilde{\psi}((\alpha)_l)^{-1},\quad \alpha\in k^* .$$

This $\Psi_{\mathfrak{l}}$ is a representation of k^* with l-topology into $K_{\mathfrak{l}}^*$, as we have $\tilde{\psi}_{\mathfrak{l}}((\alpha)_l)=1$ for $\alpha\equiv 1$ mod. l. Moreover, from (3) in **3**, and from $\psi_{\mathfrak{l}}(\iota(\alpha))=1$, we see

$$\Psi_{\mathfrak{l}}(\alpha)=\pm\varepsilon\tilde{\psi}((\alpha))^{-1}, \tag{7}$$

for any α prime to $\mathfrak{m}$, where ε is a root of unity depending only on the class of α mod. $\mathfrak{f}(\mathfrak{l})$, and $\pm$ depends on the signatures of α at real primes. This shows in particular that $|\tau\Psi_{\mathfrak{l}}(\alpha)|=|N_{k/Q}\alpha|^{\rho}$ for such α, and for any τ in $H(K')$. Notice that, if $\mathfrak{l}$ is in S', ε belongs to the finite group $\mathcal{E}$ (defined at the end of **3**). Observe also that, if the ideal (α) belongs to $<T_0>$, the principal ideal $(\Psi_{\mathfrak{l}}(\alpha))=(\tilde{\psi}((\alpha)))^{-1}$ must be $=\prod_{\sigma}\sigma(\alpha)^{-n(\sigma)}$. Hence, for these (α), $\Psi_{\mathfrak{l}}(\alpha)\boldsymbol{X}(\alpha)$ is a unit in K', all conjugates of which have the same absolute value 1, i.e., it is a root of unity ε' in K':

$$\Psi_{\mathfrak{l}}(\alpha)=\varepsilon'\boldsymbol{X}(\alpha)^{-1},\quad \alpha\in k^*, \text{ such that } (\alpha)\in<T_0> . \tag{8}$$

We shall now prove that (8) holds for *any* α prime to $\mathfrak{m}$. For this purpose, let $\mathfrak{p}$ be any prime ideal in $G(\mathfrak{m})$. Take a number π in k^* such that $\mathfrak{p}^f=(\pi)$ with a natural number f, and $\tilde{\psi}(\mathfrak{p}^f)=\eta\pi'=\eta\prod_{\sigma}\sigma\pi^{n(\sigma,\mathfrak{p})}$ with a root of unity η in K' (cf. **4**). Put $\pi''=\boldsymbol{X}(\pi)\pi'^{-1}$, and assume for a moment that π'' is not a root of unity. Then, none of a finite number of elements $\pi''-\varepsilon$ for all $\varepsilon\in\mathcal{E}$ should not be 0. The set S' (at the end of **3**) being infinite, we can find an $\mathfrak{l}$ in S' such that l is prime to π and to all these $\pi''-\varepsilon$, and the image $\mathfrak{T}_0(l)$ of $<T_0>\cap G((l))$ into $\mathfrak{S}_0(l)$ is equal to $\mathfrak{S}_0(l)$ (cf. the end of **4**). From the last assumption, there is a principal ideal (α) in $<T_0>$ such that $\alpha\pi\equiv 1$ mod. l. π being prime to $\mathfrak{m}$, we see from (7) and (8)

$$\Psi_{\mathfrak{l}}(\alpha\pi)\boldsymbol{X}(\alpha\pi)=\varepsilon'\Psi_{\mathfrak{l}}(\pi)\boldsymbol{X}(\pi)=\pm\varepsilon'\varepsilon\tilde{\psi}(\mathfrak{p}^f)^{-1}\boldsymbol{X}(\pi)=\pm\varepsilon'\varepsilon\eta^{-1}\pi'' ,$$

where $\varepsilon', \varepsilon, \eta$ belong to the group $\mathcal{E}$, hence $\varepsilon_0 = \pm\varepsilon'\varepsilon\eta$ also lies in $\mathcal{E}$. Let $\mathfrak{l}'$ be a prime factor of $\mathfrak{l}$ in K'. Since $\alpha\pi \equiv 1$ mod. l, the number $(\alpha\pi)^{l^t}$ converges to 1 with respect to l-topology as $t \to \infty$, so that the value $(\varepsilon_0\pi'')^{l^t} = \varPsi_{\mathfrak{l}}((\alpha\pi)^{l^t}) \cdot \boldsymbol{X}((\alpha\pi)^{l^t})$ must converge to 1 in $K'_{\mathfrak{l}'}$, because $\varPsi_{\mathfrak{l}}, \boldsymbol{X}$ are representation of k^* with l-topology into $K'_{\mathfrak{l}'}$. But as we have $\beta^{\mathrm{N}\mathfrak{l}'} \equiv \beta$ mod. $\mathfrak{l}'$ for any $\mathfrak{l}'$-integral β in $K'_{\mathfrak{l}'}$, this convergence of $(\varepsilon_0\pi'')^{l^t}$ must imply that $\varepsilon_0\pi'' \equiv 1$ mod. $\mathfrak{l}'$, i. e. $\mathfrak{l}'$ must divide $\pi'' - \varepsilon_0^{-1}$. This contradicts however the assumption that l is prime to all $\pi'' - \varepsilon$ for $\varepsilon \in \mathcal{E}$. We have thus proved that $\pi'' = \boldsymbol{X}(\pi)\pi'^{-1}$ is a root of unity, hence $(\tilde{\psi}(\mathfrak{p}^f)) = \prod_\sigma \sigma\mathfrak{p}^{f \cdot n(\sigma)}$. In other words, *integers* $n(\sigma, \mathfrak{p})$ *in the condition* (A) *may be taken as* $n(\sigma)$, *independent of* $\mathfrak{p}$. Thus we have arrived at the result aimed at the beginning of **4.**

This implies in particular that (8) holds for any α in k^*, prime to $\mathfrak{m}$, i. e. $\varPsi_{\mathfrak{l}}(\alpha)\boldsymbol{X}(\alpha) = \varepsilon'_{\mathfrak{l}}(\alpha)$, and $\varepsilon'_{\mathfrak{l}}(\alpha)$ is a root of unity in K'. Denote by $\mathcal{E}_0$ the (finite) group of roots of unity in K'. Then, $\varPsi_{\mathfrak{l}}(\alpha)\boldsymbol{X}(\alpha)$ induces a representation into $\mathcal{E}_0$ of the subgroup of k^* with induced l-topology, consisting of all α prime to $\mathfrak{m}$. Hence there is a power l^c of l such that $\alpha \equiv 1$ mod. l^c implies $\varepsilon'_{\mathfrak{l}}(\alpha) = 1$ for an α prime to $\mathfrak{m}$. On the other hand, we see from (7) that $\varPsi_{\mathfrak{l}}(\alpha) = \tilde{\psi}((\alpha))^{-1}$ for totally positive (i. e. positive at each real prime) α satisfying $\alpha \equiv 1$ mod. $\mathfrak{f}(\mathfrak{l})$. Thus $\tilde{\psi}((\alpha)) = \boldsymbol{X}(\alpha)$ for any totally positive $\alpha \equiv 1$ mod. $\mathfrak{f}(\mathfrak{l})l^c$. Since $\tilde{\psi}$, $\boldsymbol{X}$ does not depend on $\mathfrak{l}$, this is true for any $\mathfrak{l}$ in S. Hence, if we denote by $\mathfrak{f}$ the greatest common divisor of all $\mathfrak{f}(\mathfrak{l})l^c$ for $\mathfrak{l} \in S$, then we have $\tilde{\psi}((\alpha)) = \boldsymbol{X}(\alpha)$ for any totally positive α prime to $\mathfrak{m}$ satisfying $\alpha \equiv 1$ mod. $\mathfrak{f}$, i. e. $\tilde{\psi}((\alpha)) = \pm\boldsymbol{X}(\alpha)$ for any α in k^* satisfying $\alpha \equiv 1$ mod. $\mathfrak{m}\mathfrak{f}$. As was recalled in "Notations and terminologies…," this shows that there is a character χ of C_k of type (A_0), such that the associated character of k^* is exactly equal to our $\boldsymbol{X}$, and the associated ideal character $\tilde{\chi}$ of $G(\mathfrak{m})$ is exactly equal to $\tilde{\psi}$. Then, since $\psi_{\mathfrak{l}}$ and $\chi_{\mathfrak{l}}$ coincide on the dense set $I(\mathfrak{m})P_k$ of I_k, we have $\psi_{\mathfrak{l}} = \chi_{\mathfrak{l}}$ for each $\mathfrak{l} \in S$. Thus we have obtained the desired result, under the assumption of the condition (A).

6. Now, we shall drop this condition (A), and assume that $\{\psi^*_{\mathfrak{l}}\}$ satisfies only (CA_I)—(CA_{IV}). Let k' be an absolutely normal field of finite degree containing k and K (e. g. $k' = K'$). If we put $\psi'_{\mathfrak{l}}(a') = \psi_{\mathfrak{l}}(N_{k'/k}a')$ for an idèle a' in $I_{k'}$, then $\psi'_{\mathfrak{l}}$ is a representation of $C_{k'}$ into $U_{\mathfrak{l}}$, since we have $N_{k'/k}P_{k'} \subset P_k$ from the definition of $N_{k'/k}$. Let $\mathfrak{P}$ be a prime ideal of k' such that $N_{k'/k}\mathfrak{P} = \mathfrak{p}^f$ is prime to $\mathfrak{m}$, and π

be a $\mathfrak{P}$-prime element in $k'_{\mathfrak{P}}$. Then, from the definition, $\psi'_{\mathfrak{l}}$ is unramified at $\mathfrak{P}$ and $\psi'_{\mathfrak{l}}(\iota_{\mathfrak{P}}(\pi))=\psi_{\mathfrak{l}}(\iota_{\mathfrak{p}}(N_{(\mathfrak{P})}\pi))=\psi(\mathfrak{p})^f$, where $N_{(\mathfrak{P})}$ denotes the norm of $k'_{\mathfrak{P}}$ into $k_{\mathfrak{p}}$. This shows that the system $\{\psi'^*_{\mathfrak{l}}\}$ of representations $\psi'^*_{\mathfrak{l}}$ of $G_{k'}$ determined by $\psi'_{\mathfrak{l}}$ satisfies the conditions (CA_I)—(CA_{IV}), with $\tilde{\psi}'(\mathfrak{P})=\tilde{\psi}(N_{k'/k}\mathfrak{P})$ and the same ρ. Moreover, it satisfies (A) automatically. Hence, from the above results (in **5**), we have $(\tilde{\psi}'(\mathfrak{P}))=\prod_{\tau\in H(k')}\tau\mathfrak{P}^{n'(\tau)}$ with integers $n'(\tau)$ independent of $\mathfrak{P}$. In particular, for any automorphism φ of k', we have $(\tilde{\psi}'(\varphi\mathfrak{P}))=\prod_{\tau}\tau\varphi\mathfrak{P}^{n'(\tau)}$. When φ is in $G(k'/k)$, we have moreover $\tilde{\psi}'(\varphi\mathfrak{P})=\tilde{\psi}(N_{k'/k}\varphi\mathfrak{P})=\tilde{\psi}(\mathfrak{p})^f=\tilde{\psi}'(\mathfrak{P})$, so that $\prod_{\tau}\tau\varphi\mathfrak{P}^{n'(\tau)}=\prod_{\tau}\tau\mathfrak{P}^{n'(\tau)}$. If we take as $\mathfrak{P}$ a prime ideal of the first degree prime to $\mathfrak{m}$, and unramified over $\boldsymbol{Q}$, then we see $n'(\tau)=n'(\tau\varphi)$ for any τ in $H(k')$ and φ in $G(k'/k)$. This means that $n'(\tau)$ is determined uniquely by the isomorphism σ of k into k' induced by τ, so we may write $n'(\tau)=n(\sigma)$. Then, for *any* $\mathfrak{p}$ in $G(\mathfrak{m})$, we have

$$\tilde{\psi}(\mathfrak{p})^f=\tilde{\psi}'(\mathfrak{p})=\prod_{\sigma\in H(k)}\prod_{\varphi\in G(k'/k)}\sigma\varphi\mathfrak{P}^{n(\sigma)}=\prod_{\sigma\in H(k)}\sigma\mathfrak{p}^{fn(\sigma)}.$$

Thus we have shown that $\tilde{\psi}(\mathfrak{p})=\prod_{\sigma}\sigma\mathfrak{p}^{n(\sigma)}$ with integers $n(\sigma)$, and the condition (A) is always satisfied for the system $\{\psi^*_{\mathfrak{l}}\}$ satisfying (CA_I)—(CA_{IV}). Summing up, we have obtained the following result:

THEOREM 1. *Let k be an algebraic number field of finite degree, and $\{\chi^*_{\mathfrak{l}}\}$ be the system of representations of the Galois groups $G_k=G(A_k/k)$ determined by a character χ of C_k of type* (A_0). *Then, the conditions (CA_I)—(CA_{IV}) in* **2** *are satisfied with $\psi^*_{\mathfrak{l}}=\chi^*_{\mathfrak{l}}$, $\mathfrak{m}=\mathfrak{f}$, $\tilde{\psi}(\mathfrak{p})=\tilde{\chi}(\mathfrak{p})$ and $S=$ the set of all prime ideals. Conversely, let K be another algebraic number field of finite degree, and S be a set of prime ideals in K with positive density. If a system $\{\psi^*_{\mathfrak{l}}\}$ of representations $\psi^*_{\mathfrak{l}}$ of G_k into $U_{\mathfrak{l}}\subset K^*_{\mathfrak{l}}$, $\mathfrak{l}$ running through S, satisfies the conditions (CA_I)—(CA_{IV}), then there is one (and only one) character χ of C_k of type* (A_0) *with the property that $\psi^*_{\mathfrak{l}}$ is exactly equal to the representation $\chi^*_{\mathfrak{l}}$ associated with χ for each $\mathfrak{l}$ in S.*

§ 2. *L*-functions with characters of type (A_0).

7. Notations will be the same as in **1**, § **1**. First we shall observe the smallest possible field K_0 among K's, i.e. the field K_0 generated over $\boldsymbol{Q}$ by all values $\tilde{\chi}(\mathfrak{p})$ for $\mathfrak{p}$ in $G(\mathfrak{f})$. Notice that $\tilde{\chi}(\mathfrak{p})\cdot\sigma_0\tilde{\chi}(\mathfrak{p})=\tau\tilde{\chi}(\mathfrak{p})\cdot\sigma_0\tau\tilde{\chi}(\mathfrak{p})=\mathrm{N}\mathfrak{p}^{2\rho}$ is a rational number, hence, for any

τ in $H(K_0)$, $\tau(\tilde{\chi}(\mathfrak{p})\sigma_0\tilde{\chi}(\mathfrak{p}))=\mathrm{N}\mathfrak{p}^{2\rho}$. From this we see that $\tau\sigma_0\tilde{\chi}(\mathfrak{p})=\sigma_0\tau\tilde{\chi}(\mathfrak{p})$ holds for any τ in $H(K_0)$ and any $\mathfrak{p}$ in $G(\mathfrak{f})$. Thus, K_0 is a totally imaginary quadratic extension of a totally real field, if K_0 is not a real field. When K_0 is real, we have $\tilde{\chi}(\mathfrak{p})=\pm\mathrm{N}\mathfrak{p}^{\rho}$, and then, comparing ideal decomposition of both sides for $\mathfrak{p}$ of the first degree, we see that ρ is an integer, hence all $\tilde{\chi}(\mathfrak{p})$ are rational and $K_0=\boldsymbol{Q}$.

Hereafter, until the end of this § 2, we shall impose on χ the following condition:

(*I*) χ is of infinite order, and all values $\tilde{\chi}(\mathfrak{p})$ for $\mathfrak{p}$ in $G(\mathfrak{f})$ are algebraic integers in K_0. Moreover, when $K_0=\boldsymbol{Q}$, all $\tilde{\chi}(\mathfrak{p})$ are positive.

Clearly, the first condition in (*I*) holds if and only if all $n(\sigma)\geqq 0$ and $\rho>0$. The second condition implies that $\prod_{\tau\in H(K)}\{\tau\tilde{\chi}(\mathfrak{p})^n-1\}>0$ in any case ($n>0$), since either K_0 is totally imaginary or $K_0=\boldsymbol{Q}$ and $\tilde{\chi}(\mathfrak{p})=\mathrm{N}\mathfrak{p}^{\rho}>1$. Notice that, in the former case, K is also totally imaginary.

Remember that the representation $\chi_{\mathfrak{l}}$ associated with χ is unramified at each prime ideal $\mathfrak{p}$ in $G(\mathfrak{f}l)$, and $\tilde{\chi}(\mathfrak{p})$ are $\mathfrak{l}$-units for such $\mathfrak{p}$. Notice also that, when $\mathfrak{p}$ divides l, $\tilde{\chi}(\mathfrak{p})$ is prime to $\mathfrak{l}$ if and only if $\sigma\mathfrak{p}$ are prime to $\mathfrak{l}$ (as ideals in K') for all σ in $H(k)$ satisfying $n(\sigma)>0$. Let now $\mathfrak{q}_1,\cdots,\mathfrak{q}_r$ be all prime factors of l in k such that $\tilde{\chi}(\mathfrak{q}_i)$ is divisible by $\mathfrak{l}$, and $\mathfrak{q}_1',\cdots,\mathfrak{q}_s'$ be all the remainning prime factors of l in k, i. e. such that $\tilde{\chi}(\mathfrak{q}_i')$ is a $\mathfrak{l}$-unit. Then, for any σ satisfying $n(\sigma)>0$, $\sigma(\mathfrak{q}_1\cdots\mathfrak{q}_r)$ is divisible by $\mathfrak{l}$, while $\sigma(\mathfrak{q}_1'\cdots\mathfrak{q}_s')$ is prime to $\mathfrak{l}$. Hence, for an element α in k^*, $\alpha\equiv 1$ mod. $(\mathfrak{q}_1\cdots\mathfrak{q}_r)^i$ implies $\prod_{\sigma}\sigma\alpha^{n(\sigma)}\equiv 1$ mod. $\mathfrak{l}^i$. This shows that there is a representation $\chi_{\mathfrak{l}}'$ of C_k into $U_{\mathfrak{l}}$, determined by the character χ of $G(\mathfrak{f}\mathfrak{q}_1\cdots\mathfrak{q}_r)$. $\chi_{\mathfrak{l}}$ and $\chi_{\mathfrak{l}}'$ being the same on the dense subgroup $P_kI(\mathfrak{f}l)$ of I_k, we see $\chi_{\mathfrak{l}}'=\chi_{\mathfrak{l}}$. Since $\chi_{\mathfrak{l}}'$ is unramified at $\mathfrak{q}_i'$, *$\chi_{\mathfrak{l}}$ is unramified at any $\mathfrak{p}$ in $G(\mathfrak{f})$, either prime to l or not, such that $\tilde{\chi}(\mathfrak{p})$ is prime to $\mathfrak{l}$.*

Let now U_0 be the direct product $\prod_{\mathfrak{l}}U_{\mathfrak{l}}$ of $\mathfrak{l}$-unit groups in $K_{\mathfrak{l}}^*$ for all $\mathfrak{l}$ in K, and ω be a character of U_0. If we denote by $\omega_{\mathfrak{l}}$ the character induced by ω on $U_{\mathfrak{l}}$, considered as a subgroup of U_0, then $\omega_{\mathfrak{l}}=1$ for almost all $\mathfrak{l}$. More precisely, there is an integral ideal $\mathfrak{b}=\mathfrak{l}_1^{m_1}\cdots\mathfrak{l}_t^{m_t}$ of K such that $\omega_{\mathfrak{l}}=1$ for $\mathfrak{l}$ prime to $\mathfrak{b}$, and that $\omega_{\mathfrak{l}_i}(\alpha)=1$ for any $\alpha\equiv 1$ mod. $\mathfrak{l}_i^{m_i}$. In this case, ω will be called *definable modulo* $\mathfrak{b}$. If ω is definable modulo $\mathfrak{b}$, ω is also definable modulo any multiple of $\mathfrak{b}$. Notice that the number of characters of U_0 definable modulo $\mathfrak{b}$ is exactly equal to the Euler function $\varphi(\mathfrak{b})=\mathrm{N}\mathfrak{b}\prod_i(1-(\mathrm{N}\mathfrak{l}_i)^{-1})$, i.e. the number of prime residue classes mod. $\mathfrak{b}$, and the values of such characters are $\varphi(\mathfrak{b})$-th roots of unity.

Assigning to each idèle a in I_k an element $\chi_0(a)=(\chi_{\mathfrak{l}}(a))$ of U_0 with $\mathfrak{l}$-components $\chi_{\mathfrak{l}}(a)$, we obtain a representation χ_0 of C_k, or of C_k', into U_0. Put $\chi_\omega=\omega\circ\chi_0$. Then χ_ω is a character of C_k of finite order, so that it determines a cyclic extension $k(\chi,\omega)$ of k, by class field theory. The compositum of these $k(\chi,\omega)$ for all characters ω of U_0 is equal to the subfield of A_k corresponding to the kernel of the representation $\chi_0{}^*$ of G_k, and this field is nothing but the abelian extension $k(\chi)$ of k attached to χ by A. Weil [4].

It is trivial to notice that, when ω is definable modulo $\mathfrak{b}$, χ_ω is unramified at each $\mathfrak{p}$ in $G(\mathfrak{f})$ such that $\tilde{\chi}(\mathfrak{p})$ is prime to $\mathfrak{b}$. Thus, if we denote by $[\mathfrak{b}]$ the product of all $\mathfrak{p}$ in $G(\mathfrak{f})$ such that $\tilde{\chi}(\mathfrak{p})$ is not prime to $\mathfrak{b}$, then χ_ω determines a character $\tilde{\chi}_\omega$ of the ideal group $G(\mathfrak{f}[\mathfrak{b}])$ in k. However, this $\tilde{\chi}_\omega$ is in general not primitive, i.e. it may be extended to a larger group than $G(\mathfrak{f}[\mathfrak{b}])$ in some cases.

8. Let $L_{\mathfrak{b}}(s;\omega)=\prod_{\mathfrak{p}\in G(\mathfrak{f}[\mathfrak{b}])}(1-\tilde{\chi}_\omega(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{-1}$ be Hecke's L-function in k with this character $\tilde{\chi}_\omega$ of $G(\mathfrak{f}[\mathfrak{b}])$, and put

$$L_{\mathfrak{b}}(s)=\prod_\omega L(s;\omega)\,, \tag{9}$$

where ω runs over all the $\varphi(\mathfrak{b})$ characters of U_0 definable modulo $\mathfrak{b}$. Put furthermore

$$L_\chi(s)=\prod L_{\mathfrak{b}}(s)\,, \tag{10}$$

$\mathfrak{b}$ running over all integral ideals of K. We must now examine the absolute convergence of this infinite product in some right half s-plane.

First we observe $L_{\mathfrak{b}}(s)$. For each $\mathfrak{p}$ in $G(\mathfrak{f}[\mathfrak{b}])$, we shall denote by $f(\mathfrak{p},\mathfrak{b})$ the smallest natural number such that $\tilde{\chi}_\omega(\mathfrak{p}^{f(\mathfrak{p},\mathfrak{b})})=1$ for all ω definable modulo $\mathfrak{b}$, i.e. such that $\tilde{\chi}(\mathfrak{p})^{f(\mathfrak{p},\mathfrak{b})}\equiv 1$ mod. $\mathfrak{b}$. Such number exists certainly since $\mathfrak{b}$ is prime to $\tilde{\chi}(\mathfrak{p})$. Then, a well-known relation between characters of a finite abelian group shows:

$$L_{\mathfrak{b}}(s)=\prod_{\mathfrak{p}\in G(\mathfrak{f}[\mathfrak{b}])}\prod_\omega(1-\tilde{\chi}_\omega(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{-1}=\prod_{\mathfrak{p}}(1-\mathrm{N}\mathfrak{p}^{-f(\mathfrak{p},\mathfrak{b})s})^{-\varphi(\mathfrak{b})/f(\mathfrak{p},\mathfrak{b})}\,.$$

We shall now put, for any $\mathfrak{p}$ in $G(\mathfrak{f})$,

$$L^{(\mathfrak{p})}(s)=\prod_{\mathfrak{b}}(1-\mathrm{N}\mathfrak{p}^{-f(\mathfrak{p},\mathfrak{b})s})^{-\varphi(\mathfrak{b})/f(\mathfrak{p},\mathfrak{b})},$$

where $\mathfrak{b}$ runs over all integral ideals in K such that $\mathfrak{p}$ belongs to $G(\mathfrak{f}[\mathfrak{b}])$, i. e. $\tilde{\chi}(\mathfrak{p})$ is prime to $\mathfrak{b}$. Then, we shall evaluate the positive term series

$$(11) \qquad \sum\nolimits_0=\sum_{\mathfrak{b}}\frac{\varphi(\mathfrak{b})}{f(\mathfrak{p},\mathfrak{b})\,(\mathrm{N}\mathfrak{p})^{f(\mathfrak{p},\mathfrak{b})\sigma}}<\sum_{n=1}^{\infty}(\textstyle\sum'\varphi(\mathfrak{b}))\mathrm{N}\mathfrak{p}^{-n\sigma}$$

where σ denotes the real part of the complex number s, and the sum $\sum'\varphi(\mathfrak{b})$ in parenthesis in the right hand side is taken over all $\mathfrak{b}$ such that $\mathfrak{p}$ belongs to $G(\mathfrak{f}[\mathfrak{b}])$ and $f(\mathfrak{p},\mathfrak{b})$ divides n. These conditions are equivalent to $\tilde{\chi}(\mathfrak{p})^n\equiv 1$ mod. $\mathfrak{b}$, so that $\mathfrak{b}$ runs over all integral divisors of $\tilde{\chi}(\mathfrak{p})^n-1$. Notice that $\tilde{\chi}(\mathfrak{p})^n-1$ is a non-zero integers in K, from the condition (I). Hence, if we denote by $\phi(\mathfrak{p},n)$ this sum $\sum'\varphi(\mathfrak{b})$, we have $\Phi(\mathfrak{p},n)=|N_{K/Q}(\tilde{\chi}(\mathfrak{p})^n-1)|$. From the remark below the condition (I), we see therefore

$$\Phi(\mathfrak{p},n)=N_{K/Q}(\tilde{\chi}(\mathfrak{p})^n-1)=\prod_{\tau\in H(K)}\{\tau\tilde{\chi}(\mathfrak{p})^n-1\}.$$

In particular, $\Phi(\mathfrak{p},n)$ have the same order of magnitude as $\mathrm{N}\mathfrak{p}^{nd\rho}$ for $n\to\infty$, where $d=[K:Q]$. This implies that the series in the right hand side in (11) converges absolutely for $\sigma>d\rho$. Hence the infinite product for $L^{(\mathfrak{p})}(s)$ converges absolutely for $\sigma>d\rho$. We see moreover that *the infinite producut*

$$\prod_{\mathfrak{p}}\prod_{\mathfrak{b}}(1-\mathrm{N}\mathfrak{p}^{-f(\mathfrak{p},\mathfrak{b})s})^{-\varphi(\mathfrak{b})/f(\mathfrak{p},\mathfrak{b})}$$

converges absolutely for $\sigma>d\rho+1$. Consequently we can change the order of product, and we have

$$L_{\chi}(s)=\prod_{\mathfrak{p}\in G(\mathfrak{f})}L^{(\mathfrak{p})}(s).$$

9. Putting $u=\mathrm{N}\mathfrak{p}^{-s}$, we have

$$\begin{aligned}\frac{d}{du}\log L^{(\mathfrak{p})}(s)&=\sum_{n=1}^{\infty}\Phi(\mathfrak{p},n)u^{n-1}\\&=\sum_{n=1}^{\infty}\Big(\prod_{\tau\in H(K)}(\tau\tilde{\chi}(\mathfrak{p})^n-1)\Big)u^{n-1}\\&=\sum_{t=0}^{d}(-1)^{d-t}\sum_{i_1\cdots i_t}\sum_{n}(\tau_{i_1}\tilde{\chi}(\mathfrak{p})\cdots\tau_{i_t}\tilde{\chi}(\mathfrak{p}))^n u^{n-1},\end{aligned}$$

or

$$L^{(\mathfrak{p})}(s)=\prod_{t=0}\prod_{i_1\cdots i_t}(1-\tau_{i_1}\tilde{\chi}(\mathfrak{p})\cdots\tau_{i_t}\tilde{\chi}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{(-1)^{d-t+1}},$$

where $\{\tau_{i_1},\cdots,\tau_{i_t}\}$ runs over all combinations of all isomorphisms $\tau_1,\cdots,\tau_d$ in $H(K)$.

Put now $\tilde{\chi}_{i_1\cdots i_t}(\mathfrak{a})=\tau_{i_1}\tilde{\chi}(\mathfrak{a})\cdots\tau_{i_t}\tilde{\chi}(\mathfrak{a})$ for ideals $\mathfrak{a}$ in $G(\mathfrak{f})$, then $\tilde{\chi}_{i_1\cdots i_t}$ is a character of $G(\mathfrak{f})$, associated with the character $\chi_{i_1\cdots i_t}=\chi^{\tau_{i_1}}\cdots\chi^{\tau_{i_t}}$ of C_k of type (A_0). We have thus proved the following theorem:

THEOREM 2. *Let χ be a character of C_k of type* (A_0), *satisfying the additional condition* (I). *Let $L_{\mathfrak{b}}(s)$ be the function defined in* (9). *Then the infinite product of $L_{\mathfrak{b}}(s)$, taken over all integral ideals $\mathfrak{b}$ in K, can be expressed by L-functions with conjugates-product characters $\chi_{i_1\cdots i_t}$ of χ in the following manner:*

$$\prod_{\mathfrak{b}}L_{\mathfrak{b}}(s)=\prod_{t=0}^{d}\prod_{i_1\cdots i_t}L(s,\chi_{i_1\cdots i_t})^{(-1)^{d-t}},$$

where $d=[K:\boldsymbol{Q}]$, $\{i_1,\cdots,i_t\}$ runs over all combinations of $1,\cdots,d$ *and* $L(s,\chi_{i_1\cdots i_t})=\prod_{\mathfrak{p}\in G(\mathfrak{f})}(1-\tilde{\chi}_{i_1\cdots i_t}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{-1}$.

Notice that this function $L(s,\chi_{i_1\cdots i_t})$ may also be imprimitive, i.e. the conductor of $\chi_{i_1\cdots i_t}$ may be a proper divisor of $\mathfrak{f}$. For example, when $t=0$, $L(s,1)$ is the zeta-function of k, from which those factors due to prime divisors of $\mathfrak{f}$ are omitted.

Remark also that, if we denote by $k(\mathfrak{b})$ the compositum of cyclic extensions $k(\chi,\omega)$ for all ω definable modulo $\mathfrak{b}$, then $L_{\mathfrak{b}}(s)$ is the zeta function of $k(\mathfrak{b})$, raised to the power $\varphi(\mathfrak{b})/[k(\mathfrak{b}):k]$ and from which those factors due to prime divisors of $\mathfrak{f}[\mathfrak{b}]$ are omitted. Hence Theorem 2 may be considered, in a sense, to express the decomposition-law of prime ideals of k in $k(\mathfrak{b})$ for infinitely many $k(\mathfrak{b})$, in the language of associated zeta-functions.

§ 3. Reformulation and Generalization.

10. We use the same notations as before, and consider a character χ of C_k of type (A_0), not necessarily satisfying the condition (I) in **7**.

l being a rational prime, the completion K_l of K may be considered as an algebra of degree $d=[K:\boldsymbol{Q}]$ over $\boldsymbol{Q}_l$. Then the representation $\tilde{\chi}$ of $G(\mathfrak{f})$ into K^* determines uniquely a representation

χ_l of C_k into the multiplicative group of regular elements in K_l. Clearly, this χ_l is also a representation of $C_k'=C_k/D_k$. Let now $\xi\rightarrow R_l(\xi)$ be a regular representation of K_l with respect to a fixed basis of K_l over $\boldsymbol{Q}_l$, which is certainly a continuous mapping from K_l with l-topology into the full linear group of degree d over $\boldsymbol{Q}_l$. If we put $M_l(a)=R_l(\chi_l(a))$, M_l is a representation of C_k into that group. Since $\chi_l(a)$ are l-units, M_l is a *l-adic unimodular* representation, i. e. a representation with l-adic integral coefficients and l-adic unit determinants. M_l being also a representation of C_k', it induces an l-adic unimodular representation M_l^* of the Galois group G_k. Then the field $k(M, l)$ corresponding to the kernel of M_l^* is the compositum of fields $k(\chi, \mathfrak{l})$ for all prime divisors $\mathfrak{l}$ of l in K.

11. We now propose to characterize the character of C_k of type (A_0) by properties of representations M_l^* thus obtained. Let $\{M_l^*\}$ be a system of l-adic unimodular representations M_l^* of the Galois group $G(\bar{k}/k)$ of $\bar{k}$ over k, with the same degree d for all rational primes l. We shall denote by $k(M, l)$ the subfield of $\bar{k}$ corresponding to the kernel of M_l^*. We shall also denote by $\mathfrak{P}$ any one of prime divisors in $\bar{k}$ of a prime ideal $\mathfrak{p}$ of k, and by $\bar{G}(\mathfrak{a})$ the set of *all* prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ for all $\mathfrak{p}$ in $G(\mathfrak{a})$, $\mathfrak{a}$ being an integral ideal of k. Now, assume that the following conditions (CA'_I)—(CA'_V) are satisfied:

(CA'_I) There is an integral ideal $\mathfrak{m}$ in k with the property that $\mathfrak{P}$ is unramified in $k(M, l)$ for any $\mathfrak{P}$ in $\bar{G}(\mathfrak{m}l)$ and for any l.

This means that the matrix $M_l^*(\sigma_{\mathfrak{P}})$ is independent of the choice of Frobenius automorphism $\sigma_{\mathfrak{P}}$, for each $\mathfrak{P}$ in $\bar{G}(\mathfrak{m}l)$.

We denote by $\boldsymbol{Q}'$ the field consisting of all matrices of the form rE, $r\in\boldsymbol{Q}$, E being the unit matrix.

(CA'_{II}) The matrices $M_l^*(\sigma_{\mathfrak{P}})$ for all $\mathfrak{P}$ in $\bar{G}(\mathfrak{m}l)$ generate over $\boldsymbol{Q}'$ a semi-simple commutative algebra $\mathcal{A}_l$ of finite degree over $\boldsymbol{Q}$. Moreover, the correspondence $M_l^*(\sigma_{\mathfrak{P}})\leftrightarrows M_q^*(\sigma_{\mathfrak{P}})$ for all $\mathfrak{P}$ in $\bar{G}(\mathfrak{m}lq)$ determines an isomorphism of $\mathcal{A}_l$ onto $\mathcal{A}_q$, for all pair (l, q) of rational primes.

This implies in particular that the characteristic equation of $M_l(\sigma_{\mathfrak{P}})$ for $\mathfrak{P}$ in $\bar{G}(\mathfrak{m}l)$ must have rational coefficients.

(CA'_{III}) The characteristic equation of $M_l(\sigma_{\mathfrak{P}})$ has rational coefficients and is independent of l for all l such that $\mathfrak{P}$ belongs to $\overline{G}(\mathfrak{m}l)$.

We shall denote by $\varpi_1(\mathfrak{p}),\cdots,\varpi_d(\mathfrak{p})$ all the characteristic roots of $M_l^*(\sigma_{\mathfrak{P}})$ (with proper multiplicities) for such l. (These characteristic roots are certainly determined only by $\mathfrak{p}$, not depending on the choice of $\mathfrak{P}$.)

(CA'_{IV}) We have

$$|\varpi_i(\mathfrak{p})|=\mathrm{N}\mathfrak{p}^{\rho} \qquad (i=1,\cdots,d)$$

for all $\mathfrak{p}$ in $G(\mathfrak{m})$, where ρ is a half integer independent of $\mathfrak{p}$ and of i.

(CA'_{V}) There is a natural number n_0 such that $\varpi_i(\mathfrak{p})\mathrm{N}\mathfrak{p}^{n_0}$ are algebraic integers for all $\mathfrak{p}$ in $G(\mathfrak{m})$ and for all i.

It is trivial to notice here that the system $\{M_l^*\}$ obtained from a character χ of type (A_0) satisfies these conditions, where algebras $\mathcal{A}_l$ in (CA'_{II}) are isomorphic to the field K_0 generated over $\boldsymbol{Q}$ by all $\tilde{\chi}(\mathfrak{p})$.

In general, we see from (CA'_{II}) that $M_l^*(\sigma_{\mathfrak{P}})$ commutes with $M_l^*(\sigma_{\mathfrak{P}'})$ for all $\mathfrak{P},\mathfrak{P}'$ in $\overline{G}(\mathfrak{m}l)$. Since such $\sigma_{\mathfrak{P}}$'s are everywhere dense in $G(\bar{k}/k)$, the image $M_l^*(G(\bar{k}/k))$ must be an abelian group, i. e. the field $k(M,l)$ is an abelian extension of k. The system $\{M_l^*\}$ can therefore be considered as a system of representations of ***abelian group*** $G_k=G(A_k/k)$, and we may write $\sigma_{\mathfrak{p}}$ instead of $\sigma_{\mathfrak{P}}$.

Since commutative semi-simple algebra is a direct sum of fields, condition (CA'_{II}) implies also that all matrices $M_l^*(\sigma_{\mathfrak{p}})$ can be decomposed (in $\boldsymbol{Q}_l$) simultaneously into direct sum:

$$\begin{pmatrix} M_{l,1}^*(\sigma_{\mathfrak{p}}) & & \\ & \ddots & \\ & & M_{l,t}^*(\sigma_{\mathfrak{p}}) \end{pmatrix}$$

for all $\mathfrak{p}\in G(\mathfrak{m}l)$, in such a way that all $M_{l,i}^*(\sigma_{\mathfrak{p}})$ with a fixed i generate over $\boldsymbol{Q}'$ a field of finite degree over $\boldsymbol{Q}$. Then, $\sigma_{\mathfrak{p}}$ being dense in G_k, all matrices $M_l^*(\sigma)$, $\sigma\in G_k$, can be decomposed correspondingly into the direct sum of $M_{l,1}^*(\sigma),\cdots,M_{l,t}^*(\sigma)$, and, for any one of fixed i, the system $\{M_{l,i}^*(\sigma)\}$ satisfies all conditions (CA'_{I})—(CA'_{V}).

It is hence sufficient to consider the case where the algebras $\mathcal{A}_l$ in (CA'_{II}) are isomorphic to an algebraic number field K of finite degree. We can fix here an isomorphism μ_l of $\mathcal{A}_l$ onto K in such a way that $\mu_l(M_l(\sigma_{\mathfrak{p}}))=\mu_q(M_q(\sigma_{\mathfrak{p}}))$ for all $\mathfrak{p}$ in $G(\mathfrak{m}lq)$ and for all pairs

(l, q). We shall write this common value $\mu_l(M_l(\sigma_\mathfrak{p}))$ by $\tilde{\psi}(\mathfrak{p})$. Clearly, all $M_l{}^*(\sigma_\mathfrak{p})$, hence also all $M_l{}^*(\sigma)$, can be transformed (in $\overline{\boldsymbol{Q}}_l$) simultaneously into diagonal forms:

$$M_l{}^*(\sigma)=\begin{pmatrix} \psi_{l,1}^{**}(\sigma) & & \\ & \ddots & \\ & & \psi_{l,d}^{**}(\sigma) \end{pmatrix}.$$

Then, $\tilde{\psi}(\mathfrak{p})\rightarrow\psi_{l,i}^{**}(\sigma_\mathfrak{p})=\varpi_i(\mathfrak{p})$ for $\mathfrak{p}$ in $G(\mathfrak{m}l)$, gives an isomorphism $\mu_{l,i}$ of K into $\overline{\boldsymbol{Q}}_l$, hence it determines also a prime divisor $\mathfrak{l}_i$ of l in k. If we put $\psi_{\mathfrak{l}_i}^*=\overset{-1}{\mu}_{l,i}\circ\psi_{l,i}^{**}$, $\psi_{\mathfrak{l}_i}^*$ is a representation of G_k into $K_{\mathfrak{l}_i}^*$. In this way, we obtain a system of representations $\psi_\mathfrak{l}^*$ of G_k into $K_\mathfrak{l}^*$, which satisfies evidently all conditions (CA_I)—(CA_{IV}) in § 1. Hence $\{\psi_\mathfrak{l}^*\}$ corresponds to a character χ of C_k of type (A_0). It is also evident that our $\{M_l^*\}$ can be obtained from this χ in the manner described in **10.** Thus theorem 1 can be reformulated in the following form:

THEOREM 1′ *Let $\{M_l^*\}$ be a system of l-adic unimodular representations M_l^* of the Galois group $G(\bar{k}/k)$ with the same degree d for all rational primes l. Then $\{M_l^*\}$ satisfies the conditions (CA'_I)—(CA'_V) if and only if it is a direct sum of systems $\{M_{l,j}^*\}$ of representations of the abelian group G_k, each obtained from a character χ_i of C_k of type* (A_0) *in the manner described in* **10.**

12. Let now our character χ of type (A_0) satisfy the condition (I) in **7**, and $M_l{}^*$ be as is **10.** Consider then the matrix $M_l{}^*(\sigma_\mathfrak{q})$ for prime ideal $\mathfrak{q}$ *dividing* l. Let $\mathfrak{l}_i$ be, as in **11**, the prime divisor of l in K determined by the imbedding of K into $\overline{\boldsymbol{Q}}_l$ given by $\tilde{\chi}(\mathfrak{p})\rightarrow\varpi_i(\mathfrak{p})=\psi_{l,i}^{**}(\sigma_\mathfrak{p})$. Then, $\varpi_i(\mathfrak{q})$ is a unit in $\overline{\boldsymbol{Q}}_l$ if and only if $\tilde{\chi}(\mathfrak{q})$ is prime to $\mathfrak{l}_i$. When that is so, $\chi_{\mathfrak{l}_i}$ is unramified at $\mathfrak{q}$, i. e. $\mathfrak{q}$ is unramified in $k(\chi, \mathfrak{l}_i)$, and we have $\chi_{\mathfrak{l}_i}(\sigma_\mathfrak{q})=\tilde{\chi}(\mathfrak{q})$, or $\psi_{l,i}^{**}(\sigma_\mathfrak{q})=\varpi_i(\mathfrak{q})$ (as was seen in **7**). Changing the numbering for each $\mathfrak{q}$ if necessary, we assume that $\varpi_1(\mathfrak{q}),\cdots, \varpi_r(\mathfrak{q})$ are units and $\varpi_{r+1}(\mathfrak{q}),\cdots, \varpi_d(\mathfrak{q})$ lie in the valuation ideal in $\overline{\boldsymbol{Q}}_l$. Notice that, although we may have $\mathfrak{l}_i=\mathfrak{l}_j$ for some $i \neq j$, the sets $\{\mathfrak{l}_1,\cdots, \mathfrak{l}_r\}$ and $\{\mathfrak{l}_{r+1},\cdots, \mathfrak{l}_d\}$ are mutually disjoint. Hence, for each $\mathfrak{q}$ dividing l, the representation $M_l{}^*$ is decomposed in $\boldsymbol{Q}_l$ into the direct sum of representations M_l' and M_l'' of respective degrees r, $d-r$, in such a way that the characteristic roots of $M_l'(\sigma_\mathfrak{q})$ are exactly $\varpi_1(\mathfrak{q}),\cdots, \varpi_r(\mathfrak{q})$. It is then clear that $\mathfrak{q}$ is unramified in the subfield of A_k corresponding to the kernel of M_l'.

13. Hereafter, until the end of § 3, we shall consider a general system $\{M_l^*\}$ of l-adic representations of $G(\bar{k}/k)$ with the same degree d for all l, and use the same notations as in the beginning of **11.** Assume that $\{M_l^*\}$ satisfies the conditions (CA'_I), (CA'_{III}), (CA'_{IV}) with $\rho>0$, (CA'_V) with $n_0=0$, but not necessarily (CA'_{II}). Then all $\varpi_i(\mathfrak{p})$ are algebraic integers different from roots of unity. Assume furthermore the following conditions (B_I), (B_{II}) are satisfied:

$$(B_I) \qquad \prod_{i=1}^{d} \varpi_i(\mathfrak{p})>0 \text{ for all } \mathfrak{p} \text{ in } G(\mathfrak{m}).$$

We may consider that $\varpi_i(\mathfrak{p})$ are contained in $\bar{Q}_l$. Then, for any one of prime divisors $\mathfrak{q}$ in k of l, we change if necessary the numbering of $\varpi_i(\mathfrak{q})$ so that $\varpi_1(\mathfrak{q}),\cdots, \varpi_r(\mathfrak{q})$ are units, while $\varpi_{r+1}(\mathfrak{q}),\cdots, \varpi_d(\mathfrak{q})$ lie in the valuation ideal of $\bar{Q}_l$, where $r=r(\mathfrak{q})\leqq d$ and $r(\mathfrak{q})$ may depend on $\mathfrak{q}$. Denote by $\mathfrak{Q}$ any prime divisor of $\mathfrak{q}$ in k. Then our next condition reads:

(B_{II}) Restricted to the decomposition group $G(\mathfrak{Q})$ of $\mathfrak{Q}$ over k, M_l^* can be transformed in Q_l into the form

$$M_l^*(\sigma)=\begin{pmatrix} M_l'(\sigma) & 0 \\ * & M_l''(\sigma) \end{pmatrix}$$

simultaneously for all σ in $G(\mathfrak{Q})$, where M_l', M_l'' have respective degrees r, $d-r$. Moreover, if we denote by $k(M_l')$ the subfield of $k(M, l)$ corresponding to the kernel of $M_l'(\sigma)$, $\mathfrak{q}$ is unramified in $k(M_l')$, and the characteristic roots of $M_l'(\sigma_{\mathfrak{Q}})$ are exactly $\varpi_1(\mathfrak{q}),\cdots, \varpi_r(\mathfrak{q})$.

Clearly the condition (B_{II}) is or is not satisfied irrespective of the choice of prime divisors $\mathfrak{Q}$ of $\mathfrak{q}$. As was seen in **12,** the system $\{M_l^*\}$ obtained from a χ satisfying (I) satisfies also these conditions (B_I), (B_{II}). Our aim is now to generalize the result in § 2 to our system $\{M_l^*\}$.

We shall first consider the group $U_l(d)$ of all l-adic unimodular matrices of degree d, and the direct product $U(d)=\prod_l U_l(d)$ for all l. $b=l_1^{c_1}\cdots l_t^{c_t}$ being any natural number, we shall denote by $U^{(b)}(d)$ the subgroup of $U(d)$ consisting of all $M=(M_l)$ such that $M_{l_i}\equiv E$ mod. $l_i^{c_i}$ $(i=1,\cdots, t)$. Then the set $\{U^{(b)}(d)\}$ $(b=1, 2,\cdots)$ forms a fundamental system of neighborhoods of the identity in $U(d)$, so that any representation of $U(d)$ into full linear group over $\boldsymbol{C}$ is essentially a representation of the factor group $\mathfrak{U}_{(b)}=U(d)/U^{(b)}(d)$. We shall denote by λ_b the natural homomorphism of $U(d)$ onto $\mathfrak{U}_{(b)}$. Notice that $\mathfrak{U}_{(b)}$ may be considered as the group of all matrices of degree d over the residue ring $\boldsymbol{Z}/b\boldsymbol{Z}$ of rational integers modulo b, with determinants having inverses in the ring $\boldsymbol{Z}/b\boldsymbol{Z}$.

Denote by $\mathfrak{L}_b$ a vector space of dimension d over $\boldsymbol{Z}/b\boldsymbol{Z}$, then $\mathfrak{U}_{(b)}$ can be considered as a transformation group of $\mathfrak{L}_b$. We shall call a vector in $\mathfrak{L}_b$ *proper* when the ideal (in $\boldsymbol{Z}/b\boldsymbol{Z}$) generated by all components of it is equal to whole $\boldsymbol{Z}/b\boldsymbol{Z}$. Let now $\mathfrak{x}_0$ be any fixed one of proper vectors in $\mathfrak{L}_b$. Clearly, $\mathfrak{U}_{(b)}$ transforms $\mathfrak{x}_0$ into proper vectors, and all proper vectors are obtained from $\mathfrak{x}_0$ in this way. Therefore, if we denote by $\mathfrak{B}_{(b)}$ the subgroup of all elements in $\mathfrak{U}_{(b)}$, transforming $\mathfrak{x}_0$ into itself, the cosets of $\mathfrak{U}_{(b)}$ modulo $\mathfrak{B}_{(b)}$ correspond one-to-one to all proper vectors in $\mathfrak{L}_b$. Let now $\tilde{D}_b$ be the representation of $\mathfrak{U}_{(b)}$, "induced" (in the sense of the theory of group characters) by the unit representation (i. e. all values are 1) of $\mathfrak{B}_{(b)}$, and $\tilde{\delta}_b$ the character of $\tilde{D}_b$, i. e. the character induced by the unit character of $\mathfrak{B}_{(b)}$. Clearly, $\tilde{\delta}_b$ is a non-negative valued rational character independent of the choice of proper $\mathfrak{x}_0$. Moreover, it is evident that $\tilde{D}_b$ is the representation of $\mathfrak{U}_{(b)}$ as a permutation group of all proper vectors in $\mathfrak{L}_b$. We shall put here $D_b=\tilde{D}_b\circ\lambda_b$, $\delta_b=\tilde{\delta}_b\circ\lambda_b$, which are respectively representations and characters of $U(d)$.

For the later use, we must compute the sum $\sum_{j=0}^{\infty}\delta_{l^j}(M)$ for $M=(M_q)$ in $U(d)$, such that no characteristic root of M_q is 1. Then, for a suitably large i, $\lambda_{l^i}(M)$ fixes no proper vectors in $\mathfrak{L}_{l^i}$, so that $\delta_{l^i}(M)=0$. Clearly $\delta_{l^j}(M)=0$ for all $j\geqq i$. Now the set of all vectors in $\mathfrak{L}_{l^i}$, whose all components are divisible by $l^j (j\leqq i)$ can be identified with $\mathfrak{L}_{l^{i-j}}$, hence $\mathfrak{L}_{l^i}$ may be considered, under this identification, as a direct union of all proper vectors in $\mathfrak{L}_{l^j}$ for $j=0,1,\cdots,i$. The sum $\sum_{j=1}^{\infty}\delta_{l^j}(M)=\sum_{j=1}^{i}\delta_{l^j}(M)$ is then equal to the number of all vectors in $\mathfrak{L}_{l^i}$, left invariant by the transformation $\lambda_{l^i}(M)$, hence *it is equal to the highest power of l dividing $det(M_l-E)$.*

14. We shall now come back to our l-adic representation M_l^* of $G(\bar{k}/k)$. Putting $M^*(\sigma)=(M_l^*(\sigma))$ for $\sigma\in G(\bar{k}/k)$, we obtain a representation M^* of $G(\bar{k}/k)$ into $U(d)$. Then, $\lambda_b \circ M^*$ is a representation of $G(\bar{k}/k)$ into $\mathfrak{U}_{(b)}$, and the field $k(M, \lambda_b)$ corresponding to the kernel of $\lambda_b \circ M^*$ is a finite normal extension of k.

For prime ideal $\mathfrak{p}$ of k in $G(\mathfrak{m})$, *prime to b*, we put

$$\psi_b(\mathfrak{p}^n) = \delta_b(M^*(\sigma_{\mathfrak{P}}^n)),$$

the right hand side being clearly independent of the choice of $\sigma_{\mathfrak{P}}$, and also of prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ in $\bar{k}$. This ψ_b coincides on $G(\mathfrak{m}b)$ with the ideal character of k associated with the character $\tilde{\delta}_b$ of the Galois group $G(k(M, \lambda_b)/k)$ in the sense of Artin's theory of L-functions.

When $\mathfrak{p}$ divides b, we define $\psi_b(\mathfrak{p}^n)$ in a little different manner. Put $b = p^c \cdot b_0 = p^c l_1^{c_1} \cdots l_t^{c_t}$, where $l_i \neq p$. Let U' be the direct product $U_p(r) \times \prod_{l \neq p} U_l(d)$, where $r = r(\mathfrak{p})$ is as in (B_{II}). Then define $U'^{(b)}$ as the subgroup consisting of all $M = (M_p', M_l)$ of U' satisfying $M_{l_i} \equiv E$ mod. $l_i^{c_i}$ and $M_p' \equiv E$ mod. p^c. The factor group $\mathfrak{U}'_{(b)} = U'/U'^{(b)}$ can be considered as a transformation group of the space $\mathfrak{L}_b' = \mathfrak{L}_{b_0} + \mathfrak{L}'_{p^c}$, where $\mathfrak{L}_{b_0}$ is as before and $\mathfrak{L}'_{p^c}$ is a vector space of dimesion r over $\boldsymbol{Z}/p^c\boldsymbol{Z}$. Now a representation $\tilde{D}_b'$ and a character $\tilde{\delta}_b'$ of $\mathfrak{U}'_{(b)}$ and a character δ_b' of U' are defined in the same way as $\tilde{D}_b, \tilde{\delta}_b, \delta_b$. Then, for σ in $G(\mathfrak{P})$, we put $M'(\sigma) = (M_p'(\sigma), M_l^*(\sigma)) \in U'$, where $M_p'(\sigma)$ is a matrix defined in (B_{II}). Here, we put

$$\psi_b(\mathfrak{p}^n) = \delta_b'(M'(\sigma_{\mathfrak{P}}^n))$$

for $\mathfrak{p}$ in $G(\mathfrak{m})$ *dividing b*, the right hand side being independent of the choice of $\sigma_{\mathfrak{P}}$ and of $\mathfrak{P}$ by the condition (B_{II}).

Notice that, if b, b' are coprim natural numbers, then the space $\mathfrak{L}_{bb'}$ is isomorphic to the direct sum $\mathfrak{L}_b + \mathfrak{L}_{b'}$, and the representation $D_{bb'}$ is equivalent to the tensor product $D_b \otimes D_{b'}$, hence we have $\delta_{bb'} = \delta_b \delta_{b'}$. The same is also true for $\delta'_{bb'}$ for any $\mathfrak{p}$ dividing b or b'. This shows that $\psi_{bb'}(\mathfrak{p}^n) = \psi_b(\mathfrak{p}^n)\psi_{b'}(\mathfrak{p}^n)$ for any $\mathfrak{p}$ in $G(\mathfrak{m})$. From this we see $\sum_{b=1}^{\infty} \psi_b(\mathfrak{p}^n) = \prod_{l} (\sum_{i=0}^{\infty} \psi_{l^i}(\mathfrak{p}^n))$. On the other hand, from our first assumption, no characteristic root $\varpi_i(\mathfrak{p})$ of $M_l^*(\sigma_{\mathfrak{P}})$, and of $M_l'(\sigma_{\mathfrak{P}})$, is root of unity. Hence, from the remark at the end of **13**, $\sum_{i=1}^{\infty} \psi_{l^i}(\mathfrak{p}^n)$ is the highest power of l dividing $\det(M_l^*(\sigma_{\mathfrak{P}}^n) - E) = \prod_{i=1}^{d} (\varpi_i(\mathfrak{p})^n - 1)$ or $\det(M_l'(\sigma_{\mathfrak{P}}^n) - E) = \prod_{i=1}^{r} (\varpi_i(\mathfrak{p})^n - 1)$ according as $\mathfrak{p}$ is prime to l or not.

But we have $\prod_{i=r+1}^{d}(\varpi_i(\mathfrak{p})^n-1)\equiv(-1)^{d-r}$ mod. p from (B_{II}), so that the highest power of p dividing $\prod_{i=1}^{r}(\varpi_i(\mathfrak{p})^n-1)$ is equal to that dividing $\prod_{i=1}^{d}(\varpi_i(\mathfrak{p})^n-1)$; we have therefore

$$\sum_{b=1}^{\infty}\psi_b(\mathfrak{p}^n)=|\prod_{i=1}^{d}(\varpi_i(\mathfrak{p})^n-1)|=\prod_{i=1}^{d}(\varpi_i(\mathfrak{p})^n-1)$$

for all $\mathfrak{p}$ in $G(\mathfrak{m})$; here the second equality follows from (B_I), as $|\varpi_i(\mathfrak{p})|=\mathrm{N}\mathfrak{p}^{\rho}>1$.

15. With our "character" ψ_b, we define a "L-function" $L_b(s)$ as follows:

$$\log L_b(s)=\sum_{\mathfrak{p}\in G(m)}\sum_{n-1}^{\infty}\psi_b(\mathfrak{p}^n)n^{-1}\mathrm{N}\mathfrak{p}^{-ns}. \tag{12}$$

Observe that this $L_b(s)$ is different form Artin's L-series attached to the group character $\tilde{\delta}_b$ only by components due to prime factors of $\mathfrak{m}b$. Then, we form again an infinite product

$$L_M(s)=\prod_{b=1}^{\infty}L_b(s), \tag{13}$$

and auxiliary series for $\mathfrak{p}$ in $G(\mathfrak{m})$,

$$\log L^{(\mathfrak{p})}(s)=\sum_{n=1}^{\infty}\sum_{b=1}^{\infty}\psi_b(\mathfrak{p}^n)n^{-1}\mathrm{N}\mathfrak{p}^{-ns}$$

$$=\sum_{n=1}^{\infty}(\prod_{i=1}^{d}(\varpi_i(\mathfrak{p})^n-1))n^{-1}\mathrm{N}\mathfrak{p}^{-ns}.$$

In the same way as in § 2, we see that the series

$$\sum_{\mathfrak{p}\in G(m)}\sum_{n=1}^{\infty}\sum_{b=1}^{\infty}\psi_b(\mathfrak{p}^n)n^{-1}\mathrm{N}\mathfrak{p}^{-ns}$$

converges absolutely in some right half s-plane, and we have

$$L_M(s)=\prod_{\mathfrak{p}\in G(m)}L^{(\mathfrak{p})}(s).$$

Again by the same calculation as in § 2, we obtain a similar result:

THEOREM 3. *Let $\{M_l^*\}$ be a system of representations of $G(\bar{k}/k)$ with the same degree d for all l, satisfying the conditions (CA'_I), (CA'_{III}), (CA'_{IV}) with $\rho>0$, (CA'_V) with $n_0=0$, (B_I) and (B_{II}). Let $L_b(s)$ be the functions defined in* (12) *with ψ_b obtained from M_l^* in the above exposed manner. Then we have the following relation:*

$$\prod_{b=1}^{\infty} L_b(s)=\prod_{t=0}^{d}\prod_{i_1\cdots i_t} L(s,\varpi_{i_1\cdots i_t})^{(-1)^{d-t}}$$

between these $L_b(s)$ *and* "*L-functions*" $L(s,\varpi_{i_1\cdots i_t})$ *defined by*

$$L(s,\varpi_{i_1\cdots i_t})=\prod_{\mathfrak{p}\in G(m)}(1-\varpi_{i_1}(\mathfrak{p})\cdots\varpi_{i_t}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{-1},$$

where $\varpi_1(\mathfrak{p}),\cdots,\varpi_d(\mathfrak{p})$ *are all the characteristic roots of* $M_l^*(\sigma_{\mathfrak{P}})$.

Observe that, when M_l^* is obtained from a character χ of type (A_0) satisfying (I), we have

$$\prod_{\mathfrak{b}|a} L_{\mathfrak{b}}(s)=\prod_{b|a} L_b(s)$$

for any natural number a, where $L_{\mathfrak{b}}(s)$ are functions defined in (9) § 2. (This is an immediate consequence of the above considerations.) Hence Theorem 3 is indeed a generalization of Theorem 2.

16. As the reader may have noticed, Theorem 3 still holds if we weaken the last condition in (B_{II}) (on characteristic roots of $M'(\sigma_{\mathfrak{Q}})$) to the following one: For each n, the highest power of l dividing $\det(M_l'(\sigma_{\mathfrak{Q}}^n)-E)$ and that dividing $\prod_{i=1}^{d}(\varpi_i(\mathfrak{q})^n-1)$ are equal, where the degree of M_l' may be arbitrary. But this generalization is somewhat an apparent one, as may be seen from the following lamma:

LEMMA. Let $P(X)=X^r+\sum_{i=1}^{r}a_iX^{r-i}$, $Q(X)=X^s+\sum_{j=1}^{s}b_jX^{s-j}$ be two polynomials in $\boldsymbol{Q}_p[X]$ with p-adic integral coefficients a_i, b_j, and let $\{\omega_1,\cdots,\omega_r\}$, $\{\eta_1,\cdots,\eta_s\}$ be respectively all the roots of $P(X)=0, Q(X)=0$ in $\overline{\boldsymbol{Q}}_p$ (with proper multiplicities). Let $P(X)=P_0(X)P_1(X)$, $Q(X)=Q_0(X)Q_1(X)$ be decompositions of $P(X), Q(X)$ in $\boldsymbol{Q}_p[X]$ into products of polynomials $P_i(X), Q_i(X)$, with highest coefficients 1 $(i=0,1)$, such that all roots of $P_0(X), Q_0(X)$ are units, while all roots of $P_1(X)$, $Q_1(X)$ lie in the valuation ideal, in $\overline{\boldsymbol{Q}}_p$. Denote by $\|\xi\|$ the normalized valuation of ξ in $\overline{\boldsymbol{Q}}_p$. Let finally a finite number of elements $\alpha_1,\cdots,\alpha_m$ of $\overline{\boldsymbol{Q}}_p$ be given. Now, assume that the relation $\|\prod_i F(\omega_i)\|=\|\prod_j F(\eta_j)\|$ holds for any polynomial $F(T)=\sum_{i=1}^{t}c_iT^{t-i}$ with rational integral coefficients c_i such that $\|c_0\|=1$, $\|c_t\|=1$, satisfying $F(\alpha_i)\neq 0$ for $i=1,\cdots,m$. Then we have $P_0(X)=Q_0(X)$. On the other hand, if the relation $\|\prod_i F(\omega_i)\|\leqq\|\prod_j F(\eta_j)\|$ holds for any $F(T)$ with rational integral coefficients, satisfying $F(\alpha_i)\neq 0$ $(i=1,\cdots,m)$, then $Q(X)$ divides $P(X)$.

This lemma is a generalization of lemma 12, n°68 in Weil's book [8]. We shall give a proof of the first part. The second part is proved similarly.

PROOF. $F(T)$ being as above, put $A(F)=\prod_i F(\omega_i)$, $B(F)=\prod_j F(\eta_j)$. Then, $\|A(F)\|$ and $\|B(F)\|$ are continuous functions of coefficients $c_0,\cdots,c_t$ of $F(T)$ with respect to the p-adic topology of $\boldsymbol{Q}$. Let $G(T)=\sum_{i=0}^{t} d_iT^{t-i}$ be a polynomial in $\boldsymbol{Z}[T]$ such that $\|d_0\|=\|d_t\|=1$, and $G(\alpha_i)=0$ for some α_i. Then, take $F(T)$ as above, and put $G_n(T)=G(T)+p^nF(T)$, which is certainly in $\boldsymbol{Z}[T]$ and $\|d_0+p^nc_0\|=\|d_t+p^nc_t\|=1$ if $n\geqq 1$. Moreover, $G_n(\alpha_j)\neq 0$ $(j=1,\cdots,m)$ if we take n large enough, as $F(\alpha_j)\neq 0$ by assumption. Thus we have $\|A(G_n)\|=\|B(G_n)\|$ for large n, and, since $G_n(T)$ converges to $G(T)$ as $n\rightarrow\infty$ (in p-topology), we have $\|A(G)\|=\|B(G)\|$. Hence we can drop the condition that $F(\alpha_j)\neq 0$. Now, it is clear that $\|A(F)\|=\|B(F)\|$ holds for all $F(T)$ with rational coefficients $c_0,\cdots,c_t$, whose denominators are prime to p, such that $\|c_0\|=1$, $\|c_t\|=1$. Since such rational numbers are everywhere dense in the valuation ring $\boldsymbol{O}_p$ of $\boldsymbol{Q}_p$, and since rational numbers c such that $\|c\|=1$ are everywhere dense in the unit group of $\boldsymbol{Q}_p$, we have $\|A(F)\|=\|B(F)\|$ for all $F(T)$ in $\boldsymbol{O}_p[T]$ such that $\|c_0\|=\|c_t\|=1$. Then, let β be any unit in $\overline{\boldsymbol{Q}}_p$ with degree t over $\boldsymbol{Q}_p$, and $F(T)=T^t+\sum_{i=1}^{t} c_iT^{t-i}$ be the irreducible polynomial of β over $\boldsymbol{Q}_p$. Then $F(T)\in\boldsymbol{O}_p[T]$ and $\|c_t\|=1$. If we put $\varphi(\beta)=\|\prod_i(\beta-\omega_i)\|$, $\psi(\beta)=\|\prod_j(\beta-\eta_j)\|$, we have $\|A(F)\|=\varphi(\beta)^t$, $\|B(F)\|=\psi(\beta)^t$, so that from the relation $\|A(F)\|=\|B(F)\|$ follows $\varphi(\beta)=\psi(\beta)$. Let now α be any one of ω_i, or η_j, which is a unit in $\overline{\boldsymbol{Q}}_p$. Let d, e be the multiplicities of α in $\{\omega_1,\cdots,\omega_r\}$, $\{\eta_1,\cdots,\eta_s\}$ respectively. Put then $\lambda=\prod(\alpha-\omega_i)$, $\mu=\prod(\alpha-\eta_j)$, where products are taken for $\omega_i\neq\alpha$, and $\eta_j\neq\alpha$, with their proper multiplicities. Choose β so that $\beta\equiv\alpha$ mod. p^n with sufficiently large n, then β is a unit in $\overline{\boldsymbol{Q}}_p$. If n is large enough, we have $\|\alpha-\omega_i\|=\|\beta-\omega_i\|$ and $\|\alpha-\eta_j\|=\|\beta-\eta_j\|$ for $\omega_i\neq\alpha$, $\eta_j\neq\alpha$. Hence we see $\varphi(\beta)=\|\lambda\|\,\|\beta-\alpha\|^d$ and $\psi(\beta)=\|\mu\|\,\|\beta-\alpha\|^e$, so that $\|\beta-\alpha\|^{d-e}=\|\mu/\lambda\|$. Since λ,μ are independent of n and of β, and since we can take β, so that $\|\beta-\alpha\|$ becomes arbitrarily small, we must have $d=e$. As this holds for any root α of $P_0(X)=0$, or

$Q_0(X)=0$, the first part of the lemma is proved.—

To verify the last assertion in the condition (B_{II}), it is sufficient from this lemma to show the relation $\|\prod_{i=1}^{d} F(\varpi_i(\mathfrak{q}))\|=\|\det F(M_l'(\sigma_{\mathfrak{D}}))\|$ for all polynomials $F(T)=\sum_{i=0}^{t} c_i T^{t-i}$ in $\boldsymbol{Z}[T]$ such that $\|c_0\|=\|c_t\|=1$, satisfying $F(\alpha_i)\neq 0$ for a finite number of elements $\alpha_1,\cdots,\alpha_m$ in $\overline{\boldsymbol{Q}_l}$. Because, as $M_l'(\sigma_{\mathfrak{D}})$ is l-adic unimodular, all the characteristic roots of it are units in $\overline{\boldsymbol{Q}_l}$, hence if this relation holds, they coincide with those part of $\{\varpi_1(\mathfrak{q}),\cdots,\varpi_d(\mathfrak{q})\}$ which are units in $\overline{\boldsymbol{Q}_l}$, taking multiplicities into account.

§ 4. Application to abelian varieties. The conjecture of Hasse.

17. Let A be an abelian variety of dimension n defined over a field κ with characteristic p (maybe 0 or a prime number). If $\mathfrak{g}$ is any set of points on A, we shall understand by *the field generated by* $\mathfrak{g}$ *over* κ, the smallest field in $\bar{\kappa}$ containing κ, over which all points in $\mathfrak{g}$ are rational. We shall denotes by $g(m;\mathrm{A})$ the group of all points on A, whose orders divide m. If m is prime to p, $g(m;\mathrm{A})$ have exactly m^{2n} points, while $g(p^i;\mathrm{A})$ have p^{ir} points, where r is an integer independent of i, and we have $0\leqq r\leqq n$. Hence the field generated by $g(m;\mathrm{A})$ over κ is a finite algebraic extensiòn of κ. We shall denote furthermore by $\mathfrak{g}(l;\mathrm{A})$ the group of all points on A, whose orders are some powers of a rational prime l, i. e. $\mathfrak{g}(l;\mathrm{A})=\bigcup_{i=1}^{\infty} g(l^i;\mathrm{A})$. Then $\mathfrak{g}(l;\mathrm{A})$ is isomorphic to a direct sum of $2n$ or r additive groups $(\boldsymbol{Q}/\boldsymbol{Z})_l$ of l-adic numbers modulo 1, according as $l\neq p$ or $l=p$. When we fix an isomorphism of $\mathfrak{g}(l;\mathrm{A})$ onto the direct sum of $(\boldsymbol{Q}/\boldsymbol{Z})_l$, we shall speak of "$l$-adic coordinates" of the group $\mathfrak{g}(l;\mathrm{A})$. Since any automorphism σ in $G(\bar{\kappa}/\kappa)$ permutes points of $g(m;\mathrm{A})$ among themselves, σ induces an automorphism of the group $\mathfrak{g}(l;\mathrm{A})$. Hence the group $G(\bar{\kappa}/\kappa)$ can be represented, as a transformation group of $\mathfrak{g}(l;\mathrm{A})$, with l-adic coordinates of it. We shall denote by $M_l^*(\sigma)$ this representation matrix, which is clearly l-adic unimodular, and of degree $2n$ or r according as $l\neq p$ or $l=p$. It should be noticed that this representation M_l^* is certainly continuous, that is to say for any natural number i, there is a finite algebraic extension κ' of κ such that $M_l^*(\sigma) \equiv E$ mod. l^i for all σ in $G(\bar{\kappa}/\kappa')$. (We have only to take as κ' the field generated by $g(l^i; \mathrm{A})$ over κ.) Denote then by $\kappa(\mathrm{A}, l)$ the subfield of $\bar{\kappa}$ corresponding to the kernel of M_l^*. This $\kappa(\mathrm{A}, l)$ is clearly equal to the field generated by $\mathfrak{g}(l; \mathrm{A})$ over κ. We shall denote finally by $\kappa(\mathrm{A})$ the compositum of all fields $\kappa(\mathrm{A}, l)$.

Let us recall here some properties of endomorphisms of abelian varieties. (cf. Weil [8]).

$\mathcal{A}(\mathrm{A})$ denotes as usual the ring of endomorphisms of A, and $\mathcal{A}_0(\mathrm{A})$ denotes the tensor product $\mathcal{A}(\mathrm{A}) \otimes \boldsymbol{Q}$. $\mathcal{A}_0(\mathrm{A})$ is a semi-simple algebra of degree at most $4n^2$ over $\boldsymbol{Q}$, and $\mathcal{A}(\mathrm{A})$ is an order of $\mathcal{A}_0(\mathrm{A})$. Moreover, if $\mathcal{A}_0(\mathrm{A})$ contains a commutative semi-simple algebra C of degree $2n$ over $\boldsymbol{Q}$, the commutor of C in $\mathcal{A}_0(\mathrm{A})$ coincides with C itself (cf. Weil [5] p. 12). Since any endomorphism μ of A induces an endomorphism of the group $\mathfrak{g}(l; \mathrm{A})$, $\mathcal{A}(\mathrm{A})$ can be represented with l-adic coordinates of $\mathfrak{g}(l; \mathrm{A})$, and the representation matrix $\mathrm{M}_l(\mu)$ is an l-adic integral matrix of degree $2n$ or r according as $l \neq p$ or $l = p$. This representation M_l is faithfull for any $l \neq p$. Moreover, for $l \neq p$, the characteristic equation of $\mathrm{M}_l(\mu)$ has rational integral coefficients, and is independent of l. When μ is defined over κ, we put $\nu(\mu) = [\kappa(x) : \kappa(\mu x)]$ if this degree is finite, and put $\nu(\mu) = 0$ in other case, where x denotes a generic point of A over κ. Then we have $\nu(\mu) = \det \mathrm{M}_l(\mu)$ for $l \neq p$. Moreover, $\nu(\mu) \neq 0$ if and only if the kernel of μ is a finite group. We call μ *separable* if the field $\kappa(x)$ is separable over $\kappa(\mu x)$. If $\nu(\mu) \neq 0$ and μ is separable, $\nu(\mu)$ is equal to the number of points b in the kernel of μ, hence the highest power of l dividing $\nu(\mu)$ is exactly equal to the number of points b in $\mathfrak{g}(l; \mathrm{A})$ such that $\mu b = 0$. But this number of points is equal to the highest power of l dividing $\det \mathrm{M}_l(\mu)$, as the definition of M_l shows. Hence if μ is separable and $\nu(\mu) \neq 0$, the highest power of l dividing $\nu(\mu)$ and that dividing $\det \mathrm{M}_l(\mu)$ are the same also for $l = p$. Finally, we can extend this representation M_l to the algebra $\mathcal{A}_0(\mathrm{A})$ in the obvious manner.

When κ is the finite field of p^f elements, the mapping $\xi \rightarrow \xi^{p^f}$ is an automorphism of the universal domain, which leaves all elements in κ invariant. Hence this automorphism determines an endomorphism π_{A} of A, defined over κ. From the definition, $\kappa(x)$ is purely inseparable of degree p^{fn} over $\kappa(\pi_{\mathrm{A}} x)$. We see furthermore that, for any μ in $\mathcal{A}(\mathrm{A})$, μ is separable if and only if μ is prime to π_{A}, i. e. the left ideal $\mathcal{A}(\mathrm{A})\mu+\mathcal{A}(\mathrm{A})\pi_{\mathrm{A}}$ in $\mathcal{A}(\mathrm{A})$, generated by μ and π_{A}, is equal to $\mathcal{A}(\mathrm{A})$. Notice that, if any endomorphism μ is defined over κ, we have $\mu\pi_{\mathrm{A}}=\pi_{\mathrm{A}}\mu$. Let now $\varpi_1(\mathrm{A}),\cdots,\varpi_{2n}(\mathrm{A})$ be the characteristic roots of the matrix $\mathrm{M}_l(\pi_{\mathrm{A}})$ for $l\neq p$, then the zeta-function $\boldsymbol{Z}_{\mathrm{A}}(u)$ of A over κ is of the form:

$$\boldsymbol{Z}_{\mathrm{A}}(u)=\prod_{t=0}^{2n}\prod_{i_1\cdots i_t}(1-\varpi_{i_1}(\mathrm{A})\cdots\varpi_{i_t}(\mathrm{A})u)^{(-1)^{t+1}}$$

(cf. Taniyama [3]).

18. When the field κ is an algebraic number field k of finite degree, the system of representations M_l^* (for all l) of the group $G(\bar{k}/k)$ defined as above satisfies the conditions stated in Theorem 3, as we shall show in the following.

First we shall consider Frobenius automorphisms $\sigma_{\mathfrak{P}}$ over k of prime divisors $\mathfrak{P}$ in $\bar{k}$. For this purpose, we use the reduction of A modulo $\mathfrak{p}$, $\mathfrak{p}$ denoting the prime ideal in k divisible by $\mathfrak{P}$ (cf. Shimura [2], Taniyama [3]). Then, for almost all $\mathfrak{p}$, the variety $\mathrm{A}(\mathfrak{p})$ obtained from A by the reduction modulo $\mathfrak{p}$ is also an abelian variety, defined over the residue field $k(\mathfrak{p})$ of $p^f=\mathrm{N}\mathfrak{p}$ elements. In this case, $\mathfrak{p}$ is said to be *non-exceptional* for A. We can extend the process of reduction mod. $\mathfrak{p}$ to that of reduction mod. $\mathfrak{P}$. If $\mathfrak{p}$ is non-exceptional, this latter process of reduction mod. $\mathfrak{P}$ induces a homomorphism of the group $\mathfrak{g}(l;\mathrm{A})$ *onto* $\mathfrak{g}(l;\mathrm{A}(\mathfrak{p}))$, which is an isomorphism for $l\neq p$. It induces also an isomorphism of the ring $\mathcal{A}(\mathrm{A})$ into $\mathcal{A}(\mathrm{A}(\mathfrak{p}))$. Notice that, if we take another prime divisor $\mathfrak{P}'$ of $\mathfrak{p}$, these isomorphisms of $\mathfrak{g}(l;\mathrm{A})$ or of $\mathcal{A}(\mathrm{A})$ will be thereby altered in general, unless all points or endomorphisms in question are defined over k. We shall fix here the l-adic coordinates of $\mathfrak{g}(l;\mathrm{A})$ and of $\mathfrak{g}(l;\mathrm{A}(\mathfrak{p}))$, by which our representations M_l^*, M_l are defined. Now, since any $\sigma_{\mathfrak{P}}$ induces on the residue field $\bar{k}(\mathfrak{P})$ the antomorphism $\xi\to\xi^{p^f}$ (over $k(\mathfrak{p})$), we see $M_l^*(\sigma_{\mathfrak{P}})=M_{l,\mathfrak{P}}^{-1}\mathrm{M}_l(\pi_{\mathrm{A}(\mathfrak{p})})M_{l,\mathfrak{P}}$ for any $l\neq p$, where $M_{l,\mathfrak{P}}$ denotes the transformation matrix between the original l-adic coordinates of $\mathfrak{g}(l,\mathrm{A}(\mathfrak{p}))$ and that of $\mathfrak{g}(l;\mathrm{A}(\mathfrak{p}))$ induced by the l-adic coordinates of $\mathfrak{g}(l;\mathrm{A})$ by the reduction mod. $\mathfrak{P}$. Here notice that $\pi_{\mathrm{A}(\mathfrak{p})}$ is determined uniquely by $\mathfrak{p}$, and $M_{l,\mathfrak{P}}$ is determined uniquely by $\mathfrak{P}$, so that $M_l^*(\sigma_{\mathfrak{P}})$ does not depend on the choice of $\sigma_{\mathfrak{P}}$. This means that $\mathfrak{p}$ is unramified in the field $k(\mathrm{A};l)$ for any $l\neq p$, if $\mathfrak{p}$ is non-exceptional for A.

Hereafter, we shall write $\pi_{\mathfrak{p}}$, $\varpi_i(\mathfrak{p})$ instead of $\pi_{A(\mathfrak{p})}$, $\varpi_i(A(\mathfrak{p}))$.

Denote by $\mathfrak{m}$ the product of all prime ideals $\mathfrak{p}$ in k, which are *not* non-exceptional for A. As such $\mathfrak{p}$ are finite in number, $\mathfrak{m}$ is certainly an integral ideal of k. Then, we have seen that, for any $\mathfrak{p}$ in $G(\mathfrak{m}l)$, $\mathfrak{p}$ is unramified in $k(A; l)$, i.e. the condition (CA'_I) is satisfied in our case. As was recalled above, the characteristic equation of $M_l(\pi_{\mathfrak{p}})$, hence also that of $M_l^*(\sigma_{\mathfrak{P}})$, have rational integral coefficients independent of $l \neq p$, which proves the condition (CA'_{III}). Now the so called Riemann hypothesis for the congruence zeta function of a curve (Weil [7]) shows that we have $|\varpi_i(\mathfrak{p})| = p^{f/2} = N\mathfrak{p}^{1/2}$ for $i=1, \cdots, 2n$ (cf. Taniyama [3], § 3). This implies the condition (CA'_{IV}) with $\rho = 1/2 > 0$. Recall also that $\varpi_i(\mathfrak{p})$ are algebraic integers, from which the condition (CA'_V) follows with $n_0 = 0$. Recall moreover that $\prod_i \varpi_i(\mathfrak{p}) = \det M_l(\pi_{\mathfrak{p}}) = \nu(\pi_{\mathfrak{p}}) > 0$, which is nothing but the condition (B_I). We have therefore only to verify the condition (B_{II}).

We must therefore consider $M_p^*(\sigma)$ for σ in the decomposition group $G(\mathfrak{P})$ of $\mathfrak{P}$ over k. Recall that the group $g(p^i; A)$ has exactly p^{2in} elements, and the group $g(p^i; A(\mathfrak{p}))$ has p^{ir} elements, where $r = r(\mathfrak{p})$ is independent of i. Moreover, by the reduction modulo $\mathfrak{P}$, $g(p^i; A)$ is mapped onto $g(p^i; A(\mathfrak{p}))$ for all i. Hence, if $\mathfrak{g}_{\mathfrak{P}}(p; A)$ denotes the kernel of the homomorphism of $\mathfrak{g}(p; A)$ onto $\mathfrak{g}(p; A(\mathfrak{p}))$ determined by the reduction mod. $\mathfrak{P}$, $\mathfrak{g}_{\mathfrak{P}}(p; A)$ is isomorphic to the direct sum of $2n-r$ groups $(\boldsymbol{Q}/\boldsymbol{Z})_p$, and is a direct component of $\mathfrak{g}(p; A)$. In other words, there is a subgroup $\mathfrak{g}'_{\mathfrak{P}}(p; A)$ of $\mathfrak{g}(p; A)$, mapped isomorphically onto $\mathfrak{g}(p; A(\mathfrak{p}))$ by the reduction mod. $\mathfrak{P}$, such that $\mathfrak{g}(p; A) = \mathfrak{g}'_{\mathfrak{P}}(p; A) + \mathfrak{g}_{\mathfrak{P}}(p; A)$ (direct sum). Clearly, this kernel $\mathfrak{g}_{\mathfrak{P}}(p; A)$ is left invariant as a whole by any σ in $G(\mathfrak{P})$. Thus, if we take p-adic coordinates in $\mathfrak{g}(p; A)$ according to the direct decomposition $\mathfrak{g}(p; A) = \mathfrak{g}'_{\mathfrak{P}}(p; A) + \mathfrak{g}_{\mathfrak{P}}(p; A)$, $M_p^*(\sigma)$ must have the form:

$$M_p^*(\sigma) = \begin{pmatrix} M_p'(\sigma) & 0 \\ * & M_p''(\sigma) \end{pmatrix}$$

for any σ in $G(\mathfrak{P})$. Here, $M_p''(\sigma)$ is of degree $2n-r$, and is a representation of $G(\mathfrak{P})$ with p-adic coordinates in $\mathfrak{g}_{\mathfrak{P}}(p; A)$, while $M_p'(\sigma)$ is equal to the representation of the Galois group of the residue field $\bar{k}(\mathfrak{P})$ over $k(\mathfrak{p})$ (induced by $G(\mathfrak{P})$) with p-adic coordinates in $\mathfrak{g}(p; A(\mathfrak{p}))$ determined by those of $\mathfrak{g}'_{\mathfrak{P}}(p; A)$ by the above isomorphism. Then, just as above, we see that $M_p'(\sigma_{\mathfrak{P}})$ does not depend on the choice of

$\sigma_{\mathfrak{P}}$, so that $\mathfrak{p}$ is unramified in the subfield $k(M_p')$ of $k(\mathrm{A}\,;p)$ corresponding to the kernel of M_p'.

Here, we shall use the lemma in **16.** $\|\alpha\|$ denotes as there the normalized valuation in the field $\boldsymbol{Q}_p$. Then, as was recalled in **17,** for any separable endomorphism μ of A such that $\nu(\mu)\neq 0$, we have $\|\det \mathrm{M}_p(\mu)\|=\|\nu(\mu)\|$. Let now $F(T)=\sum_{i=0}^{t} c_i T^{t-i}$ be any polynomial with rational integral coefficients such that $\|c_0\|=\|c_t\|=1$. It is clear that $F(\pi_{\mathfrak{p}})=\sum c_i\pi_{\mathfrak{p}}^{t-i}$ belongs to $\mathcal{A}(\mathrm{A}(\mathfrak{p}))$. If $\nu(F(\pi_{\mathfrak{p}}))=0$, then $\det(\mathrm{M}_l(F(\pi_{\mathfrak{p}})))=0$ for any $l\neq p$, hence we have $F(\varpi_i(\mathfrak{p}))=0$ with some $\varpi_i(\mathfrak{p})$. Hence, if $F(\varpi_i(\mathfrak{p}))\neq 0$ for $i=1,\cdots,2n$, then $\nu(F(\pi_{\mathfrak{p}}))\neq 0$. Moreover, since $\|c_t\|=1$, $F(\pi_{\mathfrak{p}})$ is prime to $\pi_{\mathfrak{p}}$, so that $F(\pi_{\mathfrak{p}})$ is separable. We have therefore, for any $F(T)$ such that $F(\varpi_i(\mathfrak{p}))\neq 0$, $\|\det F(\mathrm{M}_p(\pi_{\mathfrak{p}}))\|=\|\det \mathrm{M}_p(F(\pi_{\mathfrak{p}}))\|$ $=\|\nu(F(\pi_{\mathfrak{p}}))\|=\|\det \mathrm{M}_l(F(\pi_{\mathfrak{p}}))\|=\|\prod_{i=1}^{2n} F(\varpi_i(\mathfrak{p}))\|$, where $l\neq p$. From the remark following the lemma, we thus see that the characteristic roots of $M_p'(\sigma_{\mathfrak{P}})=\mathrm{M}_p(\pi_{\mathfrak{p}})$ are exactly those characteristic roots of $\mathrm{M}_l(\pi_{\mathfrak{p}})$, which are units in $\overline{\boldsymbol{Q}}_p$, taking multiplicities into account. This completes the verification of the condition (B_{II}).

Hasse's zeta function $\zeta_{\mathrm{A}}(s)$ of A over k is defined by

$$\zeta_{\mathrm{A}}(s)=\prod_{\mathfrak{p}\in G(\mathfrak{m})} \boldsymbol{Z}_{\mathfrak{p}}(s)\,,$$

where $\boldsymbol{Z}_{\mathfrak{p}}(s)$ denotes the zeta function $\boldsymbol{Z}_{\mathrm{A}(\mathfrak{p})}(u)$ of $\mathrm{A}(\mathfrak{p})$ over $k(\mathfrak{p})$ with $u=\mathrm{N}\mathfrak{p}^{-s}$. Then we have

$$\zeta_{\mathrm{A}}(s)=\prod_{\mathfrak{p}\in G(\mathfrak{m})}\prod_{t=0}^{2n}\prod_{i_1\cdots i_t}(1-\varpi_{i_1}(\mathfrak{p})\cdots\varpi_{i_t}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{(-1)^{t+1}}.$$

This shows that $\zeta_{\mathrm{A}}(s)$ is nothing but the function $L_M(s)$ defined by (13) in **15,** for our system $\{M_l^*\}$ of representations with l-adic coordinates in $\mathfrak{g}(l\,;\mathrm{A})$. Thus we have seen that $\zeta_{\mathrm{A}}(s)$ can be expressed as an infinite product of "L-functions" determined as in § 3.

19. We shall give an application of Theorem 1′ to the proof of the conjecture of Hasse for $\zeta_{\mathrm{A}}(s)$ in case of complex multiplication.

Let A be as in **18,** and we make following assumptions:

(CM_I) The algebra $\mathcal{A}_0(\mathrm{A})$ contains a commutative semi-simple subalgebra C of degree $2n$ over $\boldsymbol{Q}$.

(CM_{II}) Any endomorphism in $C\cap\mathcal{A}(\mathrm{A})$ is defined over k.

Let a prime ideal $\mathfrak{p}$ in k be non-exceptional for A. By the rednction modulo $\mathfrak{p}$, C is mapped isomorphically into the algebra $\mathcal{A}_0(\mathrm{A}(\mathfrak{p}))$, and any endomorphism in this image of C is defined over $k(\mathfrak{p})$. Hence $\pi_\mathfrak{p}$ commutes with all elements in the image of C, which is a commutative semi-simple subalgebra of degree $2n$ of $\mathcal{A}_0(\mathrm{A}(\mathfrak{p}))$, so that $\pi_\mathfrak{p}$ must be contained in this image. That is to say, there is an element π in C, mapped to $\pi_\mathfrak{p}$ by the reduction modulo $\mathfrak{p}$. Now, $\mathfrak{P}$ being a prime divisor of $\mathfrak{p}$ in $\bar{k}$, we have $M_l^*(\sigma_\mathfrak{P})=M_{l,\mathfrak{P}}^{-1}\mathrm{M}_l(\pi_\mathfrak{p})M_{l,\mathfrak{P}}$ as was seen in **18**, and it is clear that $M_l(\pi)=M_{l,\mathfrak{P}}^{-1}\mathrm{M}_l(\pi_\mathfrak{p})M_{l,\mathfrak{P}}$. We have therefore $M_l^*(\sigma_\mathfrak{P})=\mathrm{M}_l(\pi)$. Remember that M_l is a faithfull representation of $\mathcal{A}_0(\mathrm{A})$, so that all matrices $M_l(\sigma_\mathfrak{P})$ for all $\mathfrak{P}$ in $G(\mathfrak{m}l)$ generates over $\boldsymbol{Q}'$ an algebra $\mathcal{A}_l$, which is isomorphic to the subalgebra of C generated over $\boldsymbol{Q}$ by all π (for all $\mathfrak{p}$ in $G(\mathfrak{m}l)$), and an isomorphism is given by $M_l^*(\sigma_\mathfrak{P})\leftrightarrows\pi$. Hence the condition (CA'_{II}) in **11**, is satisfied. Since all other conditions (CA') have been verified in **18**, Theorem **1**$'$ shows now that our system $\{M_l^*\}$ is obtained from a finite number of characters $\chi_1,\cdots,\chi_s$ of C_k of type (A_0). This implies in particular that, for any combination $(i_1,\cdots,i_t)$ of $1,\cdots,2n$, there is a character $\chi_{i_1\cdots i_t}$ of C_k of type (A_0) such that $\chi_{i_1\cdots i_t}(\mathfrak{p})=\varpi_{i_1}(\mathfrak{p})\cdots\varpi_{i_t}(\mathfrak{p})$ for any $\mathfrak{p}$ in $G(\mathfrak{m})$. Hence we have proved the following theorem.

Theorem 4. *Let* A *be an abelian variety defined over an algebraic number field k of finite degree, satisfying the conditions (CM_I) and (CM_{II}). Then the zeta function $\zeta_\mathrm{A}(s)$ of* A *over k can be expressed in the following form*

$$\zeta_\mathrm{A}(s)=\prod_{t=0}^{2n}\prod_{i_1\cdots i_t}L\ (s\,;\chi_{i_1\cdots i_t})^{(-1)^t}$$

with L-functions $L(s,\chi_{i_1\cdots i_t})$ attached to characters $\chi_{i_1\cdots i_t}$ of C_k of type (A_0), *with defining module* $\mathfrak{m}$

$$(i.\,e.\ L(s\,;\chi_{i_1\cdots i_t})=\prod_{\mathfrak{p}\in G(\mathfrak{m})}(1-\chi_{i_1\cdots i_t}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{-1})\,.$$

In particular, the conjecture of Hasse holds for our $\zeta_\mathrm{A}(s)$.

Remark that the corresponding result holds for a complete non-singular curve C defined over k, if a jacobian variety J of C and a canonical mapping of C into J are defined over k, and the conditions (CM_I), (CM_{II}) are satisfied for $\mathrm{A}=\mathrm{J}$. This is immediately seen from the known relation of zeta function of C and the characteristic roots of $\mathrm{M}_l(\pi_\mathfrak{p})$. (cf. Weil [8] n°69; as to the explicite formula for the zeta function of C, see Taniyama [3], § 4, Theorem **1**$'$).

The author once obtained the same result by another method, in case where C is a field of degree $2n$, and k contains all algebraic conjugates of C. Under these assumptions, all endomorphisms in $C \cap \mathcal{A}(A)$ is defined over k. (cf. Taniyama [3]. § 4.)[2] But even in this case, our present condition (CM_{II}) is in general much weaker than this former condition in [3]. Moreover, although the case of general C could also be treated by the method in [3] if k is sufficiently large, our present method would be preferred as more direct and giving more insight.

20. We shall give an example, first treated by A. Weil by a quite different method.

Let C be a plane algebraic curve defined by an equation

$$\alpha x^n + \beta y^m = 1,$$

where n, m are natural numbers and α, β are non-zero algebraic integers. Denote by d the greatest common divisor of m and n, and put $m = m_1 d$, $n = n_1 d$. Then the geuns g of C is given by $2g = (n-1)(m-1)-(d-1)$. If we put $\omega_{ij} = x^i y^{j-n+1} dx$, the set $\{\omega_{ij}\}$ for all $i \geqq 0, j \geqq 0$ such that $(i+1)n_1 + (j+1)m_1 \leqq n_1 m_1 d - 1$ form a base of the space D(C) of all differentials of the first kind of C. Let ζ, η be respectively n-th and m-th roots of unity. Then the correspondence $\mu_0 : (x, y) \rightarrow (\zeta x, \eta y)$ of C onto itself induces an endomorphism μ of a jacobian variety J of a complete non-singular model of C. If we denote by $\mathrm{S}(\mu_0)$ the representation matrix of μ_0 with respect to the base $\{\omega_{ij}\}$ of D(C), $\mathrm{S}(\mu_0)$ is a diagonal matrix with diagonal elements $\zeta^{i+1}\eta^{j+1}$. Hence, if n and m are coprime, we see immediately that μ (for all ζ and η) generate over $\boldsymbol{Q}$ a commutative semi-simple algebra of degree $2g$. We can assume that J is defined over the field $Q(\alpha, \beta)$. Then μ is defined over the field $\boldsymbol{Q}(\alpha, \beta, \zeta, \eta)$. Hence our Theorem is applicable to this case taking $k \supset \boldsymbol{Q}(\alpha, \beta, \zeta, \eta)$ so that a canonical mapping is defined over k.[3]

University of Tokyo.

[2] A passage in the proof of proposition 3 in [3] (p. 38, *l.* 22) would indicate that $\mathrm{N}\mathfrak{P}' = (\iota\pi_{\mathfrak{P}'}) \cdot \overline{(\iota\pi_{\mathfrak{P}'})}$ determines the ideal decomposition of $(\iota\pi_{\mathfrak{P}'})$, which is in fact not the case, since both $\mathfrak{p}_i$ and $\bar{\mathfrak{p}}_i$ may divide $\iota\pi_{\mathfrak{P}'}$. It is easy however to amend this point and obtain the desired result. See author's forthcoming paper in collaboration with G. Shimura.

[3] It may be not difficult to obtain the same result by this method in case where n, m, are not coprime, considering also this $\mathrm{S}(\mu_0)$. But I have not examined this case in detail.

Bibliography

[1] M. Deuring, Die Zetafunktionen einer algebraischen Kurven von Geschlecht Eins, Nachr. Akad. Wiss. Göttingen, 1953, 85-94.

[2] G. Shimura, On complex multiplications, Proc. International Symposium on algebraic number theory, Tokyo-Nikko, 1955, 23-30.

[3] Y. Taniyama, Jacobian varieties and number fields, ibid. 31-45.

[4] A. Weil, On a certain type of characters of the idèle-class group of an algebraic number-field, ibid. 1-7.

[5] A. Weil, On the theory of complex multiplication, ibid. 9-22.

[6] A. Weil, Sur la théorie du corps de classes, Journ. Math. Soc. of Japan, 3 (1951), 1-35.

[7] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Paris, 1948.

[8] A. Weil, Variétés abéliennes et courbes algébriques, Paris, 1948.

[9] A. Weil, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc, 73 (1952), 487-495.