ON Γ-EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

KENKICHI IWASAWA[1]

Let p be a prime number. We call a Galois extension L of a field K a Γ-extension when its Galois group is topologically isomorphic with the additive group of p-adic integers. The purpose of the present paper is to study arithmetic properties of such a Γ-extension L over a finite algebraic number field K. We consider, namely, the maximal unramified abelian p-extension M over L and study the structure of the Galois group $G(M/L)$ of the extension M/L. Using the result thus obtained for the group $G(M/L)$, we then define two invariants $l(L/K)$ and $m(L/K)$, and show that these invariants can be also determined from a simple formula which gives the exponents of the p-powers in the class numbers of the intermediate fields of K and L. Thus, giving a relation between the structure of the Galois group of M/L and the class numbers of the subfields of L, our result may be regarded, in a sense, as an analogue, for L, of the well-known theorem in classical class field theory which states that the class number of a finite algebraic number field is equal to the degree of the maximal unramified abelian extension over that field.

An outline of the paper is as follows: in §1–§5, we study the structure of what we call Γ-finite modules and find, in particular, invariants of such modules which are similar to the invariants of finite abelian groups. In §6, we give some definitions and simple results on certain extensions of (infinite) algebraic number fields, making it clear what we mean by, e.g., an unramified extension, when the ground field is an infinite algebraic number field. In the last §7, we first show that the Galois group $G(M/L)$ as considered above is a Γ-finite module, then define the invariants $l(L/K)$ and $m(L/K)$, and finally prove our main formula using the group-theoretical results obtained in previous sections.

1. **Preliminaries.** 1.1. Let p be a prime number. We shall first recall some definitions and elementary properties of p-primary abelian groups.[2]

An address delivered before the Summer Meeting of the Society in Seattle on August 23, 1956 under the title of *A theorem on Abelian groups and its application in algebraic number theory* by invitation of the Committee to Select Hour Speakers for Annual and Summer Meetings; received by the editors August 28, 1957.

[1] Guggenheim Fellow. The present research was also supported in part by a National Science Foundation grant.

[2] For the theory of abelian groups in general, cf. I. Kaplansky, *Infinite abelian groups*, University of Michigan Press, 1954.

A discrete group is called p-primary if it is the direct limit of a family of finite p-groups, or, what amounts to the same, if it is locally finite and if every element of the group has a finite order which is a power of p. A compact group is called p-primary if it is the inverse limit of finite p-groups. For a finite group, which is at the same time discrete and compact, both definitions coincide and the group is p-primary if and only if it is a p-group.

Now, let A be a p-primary discrete abelian (additive) group. If the orders of elements in A have a fixed upper bound, i.e. if $p^nA=0$ for some $n\geqq 0$, A is called a group of bounded order, or, simply, bounded. Let A' be the subgroup of elements a in A satisfying $pa=0$. If A' is a finite group of order p^l, A is called a group of finite rank l. A is called divisible if $pA=A$.

It is clear from the definition that the character group of a p-primary discrete abelian group is a p-primary compact abelian group and, conversely, the character group of a p-primary compact abelian group is a p-primary discrete abelian group.

Let $\{A, X\}$ be such a dual pair of a p-primary discrete abelian group A and a p-primary compact abelian group X. Obviously, $p^nA=0$ if and only if $p^nX=0$. In such a case, the compact abelian group X is also called bounded. As the subgroup A' of A defined above is dual to X/pX, A is of finite rank l if and only if X/pX is a finite group of order p^l. If this is the case, the compact abelian group X is called a group of finite rank l; for a finite abelian p-group, both definitions give the same rank l. Finally, A is divisible if and only if X is torsion-free.

1.2. We shall next give a typical example of such a dual pair of a p-primary discrete abelian group and a p-primary compact abelian group.

For every integer $n\geqq 0$, let Z_{p^n} denote a cyclic group of order p^n. Clearly, for each $n\geqq 0$, there exist an isomorphism ϕ_n of Z_{p^n} into $Z_{p^{n+1}}$ and a homomorphism ψ_n of $Z_{p^{n+1}}$ onto Z_{p^n}. Let Z_{p^∞} be the direct limit of the sequence of cyclic groups Z_{p^n} relative to ϕ_n. Z_{p^∞} is then a p-primary discrete abelian group and is isomorphic with the factor group Q_p/O_p, where Q_p denotes the additive group of p-adic numbers and O_p the subgroup of p-adic integers. On the other hand, the inverse limit of the groups Z_{p^n} relative to ψ_n gives a p-primary compact abelian group isomorphic with O_p which is a compact group with respect to its natural p-adic topology. Since the finite groups Z_{p^n} are self-dual, it follows that Z_{p^∞} and O_p, or, Q_p/O_p and O_p, form a dual pair of p-primary abelian groups.

The duality between Q_p/O_p and O_p can be seen also directly as follows. Q_p is a locally compact abelian group in its p-adic topology

and there is a character χ of Q_p such that the kernel of the homomorphism $a \to \chi(a)(a \in Q_p)$ is O_p. The inner product on Q_p defined by:[3]

$$(a, b) = \chi(ab), \qquad a, b \in Q_p,$$

then gives a dual pairing of Q_p with itself such that the annihilator of O_p in Q_p coincides with O_p itself. Hence, the pairing (a, b) induces a dual pairing of Q_p/O_p and O_p.

1.3. Let G be a totally disconnected compact multiplicative group with the unity element 1. A topological additive abelian group U will be called a G-module when G acts on U so that $1 \cdot u = u$ for every u in U and that the mapping $\sigma \times u \to \sigma u$ of $G \times U$ into U is continuous.

Let $\{A, X\}$ be a dual pair as considered in 1.1 and suppose both A and X are G-modules in the sense defined above. We call A and X dual G-modules if there exists a dual pairing (a, x) of A and X such that

$$(\sigma a, \sigma x) = (a, x) \tag{1}$$

for every σ in G, a in A, and x in X.

Now, let (a, x) be any dual pairing of A and X. Suppose first that only A is given a structure of a G-module. We can then define, in a unique way, the product σx of σ in G and x in X so that X becomes a G-module satisfying (1). Thus, if A is a G-module, the dual group X can be also made into a G-module so that A and X form a pair of dual G-modules with respect to a given pairing of A and X. The structure of the G-module X defined in this way depends upon the choice of the pairing (a, x), but it is uniquely determined up to an automorphism of X. Similarly, if X is a G-module, we can define a structure of a G-module on the dual group A so that A and X form a pair of dual G-modules.

1.4. Let G be a totally disconnected compact group and $\{A, X\}$ a dual pair of a p-primary discrete abelian group A and a p-primary compact abelian group X. Defining $\sigma a = a$, $\sigma x = x$ for any a in A, x in X, and σ in G, we may consider $\{A, X\}$ as a pair of dual G-modules as defined above. Let N_α be any open normal subgroup of G and $Z(G_\alpha)$ the group ring of the finite group $G_\alpha = G/N_\alpha$ over the ring of rational integers Z. We may consider $Z(G_\alpha)$ as a G-module by defining

$$\sigma w = \sigma' w, \qquad \sigma \in G, w \in Z(G_\alpha),$$

where σ' is the image of σ under the canonical homomorphism $G \to G_\alpha$. Let $\mathrm{Hom}(Z(G_\alpha), A)$ be the group of all homomorphisms of $Z(G_\alpha)$ into A. Since both $Z(G_\alpha)$ and A are G-modules, $\mathrm{Hom}(Z(G_\alpha), A)$

[3] ab is the product of a and b as elements of the field Q_p.

is also made into a G-module in a natural way.[4] Furthermore, if N_β is an open normal subgroup of G contained in N_α, the canonical homomorphism $G_\beta = G/N_\beta \to G_\alpha$ induces a natural G-isomorphism $\phi_{\beta,\alpha}$ of $\mathrm{Hom}(Z(G_\alpha), A)$ into $\mathrm{Hom}(Z(G_\beta), A)$. Hence, considering the set of all groups $\mathrm{Hom}(Z(G_\alpha), A)$ attached one for each open normal subgroup N_α of G, we can form the direct limit $M_1(G, A)$ of these discrete G-modules $\mathrm{Hom}(Z(G_\alpha), A)$ relative to the homomorphisms $\phi_{\beta,\alpha}$. By the definition, $M_1(G, A)$ is a discrete G-module. Clearly, $\mathrm{Hom}(Z(G_\alpha), A)$ can be identified with the additive group of all functions defined on G_α taking values in A, i.e. with the additive group of those functions on G with values in A which are constant on each coset of G mod N_α. Since G is totally disconnected and A is discrete, we may then consider $M_1(G, A)$ as the G-module of all continuous functions defined on G taking values in A, where the action of G on $M_1(G, A)$ is defined by:

$$(\sigma f)(\tau) = f(\sigma^{-1}\tau), \qquad f \in M_1(G, A), \sigma \in G.$$

We now consider the tensor product $Z(G_\alpha) \otimes X$ of $Z(G_\alpha)$ and X over Z. Clearly, $Z(G_\alpha) \otimes X$ is a compact G-module. Furthermore, the canonical homomorphism $G_\beta \to G_\alpha$ again induces a continuous homomorphism $\psi_{\alpha,\beta}$ of $Z(G_\beta) \otimes X$ onto $Z(G_\alpha) \otimes X$. Hence, the inverse limit of the family of compact G-modules $Z(G_\alpha) \otimes X$ relative to the homomorphisms $\psi_{\alpha,\beta}$ gives us a compact G-module $M_2(G, X)$.

Now, by the assumption, there is a dual pairing (a, x) of A and X. Then, there also exists a unique dual pairing $(s, t)_\alpha$ of the discrete G-module $\mathrm{Hom}(Z(G_\alpha), A)$ and the compact G-module $Z(G_\alpha) \otimes X$ such that

$$(s, w \otimes x)_\alpha = (s(w), x)$$

for any s in $\mathrm{Hom}(Z(G_\alpha), A)$, w in $Z(G_\alpha)$, and x in X. Since

$$(s, \psi_{\alpha,\beta}(t'))_\alpha = (\phi_{\beta,\alpha}(s), t')_\beta, \qquad s \in \mathrm{Hom}(Z(G_\alpha), A), t' \in Z(G_\beta) \otimes X,$$

for $N_\beta \subset N_\alpha$, those pairings $(s, t)_\alpha$ together define a dual pairing of $M_1(G, A)$ and $M_2(G, X)$. We can thus obtain, for each dual pair $\{A, X\}$, a pair of dual G-modules $M_1(G, A)$ and $M_2(G, X)$.

2. **Some definitions.** 2.1. Let Γ be a multiplicative topological group isomorphic with the additive group of p-adic integers O_p. We shall fix such a group Γ once and for all in the following discussions. Γ is a totally disconnected compact abelian group and, for each $n \geqq 0$, it contains an open subgroup Γ_n such that Γ/Γ_n is a cyclic group of order p^n. We have, then, a sequence of subgroups $\Gamma = \Gamma_0 \supset \Gamma_1$

[4] Cf. the definition of σf below.

$\supset\Gamma_2\supset\cdots$, and these subgroups form a fundamental system of neighborhoods of the identity 1 in Γ. Furthermore, there exists no nontrivial closed subgroup of Γ other than the Γ_n.

For convenience, we take an element γ of Γ not contained in Γ_1 and fix it once and for all in the following. For each $n\geqq 0$, put

$$\gamma_n = \gamma^{p^n}.$$

Then, each γ_n generates an infinite cyclic group which is everywhere dense in Γ_n. In particular, $\gamma=\gamma_0$ generates an everywhere dense subgroup in Γ. We also put

$$\omega_n = 1 - \gamma_n, \qquad n \geqq 0.$$

ω_n is an element of the group ring of the cyclic group generated by γ over the ring of rational integers Z.

2.2. In what follows, up to the end of §5, we shall exclusively deal with p-primary discrete or compact abelian groups which are also Γ-modules in the sense of 1.3. Therefore, if there is no risk of misunderstanding, we shall call those groups simply discrete or compact modules. Similarly, Γ-invariant subgroups, Γ-homomorphisms, etc., of those modules will be simply called submodules, homomorphisms, etc.

Let A be such a discrete module. For each $n\geqq 0$, we denote by A_n the submodule of all elements a in A such that $\sigma a=a$ for every σ in Γ_n. Since γ_n generates an everywhere dense subgroup of Γ_n, A_n is the submodule of all a in A satisfying $\gamma_n a=a$, i.e. $\omega_n a=0$. Since Γ_{n+1} is contained in Γ_n, A_n is a submodule of A_{n+1}.

LEMMA 2.1. *A is the union of the submodules A_n, $n\geqq 0$.*

PROOF. Let a be any element in A. Since $1\cdot a=a$, A is discrete and the mapping $\sigma\times a\to\sigma a$ is continuous, there exists a neighborhood Γ_n ($n\geqq 0$) of 1 in Γ such that $\sigma a=a$ for every σ in the neighborhood Γ_n. a is then contained in A_n.

We notice that, for a discrete abelian group A with operator domain Γ, the continuity of the mapping $\sigma\times a\to\sigma a$ follows, conversely, from the fact that A is the union of all A_n, $n\geqq 0$.

For each $n\geqq 0$, let A_n^* denote the submodule of A generated by elements of the form $(1-\sigma)a$ where σ and a are arbitrary elements in Γ_n and A respectively. Since γ_n generates an everywhere dense subgroup of Γ_n, A_n^* coincides with $\omega_n A=(1-\gamma_n)A$.

Now the discrete module A will be called *n-regular* if $A_n^*=A$, and A will be called *regular* if it is n-regular for all $n\geqq 0$. Clearly, a homomorphic image of an n-regular (regular) module is n-regular (regular).

In particular, any quotient module A/B of an n-regular (regular) module A is n-regular (regular). The sum of n-regular (regular) submodules of a discrete module is also n-regular (regular). Hence, every discrete module has a unique maximal n-regular (regular) submodule.

LEMMA 2.2. *Let B be a submodule of a discrete module A and let B_n and C_n be the submodules of B and $C=A/B$, respectively, defined similarly as A_n for A. Then, $B_n=A_n\cap B$, and, if B is n-regular, $C_n=(A_n+B)/B\cong A_n/B_n$.*

PROOF. It is clear from the definition that $B_n=A_n\cap B$ and that $(A_n+B)/B$ is contained in C_n. Suppose B be n-regular. Let $\bar{a}$ be any element in C_n and a an element of A in the residue class $\bar{a}$. As $\omega_n\bar{a}=0$, $\omega_n a$ is contained in B, and, as B is n-regular, $\omega_n a=\omega_n b$ for some b in B. $a'=a-b$ is then also in the same residue class $\bar{a}$ and it is contained in A_n. Hence, C_n is contained in $(A_n+B)/B$.

2.3. We now define a certain kind of discrete modules.

Let A be a discrete module and A_n ($n\geqq 0$) the submodules of A as defined in 2.2. A is called Γ-*finite* if every A_n is a group of finite rank, and A is called *strictly* Γ-*finite* if every A_n is a finite group.

Suppose A be strictly Γ-finite. Then, the order of the finite group A_n is a power of p. We denote the exponent of p in the order of A_n by $c(n;A)$. For given A, $c(n;A)$ then defines a nondecreasing function of the integers $n\geqq 0$, and we call it the *characteristic function* of the strictly Γ-finite discrete module A.

Clearly, a submodule B of a Γ-finite discrete module A is also Γ-finite. If A is strictly Γ-finite, so is B, and $c(n;B)\leqq c(n;A)$ for all $n\geqq 0$. The following lemma is also an immediate consequence of Lemma 2.2 and of the definition.

LEMMA 2.3. *Let B be a regular submodule of a discrete module A. Then, A is (strictly) Γ-finite if and only if both A/B and B are (strictly) Γ-finite, and, if A is strictly Γ-finite,*

$$c(n;A) = c(n;A/B) + c(n;B),$$

for all $n\geqq 0$.

2.4. We now consider compact modules, i.e. p-primary compact abelian groups which also form Γ-modules.

Let X be such a module. For each $n\geqq 0$, let X_n be the closed submodule of all a in X satisfying $\sigma a=a$ for every σ in Γ_n, and X_n^* the closure of the subgroup of X generated by all elements of the form $(1-\sigma)x$ where σ and x are arbitrary elements of Γ_n and X, respec-

tively. As γ_n generates an everywhere dense subgroup of Γ_n, X_n is the submodule of all a in X satisfying $\omega_n a = 0$, and X_n^* coincides with $\omega_n X$.

Now, as stated in general in 1.3, there exists a discrete module A such that A and X form a pair of dual Γ-modules, and such an A is, up to isomorphisms, uniquely determined by X. Let (a, x) be the dual pairing of A and X such that $(\sigma a, \sigma x) = (a, x)$ for every σ in Γ. Since

$$((1 - \sigma^{-1})a, x) = (a, (1 - \sigma)x), \qquad a \in A, x \in X, \sigma \in \Gamma,$$

both $\{A_n, X_n^*\}$ and $\{A_n^*, X_n\}$ are pairs of mutually orthogonal submodules of A and X, respectively, relative to the pairing (a, x). Therefore, A_n and X/X_n^* form a pair of dual Γ-modules, and so do A/A_n^* and X_n. By Lemma 2.1, A is the union of all A_n $(n \geqq 0)$. Hence, by the above, the intersection of all X_n^* $(n \geqq 0)$ is 0. It also follows that A is n-regular (i.e. $A_n^* = A$) if and only if $X_n = 0$.

Now, we call a compact module X Γ-*finite* if every group X/X_n^* has a finite rank, and we call it *strictly* Γ-*finite* if every X/X_n^* is a finite group. In other words, a compact module X is called (strictly) Γ-finite if and only if the discrete module A dual to X is (strictly) Γ-finite. An *n-regular* (*regular*) compact module X is defined similarly, either by $X_n = 0$ (for all $n \geqq 0$) or by the fact that it is dual to an n-regular (regular) discrete module.

Suppose that X be strictly Γ-finite. By the definition, X/X_n^* is a finite p-group for every $n \geqq 0$, and we denote by $c(n; X)$ the exponent of p in the order of X/X_n^*. We thus obtain a nondecreasing function $c(n; X)$ of the integers $n \geqq 0$ and call it the *characteristic function* of the strictly Γ-finite compact module X. Clearly, if A is a strictly Γ-finite discrete module dual to X, then

$$c(n; A) = c(n; X)$$

for all $n \geqq 0$.

In the following, we shall consider the structure of discrete modules and that of compact modules in parallel; by the duality between discrete and compact modules, any results on discrete (strictly) Γ-finite modules will then immediately give us corresponding results on compact (strictly) Γ-finite modules, and vice versa.

2.5. Let G be a compact group containing a closed normal subgroup X such that X is a p-primary compact abelian group and that $G/X = \Gamma$. Then Γ acts on X in an obvious way and X is thus made into a compact (Γ-)module in the sense of 2.2.[5] Furthermore, it is

[5] Of course, we understand that X is then considered as an additive group.

easy to see that the group extension G/X splits. Hence the structure of the compact group G is completely determined by the structure of the compact module X. On the other hand, given any compact module X, we can immediately find a compact group G to which X is related as stated above. Thus, there is a one-one correspondence between the set of all types of compact modules and the set of all types of group extensions of p-primary compact abelian groups by Γ.

In such a correspondence, the fact that a compact module X is Γ-finite can be interpreted for the corresponding compact group G as follows: let G_n $(n \geqq 0)$ be the closed subgroup of G such that $X \subset G_n$ and $G_n/X = \Gamma_n$. By a simple computation of commutators in G, we see that the topological commutator group $[G_n, G_n]$ of G_n is equal to the submodule $X_n^* = \omega_n X$ of X given in 2.4. Therefore X is Γ-finite if and only if $X/[G_n, G_n]$ has a finite rank for every $n \geqq 0$, or, equivalently, if and only if $G_n/[G_n, G_n]$ has a finite rank for every $n \geqq 0$.

In our later applications, Γ-finite compact modules will be obtained from compact groups such as G in the manner as described above.

3. **Modules of finite ranks.** 3.1. Clearly, every discrete or compact module of finite rank is Γ-finite.

Let A be a discrete module of finite rank. As a p-primary abelian group, A is then the direct sum of a finite group and a subgroup B isomorphic with $Z_{p^\infty}^l$, the direct sum of l copies of Z_{p^∞} $(l \geqq 0)$. B is the maximal divisible subgroup of A and is a characteristic subgroup of A. Hence B is also a (Γ-invariant) submodule of A. We shall next study the structure of such an A in the case $A = B$, i.e. in the case A is divisible.

LEMMA 3.1. *Let A be a divisible discrete module of finite rank. Then A is the direct sum of a regular submodule B and a submodule C such that $\omega_n^m C = 0$ for some $m \geqq 0$ and $n \geqq 0$. Furthermore, such a decomposition $A = B + C$ is unique for A, and B is also the unique maximal regular submodule of A.*

PROOF. Let B be the intersection of the submodules $\omega_n^m A$ for all $m \geqq 0$ and $n \geqq 0$. As a homomorphic image of divisible A, every $\omega_n^m A$ is also divisible, and, if $m' \geqq m$, $n' \geqq n$, then $\omega_{n'}^{m'} A$ is contained in $\omega_n^m A$. Since A is of finite rank, it follows that $B = \omega_n^m A$ whenever both m and n are sufficiently large, i.e. whenever $m \geqq m_0$ and $n \geqq n_0$ for some fixed $m_0 \geqq 0$, $n_0 \geqq 0$. But, then, $\omega_n B = \omega_n^{m+1} A = B$ for any $n \geqq n_0$, and B is, hence, a regular submodule of A.

Let C' be the kernel of the endomorphism of $A: a \to \omega_{n_0}^{m_0} a$. Since

$\omega_{n_0}^{m_0}A = B = \omega_{n_0}^{m_0}B$, we have $A = B + C'$, and since A and B are both divisible, we also have $A = B + p^s C'$ for any $s \geqq 0$. Now, choose s so large that $C = p^s C'$ is divisible. It then follows from the isomorphism $A/C' \cong B = \omega_{n_0}^{m_0}A$ that the rank of A is the sum of the ranks of B and C, and, hence, the sum $A = B + C$ is direct.

Next, suppose that $A = B^* + C^*$ be any direct sum decomposition of A such that B^* is regular and $\omega_n^m C^* = 0$ for some m and n. Since $\omega_{n'}^{m'} C^* = 0$ for any $m' \geqq m$ and $n' \geqq n$, we may assume that $m \geqq m_0$ and $n \geqq n_0$. We have then $B^* = \omega_n^m B^* = \omega_n^m A = B$. Therefore, $B = \omega_{n_0}^{m_0}A = \omega_{n_0}^{m_0}B + \omega_{n_0}^{m_0}C^* = B + \omega_{n_0}^{m_0}C^*$ and, consequently, $\omega_{n_0}^{m_0}C^* = 0$. Thus C^* is contained in C', and since C^* is divisible as a direct summand of A, we then see easily that $C^* = C$. The fact that B is the unique maximal regular submodule of A can be proved in a similar way.

By the duality between discrete and compact modules, we can immediately obtain the following result from the above lemma:

LEMMA 3.2. *Let X be a torsion-free compact module of finite rank. Then X is the direct sum of a regular submodule U and a submodule V such that $\omega_n^m V = 0$ for some $m \geqq 0$ and $n \geqq 0$. Furthermore, such a decomposition $X = U + V$ is unique for X, and V also is the unique minimal submodule of X such that X/V is regular.*

3.2. Let X be as in Lemma 3.2 and let l be the rank of X. As a p-primary compact abelian group, X can be then identified with O_p^l, the direct sum of l copies of O_p, and the mapping $x \to \gamma x$ defines a continuous automorphism of O_p^l. Thus, there exists an $l \times l$ matrix M with entries in O_p such that the determinant of M is a p-adic unit and that

$$\gamma x = xM$$

for any $x = (x_1, \cdots, x_l)$ in O_p^l $(x_i \in O_p)$.[6] Put $M_n = M^{p^n}$ $(n \geqq 0)$ so that

$$\gamma_n x = xM_n, \qquad \omega_n x = x(I - M_n), \qquad x \in X,$$

I being the $l \times l$ identity matrix. Since the intersection of all $X_n^* = \omega_n X$ is 0, there exists an $s \geqq 0$ such that X_s^* is contained in pX. We have then

$$M_s \equiv I \bmod p, \qquad M_s = M^{p^s}. \tag{2}$$

On the other hand, if we are given any $l \times l$ integral p-adic matrix M satisfying (2) for some $s \geqq 0$, we can uniquely define a structure of a Γ-module on O_p^l so that $\gamma x = xM$ holds for any x in the compact

[6] xM is the product of the vector ($1 \times l$ matrix) x and the $l \times l$ matrix M, and it is again a vector in $X = O_p^l$.

module $X=O_p^l$; the condition (2) then ensures the continuity of the action of Γ on O_p^l. Furthermore, two such matrices M_1 and M_2 define isomorphic compact modules on O_p^l if and only if $M_2=TM_1T^{-1}$ with a suitable integral p-adic matrix T whose determinant is a p-adic unit. Thus the classification problem for all torsion-free compact modules of rank l can be reduced to the problem of classifying all $l\times l$ integral p-adic matrices satisfying (2) for some $s\geqq 0$, with respect to the equivalence as stated above.

Now, let X and M be again as above. For any $n\geqq s+1$, it follows from (2) that

$$M_n \equiv I \mod p^2,$$

namely, that $M_n=I+p^2N$ with a suitable integral p-adic matrix N. By a simple computation, we then see that, for any $t\geqq 0$,

$$\sum_{i=0}^{p^t-1} M_n^i = p^t(I + pN_1),$$

with an integral p-adic matrix N_1. Since the determinant of $I+pN_1$ is a p-adic unit, it follows that

$$X\left(\sum_{i=0}^{p^t-1} M_n^i\right) = p^tX(I + pN_1) = p^tX.$$

Putting, in general,

$$\nu_{m,n} = \sum_{i=0}^{p^{m-n}-1} \gamma_n^i, \qquad m \geqq n \geqq 0, \tag{3}$$

we then get from the above that $\nu_{n+t,n}X=p^tX$ and, consequently, that

$$[X: \nu_{m,n}X] = [X: p^{m-n}X] = p^{l(m-n)},$$

for any integers $m\geqq n\geqq s+1$. Thus, the following lemma is proved:

LEMMA 3.3. *Let X be a torsion-free compact module of rank l. Then there exists an integer $n_0\geqq 0$ such that, for any integers m, n satisfying $m\geqq n\geqq n_0$, the index $[X: \nu_{m,n}X]$ is given by*

$$[X: \nu_{m,n}X] = p^{l(m-n)}.$$

3.3. Let X and M be as above. Since $X_n^*=\omega_nX=X(I-M_n)$, X/X_n^* is a finite module if and only if the determinant $|I-M_n|$ is different from 0. Therefore, X is strictly Γ-finite if and only if none of the p^nth roots of unity, for $n=0, 1, 2, \cdots$, is a characteristic root of the matrix M.

LEMMA 3.4. *A torsion-free compact module of finite rank is strictly* Γ*-finite if and only if it is regular.*

PROOF. As stated above, such a compact module X is strictly Γ-finite if and only if $|I-M_n| \neq 0$ for every $n \geqq 0$. But the condition $|I-M_n| \neq 0$ is equivalent to the fact that there is no $x \neq 0$ in X satisfying $x(I-M_n)=0$, i.e. $\omega_n x = 0$. Thus X is strictly Γ-finite if and only if the submodule X_n of X as defined in 2.4 is 0 for every $n \geqq 0$. The lemma then follows immediately from the remark also given in 2.4.

By the duality, we see that a divisible discrete module of finite rank is strictly Γ-finite if and only if it is regular.

LEMMA 3.5. *Let X be a torsion-free compact module of rank l and let X be strictly* Γ*-finite. Then there exists an integer n_0 such that, for $n \geqq n_0$, the characteristic function of X is given by*

$$c(n; X) = ln + u,$$

where u is a suitable integer independent of n.

PROOF. By the previous lemma, X is regular and $X_n = 0$ for every $n \geqq 0$. Hence the endomorphism $x \to \omega_n x$ of X is one-one, and we see that

$$[X: \nu_{m,n}X] = [\omega_n X: \omega_n \nu_{m,n} X] = [\omega_n X: \omega_m X],$$

for any $m \geqq n \geqq 0$. But, Lemma 3.3, $[X: \nu_{m,n}X] = p^{l(m-n)}$ when $m \geqq n \geqq n_0$. Therefore, if $n \geqq n_0$,

$$[X: \omega_n X] = [X: \omega_{n_0} X][\omega_{n_0} X: \omega_n X] = [X: \omega_{n_0} X] p^{l(n-n_0)},$$

and if we put $[X: \omega_{n_0} X] p^{-ln_0} = p^u$, then

$$c(n; X) = ln + u, \qquad n \geqq n_0.$$

Again, by the duality, we obtain the corresponding result on divisible discrete modules of finite rank l; if A is such a module, there exists an integer $n_0 \geqq 0$ such that

$$c(n; A) = ln + u, \qquad n \geqq n_0,$$

with a suitable constant u.

4. Bounded modules. 4.1. We shall next consider Γ-finite discrete modules of bounded order. Clearly, all those modules are also strictly Γ-finite.

We shall first define an important class of such modules. Let m be any non-negative integer. Let $M_1(\Gamma, Z_{p^m})$ be, as defined in general in 2.4, the discrete Γ-module formed by all continuous functions on Γ

with values in Z_{p^m}. Clearly, if a is any element in $M_1(\Gamma, Z_{p^m})$, then $p^m a = 0$. Hence, $M_1(\Gamma, Z_{p^m})$ is a bounded module, and we denote it simply by $E(m)$. As noticed above, $p^m E(m) = 0$, and, in particular, $E(0) = 0$.

LEMMA 4.1. *Let $0 \leqq l \leqq m$. Then $p^{m-l}E(m)$ is the submodule of all a in $E(m)$ such that $p^l a = 0$, and*

$$E(m)/p^{m-l}E(m) \cong p^l E(m) \cong E(m-l).$$

PROOF. The endomorphism $c \to p^l c$ of the cyclic group Z_{p^m} maps Z_{p^m} onto $p^l Z_{p^m} \cong Z_{p^{m-l}}$ and its kernel is $p^{m-l}Z_{p^m}$. Hence, the endomorphism $a \to p^l a$ of $E(m)$ induces the above isomorphisms.

LEMMA 4.2. *The discrete module $E(m)$ is bounded, regular and strictly Γ-finite, and its characteristic function is given by*

$$c(n; E(m)) = mp^n, \qquad n \geqq 0.$$

PROOF. By the definition, $E(m)$ is the union of a sequence of submodules $\mathrm{Hom}(Z(\Gamma/\Gamma_n), Z_{p^m})$, $n \geqq 0$, each considered as the submodule of all continuous functions on Γ with values in Z_{p^m} which are constant on every coset of Γ mod Γ_n. It is then clear that $\mathrm{Hom}(Z(\Gamma/\Gamma_n), Z_{p^m})$ coincides with the submodule $E(m)_n$ of all a in $E(m)$ such that $\sigma a = a$ for every σ in Γ_n. Since $\mathrm{Hom}(Z(\Gamma/\Gamma_n), Z_{p^m})$ is a group of order p^{mp^n}, $E(m)$ is strictly Γ-finite and $c(n; E(m)) = mp^n$.

Now, let $n \geqq 0$ be fixed. For any element a in $E(m)$, choose an integer $s \geqq n$ so that a is in $E(m)_s$ and that $\nu_{s,n} a = 0$, where $\nu_{s,n}$ is defined as (3) in 3.2. This is always possible, because if a is in $E(m)_t$, $t \geqq n$ and $s = t + m$, then $\nu_{s,n} a = p^m \nu_{t,n} a = 0$. On the other hand, as a (Γ_n/Γ_s)-group, $E(m)_s = \mathrm{Hom}(Z(\Gamma/\Gamma_s), Z_{p^m})$ is isomorphic with the direct sum of p^n copies of $Z_{p^m}(\Gamma_n/\Gamma_s) = Z(\Gamma_n/\Gamma_s) \otimes Z_{p^m}$. Hence, the cohomology groups $H^i(\Gamma_n/\Gamma_s, E(m)_s)$ are 0 for all i. Since $\nu_{s,n} a = 0$ and since Γ_n/Γ_s is a cyclic group generated by the coset of γ_n mod Γ_s, there then exists an element b in $E(m)_s$ such that $a = (1 - \gamma_n)b = \omega_n b$. As a was an arbitrary element of $E(m)$, $E(m)$ is n-regular for every $n \geqq 0$, and the lemma is proved.

4.2. Now, let A be a discrete module such that $pA = 0$. We may then consider A as a vector space over the prime field P of characteristic p and the endomorphism $a \to \omega_0 a = (1 - \gamma)a$ as a linear transformation of the vector space. Since P is a field of characteristic p,

$$\omega_n a = (1 - \gamma^{p^n})a = (1 - \gamma)^{p^n} a = \omega_0^{p^n} a, \qquad n \geqq 0,$$

for every a in A. Hence, given any element a of A, there always exists, by Lemma 2.1, an integer $i \geqq 0$ such that $\omega_0^i a = 0$. Suppose that A is

Γ-finite and that the submodule A_0 of A defined as before has a finite order p^s ($s \geqq 0$). We then see easily that the vector space A is decomposed into the direct sum of s subspaces $A^{(j)}$ such that each $A^{(j)}$ is a direct indecomposable submodule of A and has either a finite or a countable number of basis $a_i^{(j)}$, $0 \leqq i < \dim A^{(j)}$, over P, with the property $\omega_0 a_0^{(j)} = 0$ and $\omega_0 a_i^{(j)} = a_{i-1}^{(j)}$ for $i > 0$.

Now, consider the module $E(1)$. Since $pE(1) = 0$, $\dim E(1) = \infty$, and since $E(1)_0$ has order p, it follows from the above that $E(1)$ is direct indecomposable and has a basis e_i, $0 \leqq i < \infty$, such that $\omega_0 e_0 = 0$, $\omega_0 e_i = e_{i-1}$ for $i > 0$.

LEMMA 4.3. *Let A be a Γ-finite discrete module such that $pA = 0$. Then, A is the direct sum of a finite submodule and a finite number of submodules each isomorphic with $E(1)$.*

PROOF. By what was mentioned above, A is the direct sum of a finite number of submodules $A^{(j)}$ as described there. Suppose $A^{(j)}$ is infinite dimensional. Then, $A^{(j)}$ has a basis $a_i^{(j)}$, $0 \leqq i < \infty$, such that $\omega_0 a_0^{(j)} = 0$ and $\omega_0 a_i^{(j)} = a_{i-1}^{(j)}$ for $i > 0$, and it is clear that there is an isomorphism ϕ of the module $E(1)$ onto $A^{(j)}$ such that $\phi(e_i) = a_i^{(j)}$, $0 \leqq i < \infty$. Thus, every infinite dimensional $A^{(j)}$ is isomorphic with $E(1)$, and the lemma is proved.

It follows immediately from the lemma that if the rank of a Γ-finite discrete module A is infinite, A contains a submodule isomorphic with $E(1)$; for the submodule A' of all a in A satisfying $pa = 0$ is then an infinite Γ-finite discrete module with the property $pA' = 0$ and, hence, contains a submodule isomorphic with $E(1)$.

Now, let B be an infinite submodule of $E(1)$. By the above, B contains a submodule B' isomorphic with $E(1)$. Then, by Lemma 4.2, the submodules $E(1)_n$ and $B_n' = E(1)_n \cap B'$ have the same order p^n. Hence $E(1)_n = B_n'$ for all $n \geqq 0$, and $E(1) = B' = B$. Thus, there is no infinite submodule of $E(1)$ except $E(1)$ itself. It follows, in particular, that a regular submodule of $E(1)$ is either 0 or $E(1)$ itself, for a nontrivial finite submodule of $E(1)$ obviously can not be regular.

4.3. We shall now prove some lemmas on the modules $E(m)$.

LEMMA 4.4. *Let B be a regular submodule of $E(m)$, $m \geqq 0$. Then, $B = p^l E(m)$ for some l, $0 \leqq l \leqq m$.*

PROOF. If $m = 0$, the lemma is trivial. Suppose that $m > 0$ and that the lemma is proved for $m-1$. Consider the submodule $\overline{B} = (B + pE(m))/pE(m)$ of $E(m)/pE(m)$. $\overline{B}$ is a regular submodule of $E(m)/pE(m)$ and the latter is isomorphic with $E(1)$ by Lemma 4.1. Hence, by the remark in 4.2, either $\overline{B} = E(m)/pE(m)$ or $\overline{B} = 0$. In

the first case, $E(m)=B+pE(m)$ and, consequently, $E(m)=B$.[7] In the second case, B is contained in $pE(m)$. But, as $pE(m)\cong E(m-1)$ by Lemma 4.1, it follows from the induction assumption that $B=p^{l-1}(pE(m))=p^lE(m)$ for some $0\leqq l\leqq m$.

LEMMA 4.5. *Let m be any positive integer. Then, $E(m)$ has a basis e_i, $0\leqq i<\infty$, such that*

(i) *every e_i has order p^m,*

(ii) *$\omega_0 e_0=0$ and $\omega_0 e_i=e_{i-1}$ for $i>0$.*

PROOF. For $m=1$, the lemma is already proved in 4.2. Let $m>1$. By Lemma 4.1, $E(m)/pE(m)\cong E(1)$. Hence, we take a basis $\bar{e}_i$, $0\leqq i<\infty$, of $E(m)/pE(m)$ such that $\omega_0\bar{e}_0=0$ and $\omega_0\bar{e}_i=\bar{e}_{i-1}$ for $i>0$. Let e_0' be an element of $E(m)$ such that $\bar{e}_0$ is the coset of e_0' mod $pE(m)$. Since $\omega_0\bar{e}_0=0$, $\omega_0 e_0'$ is contained in $pE(m)$. But, by Lemmas 4.1, 4.2, $pE(m)$ is regular. Hence there is an element b_0 in $pE(m)$ such that $\omega_0 e_0'=\omega_0 b_0$. Put $e_0=e_0'-b_0$. Then, e_0 is still in the coset $\bar{e}_0$ and $\omega_0 e_0=0$. Let e_1' be an element of $E(m)$ such that $\bar{e}_1$ is the coset of e_1' mod $pE(m)$. Since $\omega_0\bar{e}_1=\bar{e}_0$, $\omega_0 e_1'-e_0$ is contained in $pE(m)$, and, as $pE(m)$ is regular, there is an element b_1 in $pE(m)$ such that $\omega_0 e_1'-e_0=\omega_0 b_1$. Put $e_1=e_1'-b_1$. Then, e_1 is again in the coset $\bar{e}_1$ and $\omega_0 e_1=e_0$. Proceeding similarly, we can find elements $e_0, e_1, e_2, \cdots$ in $E(m)$, successively, so that each e_i is in the coset $\bar{e}_i$ and satisfies the condition (ii) of the lemma. As the cosets of e_i mod $pE(m)$ form a basis of $E(m)/pE(m)$, the elements e_i generate the group $E(m)$. Let n be any positive integer. Take an integer s such that all $e_0, e_1, \cdots, e_{n-1}$ are contained in $E(m)_s$. Since $e_0, e_1, \cdots, e_{n-1}$ are independent mod $pE(m)$ and, consequently, also mod $pE(m)_s$, and since $E(m)_s=\mathrm{Hom}\,(Z(\Gamma/\Gamma_s), Z_{p^m})$ is an abelian group of type $(p^m, \cdots, p^m)$ with rank p^s, the n elements $e_0, e_1, \cdots, e_{n-1}$ generate a subgroup of order p^{mn} in $E(m)_s$. Therefore, every one of $e_0, e_1, \cdots, e_{n-1}$ has order p^m and they form a basis of the subgroup generated by themselves. Thus, the lemma is proved.

LEMMA 4.6. *Let A be a regular discrete module satisfying $p^mA=0$, $m>0$, and let B be a submodule of A containing pA such that $B/pA\cong E(1)$. Then, there exists a homomorphism ϕ of $E(m)$ into A such that $\phi(E(m))+pA=B$ and $\phi^{-1}(pA)=pE(m)$.*

PROOF. Since $B/pA\cong E(1)$, we can find a basis $\bar{a}_i$, $0\leqq i<\infty$, of B/pA such that $\omega_0\bar{a}_0=0$ and $\omega_0\bar{a}_i=\bar{a}_{i-1}$ for $i>0$. As A is regular, the

[7] In general, if B is a subgroup of a bounded p-primary abelian group A and if $A=B+pA$, then $A=B$; $A=B+pA$ implies $A=B+p(B+pA)=B+p^2A=\cdots=B+p^nA=B$. This will be often used in the following arguments.

homomorphic image pA of A is also regular. Hence, by a similar argument as in the proof of Lemma 4.5, we can find elements a_i, $0 \leqq i < \infty$, in B such that a_i is in the coset $\bar{a}_i$ and that $\omega_0 a_0 = 0$ and $\omega_0 a_i = a_{i-1}$ for $i > 0$. Now, let e_i, $0 \leqq i < \infty$, be a basis of $E(m)$ as given in Lemma 4.5. Since $p^m a_i = 0$, $0 \leqq i < \infty$, there is a homomorphism ϕ of the module $E(m)$ into B such that $\phi(e_i) = a_i$, $0 \leqq i < \infty$. It is then clear from the choice of a_i that $\phi(E(m)) + pA = B$ and that ϕ induces an isomorphism of $E(m)/pE(m)$ onto B/pA. Hence $\phi^{-1}(pA) = pE(m)$.

4.4. Let $m_1, \cdots, m_s$ be any set of non-negative integers. We denote by $E(m_1, \cdots, m_s)$ the direct sum of $E(m_1), \cdots, E(m_s)$:

$$E(m_1, \cdots, m_s) = E(m_1) + \cdots + E(m_s).$$

If $m_1 = \cdots = m_s = m$, $E(m_1, \cdots, m_s)$ will be denoted also by $E(m)^s$. Clearly, $E(m_1, \cdots, m_s)$ may be also defined as the module of all continuous functions on Γ with values in the direct sum $Z_{p^{m_1}} + \cdots + Z_{p^{m_s}}$. It follows immediately from Lemma 4.2 that $E(m_1, \cdots, m_s)$ is a bounded, regular, strictly Γ-finite, discrete module and its characteristic function is given by

$$c(n; E(m_1, \cdots, m_s)) = mp^n, \qquad n \geqq 0,$$

where $m = \sum_{i=1}^{s} m_i$.

LEMMA 4.7. *Let D be a submodule of $E(m)^s$ isomorphic with $E(1)$. Then, there exists a submodule C of $E(m)^s$ such that $C \cong E(m)$ and $p^{m-1}C = D$.*

PROOF. As stated in the proof of Lemma 4.1, the endomorphism $a \to p^{m-1}a$ of $E(m)^s$ induces an isomorphism of $E(m)^s/pE(m)^s$ onto $p^{m-1}E(m)^s$. Furthermore, by the same lemma, $p^{m-1}E(m)^s$ is the submodule of all a in $E(m)^s$ satisfying $pa = 0$. Hence, D is contained in $p^{m-1}E(m)^s$, and there exists a submodule B of $E(m)^s$ containing $pE(m)^s$ such that $p^{m-1}B = D$, $B/pE(m)^s \cong D \cong E(1)$. Since $pE(m)^s$ is regular by Lemmas 4.1, 4.2, it follows from Lemma 4.6 that there is a homomorphism ϕ of $E(m)$ onto a submodule $C = \phi(E(m))$ of $E(m)^s$ such that $C + pE(m)^s = B$ and $\phi^{-1}(pE(m)^s) = pE(m)$, inducing an isomorphism of $E(m)/pE(m)$ onto $B/pE(m)^s$. Since the endomorphism $a' \to p^{m-1}a'$ of $E(m)$ also induces an isomorphism of $E(m)/pE(m)$ onto $p^{m-1}E(m)$, ϕ maps the submodule $p^{m-1}E(m)$ of $E(m)$ isomorphically onto the submodule $D = p^{m-1}B = p^{m-1}C$ of C. Hence ϕ must be an isomorphism, and the lemma is proved.

LEMMA 4.8. *Let D be a submodule of $E(m_1, \cdots, m_s)$, isomorphic with $E(1)$. Then, $E(m_1, \cdots, m_s)/D$ is a homomorphic image of some $E(n_1, \cdots, n_t)$ where $\sum_{j=1}^{t} n_j < \sum_{i=1}^{s} m_i$.*

PROOF. We use induction on s. If $s=1$, the lemma is an immediate consequence of Lemmas 4.1, 4.4. Suppose $s>1$. We may of course assume $m_1 \geqq m_2 \geqq \cdots \geqq m_s > 0$. Put $m=m_s$ and

$$A = E(m_1, \cdots, m_s) = A' + A'',$$
$$A' = E(m_1, \cdots, m_{s-1}),\ A'' = E(m_s).$$

If D is contained in A', then $A/D \cong (A'/D)+A''$, and the lemma can be proved immediately by applying the induction assumption on $A'/D = E(m_1, \cdots, m_{s-1})/D$. Hence, we may assume that D is not contained in A'.

Now, let B denote the submodule of all a in A satisfying $p^m a = 0$, and put

$$B' = B \cap A', \qquad N' = p^{m-1}B', \qquad N'' = p^{m-1}A''.$$

Then, $B \cong E(m)^s$, $N'' = p^{m-1}E(m) \cong E(1)$, and we have also the following direct sum decompositions:

$$B = B' + A'', \qquad p^{m-1}B = N' + N''.$$

Since $p^{m-1}B$ is the submodule of all a in A satisfying $pa=0$, D is contained in $p^{m-1}B$. But, by the assumption made above, D is not contained in N'. Hence, $(N'+D)/N'$ is a nontrivial submodule of $p^{m-1}B/N' \cong N'' \cong E(1)$. As a homomorphic image of $D \cong E(1)$, $(N'+D)/N'$ is also regular. Hence, by the remark in 4.2, or by Lemma 4.4, $N'+D = p^{m-1}B$.

Now, by Lemma 4.7, B contains a submodule C such that $C \cong E(m)$ and $p^{m-1}C = D$. It then follows that

$$p^{m-1}B = N' + D = p^{m-1}B' + p^{m-1}C = p^{m-1}(B' + C).$$

As B is isomorphic with $E(m)^s$, pB is the submodule of all b in B such that the $p^{m-1}b = 0$. Hence the above equality implies that $B = (B'+C) + pB$ and, consequently, that $B = B' + C$. Therefore,

$$A = A' + A'' = A' + B = A' + B' + C = A' + C,$$

though the sums are not necessarily direct. But, then A/D is a homomorphic image of the direct sum of $A' = E(m_1, \cdots, m_{s-1})$ and $C/D = C/p^{m-1}C \cong E(m-1)$. It is thus proved that A/D is a homomorphic image of $E(m_1, \cdots, m_{s-1}, m_s-1)$, q.e.d.

4.5. A discrete module E will be called *elementary* if E is bounded, regular, and Γ-finite.

LEMMA 4.9. *A discrete module E is elementary if and only if E is a homomorphic image of a module $E(m_1, \cdots, m_s)$.*

PROOF. Let E be an elementary discrete module. As a homomorphic image of a regular module E, the submodule pE is also regular. Hence, by Lemma 2.3, the regular module E/pE is also Γ-finite, for E is Γ-finite by the definition. Then, by Lemma 4.3, E/pE is the direct sum of a finite number of submodules $\overline{E}^{(1)}, \cdots, \overline{E}^{(s)}$ each isomorphic with $E(1)$. Let $E^{(i)}$ be a submodule of E containing pE such that $\overline{E}^{(i)} = E^{(i)}/pE$. Since $p^m E = 0$ for some $m \geqq 0$, there exists, by Lemma 4.6, a homomorphism ϕ_i $(1 \leqq i \leqq s)$ of $E(m)$ onto a submodule $B^{(i)}$ of E such that $B^{(i)} + pE = E^{(i)}$. We have, then, $E = E^{(1)} + \cdots + E^{(s)} = B^{(1)} + \cdots + B^{(s)} + pE$, and, consequently, also $E = B^{(1)} + \cdots + B^{(s)}$. Since $B^{(i)} = \phi_i(E(m))$, it is clear that E is a homomorphic image of $E(m)^s = E(m, \cdots, m)$.

Suppose, conversely, E is a homomorphic image of a module $E(m_1, \cdots, m_s)$. Among all such $E(m_1, \cdots, m_s)$ of which E is a homomorphic image, we choose an $E(m_1, \cdots, m_s)$ for which $\sum_{i=1}^{s} m_i$ is minimal. Put $E = E(m_1, \cdots, m_s)/D$. Suppose, now, that D is an infinite module. Then, since D is bounded, it can not be of finite rank. Hence, by the remark in 4.2, D has a submodule D' isomorphic with $E(1)$. But, by Lemma 4.8, $E(m_1, \cdots, m_s)/D'$ is then a homomorphic image of a module $E(n_1, \cdots, n_t)$ where $\sum_{j=1}^{t} n_j < \sum_{i=1}^{s} m_i$. Hence E is also a homomorphic image of $E(n_1, \cdots, n_t)$ with $\sum_{j=1}^{t} n_j < \sum_{i=1}^{s} m_i$, and this contradicts the choice of $E(m_1, \cdots, m_s)$. It is thus proved that D is a finite module.

Now, since $E(m_1, \cdots, m_s)$ is bounded and regular, so is $E = E(m_1, \cdots, m_s)/D$. We shall next prove that E is (strictly) Γ-finite. Put $A = E(m_1, \cdots, m_s)$ and denote, as usual, by A_n the submodule of all a in A satisfying $\omega_n a = 0$, and by E_n the submodule of E defined similarly for E. By the definition, $A_n = \omega_n^{-1}(0)$ and $E_n = \omega_n^{-1}(D)/D$. However, as $\omega_n A = A$, $\omega_n^{-1}(D)/\omega_n^{-1}(0)$ is isomorphic with D. Since D is finite, it then follows that the order of E_n is equal to the order of A_n. Thus, by the remark at the beginning of 4.4, we see that E_n is a finite module of order p^{mp^n} where $m = \sum_{i=1}^{s} m_i$. E is, therefore, Γ-finite, and the lemma is completely proved.

At the same time, the following lemma is also proved by the above argument:

LEMMA 4.10. *Let E be an elementary discrete module. Then, there is a module $E(m_1, \cdots, m_s)$ and a finite submodule D of $E(m_1, \cdots, m_s)$ such that $E \cong E(m_1, \cdots, m_s)/D$. The characteristic function of E is then given by*

$$c(n; E) = mp^n, \qquad n \geqq 0,$$

where $m = \sum_{i=1}^{s} m_i$.

LEMMA 4.11. *Let B be a finite submodule of an elementary discrete module E. Then*

$$c(n; E/B) = c(n; E),$$

for all $n \geqq 0$.

PROOF. Let $E \cong E(m_1, \cdots, m_s)/D$, as stated in the previous lemma. Then, there is a submodule C of $E(m_1, \cdots, m_s)$ containing D such that

$$E/B \cong E(m_1, \cdots, m_s)/C, \qquad B \cong C/D.$$

As C is also a finite module, we have, by Lemma 10,

$$c(n; E/B) = mp^n = c(n; E),$$

where $m = \sum_{i=1}^{s} m_i$.

LEMMA 4.12. *A homomorphic image of an elementary discrete module is again elementary.*

This follows immediately from Lemma 4.9.

LEMMA 4.13. *Let B be a submodule of a discrete module A. If both A/B and B are elementary, so is A.*

PROOF. Since both A/B and B are bounded, regular modules, A is also bounded and regular. By Lemma 2.3, A is also Γ-finite.

LEMMA 4.14. *Let B and C be submodules of a discrete module A. If both B and C are elementary, the sum $B+C$ in A is also an elementary module.*

PROOF. Clearly, if both B and C are elementary, the direct sum of B and C is also elementary. Since the sum $B+C$ in A is a homomorphic image of the direct sum of B and C, $B+C$ is also elementary by Lemma 4.12.

4.6. We now consider bounded Γ-finite discrete modules in general.

LEMMA 4.15. *A bounded Γ-finite discrete module A has the unique maximal elementary submodule E in which every elementary submodule of A is contained. A/E is then a finite module.*

PROOF. Clearly, for any elementary submodule E' of A, we have $c(0; E') \leqq c(0; A)$. Hence, there exists an elementary submodule E of A such that $c(0; E') \leqq c(0; E)$ for any elementary submodule E' of A. Put $E'' = E + E'$. By Lemma 4.14, E'' is also elementary, and $E \subset E''$, $c(0; E) \leqq c(0; E'')$. Therefore $c(0; E) = c(0; E'')$ and, by Lemma 4.10, $c(n; E) = c(n; E'')$ for all $n \geqq 0$. Then, for every $n \geqq 0$, E_n and E_n''

have the same order and, consequently, $E_n = E_n''$. Hence, it follows from Lemma 2.1 that $E = E''$, $E' \subset E$, i.e. that every elementary submodule of A is contained in E.

Suppose, next, A/E be an infinite module. Then, the bounded module A/E can not be of finite rank. Since A/E is Γ-finite by Lemma 2.3, it has a submodule isomorphic with $E(1)$, by the remark in 4.2. Hence, A has a submodule B containing E such that $B/E \cong E(1)$. As both B/E and E are elementary, so is B by Lemma 4.13. However, this contradicts the fact that every elementary submodule of A is contained in E. It is, hence, proved that A/E is a finite module.

Now, as above, let A be a bounded Γ-finite discrete module and E the maximal elementary submodule of A. By Lemma 2.3, we have

$$c(n; A) = c(n; A/E) + c(n; E), \qquad n \geqq 0.$$

But, as A/E is a finite module, $c(n; A/E)$ is constant for all sufficiently large n. By Lemma 4.10, we have therefore the following

LEMMA 4.16. *Let A be a bounded Γ-finite discrete module. Then, there exists an integer $n_0 \geqq 0$ such that, for $n \geqq n_0$, the characteristic function of A is given by*

$$c(n; A) = mp^n + u,$$

where m and u are suitable non-negative integers independent of n.

Obviously, for given A, the integers m and u in the lemma are uniquely determined by the above equality, and they give us invariants of the module A. In particular, we call the invariant m the *weight* of the bounded Γ-finite discrete module A and denote it by $w(A)$. As the above proof shows, the weight of A is given by

$$w(A) = c(0; E) = \sum_{i=1}^{s} m_i,$$

if E is the maximal elementary submodule of A and if

$$E = E(m_1, \cdots, m_s)/D$$

with finite D. We also notice that $w(A) = 0$ if and only if A is a finite module.

LEMMA 4.17. *Let A be a bounded Γ-finite discrete module and B a submodule of A. Then, A/B is also Γ-finite and*

$$w(A) = w(A/B) + w(B).$$

PROOF. Let E be the maximal elementary submodule of A and E'

the maximal elementary submodule of B. Since $(E+B)/B$ is a homomorphic image of E, it is elementary by Lemma 4.11. Clearly, $A/(E+B)$ is a finite module and, hence, is Γ-finite. Therefore, by Lemma 2.3, A/B is also Γ-finite. It is then easy to see that $(E+B)/B$ is the maximal elementary submodule of A/B and that $w(A/B) = w((E+B)/B)$. As E' is an elementary submodule of A, it is contained in $E \cap B$, and $E \cap B/E'$ is a finite module, for B/E' is finite. By Lemma 4.11, we then have $w(E/E \cap B) = w(E/E')$ and, hence, $w(A/B) = w((E+B)/B) = w(E/E \cap B) = w(E/E')$. Now, by Lemma 2.3,

$$c(n; E) = c(n; E/E') + c(n; E'), \qquad n \geqq 0.$$

Putting $n=0$, we obtain

$$w(E) = w(E/E') + w(E').$$

As $w(E) = w(A)$ and $w(E') = w(B)$ by the definition, and as it is shown above that $w(E/E') = w(A/B)$, the lemma is proved.

Now, let A be again a bounded Γ-finite discrete module, E the maximal elementary submodule of A, and $E \cong E(m_1, \cdots, m_s)/D$ with finite D. We shall next show that the module $E(m_1, \cdots, m_s)$ with the property described above is uniquely determined by A.

Let i be any non-negative integer and let $A^{(i)}$ denote the submodule of all a in A satisfying $p^i a = 0$. Put $E' = E \cap A^{(i)}$. Since $A^{(i)}/E'$ is a finite module, we have, by Lemma 4.17, $w(A^{(i)}) = w(E')$. Now, consider the endomorphism $\phi: b \to p^i b$ of $E(m_1, \cdots, m_s)$, and denote by B the kernel of ϕ and by C the inverse image of D under ϕ. Clearly, $E' \cong C/D$ and, hence, $w(E') = w(C/D)$. Since D is finite, C/B is also finite. By Lemma 4.17, we have then $w(C/D) = w(C) = w(B)$. Therefore, $w(A^{(i)}) = w(B)$. However, by the definition, B is the submodule of all b in $E(m_1, \cdots, m_s)$ satisfying $p^i b = 0$. Hence, obviously, $B \cong E(n_1, \cdots, n_s)$ where $n_j = \min(m_j, i)$, $j = 1, \cdots, s$. As $w(B) = \sum_{j=1}^{s} n_j$, we have

$$w(A^{(i)}) = \sum_{j=1}^{s} \min(m_j, i).$$

Since i is an arbitrary non-negative integer and $A^{(i)}$ is a module defined uniquely by A and i, the above equality shows that the nonzero integers in $m_1, \cdots, m_s$ are uniquely determined by A. The module $E(m_1, \cdots, m_s)$ is therefore also uniquely determined by A.

As shown above, the nonzero integers in $m_1, \cdots, m_s$ are invariants of the bounded Γ-finite discrete module A and those invariants determine the structure of A up to finite modules. Furthermore, they

have, in various respects, similar properties as the invariants of finite abelian groups. For instance, we can prove, by a similar argument as above, that

$$w(p^i A) = \sum_{j=1}^{s} \max(m_j - i, 0),$$

for any integer $i \geqq 0$. Using Lemma 4.17, it then follows, in particular, that

$$w(A^{(1)}) = w(A/pA). \tag{4}$$

4.7. We shall now briefly state, without proofs, the results on the structure of bounded Γ-finite compact modules which correspond, by the duality between discrete and compact modules, to what we have proved above for bounded Γ-finite discrete modules.

For any non-negative integer m, we denote by $Y(m)$ the compact module $M_2(\Gamma, Z_{p^m})$ as defined in general in 1.4. Since the finite group Z_{p^m} is self-dual, $E(m)$ and $Y(m)$ form a pair of dual Γ-modules, and it follows that $Y(m)$ is a bounded Γ-finite compact module. More generally, for any non-negative integers $m_1, \cdots, m_s$, we denote by $Y(m_1, \cdots, m_s)$ the direct sum of $Y(m_i)$, $i=1, \cdots, s$. $Y(m_1, \cdots, m_s)$ is again a bounded Γ-finite compact module and it is dual to the discrete module $E(m_1, \cdots, m_s)$.

A compact module Y is called *elementary* if it is bounded, regular and Γ-finite, i.e. if Y is dual to an elementary discrete module. By Lemma 4.9, a compact module Y is elementary if and only if it is isomorphic with a submodule W of some $Y(m_1, \cdots, m_s)$. In fact, if Y is elementary, we can find $Y(m_1, \cdots, m_s)$ and a submodule W of $Y(m_1, \cdots, m_s)$ isomorphic with Y such that $Y(m_1, \cdots, m_s)/W$ is finite.

In general, a bounded Γ-finite compact module X has the unique minimal submodule U such that X/U is elementary. U is a finite module and, by the above, X/U is isomorphic with a submodule of a module $Y(m_1, \cdots, m_s)$ having a finite index in $Y(m_1, \cdots, m_s)$. The nonzero integers in $m_1, \cdots, m_s$ are, then, invariants of X and they determine the structure of X up to finite modules. The sum $m = \sum_{i=1}^{s} m_i$ is again called the *weight* of X and is denoted by $w(X)$. For the characteristic function $c(n; X)$ of X, we also have the result corresponding to Lemma 4.16, for $c(n; X) = c(n; A)$ if A is a bounded Γ-finite discrete module dual to X.

5. **Γ-finite modules in general.** 5.1. We now consider the Γ-module $M_1(\Gamma, Z_{p^\infty})$ defined in 1.4 and denote it by $E(\infty)$. By the definition,

$E(\infty)$ consists of all continuous functions on Γ with values in Z_{p^∞}. Since Γ is totally disconnected, every continuous function in $E(\infty)$ takes only a finite number of distinct values in the discrete group Z_{p^∞}, which, on the other hand, may be considered as the union of finite cyclic groups Z_{p^l}, $l \geqq 0$. Hence, if, for each $l \geqq 0$, $E(\infty)^{(l)}$ denotes the submodule of all a in $E(\infty)$ satisfying $p^l a = 0$, $E(\infty)^{(l)}$ is naturally isomorphic with $E(l)$, and $E(\infty)$ is the union of all those $E(\infty)^{(l)}$, $l \geqq 0$. It then follows immediately that $E(\infty)$ is a discrete module in the sense of 2.2 and that it is also regular and Γ-finite, though not bounded.

More generally, for any $m_1, \cdots, m_s$ which are either non-negative integers or ∞, we denote by $E(m_1, \cdots, m_s)$ the direct sum of $E(m_i)$, $i = 1, \cdots, s$. Clearly, $E(m_1, \cdots, m_s)$ is again a regular Γ-finite discrete module.

Now, let A be a discrete module. For any integer $l \geqq 0$, let $A^{(l)}$ denote the submodule of all a in A satisfying $p^l a = 0$.

LEMMA 5.1. *Let $E(\infty)^s$ be the direct sum of s copies of $E(\infty)$, $s \geqq 0$. A discrete module A is isomorphic with $E(\infty)^s$ if and only if A is divisible and $A^{(1)} \cong E(1)^s$.*

PROOF. The lemma is trivial for $s = 0$. Using the remark on $E(\infty)^{(l)}$ mentioned at the beginning, it is also easy to see that $E(\infty)^s$ has the properties stated above.

Now, let $s \geqq 1$ and let A be any discrete module having the properties given in the lemma. We first prove the existence of a set of elements $a_{ij}^{(k)}$ in A, $1 \leqq i \leqq s$, $0 \leqq j < \infty$, $1 \leqq k < \infty$, such that the elements $a_{ij}^{(k)}$, $1 \leqq i \leqq s$, $0 \leqq j < \infty$, form a basis of $A^{(k)}$, such that $pa_{ij}^{(k)} = a_{ij}^{(k-1)}$ for $k > 1$ and that $\omega_0 a_{i0}^{(k)} = 0$ and $\omega_0 a_{ij}^{(k)} = a_{i,j-1}^{(k)}$ for $j > 0$. We use induction on the upper index k. Since $A^{(1)} \cong E(1)^s$, it is clear from Lemma 4.5 that there exist elements $a_{ij}^{(1)}$, $1 \leqq i \leqq s$, $0 \leqq j < \infty$, satisfying the above conditions for $k = 1$. Suppose we have found such elements $a_{ij}^{(k)}$ in A for $1 \leqq i \leqq s$, $0 \leqq j < \infty$, $1 \leqq k \leqq l$. Let i be fixed. Since A is divisible and $pA^{(l+1)} = A^{(l)}$, there is an element a in $A^{(l+1)}$ such that $pa = a_{i0}^{(l)}$. We have then $p(\omega_0 a) = \omega_0 a_{i0}^{(l)} = 0$. Hence, $\omega_0 a$ is an element of $A^{(1)} \cong E(1)^s$, and there is an element b in $A^{(1)}$ such that $\omega_0 a = \omega_0 b$. Put $a_{i0}^{(l+1)} = a - b$. Then, $pa_{i0}^{(l+1)} = a_{i0}^{(l)}$ and $\omega_0 a_{i0}^{(l+1)} = 0$. Next we take an element a' in $A^{(l+1)}$ such that $pa' = a_{i1}^{(l)}$. We have then $p(\omega_0 a') = \omega_0 a_{i1}^{(l)} = a_{i0}^{(l)} = pa_{i0}^{(l+1)}$. Hence, $\omega_0 a' - a_{i0}^{(l+1)}$ is contained in $A^{(1)}$, and there is an element b' in $A^{(1)}$ such that $\omega_0 a' - a_{i0}^{(l+1)} = \omega_0 b'$. Put $a_{i1}^{(l+1)} = a' - b'$. Then, $pa_{i1}^{(l+1)} = a_{i1}^{(l)}$ and $\omega_0 a_{i1}^{(l+1)} = a_{i0}^{(l+1)}$. Proceeding similarly, we can obtain elements $a_{ij}^{(l+1)}$, $1 \leqq i \leqq s$, $0 \leqq j < \infty$, in $A^{(l+1)}$ such that $pa_{ij}^{(l+1)} = a_{ij}^{(l)}$, $\omega_0 a_{i0}^{(l+1)} = 0$ and $\omega_0 a_{ij}^{(l+1)} = a_{i,j-1}^{l+1}$ for

$j>0$. Let B be the subgroup of $A^{(l+1)}$ generated by those $a_{ij}^{(l+1)}$, $1\leqq i\leqq s$, $0\leqq j<\infty$. Since the elements $a_{ij}^{(l)}$ form a basis of $A^{(l)}$, we have $pB=A^{(l)}=pA^{(l+1)}$. But, as $A^{(l)}$ is contained in $A^{(l)}$, and, hence, also in B, we see immediately that $B=A^{(l+1)}$. From $pa_{ij}^{(l+1)}=a_{ij}^{(l)}$, it then follows that the elements $a_{ij}^{(l+1)}$ form a basis of $A^{(l+1)}$. Thus, by induction, the existence of $a_{ij}^{(k)}$, $1\leqq i\leqq s$, $0\leqq j<\infty$, $1\leqq k<\infty$, is proved. We notice that every $a_{ij}^{(k)}$ has order p^k.

Now, let $\overline{A}$ be another divisible discrete module such that $\overline{A}^{(1)}\cong E(1)^s$. Then, $\overline{A}$ also contains a set of elements $\bar{a}_{ij}^{(k)}$, $1\leqq i\leqq s$, $0\leqq j<\infty$, $1\leqq k<\infty$, having similar properties as $a_{ij}^{(k)}$. But, it is then clear that there is an isomorphism ϕ of the module A onto the module $\overline{A}$ such that $\phi(a_{ij}^{(k)})=\bar{a}_{ij}^{(k)}$. Thus, any two discrete modules having the properties stated in the lemma are isomorphic with each other. Since $E(\infty)^s$ has these properties, the lemma is proved.

LEMMA 5.2. *Let A be a discrete module and B a submodule of A isomorphic with $E(\infty)^s$, $s\geqq 0$. Then, A is the direct sum of B and a suitable submodule C: $A=B+C$.*

PROOF. Let D be a submodule of A such that $B\cap D=0$. Suppose $A\neq B+D$. Then, there exists an element a in A such that a is not in $B+D$ but both pa and $\omega_0 a$ are in $B+D$. Put $pa=b+d$, $b\in B$, $d\in D$. Since $B\cong E(\infty)^s$, there is an element b_0 in B such that $b=pb_0$. Put $a'=a-b_0$ so that $pa'=d$. Put also $\omega_0 a'=b_1+d_1$, $b_1\in B$, $d_1\in D$. Then, $pb_1+pd_1=\omega_0 pa'=\omega_0 d$, and, since $B\cap D=0$, it follows that $pb_1=0$. As $B\cong E(\infty)^s$, there then exists an element b_2 in B such that $pb_2=0$, $\omega_0 b_2=b_1$. Put $a''=a'-b_2$. Then, $pa''=d$ and $\omega_0 a''=d_1$. Hence, if D^* denotes the subgroup of A generated by D and a'', D^* contains D as a subgroup of index p, $B\cap D^*=0$ and D^* is Γ-invariant, i.e. a submodule of A. Now, take a maximal submodule C of A such that $B\cap C=0$. By the above, we have then $A=B+C$, and the lemma is proved.

5.2. To study the structure of Γ-finite discrete modules in general, we shall first prove the following

LEMMA 5.3. *Let A be a Γ-finite discrete module, A' the submodule of all a in A satisfying $pa=0$. Let B be an elementary submodule of A containing A', and C a submodule of A such that pC is contained in B. Suppose $w(B/pB)\leqq w(C/B)$. Then $pC=B$, and C/B is isomorphic with B/pB.*

PROOF. The endomorphism $c\to pc$ of C obviously induces a homomorphism ϕ of C/B into B/pB. Suppose that pc ($c\in C$) is contained in pB. Then $pc=pb$ for some b in B, and $c-b$ is contained in A', and,

hence, in B. Thus, c is also contained in B, and we see that ϕ is an isomorphism of C/B into B/pB. It then follows from Lemma 4.17, that $w(C/B) \leqq w(B/pB)$ and, consequently, by the assumption, that $w(C/B) = w(B/pB)$.

Now, since B is elementary, so is B/pB by Lemma 4.12. Hence, by Lemma 4.3, $B/pB \cong E(1)^t$ where $t = w(E(1)^t) = w(B/pB)$. However, it is easy to see that no submodule of $E(1)^t$ has weight t unless it coincides with $E(1)^t$ itself. Therefore, $\phi(C/B) = B/pB$ and ϕ is an isomorphism of C/B onto B/pB. It then follows that $pC + pB = B$ and, hence, that $pC = B$.

Now, let A be any Γ-finite discrete module. By Lemma 4.14, the union of all elementary submodules in A is a submodule of A. We shall first study the structure of A in the case where A itself is the union of all elementary submodules of A.

Let C be any bounded submodule of such a discrete module A. Then the maximal elementary submodule E of C has a finite index in C, and we can find a finite number of elements a_i which generate C mod E. Since, by the assumption, every a_i is contained in some elementary submodule of A, it follows from Lemma 4.14, that C is also contained in an elementary submodule of A.

Now, for any elementary submodule E of A, let E^* denote the submodule of all a in A such that pa is contained in E. Then, among all elementary submodules of A, we choose an E for which the weight $w(E^*/E)$ attains the minimum. Since E^* is obviously a bounded module, there exists, by the above remark, an elementary submodule B of A containing E^*. Put $\overline{A} = A/E$, $\overline{B} = B/E$. $\overline{E}^* = E^*/E$ is then the submodule of all $\bar{a}$ in $\overline{A}$ satisfying $p\bar{a} = 0$. But, as $\overline{E}^*$ is contained in $\overline{B}$, $\overline{E}^*$ is also the submodule of all $\bar{a}$ in $\overline{B}$ satisfying $p\bar{a} = 0$. Hence, by (4) in 4.6, $\overline{E}^*$ has the same weight as $\overline{B}/p\overline{B}$: $w(\overline{E}^*) = w(\overline{B}/p\overline{B})$. Let B^* be the submodule of all b in A such that pb is contained in B. Then, $\overline{B}^* = B^*/E$ is the submodule of all $\bar{b}$ in $\overline{A}$ such that $p\bar{b}$ is contained in $\overline{B}$, and, by the choice of E, $w(\overline{B}/p\overline{B}) = w(\overline{E}^*) = w(E^*/E) \leqq w(B^*/B) = w(\overline{B}^*/\overline{B})$. Hence, applying Lemma 5.3 to $\overline{B}$ and $\overline{B}^*$, we see that $p\overline{B}^* = \overline{B}$ and $\overline{B}^*/\overline{B} \cong \overline{B}/p\overline{B}$.

Put $\tilde{A} = A/B$ and $\tilde{A}' = B^*/B$. $\tilde{A}'$ is then the submodule of all $\tilde{a}$ in $\tilde{A}$ satisfying $p\tilde{a} = 0$ and $\tilde{A}' \cong \overline{B}^*/\overline{B} \cong \overline{B}/p\overline{B}$. As B is elementary, $\overline{B}$ and $\overline{B}/p\overline{B}$ are also elementary. Hence $\tilde{A}'$ is an elementary module with $p\tilde{A}' = 0$, and it is therefore isomorphic with $E(1)^t$, $t \geqq 0$. Let a be an arbitrary element in A. By the remark mentioned above, there then exists an elementary submodule C of A containing both a and E^*. Applying the above argument for $\overline{C} = C/E$ instead of $\overline{B} = B/E$, we see that there is a submodule $\overline{C}^*$ of $\overline{A} = A/E$ such that $p\overline{C}^* = \overline{C}$.

Therefore, there also exists an element c in A such that $pc \equiv a \bmod E$, and, hence, such that $pc \equiv a \bmod B$. Thus the module $\tilde{A} = A/B$ is divisible and, by Lemma 5.1, it is isomorphic with $E(\infty)^t$.

Now, since B is bounded, $p^m B = 0$ for some $m \geqq 0$. Consider, then, the endomorphism $a \to p^m a$ of A and denote its kernel by $A^{(m)}$. As A/B is isomorphic with $E(\infty)^t$ and B is contained in $A^{(m)}$, the endomorphism induces an isomorphism $p^m A \cong E(\infty)^t/K$ where K is a bounded submodule of $E(\infty)^t$ isomorphic with $A^{(m)}/B$. On the other hand, $A/B \cong E(\infty)^t$ is divisible by Lemma 5.1, and we have $p^m A + B = A$. Applying Lemma 4.9 to the elementary module B, it then follows immediately that if a Γ-finite discrete module A is the union of its elementary submodules, A is isomorphic with a module $E(m_1, \cdots, m_s)/D$ where $m_1, \cdots, m_s$ are either non-negative integers or ∞ and D is a suitable bounded submodule of $E(m_1, \cdots, m_s)$.

5.3. Let A be as above. Among all modules $E(m_1, \cdots, m_s)$, $0 \leqq m_i \leqq \infty$, such that $A \cong E(m_1, \cdots, m_s)/D$ with bounded D, we choose an $E(m_1, \cdots, m_s)$ for which the weight $w(D)$ is minimal. We shall next show that $w(D)$ is then 0, i.e. that D is a finite module.

Suppose D be infinite. By the remark in 4.2, the bounded module D then contains a submodule D' isomorphic with $E(1)$. Following the proof of Lemma 4.8, we may assume that $m_1 \geqq \cdots \geqq m_s > 0$ and that D' is not contained in the direct summand $E(m_1, \cdots, m_{s-1})$ of $E(m_1, \cdots, m_s)$. Suppose, first, that $m = m_s$ is not ∞. By the same argument as in the proof of Lemma 4.8, we can then see that $E(m_1, \cdots, m_s)$ has a submodule C such that $C = E(m)$, $p^{m-1}C = D'$ and $E(m_1, \cdots, m_s) = E(m_1, \cdots, m_{s-1}) + C$, though the sum is not necessarily direct. The intersection of $E(m_1, \cdots, m_{s-1})$ and C is finite, for, otherwise, it would contain $D' = p^{m-1}C \cong E(1)$. A homomorphism of $E(m_1, \cdots, m_s) = E(m_1, \cdots, m_{s-1}) + E(m_s)$ onto $E(m_1, \cdots, m_s) = E(m_1, \cdots, m_{s-1}) + C$, mapping $E(m_1, \cdots, m_{s-1})$ and $E(m_s)$ isomorphically onto $E(m_1, \cdots, m_{s-1})$ and C respectively, induces a homomorphism ϕ of $E(m_1, \cdots, m_{s-1}, m_s - 1)$ onto $E(m_1, \cdots, m_s)/D'$ whose kernel K is a finite module. Let ψ denote the homomorphism of

$$E(m_1, \cdots, m_{s-1}, m_s - 1) \text{ onto } E(m_1, \cdots, m_s)/D$$

which is the product of ϕ and the canonical homomorphism $E(m_1, \cdots, m_s)/D' \to E(m_1, \cdots, m_s)/D$. The kernel D^* of ψ then satisfies $D^*/K \cong D/D'$. Since K is finite, we have, by Lemma 4.17, $w(D^*) = w(D^*/K) = w(D/D') = w(D) - w(D') = w(D) - 1$. As A is obviously isomorphic with $E(m_1, \cdots, m_{s-1}, m_s - 1)/D^*$, this contradicts the choice of D.

Assume, next, $m_s=\infty$ so that $m_1=\cdots=m_s=\infty$, $E(m_1,\cdots,m_s)=E(\infty)^s$. Let E' be the submodule of all a in $E(\infty)^s$ satisfying $pa=0$. Since $E'\cong E(1)^s$ and D' is a submodule of E' isomorphic with $E(1)$, it is easily seen that E' has a basis $a_{ij}^{(1)}$, $1\leqq i\leqq s$, $0\leqq j<\infty$ such that $\omega_0 a_{i0}^{(1)}=0$, $\omega_0 a_{ij}^{(1)}=a_{i,j-1}^{(1)}$ for $j>0$ and that $a_{sj}^{(1)}$, $0\leqq j<\infty$, form a basis of D'. As shown in the proof of Lemma 5.1, we can then find elements $a_{ij}^{(k)}$ in $E(\infty)^s$, $1\leqq i\leqq s$, $0\leqq j<\infty$, $1\leqq k<\infty$, which include those $a_{ij}^{(1)}$ above and satisfy the conditions stated there. Let B be the submodule of $E(\infty)^s$ generated by $a_{ij}^{(k)}$, $1\leqq i\leqq s-1$, $0\leqq j<\infty$, $1\leqq k<\infty$, and C the submodule of $E(\infty)^s$ generated by $a_{sj}^{(k)}$, $0\leqq j<\infty$, $1\leqq k<\infty$. $E(\infty)^s$ is then the direct sum of B and C, and D' is the submodule of all a in C satisfying $pa=0$. Clearly, $B\cong E(\infty)^{s-1}$, $C\cong E(\infty)$, and the endomorphism $c\to pc$ of C induces an isomorphism of C/D' onto $C\cong E(\infty)$. These isomorphisms then define an isomorphism ϕ of $E(\infty)^s$ onto $E(\infty)^s/D'$ in an obvious way and we denote by ψ the homomorphism of $E(\infty)^s$ onto $E(\infty)^s/D$, which is the product of ϕ and the canonical homomorphism $E(\infty)^s/D'\to E(\infty)^s/D$. Denoting the kernel of ψ by D^*, we have thus $E(\infty)^s/D\cong E(\infty)^s/D^*$ and $D^*\cong D/D'$. However, it then follows from Lemma 4.17 that $w(D^*)=w(D)-w(D')=w(D)-1$, and this again contradicts the choice of D.

We have thus proved the following.

LEMMA 5.4. *Let A be a Γ-finite discrete module. Suppose that A is the union of all elementary submodules of A. Then, there exists a module $E(m_1,\cdots,m_s)$, $0\leqq m_i\leqq\infty$, and a finite submodule D of $E(m_1,\cdots,m_s)$ such that A is isomorphic with $E(m_1,\cdots,m_s)/D$.*

5.4. We now consider an arbitrary Γ-finite discrete module A. Let C denote the union of all elementary submodules of A. By Lemma 5.4, $C\cong E(m_1,\cdots,m_s)/D$, $0\leqq m_i\leqq\infty$, with a finite submodule D of $E(m_1,\cdots,m_s)$. As can be seen from the proof of Lemma 5.4 (or, directly from the fact $C\cong E(m_1,\cdots,m_s)/D$), C has an elementary submodule E such that $C/E\cong E(\infty)^t$ for some $t\geqq 0$. Then, applying Lemma 5.2 to A/E and C/E, we see that A has a submodule B^* containing E such that A/E is the direct sum of B^*/E and C/E. By Lemma 2.3, B^*/E is Γ-finite. Hence, if B^*/E were not of finite rank, B^* would contain, by the remark in 4.2, a submodule E^* such that $E^*/E\cong E(1)$. But, then, E^* would be also elementary by Lemma 4.13, and were not contained in C, a contradiction to the definition of C. Therefore, B^*/E must be a module of finite rank. Let B' be the submodule of B^* containing E such that B^*/B' is finite and B'/E is divisible. As an abelian group, B'/E is then isomorphic with

$Z_{p^\infty}^l$ for some $l \geqq 0$. Now, since E is elementary, $p^n E = 0$ for some $n \geqq 0$. Put, then, $B = p^n B'$. Considering the endomorphism $b \to p^n b$ of B', we see that B is isomorphic with a quotient module of B'/E modulo a finite submodule. Hence, as an abelian group, B is again isomorphic with $Z_{p^\infty}^l$. Furthermore, since B'/E is divisible, it holds that $B' = B + E$, and $B + C = B' + C$ has a finite index in $A = B^* + C$. On the other hand, since B is of finite rank and E is bounded, $B \cap C = B \cap E$ is a finite module. Therefore, the following theorem is proved:

THEOREM 1. *Let A be a Γ-finite discrete module. Then, A has submodules B and C with the following properties:*

(i) *both $A/(B+C)$ and $B \cap C$ are finite modules,*

(ii) *B is divisible and of finite rank, i.e., B is, as a discrete abelian group, isomorphic with $Z_{p^\infty}^l$ for some $l \geqq 0$,*

(iii) *C is isomorphic with $E(m_1, \cdots, m_s)/D$ for some $m_1, \cdots, m_s$, $0 \leqq m_i \leqq \infty$, and for a finite submodule D of $E(m_1, \cdots, m_s)$.*

We notice that the structure of a discrete module like B was studied in §3.

We now consider the uniqueness of submodules given in the theorem. Let B and C be any submodules of A having the properties (i), (ii), (iii) above; B and C need not be those which were considered in the above proof of Theorem 1. Then, A/C is of finite rank and $(B+C)/C$ is divisible. Take any elementary submodule E of A. By Lemma 4.12, $(E+C)/C$ is elementary and, hence, is bounded. But, as A/C is of finite rank, $(E+C)/C$ is finite. Since $(E+C)/C$ is also regular, we have $(E+C)/C = 0$, i.e. $E + C = C$. Thus, every elementary submodule of A is contained in C. On the other hand, it follows easily from $C \cong E(m_1, \cdots, m_s)/D$ that C is the union of its elementary submodules. Therefore, C is also the union of all elementary submodules of A and is thus uniquely determined by A.

Now, let A^* be any submodule with a finite index in A. By a similar argument as above, we see that every elementary submodule of A is contained in A^*. Hence, C is also a submodule of A^*. On the other hand, if the index of A^* in A is p^n, $p^n A$ is contained in A^*. Hence $B = p^n B$ is contained in A^*, and so is $B + C$. Thus $B + C$ is the minimal submodule of A having a finite index in A and is uniquely characterized by this property.

A simple example shows that the module B satisfying (i), (ii), (iii) together with C is not unique for given A. However, the rank l of B is uniquely determined by A, for it is equal to the rank of $(B+C)/C$.

Finally, for any integer $i \geqq 0$, let $A^{(i)}$ be the submodule of all a in A

satisfying $p^i a = 0$. Since A/C is of finite rank, $A^{(i)} \cap C$ has a finite index in $A^{(i)}$. Hence, by a similar argument as in 4.6, we see from $C \cong E(m_1, \cdots, m_s)/D$ that

$$w(A^{(i)}) = \sum_{j=1}^{s} \min(m_j, i), \qquad i \geqq 0.$$

Therefore, nonzero m_j's in $m_1, \cdots, m_s$ are uniquely determined by A and they give us a set of invariants of the module A. Clearly, the module $E(m_1, \cdots, m_s)$ is then also uniquely determined by A, and so is the sum $m = \sum_{j=1}^{s} m_j$. Here, m is meant to be ∞ if one of m_j is ∞.

We have thus obtained the following corollary to Theorem 1.

COROLLARY. *Let B and C be any submodules of a Γ-finite discrete module A, having the properties* (i), (ii), (iii) *stated in Thorem* 1. *Then, the modules C, $B+C$ and $E(m_1, \cdots, m_s)$ are uniquely determined by A with these properties, and so are the rank l of the module B and the sum $m = \sum_{j=1}^{s} m_j$.*

In the following, we shall denote the invariants l and m of A by $l(A)$ and $m(A)$ respectively. $l(A)$ is a non-negative integer and $m(A)$ is either a non-negative integer or ∞. As can be seen easily, $m(A)$ is the supremum of the weights $w(D)$ of bounded submodules D in A. In particular, if A itself is bounded, $m(A) = w(A)$.

We now apply Lemma 3.1 to the submodule B in Theorem 1. B is then the direct sum of a regular submodule B' and a submodule B'' such that $\omega_{u'}^{v'} B'' = 0$ for some u' and v'. Put $M = B' + C$. Since B' and C are both regular, so is M. Furthermore, since $\omega_{u'}^{v'} B'' = 0$ and $A/(B+C)$ is finite, $\omega_u^v(A/M) = 0$ for some u and v. It follows that $\omega_u^v A = M$, and we see, as in the proof of Lemma 3.1, that M is the unique maximal regular submodule of A in which every regular submodule of A is contained.[8] Thus the following theorem is proved:

THEOREM 2. *Let M be the unique maximal regular submodule of a Γ-finite discrete module A. Then, M is the sum of a divisible regular submodule B' of finite rank and the characteristic submodule C of A given in Theorem* 1. *A/M is a module of finite rank and $\omega_u^v(A/M) = 0$ for some $u \geqq 0$ and $v \geqq 0$.*

5.5. We now consider a special kind of Γ-finite discrete modules.

LEMMA 5.5. *For a Γ-finite discrete module A, the following conditions are mutually equivalent:*

[8] The existence of such a unique maximal regular submodule of A was already noticed in 2.2.

(i) *the invariant* $m(A)$ *is finite,*

(ii) *the maximal regular submodule* M *of* A *is strictly* Γ*-finite,*

(iii) *if* A_n' *denotes the maximal divisible submodule of* A_n $(n \geqq 0)$, *the rank of* A_n' *has a fixed upper bound for all* $n \geqq 0$.

PROOF. Let $M = B' + C$ as in the above. By Lemma 3.4, B' is strictly Γ-finite. Hence M is strictly Γ-finite if and only if C is so. But it is easy to see that $C \cong E(m_1, \cdots, m_s)/D$ is strictly Γ-finite if and only if $m(A) = \sum_{i=1}^{s} m_i$ is finite. (i) and (ii) are therefore equivalent.

Now, by Lemma 2.2, $(A/M)_n \cong A_n/M_n$. If M is strictly Γ-finite, M_n is a finite module and it follows from the above isomorphism that the rank of A_n' is at most equal to the rank of $(A/M)_n$. The rank of A_n' is, hence, not greater than the rank of A/M and we see that (ii) implies (iii). On the other hand, if $m(A)$ is infinite, then at least one of $m_1, \cdots, m_s$ in $E(m_1, \cdots, m_s)/D$ is infinite and the rank of $A_n' \cap C$ is at least p^n, as can be seen readily from the definition of $E(\infty)$. Therefore (iii) implies (i), and the lemma is proved.

Now, assume that $m(A)$ is finite. C is then elementary; in fact, it is the maximal elementary submodule of A, having the weight $w(C) = m(A)$. Therefore, $p^m C = 0$ for $m = m(A)$. On the other hand, as $A/(B+C)$ is finite, $p^n A$ is contained in $B + C$ for all sufficiently large $n \geqq 0$. Hence $p^{m+n}A$ is a submodule of $p^m B + p^m C = p^m B$. However, as B is divisible, $p^m B = B = p^{m+n}B$. Therefore, $p^{m+n}A = B$, and it follows that B is the intersection of all $p^n A$, $n \geqq 0$, and is the unique maximal divisible submodule of A.

We summarize our results in the following

THEOREM 3. *Let* A *be a* Γ*-finite discrete module such that the invariant* $m(A)$ *is finite. Then the submodules* B *and* C *in Theorem* 1 *are both uniquely determined by* A; B *is the unique maximal divisible submodule of* A *and* C *is the unique maximal elementary submodule of* A. *The invariant* $l(A)$ *is the rank of* B *as well as that of the maximal divisible submodule of* A/C, *and the invariant* $m(A)$ *is the weight of* C *as well as that of the bounded* Γ*-finite discrete module* A/B. *Furthermore, the maximal regular submodule* M *of* A *is strictly* Γ*-finite.*

We consider next a strictly Γ-finite module A. The rank of the module A_n' in Lemma 5.5 is then 0, and we know that $m(A)$ is finite. By Lemma 3.4, the maximal divisible submodule B of A is regular. Hence $B + C$ is also regular and it coincides with the maximal regular submodule M. Now, by Lemma 2.3, we have

$$c(n; A) = c(n; A/M) + c(n; M), \qquad n \geqq 0.$$

Let B' and C' be discrete modules such that $B' \cong B$ and $C' \cong C$, and let A' be the direct sum of B' and C'. It is clear that there is a homomorphism ϕ of A' onto $M = B + C$, mapping B' and C' isomorphically onto B and C, respectively. The kernel D' of ϕ is then a finite module isomorphic with $B \cap C$. Since $A' = B' + C'$ is regular and $\omega_n(A') = A'$ for every $n \geqq 0$, $\omega_n^{-1}(D')/\omega_n^{-1}(0)$ has the same finite order as D'. Hence $(A'/D')_n = \omega_n^{-1}(D')/D'$ also has the same order as $A_n' = \omega_n^{-1}(0)$, and we have $c(n; M) = c(n; A'/D') = c(n; A') = c(n; B') + c(n; C') = c(n; B) + c(n; C)$, for all $n \geqq 0$. Therefore,

$$c(n; A) = c(n; A/M) + c(n; B) + c(n; C), \qquad n \geqq 0.$$

However, as A/M is finite, $c(n; A/M)$ is constant for all sufficiently large n. Hence, by Lemmas 3.5, 4.10, we immediately obtain the following

THEOREM 4. *Let A be a strictly Γ-finite discrete module. Then the invariant $m(A)$ is finite and $B + C = M$ for the submodules B, C and M in Theorem 3. Furthermore, there exists a non-negative integer n_0 such that, for $n \geqq n_0$, the characteristic function of A is given by*

$$c(n; A) = l(A)n + m(A)p^n + u,$$

with a suitable integer u independent of n.

Now, for any function of the form $f(n) = ln + mp^n + u$, the coefficients l, m and u are uniquely determined by f. Hence, if A is a strictly Γ-finite discrete module, the invariants $l(A)$ and $m(A)$ are uniquely determined from the characteristic function $c(n; A)$ of A by the above formula. On the other hand, such an A is bounded if and only if $l(A) = 0$ and it is of finite rank if and only if $m(A) = 0$. Therefore, we can see from the characteristic function of A whether or not A is bounded or of finite rank.

5.6. Now, let O_p be, as before, the additive group of p-adic integers and let $Y(\infty)$ denote the module $M_2(\Gamma, O_p)$ defined in 1.4. Since O_p is a compact abelian group dual to the discrete abelian group Z_{p^∞}, $Y(\infty) = M_2(\Gamma, O_p)$ is a compact module in the sense of 2.2 and is dual to the discrete module $E(\infty) = M_1(\Gamma, Z_{p^\infty})$. More generally, for any $m_1, \cdots, m_s$, $0 \leqq m_i \leqq \infty$, we denote by $Y(m_1, \cdots, m_s)$ the direct sum of $Y(m_i)$, $i = 1, \cdots, s$. Clearly, $Y(m_1, \cdots, m_s)$ is a regular Γ-finite compact module dual to the regular Γ-finite discrete module $E(m_1, \cdots, m_s)$.

By the duality between discrete and compact modules, we can then immediately obtain theorems on Γ-finite compact modules which correspond to the above results on Γ-finite discrete modules. We state here only some of them.

THEOREM 5. *Let X be a Γ-finite compact module. Then, X has submodules U and V with the following properties*:

(i) *both $X/(U+V)$ and $U \cap V$ are finite modules,*

(ii) *X/U is torsion-free and of finite rank, i.e., X/U is, as a compact abelian group, isomorphic with O_p^l for some $l \geqq 0$,*

(iii) *X/V is isomorphic with a submodule of finite index in $Y(m_1, \cdots, m_s)$ for some $m_1, \cdots, m_s$, $0 \leqq m_i \leqq \infty$.*

COROLLARY. *Let U and V be any submodules of a Γ-finite compact module A with the properties* (i), (ii), (iii) *in the above theorem. Then, the modules V, $U \cap V$ and $Y(m_1, \cdots, m_s)$ are uniquely determined by X, and so are the rank l of X/U and the sum $m = \sum_{i=1}^{s} m_i$.*

Thus, we have again invariants $l = l(X)$ and $m = m(X)$ for any Γ-finite compact module X. Clearly, if A is a discrete module dual to X, then $l(X) = l(A)$, $m(X) = m(A)$. We also notice that the structure of a module like X/U was studied in §3.

THEOREM 6. *Let X be a Γ-finite compact module such that $m(X)$ is finite. Then the submodules U and V in Theorem* 5 *are both uniquely determined by X; U is the torsion submodule of X and V is the unique minimal submodule of X such that X/V is elementary. The invariant $l(X)$ is the rank of X/U as well as that of the factor torsion module of V, and the invariant $m(X)$ is the weight of X/V as well as that of the bounded Γ-finite compact module U. Furthermore, if S is the unique minimal submodule of X such that X/S is regular, then X/S is also strictly Γ-finite.*

6. Unramified extensions. 6.1. Let Ω be the field of all algebraic numbers. In what follows, we shall always consider the structure of various algebraic number fields, i.e. the structure of various subfields of Ω. So, if there is no risk of misunderstanding, we shall call those algebraic number fields simply fields. By the definition, our fields are algebraic extensions of the field of rational numbers Q, but they need not be finite extensions of Q; in other words, our fields are not necessarily finite algebraic number fields.

If both E and F are such fields and if E is a Galois extension of F, we denote the Galois group of the extension E/F by $G(E/F)$. $G(E/F)$ is a totally disconnected compact group in Krull's topology. For any prime divisor of E, archimedean or non-archimedean, the decomposition group and the inertia group of the prime divisor for the extension E/F can be defined just as in the case of finite algebraic number fields.[9] They are closed subgroups of $G(E/F)$ and have sim-

[9] For an archimedean prime divisor, the inertia group is defined to be the same as the decomposition group.

ilar properties as those defined for finite algebraic number fields.

Let $\mathfrak{p}$ be a prime divisor of Ω and T the inertia group of $\mathfrak{p}$ for the extension Ω/Q. Let K and L be fields such that $K \subset L$. Then $T \cap G(\Omega/K)$ and $T \cap G(\Omega/L)$ are the inertia groups of $\mathfrak{p}$ for Ω/K and Ω/L, respectively, and the latter is a subgroup of the former. Now, the prime divisor $\mathfrak{p}$ is said to be ramified for the extension L/K if $T \cap G(\Omega/K) \neq T \cap G(\Omega/L)$, and it is said to be unramified for L/K if $T \cap G(\Omega/K) = T \cap G(\Omega/L)$. Obviously, $\mathfrak{p}$ is unramified if and only if $T \cap G(\Omega/K)$ is contained in $G(\Omega/L)$.

A prime divisor $\mathfrak{p}'$ of K (or a prime divisor $\mathfrak{p}''$ of L) is said to be unramified for L/K if and only if every extension $\mathfrak{p}$ of $\mathfrak{p}'$ (of $\mathfrak{p}''$) on Ω is unramified for L/K. Otherwise $\mathfrak{p}'(\mathfrak{p}'')$ is said to be ramified for L/K. If L/K is a Galois extension and T is the inertia group, for Ω/Q, of an extension $\mathfrak{p}$ of $\mathfrak{p}''$ on Ω, then the inertia group of $\mathfrak{p}''$ for the extension L/K is given by the image of $T \cap G(\Omega/K)$ under the canonical homomorphism $G(\Omega/K) \to G(L/K) = G(\Omega/K)/G(\Omega/L)$. Hence, $\mathfrak{p}''$ is unramified for L/K if and only if the inertia group of $\mathfrak{p}''$ for L/K is trivial. We also notice that our definition of ramified or unramified prime divisors coincides with the usual one when both L and K are finite algebraic number fields.

Now, an extension L/K is called an unramified extension if and only if every prime divisor of K, or, equivalently, every prime divisor of L, is unramified for the extension L/K. The following properties of unramified extensions are immediate consequences of the definition: if L/K is unramified and L'/K is conjugate with L/K in Ω, then L'/K is also unramified; if $F \subset K \subset L$, then L/F is unramified if and only if both L/K and K/F are unramified; if $F \subset E$, $F \subset K$ and E/F is unramified, then the composite $L = EK$ of E and K in Ω is unramified over K; if L/K is the composite, in Ω, of a family of unramified extensions L_α/K, then L/K is also unramified. From these, it follows in particular that every field K has a unique maximal unramified extension L in Ω which contains every unramified extension of K in Ω; L is a Galois extension of K. Similarly, there also exists a unique maximal unramified abelian extension A of K in Ω which contains every unramified abelian extension of K in Ω. If K is a finite algebraic number field, A is nothing but the Hilbert's class field over K, and it is well-known that A/K is a finite extension with degree equal to the class number of K. If the degree of K/Q is infinite, A/K is not necessarily a finite extension,[10] but we shall still call A the Hilbert's class field over K.

---

[10] Cf. 7.7 below.

6.2. We shall next show that every unramified extension can be obtained by composing, in a suitable manner, finite unramified extensions of finite algebraic number fields.

LEMMA 6.1. *Given any finite unramified extension L/K, there exist finite algebraic number fields E and F such that*

(i) *E is an unramified extension of F, and*

(ii) *$F \subset K$, $E \subset L$ and $L = EK$.*

If L/K is furthermore a Galois extension, then the fields E and F can be chosen so that E/F is also a Galois extension and its Galois group is isomorphic with the Galois group of L/K.

PROOF. Let S be the space of all nonempty closed subsets of the compact group $G(\Omega/Q)$. We may regard $G(\Omega/Q)$ as a subspace of S by identifying each element of $G(\Omega/Q)$ with the subset consisting of that single element. Now, as a separable compact topological group, $G(\Omega/Q)$ can be topologized by a metric $\rho(a, b)(a, b \in G(\Omega/Q))$, and, as is known, this metric can be extended to a metric $\rho(A, B)$ $(A, B \in S)$ on S so that S becomes a compact metric space.[11] Define a function $\rho'(A, B)$ on $S \times S$ by

$$\rho'(A, B) = \inf \rho(a, b), \qquad a \in A, b \in B.$$

Then, $\rho'(A, B)$ is a non-negative continuous function on $S \times S$ and $\rho'(A, B) > 0$ if and only if A and B are disjoint.

In proving the lemma, we may of course assume that both K and L are infinite extensions of Q and that $K \neq L$. Since L/K is a finite extension, there exist finite algebraic number fields K_0 and L_0 such that $K_0 \subset K$, $L_0 \subset L$, $K_0 \subset L_0$, $L = KL_0$ and $[L_0 : K_0] = [L : K]$. We then choose a sequence of fields, $K_0 \subset K_1 \subset K_2 \subset \cdots$, so that each K_n is a finite extension of Q and that K is the union of all K_n. Put $L_n = K_n L_0$ for $n \geqq 1$. Then we have again a sequence of fields, $L_0 \subset L_1 \subset L_2 \subset \cdots$, such that each L_n is finite over Q, that L is the union of all L_n and that $[L_n : K_n] = [L : K]$ for every $n \geqq 0$. Put

$$G = G(\Omega/K), \qquad G_n = G(\Omega/K_n), \quad n = 0, 1, 2, \cdots$$
$$H = G(\Omega/L), \qquad H_n = G(\Omega/L_n), \quad n = 0, 1, 2, \cdots.$$

As K is the union of all K_n, G is the intersection of all G_n, and as L is the union of all L_n, H is the intersection of all H_n. Furthermore, since $L = KL_n$, $H = G \cap H_n$ for every $n \geqq 0$. Let C be the set-theoretical complement of H in G. As $K \neq L$ and $[G : H] = [L : K]$ is finite, C is

[11] Cf. D. Montgomery and L. Zippin, *Topological transformation groups*, New York, Interscience Publishers, 1955, p. 17.

a nonempty compact subset of $G(\Omega/Q)$. From the fact that $[G_n: H_n] = [L_n: K_n] = [L: K] = [G: H]$, it also follows easily that G_n is the disjoint union of H_n and CH_n.

Now, let $\mathfrak{p}_1', \cdots, \mathfrak{p}_s'$ be all the prime divisors of the finite algebraic number field L_0 which are ramified for the extension L_0/K_0. For each j $(1 \leqq j \leqq s)$, let T_j be the inertia group, for Ω/Q, of an extension $\mathfrak{p}_j$ of $\mathfrak{p}_j'$ on Ω, and let ϕ_j be a continuous function on $G(\Omega/Q) \times S$ defined by

$$\phi_j(\sigma, A) = \rho'(\sigma T_j \sigma^{-1}, CA), \qquad \sigma \in G(\Omega/Q), A \in S.$$

By the definition of C, we have $CH = C$. Hence $\sigma T_j \sigma^{-1} \cap CH = (\sigma T_j \sigma^{-1} \cap G) \cap C$. But, since L/K is unramified and $\sigma T_j \sigma^{-1}$ is the inertia group of the prime divisor $\mathfrak{p}_j^{\sigma}$ for Ω/Q, $\sigma T_j \sigma^{-1} \cap G$ is contained in H and the intersection $(\sigma T_j \sigma^{-1} \cap G) \cap C$ is empty. Therefore, $\phi_j(\sigma, H) > 0$ for every σ in $G(\Omega/Q)$ and for every j, $1 \leqq j \leqq s$. On the other hand, since H is the intersection of all H_n, H is the limit of the sequence, $H_0, H_1, H_2, \cdots$, in S. Using the compactness of $G(\Omega/Q)$, it then follows that there exists an integer $n_0 \geqq 0$ such that $\phi_j(\sigma, H_{n_0}) > 0$ for every σ in $G(\Omega/Q)$ and for every j, $1 \leqq j \leqq s$. But, then, $\sigma T_j \sigma^{-1} \cap CH_{n_0}$ is empty by the definition of ϕ_j and, as G_{n_0} is the disjoint union of H_{n_0} and CH_{n_0}, $\sigma T_j \sigma^{-1} \cap G_{n_0}$ must be contained in H_{n_0}. Thus, for every σ in $G(\Omega/Q)$ and for every j, $1 \leqq j \leqq s$, the prime divisor $\mathfrak{p}_j^{\sigma}$ of Ω is unramified for the extension L_{n_0}/K_{n_0}.

Now, let $\mathfrak{p}$ be any prime divisor of Ω different from $\mathfrak{p}_j^{\sigma}$, $\sigma \in G(\Omega/Q)$, $1 \leqq j \leqq s$. The restriction $\mathfrak{p}'$ of $\mathfrak{p}$ on L_0 is then different from $\mathfrak{p}_1', \cdots, \mathfrak{p}_s'$ and it is unramified for L_0/K_0. $\mathfrak{p}$ is therefore unramified for L_0/K_0 and, hence, also for L_{n_0}/K_{n_0}. This, combined with the above, shows that L_{n_0}/K_{n_0} is an unramified extension. Putting $F = K_{n_0}$, $E = L_{n_0}$, the conditions (i), (ii) of the lemma are then satisfied.

If L/K is a Galois extension, we can choose K_0 and L_0 in the above so that L_0/K_0 is also a Galois extension. Every L_n/K_n is then also a Galois extension and its Galois group $G(L_n/K_n)$ is canonically isomorphic with $G(L/K)$. Thus, in particular, $G(E/F)$ is isomorphic with $G(L/K)$ and the lemma is completely proved.

THEOREM 7. *An extension L/K $(K \subset L \subset \Omega)$ is an unramified extension if and only if there exists a family of extensions $\{L_\alpha/K_\alpha\}$ of finite algebraic number fields K_α and L_α such that*

(i) *every L_α/K_α is an unramified extension, and that*

(ii) *K is the composite of all K_α and L is the composite of all L_α.*

PROOF. Suppose first that there exists such a family of extensions $\{L_\alpha/K_\alpha\}$. Put $L_\alpha' = KL_\alpha$. Since L_α/K_α is unramified, L_α'/K is also unramified. Since L is the composite of all L_α', L/K is again unramified.

Suppose, conversely, that L/K is unramified. Let $\{L_i/K\}$ be a family of finite extensions such that L is the composite of all L_i, and let $\{K_j/Q\}$ be a family of finite extensions such that K is the composite of all K_j. By Lemma 6.1, there exist, for each i, finite algebraic number fields E_i and F_i such that E_i/F_i is unramified and $L_i = KE_i$. Put $K_{i,j} = F_iK_j$, $L_{i,j} = E_iK_j$. Then the family of extensions $\{L_{i,j}/K_{i,j}\}$ has the properties (i), (ii) stated in the theorem.

COROLLARY. *Let K be a field and $\{K_\alpha\}$ a family of finite algebraic number fields such that K is the union of all K_α. Then the maximal unramified extension of K in Ω is the composite of all finite unramified extensions of all fields K_α in the family.*

We next consider abelian extensions. If the extension L/K in Lemma 6.1 is abelian, we may take also an abelian extension for E/F in the lemma. By a similar argument as in the proof of Theorem 7, we can then immediately obtain the following

THEOREM 8. *An extension L/K ($K \subset L \subset \Omega$) is an unramified abelian extension if and only if there exists a family of extensions $\{L_\alpha/K_\alpha\}$ of finite algebraic number fields K_α and L_α such that*

(i) *every L_α/K_α is an unramified abelian extension, and that*

(ii) *K is the composite of all K_α and L is the composite of all L_α.*

COROLLARY. *Let K be a field and $\{K_\alpha\}$ a family of finite algebraic number fields such that K is the union of all K_α. For each α, let L_α denote the Hilbert's class field over K_α. Then the Hilbert's class field over K is the composite of all such L_α.*

6.3. As before, let p denote a prime number. An extension L/K is called a p-extension if L/K is a Galois extension and the Galois group $G(L/K)$ is a p-primary compact group. Every field K has a unique maximal (abelian) p-extension in Ω which contains every (abelian) p-extension of K in Ω. By the properties of unramified extensions stated in 6.1, K has also a unique maximal unramified p-extension and a unique maximal unramified abelian p-extension in Ω. The latter is nothing but the p-part of the Hilbert's class field over K, and, if K/Q is finite, its degree over K is equal to the highest power of p dividing the class number of K.

Using again Lemma 6.1, we get immediately such results on unramified (abelian) p-extensions which are similar to those on unramified abelian extensions given in Theorem 8 and its corollary. We state here only the following

THEOREM 9. *Let K be a field and $\{K_\alpha\}$ a family of finite algebraic number fields such that K is the union of all K_α. For each α, let L_α denote*

the maximal unramified abelian p-extension of K_α in Ω. Then the maximal unramified abelian p-extension of K in Ω is the composite of all such L_α.

7. **Γ-extensions.** 7.1. Let p be a prime number and let Γ be, as in previous sections, a fixed p-primary compact abelian group isomorphic with the additive group of p-adic integers. An extension L of a field K is called a Γ-*extension* of K if L/K is a Galois extension and if the Galois group $G(L/K)$ is isomorphic with Γ.

Let L/K be such a Γ-extension and let, for simplicity, $G(L/K)$ be identified with Γ. For each $n \geqq 0$, we denote by K_n the intermediate field of K and L such that $G(L/K_n) = \Gamma_n$. We have then a sequence of fields:

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset L,$$

such that K_n is a cyclic extension of degree p^n over K and L is the union of all K_n, $n \geqq 0$.

LEMMA 7.1. *Let K be a finite algebraic number field and L a Γ-extension of K. Then a prime divisor $\mathfrak{p}$ of K is ramified for L/K only when $\mathfrak{p}$ is a non-archimedean prime divisor dividing the rational prime p.*

PROOF. Assume that $\mathfrak{p}$ is ramified for L/K and denote by T the inertia group of $\mathfrak{p}$ for the abelian extension L/K. Since T is a non-trivial closed subgroup of Γ, T must be equal to Γ_n for some $n \geqq 0$. Hence T is an infinite group and it follows immediately that $\mathfrak{p}$ is non-archimedean. Let $\mathfrak{p}'$ be an extension of $\mathfrak{p}$ on K_n. For any integer $m \geqq n$, $\mathfrak{p}'$ is then completely ramified for the extension K_m/K_n and its ramification is p^{m-n}. Therefore, if $\mathfrak{p}$ and, hence, $\mathfrak{p}'$ did not divide p, we would have

$$N(\mathfrak{p}') \equiv 1 \mod p^{m-n},$$

where $N(\mathfrak{p}')$ denotes the absolute norm of the prime divisor $\mathfrak{p}'$. But, since m can be taken arbitrarily large, this is obviously a contradiction, and the lemma is proved.

From the lemma, it follows in particular that there exist only a finite number of prime divisors of K which are ramified for L/K. On the other hand, since an unramified abelian extension of K is always a finite extension, there exists at least one prime divisor which is ramified for L/K.

LEMMA 7.2. *Let K and L be as in Lemma* 7.1 *and let s be the number of prime divisors of K which are ramified for L/K. Furthermore, let L' be an unramified p-extension of L such that L'/K is an abelian exten-*

sion. Then the Galois group $G(L'/K)$ is a p-primary compact abelian group of finite rank and the rank of the factor torsion group of $G(L'/K)$ is at most s.

PROOF. Put $G=G(L'/K)$ and $N=G(L'/L)$. It is clear that G is a p-primary compact group, for both N and $G/N=G(L/K)=\Gamma$ are such groups. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ be all the prime divisors of K which are ramified for L/K and let $T_1, \cdots, T_s$ denote the inertia groups of $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$, respectively, for the abelian extension L'/K. Since L'/L is an unramified extension, the intersection $T_i \cap N$ is 1, and we have $T_i \cong T_iN/N$. T_i is thus isomorphic with a nontrivial subgroup of $\Gamma=G/N$ and, hence, also isomorphic with Γ itself. Let T be the product of the subgroups $T_1, \cdots, T_s$ in G and E the intermediate field of K and L' such that $T=G(L'/E)$. As L'/L is an unramified extension, no prime divisor of K, different from $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$, is ramified for L'/K. It then follows from the definition of T that E/K is an unramified abelian extension. Therefore, E/K is a finite extension and G/T is a finite group. From this and from the fact that T is the product of $T_1, \cdots, T_s$, each isomorphic with Γ, the lemma follows immediately by a simple group-theoretical consideration.

We notice that the rank of the factor torsion group of $G(L'/L)$ is at most $s-1$. Hence, if $s=1$, $G(L'/L)$ is a finite group.

7.2. As before, let L be a Γ-extension of a finite algebraic number field K. Let M be an unramified abelian p-extension of L such that M/K is also a Galois extension. We put $G=G(M/K)$, $X=G(M/L)$. Then X is a closed normal subgroup of G and $G/X=G(L/K)=\Gamma$. As X is a p-primary compact abelian group, G is such a compact group as we considered in 2.5, and X is thus made into a compact Γ-module in a natural way. We shall next show that this compact Γ-module X is Γ-finite.

For each $n \geqq 0$, put $G_n=G(M/K_n)$. Then X is contained in G_n and $G_n/X=\Gamma_n$. By 2.5, we have only to prove that, if $[G_n, G_n]$ is the topological commutator group of G_n, then $G_n/[G_n, G_n]$ has a finite rank for every $n \geqq 0$. Let L_n denote the intermediate field of K and M such that $G(M/L_n)=[G_n, G_n]$. By the definition of $[G_n, G_n]$, L_n is the maximal abelian extension of K_n contained in M. Hence, in particular, L is contained in L_n. On the other hand, as $G(L/K_n)=\Gamma_n \cong \Gamma$, L/K_n is a Γ-extension. Therefore, we may apply Lemma 7.2 to K_n, L and L_n, and we see that $G(L_n/K_n)=G_n/[G_n, G_n]$ has a finite rank. Our assertion is thus proved.

Now, let $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ be all the prime divisors of K which are ramified for L/K. The inertia groups of $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ for L/K are then nontrivial subgroups of Γ and we can find a suitable integer $n_0 \geqq 0$ such

that Γ_{n_0} is contained in all these inertia groups. Then a prime divisor of K_{n_0}, which is ramified for L/K_{n_0}, is not decomposed for any extension K_n/K_{n_0}, $n \geqq n_0$, and the number of the prime divisors of K_n which are ramified for L/K_n remains the same for all K_n, $n \geqq n_0$. Thus, it follows from Lemma 7.2 that the rank of the factor torsion group of $G_n/[G_n, G_n]$ has a fixed upper bound for all $n \geqq 0$. But, since $[G_n, G_n] = \omega_n X = X_n^*$, this implies that the rank of the factor torsion module of X/X_n^* also has a fixed upper bound for all $n \geqq 0$. Now, let A be a discrete Γ-module dual to the compact Γ-module X and let A_n ($n \geqq 0$) be the submodules of A as defined before. Then the duality between A and X implies a duality between A_n and X/X_n^*, and also a duality between the maximal divisible submodule of A_n and the factor torsion module of X/X_n^*. Hence, by above, the maximal divisible submodule of A_n has a fixed upper bound for all $n \geqq 0$. It then follows from Lemma 5.5 that the invariant $m(A)$ of A is finite, and, as the invariant $m(X)$ of X is equal to $m(A)$, the following theorem is proved:

THEOREM 10. *Let L be a Γ-extension of a finite algebraic number field K and M an unramified abelian p-extension of L such that M/K is also a Galois extension. Then the Galois group $G(M/L)$ is a Γ-finite compact Γ-module with respect to $\Gamma = G(L/K)$, and the invariant $m(X)$ of the compact Γ-module $X = G(M/L)$ is finite. The structure of $G(M/L)$ as a p-primary compact abelian group with operator domain $G(L/K)$ is thus given by Theorem 6.*

7.3. Let K and L be as above. We now take as M the maximal unramified abelian p-extension of L in Ω, i.e. the p-part of the Hilbert's class field over L; M/K is then obviously a Galois extension. By Theorem 10, the Galois group $G(M/L)$ is a Γ-finite compact Γ-module with respect to $\Gamma = G(L/K)$ and we denote the invariants $l(X)$ and $m(X)$ of the Γ-module $X = G(M/L)$ by $l(L/K)$ and $m(L/K)$, respectively. By the above theorem, not only $l(L/K)$ but also $m(L/K)$ are non-negative integers, and they give us information on the structure of the Galois group $G(M/L)$ of the maximal unramified abelian p-extension M over L. For instance, $G(M/L)$ is of bounded order if and only if $l(L/K) = 0$ and it is of finite rank if and only if $m(L/K) = 0$.

Actually, $l(L/K)$ depends only upon L (and M), but not upon K, for it is an invariant of the Galois group $G(M/L)$ considered merely as an abelian group. On the other hand, the invariant $m(L/K)$ is defined by means of the Γ-structure of $G(M/L)$ and, hence, essentially depends upon the ground field K. In fact, if we consider the Γ-extension L/K_n ($n \geqq 0$) instead of L/K, then we see easily that

$$m(L/K_n) = p^n m(L/K).$$

Now, let K' be any finite extension of K and L' the composite of K' and L in $\Omega: L' = K'L$. Then $K' \cap L = K_n$ for some $n \geqq 0$ and $G(L'/K') \cong G(L/K_n) \cong \Gamma$. Hence L'/K' is also a Γ-extension. If M is, as before, the maximal unramified abelian p-extension of L in Ω, the composite ML' of M and L' in Ω is contained in the maximal unramified abelian p-extension M' of L' in Ω, and $G(ML'/L')$ is a factor group of $G(M'/L')$. On the other hand, $G(ML'/L')$ is canonically isomorphic with $G(M/M \cap L')$ which is a subgroup of finite index $[M \cap L' : L]$ in $G(M/L)$. Thus the Galois group $G(M/L)$ is, up to a finite factor group, isomorphic with a factor group of the Galois group $G(M'/L')$, and this is so even when both groups are considered as modules over the same operator domain $\Gamma = G(L'/K') = G(L/K_n)$. It then follows immediately that

$$l(L/K_n) \leqq l(L'/K'), \quad m(L/K_n) \leqq m(L'/K'),$$

or, by the above, that

$$l(L/K) \leqq l(L'/K'), \quad m(L/K) \leqq p^{-n} m(L'/K').$$

7.4. We shall next give another arithmetic characterization of the invariants $l(L/K)$ and $m(L/K)$. Let K, L and M be as in 7.3 and put $G = G(M/K)$, $X = G(M/L)$, $\Gamma = G/X = G(L/K)$, $G_n = G(L/K_n)$, $n \geqq 0$. As in 7.2, we choose an integer n_0 such that, for any $n \geqq n_0$, the field K_n has the same number of prime divisors which are ramified for L/K_n. We then denote by $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ all the prime divisors of K_{n_0} which are ramified for L/K_{n_0}. Let $\mathfrak{p}_i^*$ $(1 \leqq i \leqq s)$ be an extension of $\mathfrak{p}_i$ on M and T_i the inertia group of $\mathfrak{p}_i^*$ for the extension M/K_{n_0}. Since M/L is unramified, $T_i \cap X = 1$, and since $\mathfrak{p}_i$ is completely ramified for K_n/K_{n_0} for any $n \geqq n_0$, $T_i X = G_{n_0}$. Hence T_i is naturally isomorphic with $\Gamma_{n_0} = G_{n_0}/X$ and it contains an element σ_i such that the coset of σ_i mod X is the element $\gamma_{n_0}^{-1}$ of Γ_{n_0}. Put $\sigma = \sigma_1$ and $\sigma_i = \sigma x_i$, $1 \leqq i \leqq s$, with x_i in X. For any $t \geqq 0$, we have then

$$\sigma_i^{p^t} = \sigma^{p^t} x_i^{\nu}, \tag{5}$$

where $\nu = \nu_{n_0+t, n_0}$ is defined as (3) in 3.2.

We now fix an integer $n \geqq n_0$ and put $G' = G_n/[G_n, G_n] = G(L_n/K_n)$ and $X' = X/[G_n, G_n] = G(L_n/L)$, where L_n denotes, as before, the maximal abelian extension of K_n contained in M. Let $\mathfrak{p}_i'$ $(1 \leqq i \leqq s)$ be the unique extension of $\mathfrak{p}_i$ on K_n and let T_i' denote the inertia group of $\mathfrak{p}_i'$ for the abelian extension L_n/K_n. Since the inertia group of $\mathfrak{p}_i^*$ for the extension M/K_n is $T_i \cap G_n = T_i^{p^t}$, where $t = n - n_0$, T_i' is the image of $T_i^{p^t}$ under the canonical homomorphism $G_n \to G'$ and, hence,

is the closure of the cyclic subgroup of G' generated by the coset of $\sigma_i^{p^t}$ mod $[G_n, G_n]$. On the other hand, as $G_n = T_1^{p^t}X$, G' is the direct product of T_1' and X': $G' = T_1' \times X'$. Therefore, if we denote by T' the product of the subgroups $T_1', \cdots, T_s'$ in G' and if we put

$$T' = T_1' \times Y', \qquad Y' \subset X',$$

it follows from (5) that Y' is the closure of the subgroup of G' generated by the cosets of $x_i^{p^\nu}$ mod $[G_n, G_n]$ for $1 \leqq i \leqq s$.

Now, let E_n be the intermediate field of K_n and L_n such that $G(L_n/E_n) = T'$. From the definition of T', it follows that E_n is the maximal unramified extension of K_n contained in L_n, and, hence, is the maximal unramified abelian extension of K_n contained in M. As M was the maximal unramified abelian p-extension of L in Ω, it is easy to see from Theorem 9 that E_n is the maximal unramified abelian p-extension of K_n in Ω, i.e., the p-part of the Hilbert's class field over K_n. E_n/K_n is therefore a finite extension and the degree $[E_n: K_n]$ is equal to the highest power of p dividing the class number of K_n. By the above, $G(E_n/K_n) = G'/T' \cong X'/Y'$. Let Y_n be the closure of the subgroup of X generated by $[G_n, G_n]$ and $x_i^{p^\nu}$, $1 \leqq i \leqq s$, where $\nu = \nu_{n,n_0}$. Then, $Y' = Y_n/[G_n, G_n]$ and we have $G(E_n/K_n) \cong X/Y_n$.

We now consider the group Y_n for every $n \geqq n_0$. For simplicity, put $Y = Y_{n_0}$. If we use the additive notation for the group X, Y_n is the closure of the subgroup of X generated by $X_n^* = [G_n, G_n]$ and $\nu_{n,n_0}x_i$, $1 \leqq i \leqq s$. As $X_n^* = \omega_n X = \nu_{n,n_0}\omega_{n_0}X = \nu_{n,n_0}X_{n_0}^*$ and $\nu_{n_0,n_0}x_i = x_i$, we then see that $Y_n = \nu_{n,n_0}Y$, and the isomorphism $G(E_n/K_n) \cong X/Y_n$ immediately implies that

$$[E_n: K_n] = [X: \nu_{n,n_0}Y],$$

for any $n \geqq n_0$.

7.5. We shall next compute the group index on the right hand side of the above equality. As in Theorem 6, let V be the minimal submodule of X such that $\overline{X} = X/V$ is elementary. V is then a module of finite rank, and if we denote by W the finite torsion submodule of V, $\overline{V} = V/W$ is a torsion-free compact module of finite rank $l = l(X)$. Therefore, if n_0 is large enough, then, by Lemma 3.3,

$$[\overline{V}: \nu_{n,n_0}\overline{V}] = p^{l(n-n_0)}, \tag{6}$$

for any $n \geqq n_0$. For large n_0, we also have that $\omega_{n_0}W = 0$ and $\nu_{n,n_0}W = p^tW$ with $t = n - n_0$. In the following, we shall assume, as we can, that n_0 is chosen so large that all these conditions are satisfied, together with what is mentioned at the beginning of 7.4.

Now, we have

$$[X:\nu Y] = [X:\nu X][\nu X:\nu Y], \qquad \nu = \nu_{n,n_0},$$

and

$$\begin{aligned}[X:\nu X] &= [X:\nu X + V][\nu X + V:\nu X] \\ &= [\overline{X}:\nu\overline{X}][V:\nu X \cap V].\end{aligned}$$

Let x be an element of X such that νx is contained in V. Then $\omega_n x = \omega_{n_0}\nu_{n,n_0}x$ is also in V. But, as $\overline{X}=X/V$ is regular and $\overline{X}_n=0$, x itself must be in V. Therefore $\nu X\cap V=\nu V$, and it follows that

$$[X:\nu X] = [\overline{X}:\nu\overline{X}][V:\nu V].$$

Now, we can see from the proof of Lemma 3.3 that $\nu\bar{v}=0$, $\bar{v}\in\overline{V}$, implies $\bar{v}=0$.[12] Hence, by a similar argument as above, we obtain that $\nu V\cap W=\nu W$ and $[V:\nu V]=[\overline{V}:\nu\overline{V}][W:\nu W]$. On the other hand, since $\overline{X}$ is a regular module and $\overline{X}_{n_0}=0$, the endomorphism $\bar{x}\to\omega_{n_0}\bar{x}$ of $\overline{X}$ is one-one. Therefore, using $\omega_n=\omega_{n_0}\nu_{n,n_0}$, we also have

$$[\overline{X}:\nu\overline{X}] = [\omega_{n_0}\overline{X}:\omega_n\overline{X}] = [\overline{X}:\overline{X}_n^*][\overline{X}:\overline{X}_{n_0}^*]^{-1}.$$

Thus, we obtain

$$[X:\nu X] = [\overline{X}:\overline{X}_n^*][\overline{X}:\overline{X}_{n_0}^*]^{-1}[\overline{V}:\nu\overline{V}][W:\nu W].$$

We next compute $[\nu X:\nu Y]$. As is readily seen,

$$[\nu X:\nu Y] = [X:Y][X^0:Y^0]^{-1},$$

where X^0 is the submodule of all x in X satisfying $\nu x=0$ and $Y^0 = Y\cap X^0$. By the above argument, we know that X^0 is contained in W. However, as W is a finite module, $\nu W=p^tW=0$ whenever $t=n-n_0$ is sufficiently large. Hence, there exists an integer $n_1\geqq n_0$ such that, if $n\geqq n_1$, then $\nu W=0$, $X^0=W$, $Y^0=Y\cap W$ and, consequently, $[\nu X:\nu Y]=[X:Y][W:Y\cap W]^{-1}$.

Putting all these together, we then see that, for any $n\geqq n_1$,

$$[X:\nu_{n,n_0}Y] = p^u[\overline{X}:\overline{X}_n^*][\overline{V}:\nu_{n,n_0}\overline{V}],$$

with an integer u independent of n. Here the factor $[\overline{V}:\nu_{n,n_0}\overline{V}]$ on the right hand side is given by (6), and the other factor $[X:X_n^*]$ is a power of p whose exponent is given by

$$c(n;\overline{X}) = m(X)p^n,$$

for $\overline{X}=X/V$ is an elementary compact Γ-module of weight $w(\overline{X})$

[12] The endomorphism $\bar{v}\to\nu\bar{v}$ of $\overline{V}$ is the product of the endomorphism $\bar{v}\to p^t\bar{v}$ and an automorphism of $\overline{V}$.

$=m(X)$. It then follows immediately that, for any $n \geqq n_1$, $[E_n: K_n] = [X: \nu_{n,n_0} Y]$ is a power of p whose exponent is equal to

$$l(X)n + m(X)p^n + u',$$

where u' is an integer independent of n.

Changing the notation slightly, we can now state our result as follows:

THEOREM 11. *Let K be a finite algebraic number field and L a Γ-extension of K. For each $n \geqq 0$, let K_n be the intermediate field of K and L with degree p^n over K, and let p^{e_n} be the highest power of p dividing the class number of K_n. Then, there exist an integer $n_0 \geqq 0$ and an integer c such that, for any $n \geqq n_0$,*

$$e_n = ln + mp^n + c,$$

where $l = l(L/K)$ and $m = m(L/K)$ are the invariants of L/K as defined in 7.3.

The theorem shows, in particular, that the invariants $l(L/K)$ and $m(L/K)$ are uniquely determined by e_n ($n \geqq 0$), and, hence, also by the extension L/K, without knowing the structure of the extension M over L.

7.6. In some special cases, the result of Theorem 11 can be obtained more simply in the following manner: suppose, namely, that the field K has only one prime divisor $\mathfrak{p}$ which is ramified for the extension L/K and suppose also that the inertia group of $\mathfrak{p}$ for L/K coincides with $\Gamma = G(L/K)$. Then, for each $n \geqq 0$, the field K_n also has exactly one prime divisor $\mathfrak{p}_n$ which is ramified for L/K_n, namely, the unique extension of $\mathfrak{p}$ on K_n. Applying the same argument as in 7.4 for the case $s=1$, we then see that the Galois group $G(L_n/K_n) = G_n/[G_n, G_n]$ is the direct product of $X/[G_n, G_n]$ and the inertia group of $\mathfrak{p}_n$ for the abelian extension L_n/K_n, and, consequently, that the Galois group $G(E_n/K_n)$ of the maximal unramified abelian p-extension E_n over K_n is isomorphic with X/X_n^*. Therefore, the compact Γ-module X is strictly Γ-finite and, for every $n \geqq 0$, the degree $p^{e_n} = [E_n: K_n]$ is equal to the order of X/X_n^*. We have thus:

$$e_n = c(n; X), \qquad n \geqq 0,$$

with the characteristic function $c(n; X)$ of the strictly Γ-finite compact Γ-module X, and the result in Theorem 11 then follows immediately from the dual of Theorem 4.

7.7. We finally give here some examples of Γ-extensions of finite algebraic number fields, illustrating the results obtained above.

For each $n \geqq 0$, let C_n denote the field obtained by adjoining all p^nth roots of unity to the field of rational numbers Q. If $p \neq 2$, C_{n+1} is a cyclic extension of degree $(p-1)p^n$ over Q and we denote by F_n the cyclic subextension of C_{n+1}/Q with degree p^n over Q. On the other hand, if $p=2$, we denote by F_n the maximal real subfield of C_{n+2}; F_n is again a cyclic extension of degree p^n $(=2^n)$ over Q. In both cases, we have then a sequence of fields:

$$Q = F_0 \subset F_1 \subset F_2 \subset \cdots,$$

and the union of all these F_n $(n \geqq 0)$ obviously gives us a Γ-extension E of Q. Suppose next that E' be any Γ-extension of Q and denote by F_n' the subfield of E' such that $[F_n' : Q] = p^n$. By Lemma 7.1, the conductor of the cyclic extension F_n'/Q is a power of p, and it follows immediately that $F_n' = F_n$ for every $n \geqq 0$. Therefore, E' must coincide with E and we know that E is the unique Γ-extension of the field of rational numbers Q. Now, it can be proved that, for every $n \geqq 0$, the class number of F_n is prime to p.[13] Hence, we see from Theorem 9 that the maximal unramified abelian p-extension of E just coincides with E itself and, consequently, that

$$l(E/Q) = m(E/Q) = 0.$$

More generally, for any finite algebraic number field K, the composite of K and E in Ω always defines a Γ-extension L over K, though this is not necessarily the unique Γ-extension of K.

Consider, in particular, the case where $p \neq 2$ and K is the cyclotomic field of pth roots of unity. Then the subfield K_n of $L = KE$ with degree p^n over K is nothing but C_{n+1}, and the assumptions stated in 7.6 are satisfied for the Γ-extension L/K. Therefore, by Theorem 11 or by the remark in 7.6, we immediately obtain the following

THEOREM 12. *Let $p \neq 2$ and let C_n denote the cyclotomic field of p^nth roots of unity $(n \geqq 0)$. Furthermore, let $K = C_1$ and let L be the union of all C_n, $n \geqq 0$. Then there exists an integer $n_0 \geqq 0$ such that, for $n \geqq n_0$, the exponent e_n of the highest power of p dividing the class number of C_{n+1} is given by*

$$e_n = ln + mp^n + c,$$

where $l = l(L/K)$ and $m = m(L/K)$ are the invariants of the Γ-extension L/K as defined in 7.3, and c is a suitable integer independent of n.

[13] Cf. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg vol. 20 (1956) pp. 257–258.

Of course, a similar result can be obtained for $p=2$, if we only put $K=C_2$ and denote by e_n the highest power of 2 dividing the class number of C_{n+2}. However, for any regular prime p including $p=2$, we know a more precise result that $e_n=0$ for all $n\geqq 0$.[14] Thus, in such a case, the maximal unramified abelian p-extension M of L coincides with L itself and both invariants $l(L/K)$ and $m(L/K)$ are 0. On the other hand, if p is irregular, it can be shown that at least one of $l(L/K)$ and $m(L/K)$ is different from 0; in such a case, M is therefore an infinite extension of L.

Further arithmetic properties of our invariants will be studied in our forthcoming papers.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

[14] Cf. (12) above.