CLASS FIELD THEORY

C. CHEVALLEY

STEVENS & CO.
1841 BROADWAY, NEW YORK 23, NEW YORK

CLASS FIELD THEORY

C. CHEVALLEY

NAGOYA UNIVERSITY
1953 — 1954

This book consists of the preparatory notes for a course I gave on class field theory at Nagoya University in 1953–54; it should therefore not be considered as an attempt to give a completely satisfactory exposition of the theory; nor should the reader look in it for a bibliography of the recent works on the subject. It will perhaps suffice to acknowledge here that the main ideas which were used in this presentation are due to Artin, Hochschild, Nakayama and Tate.

I wish also to express my thanks to Messrs. S. Kuroda, T. Nakayama, T. Kubota and T. Ono who not only wrote down the first two sections but who also took the trouble to prepare the whole volume for print and thereby detected various mistakes which appeared in its original form.

Nagoya University C. CHEVALLEY

March 1954

CONTENTS

INTRODUCTION

The object of these lectures was to introduce the listeners to the use of cohomological methods in class field theory.

Class field theory originated in the discovery by Hilbert of the relationship which exists between abelian unramified extension of a field K of algebraic numbers and the group of ideal classes in K. Hilbert's contribution was mostly in the way of conjectures; moreover, it seems likely that he was mostly interested in the fact that all ideals of K become principal in the "absolute class field" of K (Hauptidealsatz), a fact which appears now rather as a corollary of the main theorems than as a fundamental phenomenon. Class field theory proper was created by Takagi and Artin. To Takagi is due the discovery of the 1-1 correspondence which exists between all abelian overfield L of K and certain subgroups H of the groups of ideals in K; H is the group generated by the relative norms of ideals of L which are prime to a certain ideal $\mathfrak{f}$ of K (the conductor) and by the principal ideal (α), where $\alpha \equiv 1 \pmod{\mathfrak{f}}$. Let H_0 be the group of all ideals prime to $\mathfrak{f}$ in K; then Takagi had shown that H_0/H is isomorphic to the Galois group $\mathfrak{G}$ of L/K. Artin's general law of reciprocity established effectively an isomorphism between H_0/H and $\mathfrak{G}$; this law includes all reciprocity laws previously known, beginning with the famous Gaussian quadratic reciprocity law.

After Takagi and Artin, no really important progress was made until quite recently, with the use of the methods of cohomology theory. One of the most baffling features of classical class field theory was that it appeared to say practically nothing about normal extensions which were not abelian. It was discovered by A. Weil and, from a different point of view, by T. Nakayama that class field theory was actually much richer than hitherto suspected; in fact, it can now be formulated in the form of statements about normal extensions without any mention whatsoever of abelian extensions. Of course, it is true that it is only in the abelian case that these statements lead to laws of decomposition for prime ideals of the subfield and to the law of reciprocity. Nevertheless, it is clear that, by now, we know something about the arithmetic of non abelian extensions. In fact, since the work of J. Tate, it may be said that we know almost everything which may be formulated in terms of cohomology in the idèle class group, and generally a great deal about everything which can be formulated in cohomological terms. However, the generalized L-series of Artin indicates that the questions one would like most to solve by now are rather connected with the theory of characters of the Galois group than with its cohomological invariants. The special features of the abelian case originate in the fact that the second cohomology group of a finite group $\mathfrak{G}$ over the integers is the group of 1-dimensional characters of $\mathfrak{G}$, i.e. the group of all characters of $\mathfrak{G}$ when $\mathfrak{G}$ is abelian. The failure of class field theory to give a suitable generalization of the law of reciprocity to the non abelian case may be due to an overemphasis on the purely multiplicative features of fields; it is not impossible that the additive properties would occur essentially in the laws of decomposition of prime ideals; but this is still in the realm of thin air conjecturing.

§1. IDÈLE AND IDÈLE CLASS

Let K be an algebraic number field of finite degree, i.e. a finite extension of the field $\mathbf{Q}$ of rational numbers. Let P be the set of all *places* of K. The completion of K at $\mathfrak{p}\in P$ is denoted by $K_\mathfrak{p}$. Let, for $\mathfrak{p}\in P$, $w_\mathfrak{p}$ be the *normalized valuation* of K at $\mathfrak{p}$, which is defined as follows:

1) if $\mathfrak{p}$ is finite, if p is the rational prime below $\mathfrak{p}$, and if $N_{K_\mathfrak{p}/\mathbf{Q}_p}(a) = p^\nu\cdot$unit in $\mathbf{Q}_p$, then $w_\mathfrak{p}(a) = p^{-\nu}$.

2) if $\mathfrak{p}$ is real-infinite and γ is the corresponding isomorphism of K into the real number field, then $w_\mathfrak{p}(a) = |\gamma(a)|$,

3) if $\mathfrak{p}$ is complex-infinite and γ is the corresponding isomorphism of K into the complex number field, then $w_\mathfrak{p}(a) = |\gamma(a)|^2$; here also a positive power of a valuation in the usual sense is called a valuation. We have $\prod_{\mathfrak{p}\text{ infinite}} w_\mathfrak{p}(a) = |N(a)|$, and thus the *fundamental product formula*

$$\prod_{\mathfrak{p}\in P} w_\mathfrak{p}(a) = 1 \quad \text{for} \quad a(\neq 0)\in K.$$

A mapping $\mathfrak{p}\to\mathfrak{a}_\mathfrak{p}\in K_\mathfrak{p}$ which satisfies the following conditions is called an *idèle* of K; $\mathfrak{a}_\mathfrak{p}$ is $\neq 0$ in $K_\mathfrak{p}$ and $w_\mathfrak{p}(\mathfrak{a}_\mathfrak{p}) = 1$ for almost all $\mathfrak{p}$. $\mathfrak{a}_\mathfrak{p}$ is called the $\mathfrak{p}$-component of the idèle. If we define the product of two idèles $\mathfrak{p}\to\mathfrak{a}_\mathfrak{p}$ and $\mathfrak{p}\to\mathfrak{b}_\mathfrak{p}$ to be the idèle $\mathfrak{p}\to\mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}$, then the set of all idèles of K forms a group. We denote this group by J or J_K.

For $x(\neq 0)\in K$, $\mathfrak{p}\to x_\mathfrak{p} = x$ defines an idèle (x); (x) is called a principal idèle of K. We denote the group of principal idèles by P or P_K. Obviously the correspondence $x\to(x)$ gives the isomorphism: $P_K\cong K^\times$, where $K^\times$ is the multiplicative group of all non zero elements in K. Thus we may identify K and P_K.

The factor gruop $\mathfrak{C} = J/P$ is called the group of *idele classes*. If we put $w_\mathfrak{p}(\mathfrak{a}) = w_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$ for $\mathfrak{a}\in J$, $w_\mathfrak{p}$ defines a homomorphism from J into $\mathbf{R}^+$, where $\mathbf{R}^+$ is the multiplicative group of all positive real numbers. As the product $\prod_\mathfrak{p} w_\mathfrak{p}(\mathfrak{a})$ is essentially a finite product, we can define $\lambda(\mathfrak{a}) = \prod_\mathfrak{p} w_\mathfrak{p}(\mathfrak{a})$ for all $\mathfrak{a}\in J$. If $\mathfrak{a}$ is a principal idèle, we have $\lambda(\mathfrak{a}) = 1$ by the product formula in K. So, λ defines a homomorphism of $\mathfrak{C}$ into $\mathbf{R}^+$. We denote the kernel of this homomorphism by $\mathfrak{C}_0$.

For a finite place $\mathfrak{p}$, we denote the group of units in $K_\mathfrak{p}$ by $U_\mathfrak{p}$.

THEOREM 1.1. *$U_\mathfrak{p}$ is a compact group (under the usual $\mathfrak{p}$-adic topology).*

Let $V^{(n)}$ be the group of elements $\equiv 1 \pmod{\mathfrak{p}^n}$ in $K_\mathfrak{p}$. Obviously the factor group $U_\mathfrak{p}/V^{(n)}$ is finite and $\bigcap_{n=1} V^{(n)}=\{1\}$. For $u\in U_\mathfrak{p}$, we denote the residue class of u mod $\mathfrak{p}^n$ by u_n. Then the correspondence: $u\to(u_1, u_2, \ldots, u_n, \ldots)$ $\in\prod_n U_\mathfrak{p}/V^{(n)}$ gives a homeomorphic isomorphism $U_\mathfrak{p}\cong H$, where H is the set of all $(u_1, u_2, \ldots, u_n, \ldots)$ in $\prod_n U_\mathfrak{p}/V^{(n)}$ such that $u_{n+1}\equiv u_n \pmod{\mathfrak{p}^n}$ $(n=1, 2, \ldots)$. But the group $\prod_n U_\mathfrak{p}/V^{(n)}$ is compact and H is closed in it, so H is compact, and our theorem is proved.

For an infinite place $\mathfrak{p}$, the group $U_\mathfrak{p}$ is defined as follows: if $K_\mathfrak{p}$ is real, $U_\mathfrak{p}$ is the set of all numbres >0 and if $K_\mathfrak{p}$ is not real, $U_\mathfrak{p}=K_\mathfrak{p}^\times$. In either case the group $U_\mathfrak{p}$ is locally compact. Since the infinite places are finite in number, it follows from these considerations, that the product group $U=\prod_\mathfrak{p} U_\mathfrak{p}$ is locally compact. Then, if we take all neighbourhoods of 1 in U as a fundamental system of neighbourhood of 1 in J, J becomes a locally compact group and J/U is a discrete group. When we speak of a topology in J in the sequel, we shall mean, if not otherwise said, this topology of J.

The above defined $w_\mathfrak{p}$ is continuous on J. To show this it is sufficient to prove the continuity on U. But if $\mathfrak{p}$ is finite, $w_\mathfrak{p}=1$ and it is trivially continuous. It is obviously continuous, when $\mathfrak{p}$ is infinite. Next, the product $\lambda=\prod_\mathfrak{p} w_\mathfrak{p}$ is continuous too on J. For $w_\mathfrak{p}(\mathfrak{a})=1$ on U, if $\mathfrak{p}$ is finite and there is only a finite number of infinite places.

THEOREM 1.2. *P is discrete in J.*

It is sufficient to show that $P\cap U$ is discrete in U. For $x\in P\cap U$, we have $w_\mathfrak{p}(x)=1$ for all finite places. Therefore x must be an integer in K. Let $(\omega_1, \ldots, \omega_n)$ be a base of integers in K. Then $x=\sum_{i=1}^{n}\nu_i\omega_i$ where the ν_i's are rational integers. If a is a real number >0, let N be the set of $\mathfrak{a}\in U$ such that $w_\mathfrak{p}(\mathfrak{a}_\mathfrak{p}-1)<a$ for all infinite $\mathfrak{p}$. As $w_\mathfrak{p}$ is continuous, N is a neighbourhood of 1 in U. We shall show that, if a is small enough, then $N\cap P=\{1\}$. Let $\gamma_1, \ldots, \gamma_n$ be isomorphisms of K into $\mathbf{C}$ (the field of all complex numbers). We claim that there is a number $b>0$ such that 1 is the only integer x in K which satisfies $|\gamma_i(x-1)|<b$ $(i=1, \ldots, n)$. Now, put $1=\sum_i\alpha_i\omega_i$. Since det $(\gamma_i(\omega_j))$

$=0$. $\sum_{j=1}^{n}|(\alpha_j-\nu_j)\gamma_i(\omega_j)|<b$ implies that $|\alpha_j-\nu_j|<\frac{1}{2}$ if b is small enough. As α_j and ν_j are integers, we have $\alpha_j=\nu_j$ $(j=1,\ldots,n)$. Thus $x=1$. Since each $\gamma_i(x)$ is either $w_{\mathfrak{p}}(x)$ or $w_{\mathfrak{p}}^{(\rho)}(x)$, there is $a>0$ such that the conditions $w_{\mathfrak{p}}(x-1)<a$ (infinite $\mathfrak{p}$) imply $|\gamma_i(x-1)|<b$ $(i=1,\ldots,n)$, and our statement is proved.

Next we want to show that $\mathfrak{C}_0$ is compact. We start with

LEMMA 1.1 (*Minkowski*). *Let $L_1,\ldots,L_n$ be linearly independent linear forms on $\mathbf{C}^n$ such that $\overline{L_i}\in\{L_1,\ldots,L_n\}$ $(1\leqq i\leqq n)$. We denote by D the determinant of $L_1,\ldots,L_n$. Let α_i $(i=1,\ldots,n)$ be numbers >0 such that $\alpha_1\ldots\alpha_n\geqq |D|$, $\alpha_i=\alpha_j$ if $L_j=\overline{L_i}$. Then there is a $\mathfrak{z}\neq 0$ in $\mathbf{Z}^n$ such that $|L_i(\mathfrak{z})|\leqq\alpha_i$ $(1\leqq i\leqq n)$, $\mathbf{Z}$ being the set of rational integers.*

First we shall treat the case where all L_i are real forms. Now, assume that the assertion is true when $\alpha_1\cdots\alpha_n>|D|$. For any rational integer $k>0$, we have $\Pi\left(\alpha_i+\frac{1}{k}\right)>|D|$. Therefore there is a $\mathfrak{z}_k\neq 0$ in $\mathbf{Z}^n$ such that $|L_i(\mathfrak{z}_k)|\leqq\alpha_i+\frac{1}{k}$ $(1\leqq i\leqq n)$. As $L_1,\ldots,L_n$ are linearly independent and the $|L_i(\mathfrak{z}_k)|$ are bounded, $|\mathfrak{z}_k|$ remains bounded. Therefore, there is a $\mathfrak{z}$ such that $\mathfrak{z}=\mathfrak{z}_k$ for infinitely many k. Hence we get $|L_i(\mathfrak{z})|\leqq\alpha_i$. Thus, we may assume that $\alpha_1\cdots\alpha_n>|D|$. Let P be the set of $\mathfrak{x}\in\mathbf{R}_n$ such that $|L_i(\mathfrak{x})|\leqq\alpha_i/2$. Then, P is the inverse image of a parallelotope of sides $\alpha_1,\ldots,\alpha_n$ under the mapping $\mathfrak{x}\rightarrow(L_1(\mathfrak{x}),\ldots,L_n(\mathfrak{x}))$. It follows that the volume of $P=\frac{\alpha_1\cdots\alpha_n}{|D|}>1$. We take $\mathfrak{z}=(m_1,\ldots,m_n)\in\mathbf{Z}^n$ such that $|m_i|\leqq N$. There are $(2N+1)^n$ such $\mathfrak{z}$'s: $\mathfrak{z}_1,\ldots,\mathfrak{z}_{(2N+1)^n}$. Let δ be the diameter of P. Then all $\mathfrak{z}_k+P$ are contained in the cube of side $2N+\delta$ with center at origin. We have $\sum_{k=1}^{(2N+1)^n}\mathrm{vol}\,(\mathfrak{z}_k+P)$ $=(2N+1)^n\,\mathrm{vol}\,P$, while the volume of our cube is $(2N+\delta)^n$. But, if N tends to infinity we have $\frac{(2N+1)^n\,\mathrm{vol}\,P}{(2N+\delta)^n}\rightarrow\mathrm{vol}\,P>1$. Thus, for sufficiently large N, $\sum\mathrm{vol}\,(\mathfrak{z}_k+P)$ is strictly larger than the volume of our cube. Hence $(\mathfrak{z}_k+P)$ $\cap(\mathfrak{z}_l+P)\neq\phi$ for some k, l $(k\neq l)$. Therefore there exist, $\mathfrak{x}, \mathfrak{y}\in P$ such that $\mathfrak{z}_k+\mathfrak{x}=\mathfrak{z}_l+\mathfrak{y}$. We have $\mathfrak{y}-\mathfrak{x}\in\mathbf{Z}^n$. Since $|L_i(\mathfrak{y})|$, $|L_i(\mathfrak{x})|\leqq\frac{\alpha_i}{2}$, we have $|L_i(\mathfrak{y}-\mathfrak{x})|$ $\leqq\alpha_i$. This settles the special case under consideration. Next, we consider the general case. Put $L_i'=L_i$, $\alpha_i'=\alpha_i$ if L_i is real. If not, assume $\overline{L_i}=L_j$, $i<j$ and set

$$\begin{aligned} L_i &= L_i = L_i' + \sqrt{-1}L_j' \\ L_j &= L_i = L_i' - \sqrt{-1}L_j' \end{aligned} \qquad \alpha_i' = \alpha_j' = \frac{\alpha_i}{\sqrt{2}} = \frac{\alpha_j}{\sqrt{2}}.$$

Then the L_i''s are real forms. Suppose that there are r pairs of complex conjugate forms among the L_i's. It is easily verified that

$$\det(L_1', \ldots, L_n') = \frac{\det(L_1, \ldots, L_n)}{(-2\sqrt{-1})^r} = \frac{|D|}{2^r}. \quad \text{Therefore}$$

$$\alpha_1' \cdots \alpha_n' = \frac{\alpha_1 \cdots \alpha_n}{2^r} \geqq |\det(L_1', \ldots, L_n')|.$$

From the first case there is a $\mathfrak{z}(\neq 0) \in Z_n$ such that $|L_i'(\mathfrak{z})| \leqq \alpha_i'$. Therefore $|L_i(\mathfrak{z})| \leqq \alpha_i$. This completes the proof of our lemma.

THEOREM 1. 3. *Let K be a field of algebraic numbers. For each $\mathfrak{p}$, let $a_\mathfrak{p} > 0$ be given such that:*

1) *for $\mathfrak{p}$ finite, $a_\mathfrak{p} \in$ group $W_\mathfrak{p}$ of values of the normalized valuation $w_\mathfrak{p}$ at $\mathfrak{p}$.*
2) *Almost all $a_\mathfrak{p}$ are $=1$.*
3) $\prod_\mathfrak{p} a_\mathfrak{p} \geqq \sqrt{|\varDelta|}$, *where $\varDelta$ is the discriminant of K.*

Then, there is a number $x \neq 0$ in K with $w_\mathfrak{p}(x) \leqq a_\mathfrak{p}$ for all $\mathfrak{p}$.

For finite $\mathfrak{p}$, let $a_\mathfrak{p} = w_\mathfrak{p}(\pi_\mathfrak{p}^{e(\mathfrak{p})})$, where $\pi_\mathfrak{p}$ is an element of order 1 at $\mathfrak{p}$ in $K_\mathfrak{p}$. From condition 2, $e(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$, so we may speak of the ideal $\mathfrak{a} = \prod \mathfrak{p}^{e(\mathfrak{p})}$. Since $a_\mathfrak{p} = N_K(\mathfrak{p}^{e(\mathfrak{p})})^{-1}$, we have $N_K\mathfrak{a} = (\prod_{\mathfrak{p}\text{ finite}} a_\mathfrak{p})^{-1}$. Let $(\alpha_1, \ldots, \alpha_n)$ be a base of $\mathfrak{a}$. Any $x \in \mathfrak{a}$ may be written as $x = \sum_{i=1}^n m_i\alpha_i$, where the m_i's are rational integers. Let $\gamma_1, \ldots, \gamma_n$ be the isomorphisms of K into $\mathbf{C}$, where $\gamma_1, \ldots, \gamma_r$ are real and γ_{r+k}, and γ_{r+s+k} are conjugate imaginary; $r + 2s = n$. For the infinite place $\mathfrak{p}_i$ which corresponds to γ_i, we put $b_i = a_{\mathfrak{p}_i}$ or $b_i = \sqrt{a_{\mathfrak{p}_i}}$ according as to whether $\mathfrak{p}_i$ is real or not. Now we consider the linear froms $L_i = \sum_{j=1}^n x_j\gamma_i(\alpha_j)$. As the absolute value of the determinant of $L_1, \ldots, L_n$ is $N\mathfrak{a}\sqrt{|\varDelta|} \neq 0$, and $\prod_{i=1}^n b_i = \prod_{\mathfrak{p}\text{ infinite}} a_\mathfrak{p} \geqq \frac{\sqrt{|\varDelta|}}{\prod_{\mathfrak{p}\text{ finite}} a_\mathfrak{p}} = N\mathfrak{a}\sqrt{|\varDelta|}$, there is an $x = \sum_j m_j\alpha_j \in K$ such that $|L_i(x)| \leqq b_i$, by Minkowski's lemma. This means that $w_\mathfrak{p}(x) \leqq a_\mathfrak{p}$ for all $\mathfrak{p}$.

THEOREM 1. 4. *$\mathfrak{C}_0$ is compact.*

It is sufficient to show that any class of $\mathfrak{C}_0$ is represented by an idèle which belongs to some fixed compact subset in J. Let $\mathfrak{a}$ be any representative of a class in $\mathfrak{C}_0$. By the definition of $\mathfrak{C}_0$, we have $\prod_\mathfrak{p} w_\mathfrak{p}(\mathfrak{a}) = 1$. Let $\mathfrak{q}$ be an arbitrary fixed infinite place. From the theorem 1.3 there is an $x(\neq 0)\in K$ such that $w_{\mathfrak{p}}(x)\leqq w_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{p}\neq\mathfrak{q}$ and $w_{\mathfrak{q}}(x)\leqq\sqrt{\Delta}\, w_{\mathfrak{q}}(\mathfrak{a})$. By the product formula, we have $\prod_{\mathfrak{p}} w_{\mathfrak{p}}(x\mathfrak{a}^{-1}) = \prod_{\mathfrak{p}\neq\mathfrak{q}} w_{\mathfrak{p}}(x\mathfrak{a}^{-1})\cdot w_{\mathfrak{q}}(x\mathfrak{a}^{-1}) = 1$. Hence $w_{\mathfrak{q}}(x\mathfrak{a}^{-1}) = \dfrac{1}{\prod_{\mathfrak{p}\neq\mathfrak{q}} w_{\mathfrak{p}}(x\mathfrak{a}^{-1})}\geqq 1$. On the other hand, $w_{\mathfrak{p}}(x\mathfrak{a}^{-1})\geqq\prod_{\mathfrak{r}'\neq\mathfrak{q}} w_{\mathfrak{r}'}(x\mathfrak{a}^{-1}) = \dfrac{1}{w_{\mathfrak{q}}(x\mathfrak{a}^{-1})}\geqq\dfrac{1}{\sqrt{|\Delta|}}$. Thus we get the following inequalities:

$$1/\sqrt{\Delta}\leqq w_{\mathfrak{p}}(x\mathfrak{a}^{-1})\leqq 1\quad(\mathfrak{p}\neq\mathfrak{q}),$$
$$1\leqq w_{\mathfrak{q}}(x\mathfrak{a}^{-1})\leqq\sqrt{\Delta}\,.$$

For a finite $\mathfrak{p}$, put $W_{\mathfrak{p}} = \left\{\left(\frac{1}{p^f}\right)^k\right\}$, where p is the prime number below $\mathfrak{p}$ and f is a fixed positive integer for each $\mathfrak{p}$. Then, by the former inequality, there is a fixed finite set of places such that $w_{\mathfrak{p}}(x\mathfrak{a}^{-1}) = 1$ whenever $\mathfrak{p}$ is outside of this set. As for a $\mathfrak{p}$ in this set, the order of $x\mathfrak{a}^{-1}$ at $\mathfrak{p}$ is bounded, again by the above inequalities. Hence, the integral ideal $(x\mathfrak{a}^{-1})$ can have only prime ideals from a fixed finite set as prime components, and has them with bounded exponents. Thus, $(x\mathfrak{a}^{-1})$ is one of a finite mumber of ideals which may be represented as $(\mathfrak{b}_1),\ldots,(\mathfrak{b}_{k_0})$, where $\mathfrak{b}_k$'s are idèles with $\mathfrak{b}_{k\mathfrak{p}} = 1$ for $\mathfrak{p}$ at infinity. We get $x\mathfrak{a}^{-1} = \mathfrak{b}_k\mathfrak{m}$, where the $\mathfrak{p}$-component $\mathfrak{m}_{\mathfrak{p}}$ of $\mathfrak{m}$ is a unit for finite $\mathfrak{p}$ and $1\leqq w_{\mathfrak{p}}(\mathfrak{m}_{\mathfrak{p}})\leqq\sqrt{|\Delta|}$ for infinite $\mathfrak{p}$. Hence $\mathfrak{m}$ belongs to the compact set $M = \prod_{\mathfrak{p}\text{ finite}} U_{\mathfrak{p}}\times\prod_{\mathfrak{p}\text{ infinite}} C_{\mathfrak{p}}$, where $C_{\mathfrak{p}}$ is the closed set defined by the above inequalities for $\mathfrak{p}$ at infinity. Thus $\mathfrak{a} = x\mathfrak{b}_k^{-1}\mathfrak{m}^{-1}$ is represented by the idèle $\mathfrak{b}_k^{-1}\mathfrak{m}^{-1}$ which is contained in the compact set $\bigcup_k \mathfrak{b}_k^{-1}M^{-1}$. This proves our assertion.

We have now readily

THEOREM 1.5. $\mathfrak{C} = \mathfrak{C}_0\times\mathbf{R}^+$ (*topologically and algebraically*).

Let L be a finite algebraic extension of K. With any idèle $\mathfrak{a}\in J_K$, we associate an idèle $\iota_{K/L}\mathfrak{a}\in J_L$ whose $\mathfrak{P}$-component is $(\iota_{K/L}\mathfrak{a})_{\mathfrak{P}} = \mathfrak{a}_{\mathfrak{p}}$ if $\mathfrak{p}$ is the place below $\mathfrak{P}$. Obviously this mapping $\iota_{K/L}$ is a monomorphism of J_K into J_L. We have $\iota_{K/M} = \iota_{L/M}\circ\iota_{K/L}$ if $K\subset L\subset M$.

If L/K is a normal extension with the Galois group $\mathfrak{G}(L/K)$, we shall make $\mathfrak{G}(L/K)$ operate on J_L in the following way. Let s be in $\mathfrak{G}(L/K)$. Since s permutes the place of L among each other, s gives an isomorphism of $L_{\mathfrak{P}}$ with $L_{s\mathfrak{P}}$. For each idèle $\mathfrak{a}\in J_L$, we define the idèle $s\mathfrak{a}$ by $(s\mathfrak{a})_{\mathfrak{P}} = s(\mathfrak{a}_{s^{-1}\mathfrak{P}})$.

THEOREM 1.6. ***The group of fixed elements in J_L with respect to $\mathfrak{G}(L/K)$ is***

$\iota_{K/L}(J_K)$.

Obviously any element in $\iota_{K/L}(J_K)$ is fixed. Conversely, let $\mathfrak{a}$ be an idèle which is fixed by all s: $\mathfrak{a}_{\mathfrak{P}} = (s\mathfrak{a})_{\mathfrak{P}} = s(\mathfrak{a}_{s^{-1}\mathfrak{P}})$. If s belongs to the decomposition group $\mathfrak{H}$ of $\mathfrak{P}$, we have $s\mathfrak{P} = \mathfrak{P}$. Now, $\mathfrak{H}$ can be considered as the full Galois group of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. So we get $\mathfrak{a}_{\mathfrak{P}} \in K_{\mathfrak{p}}$ for all $\mathfrak{P}$. Hence, we have $\mathfrak{a}_{\mathfrak{P}} = (s\mathfrak{a})_{\mathfrak{P}} = \mathfrak{a}_{s^{-1}\mathfrak{P}}$ for any $s \in \mathfrak{G}(L/K)$. Thus we have $\mathfrak{a} = \iota_{K/L}(\mathfrak{b})$, where $\mathfrak{b}_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{P}}$ if $\mathfrak{p}$ is the place below $\mathfrak{P}$.

THEOREM 1.7. $P_L \cap \iota_{K/L} J_K = \iota_{K/L} P_K$.

Let L'/K be a mormal extension over K which contains L. For each $(x)_L \in P_L \cap \iota_{K/L} J_K$, we have $(x)_L = \iota_{K/L}\mathfrak{x}$, $\mathfrak{x} \in J_K$, and therefore $(x)_{L'} = \iota_{K/L'}\mathfrak{x}$. If the assertion is true for L'/K, $\mathfrak{x}$ must be principal in K. This reduces the general case to the case of a normal extension L/K. But in this case the assertion is almost trivial from theorem 1.6.

THEOREM 1.8 (*E. Noether, generalizing "Theorem 90" of Hilbert*). *Let L/K be normal. If a mapping $s \to a(s)$ of $\mathfrak{G}(L/K)$ into $L^{\times}$ satisfies the condition: $a(st) = a(s)(sa(t))$ for all $s, t \in \mathfrak{G}$, then there is a $b \in L^{\times}$ such that $a(s) = b^{1-s}$ for all s.*

Let ω be an element in L; we put $x = \sum_{t\in\mathfrak{G}} (t\omega)a(t)$. Then, we have $sx = \sum_{t\in\mathfrak{G}} (st\omega)\, sa(t) = \sum_{t\in\mathfrak{G}} (st\omega) \dfrac{a(st)}{a(s)}$. Hence, $a(s)sx = \sum_{t\in\mathfrak{G}} (st\omega)a(st) = x$. So, if $x \neq 0$ then $a(s) = x^{1-s}$. Now, we show the existence of such an x. Let $(\omega_1, \dots, \omega_n)$ be a base of L/K. If $x_i = \sum_{t\in\mathfrak{G}} (t\omega_i)a(t) = 0$ for all i, we have $a(t) = 0$ for all t, because $(\det(t\omega_i))^2 = \det(S_p(\omega_i\omega_j)) \neq 0$, and this is a contradiction.

COROLLARY (*"Theorem 90" of Hilbert*). *Let L/K be a cyclic extension and s a generator of $\mathfrak{G}(L/K)$. Let a be in L. If $N_{L/K}a = 1$, then there is a $b \in L$ such that $a = b^{1-s}$.*

Put $f(e) = 1, f(s) = a, f(s^2) = a(sa), \dots, f(s^{n-1}) = a(sa) \cdots (s^{n-2}a)$, where n denotes the order of s. Then $s^i \to f(s^i)$ satisfies the condition of theorem 1.8.

For $L \supset K$, we define a mapping $\iota_{K/L}$: $\mathfrak{C}_K \to \mathfrak{C}_L$ by putting $\iota_{K/L}(\mathfrak{a}P_K) = \iota_{K/L}\mathfrak{a} \cdot P_L$ for any $\mathfrak{a} \in J_K$. If L/K is normal, then $\mathfrak{G}(L/K)$ operates on J_L and its operations obviously preserve P_L. Thus, we may make $\mathfrak{G}(L/K)$ operate on $\mathfrak{C}_L$; the elements of $\iota_{K/L}\mathfrak{C}_K$ is then left fixed by the operations of $\mathfrak{G}(L/K)$.

THEOREM 1.9. *The set of fixed elements in* $\mathfrak{C}_L$ *with respect to* $\mathfrak{G}(L/K)$ is $\iota_{K/L}(\mathfrak{C}_K)$.

Let $\mathfrak{k}$ be an element of $\mathfrak{C}_L$ such that $s\mathfrak{k}=\mathfrak{k}$ for all $s\in\mathfrak{G}(L/K)$. For any idèle $\mathfrak{a}\in\mathfrak{k}$, we have $s\mathfrak{a}=\mathfrak{a}\cdot(x_s)$, $x_s\in L^\times$, for all s and $st\mathfrak{a}=s(t\mathfrak{a})=s\mathfrak{a}\cdot s(x_t)$ $=\mathfrak{a}\cdot(x_s(s\cdot x_t))=\mathfrak{a}(x_{st})$. So $x_{st}=x_s(sx_t)$ and therefore $x_s=y^{1-s}$ with some $y\neq 0$ in L. Therefore $s\mathfrak{a}=\mathfrak{a}\dfrac{y}{sy}$. Hence $s(\mathfrak{a}y)=\mathfrak{a}y$. Since s is any element in $\mathfrak{G}(L/K)$, we get $\mathfrak{a}y\in\iota_{K/L}(J_K)$ from theorem 1.6. This means that $\mathfrak{k}\in\iota_{K/L}(\mathfrak{C}_K)$.

Now, let Ω be the field of all algebraic numbers, i.e. the algebraic closure of the rational number field $\mathbf{Q}$. Ω is represented as the union of fields K_n of finite degree: $\Omega=\bigcup_{n=1}^{\infty}K_n$. $K_n\subset K_{n+1}$.

Now we consider all sequences of idèle classes $(x_\nu, x_{\nu+1}, \dots, x_n, x_{n+1}, \dots)$ such that $x_n\in\mathfrak{C}_{K_n}$, $x_{n+1}=\iota_{K_n/K_{n+1}}x_n$ $(n\geqq\nu)$. We identify any two sequences of the respective forms $(x_\mu, x_{\mu+1}, \dots)$ and $(x_{\mu-h}, x_{\mu-h+1}, \dots)$. The set of all these sequences, with these identifications is written by $\mathfrak{C}_\Omega$. The correspondence: $x\to(x, \iota_{K_\nu/K_{\nu+1}}x, \dots)$ gives a monomorphism of $\mathfrak{C}_{K_\nu}$ into $\mathfrak{C}_\Omega$. If we identify the image of this mapping with $\mathfrak{C}_{K_\nu}$, the map $\iota_{K_\nu/K_{\nu+1}}$ may be regarded as the inclusion mapping of $\mathfrak{C}_{K_\nu}$ into $\mathfrak{C}_{K_{\nu+1}}$ and we get $\mathfrak{C}_\Omega=\bigcup_{n=1}^{\infty}\mathfrak{C}_{K_n}$. $\mathfrak{G}(\Omega/\mathbf{Q})$ operates on $\mathfrak{C}_\Omega$, because, if K is normal over $\mathbf{Q}$, then $\mathfrak{G}(\Omega/\mathbf{Q})$ operates on K and so it operates on $\mathfrak{C}_K$. Now, let K be any intermediate field: $\Omega\supset K\supset\mathbf{Q}$. Then the group $\mathfrak{G}(\Omega/K)$ operates on $\mathfrak{C}_\Omega$ and the set of all fixed elements with respect to this group is $\mathfrak{C}_K$.

§2. MODULES $\mathfrak{N}(\mathfrak{G}, A)$, I AND J

Let $\mathfrak{G}$ be a group. By a (left) $\mathfrak{G}$-module is meant an object formed by $\mathfrak{G}$, an additive group A and a mapping φ of $\mathfrak{G}\times A$ into A such that φ is additive with respect to its second argument and

$$(st)a = s(ta), \qquad ea = a \tag{2.1}$$

with s, t are elements of $\mathfrak{G}$, e the unit element of $\mathfrak{G}$ and a is an element of A and where we put $\varphi(s, a) = sa$. A left $\mathfrak{G}$-module may always be considered as a right $\mathfrak{G}$-module (and vice versa) if we put $as = s^{-1}a$ ($s\in\mathfrak{G}$, $a\in A$).

Let R be a ring with unit element. By a left R-module is meant an object formed by R, an additive group A and a mapping φ of $R\times A$ into A such that φ is bi-additive and (2.1) holds with elements s, t of R and the unit element e of R. Let $\mathbf{Z}[\mathfrak{G}]$ be the group ring of $\mathfrak{G}$ over the ring $\mathbf{Z}$ of rational integers. A (left) $\mathfrak{G}$-module may be considered as a left $\mathbf{Z}[\mathfrak{G}]$-module, and conversely.

Let $\mathfrak{G}$ be a finite group, and A be a $\mathfrak{G}$-module. Denote the element $\sum_{s\in\mathfrak{G}} s$ of the group ring $\mathbf{Z}[\mathfrak{G}]$ by σ. We have

$$\sigma t = t\sigma = \sigma$$

for every $t\in\mathfrak{G}$. Let $A^{\mathfrak{G}}$ be the set of element a of A satisfying $sa = a$ for every $s\in\mathfrak{G}$. $A^{\mathfrak{G}}$ is a ($\mathfrak{G}$-)submodule of A. So is σA, and we have $\sigma A\subset A^{\mathfrak{G}}$. We denote the factor module $A^{\mathfrak{G}}/\sigma A$ by $\mathfrak{N}(\mathfrak{G}\,;A)$, or simply by $\mathfrak{N}(A)$.

Let A, B be $\mathfrak{G}$-modules and let there be a homomorphism (i.e. a $\mathfrak{G}$-linear mapping) of A into B. Clearly $A^{\mathfrak{G}}$, σA are mapped by f respectively into $B^{\mathfrak{G}}$, σB. So we obtain a homomorphism

$$f^{\mathfrak{N}}:\ \mathfrak{N}(\mathfrak{G}\,;A)\to\mathfrak{N}(\mathfrak{G}\,;B).$$

If g is a homomorphism of B into a third $\mathfrak{G}$-module C, we have

$$(g\circ f)^{\mathfrak{N}} = g^{\mathfrak{N}}\circ f^{\mathfrak{N}}.$$

Let again A, B be two $\mathfrak{G}$-modules. Let $A\otimes B$ be their tensor product over $\mathbf{Z}$. For each $s\in\mathfrak{G}$, the mapping $(a, b)\to sa\otimes sb$ of $A\times B$ into $A\otimes B$ is bi-additive and defines thus an additive map λ_s of $A\otimes B$ into itself such that $\lambda_s(a\otimes b)$

$= sa \otimes sb$. Putting $s\theta = \rho_s(\theta)$ ($\theta \in A \otimes B$), we consider $A \otimes B$ as a $\mathfrak{G}$-module. Let $\alpha \in \mathfrak{N}(\mathfrak{G}; A)$ and a be a representative of α in $A^{\mathfrak{G}}$. Similarly, let $\beta \in \mathfrak{N}(\mathfrak{G}; B)$ and b a representative of β in $B^{\mathfrak{G}}$. We have

$$s(a \otimes b) = sa \otimes sb = a \otimes b$$

and therefore $a \otimes b \in (A \otimes B)^{\mathfrak{G}}$. Let γ be the class of $a \otimes b$ in $\mathfrak{N}(\mathfrak{G}; A \otimes B)$. Here γ depends only on α and β. For, with $a' \in A$,

$$\begin{aligned}(a + \sigma a') \otimes b &= a \otimes b + \sum_{s \in \mathfrak{G}} sa' \otimes b \\ &= a \otimes b + \sum_{s \in \mathfrak{G}} sa' \otimes sb = a \otimes b + \sigma(a' \otimes b) \in \gamma\end{aligned}$$

and similarly $a \otimes (b + \sigma b') \in \gamma$ for $b' \in B$. Thus the mapping $(\alpha, \beta) \to \gamma$ of $\mathfrak{N}(\mathfrak{G}; A) \times \mathfrak{N}(\mathfrak{G}; B)$ into $\mathfrak{N}(\mathfrak{G}; A \otimes B)$ is bi-additive and we obtain an additive map

$$T: \mathfrak{N}(\mathfrak{G}; A) \otimes \mathfrak{N}(\mathfrak{G}; B) \to \mathfrak{N}(\mathfrak{G}; A \otimes B),$$

which is in fact a ($\mathfrak{G}$-)homomorphism.

Let u, v be homomorphisms of A, B into $\mathfrak{G}$-modules A', B' respectively. Then we have a homomorphism $u \otimes v$ of $A \otimes B$ into $A' \otimes B'$ such that $(u \otimes v)(a \otimes b) = ua \otimes vb$ $(a \in A,\ b \in B)$. Let T' be the homomorphism of $\mathfrak{N}(\mathfrak{G}; A') \otimes \mathfrak{N}(\mathfrak{G}; B')$ into $\mathfrak{N}(\mathfrak{G}; A' \otimes B')$ defined similarly as T. Thus we obtain a diagram

$$\begin{array}{ccc}\mathfrak{N}(\mathfrak{G}; A) \otimes \mathfrak{N}(\mathfrak{G}; B) & \xrightarrow{T} & \mathfrak{N}(\mathfrak{G}; A \otimes B) \\ {\scriptstyle u^{\mathfrak{N}} \otimes v^{\mathfrak{N}}} \downarrow & & \downarrow {\scriptstyle (u \otimes v)^{\mathfrak{N}}} \\ \mathfrak{N}(\mathfrak{G}; A') \otimes \mathfrak{N}(\mathfrak{G}; B') & \xrightarrow{T'} & \mathfrak{N}(\mathfrak{G}; A' \otimes B')\end{array}$$

and this diagram is commutative as we readily verify. (A diagram is a graph each of whose vertices is a module and each of whose edges has an orientation and means a homomorphism, and a diagram is said to be commutative when all ways leading from M to N, with any given pair (M, N) of vertices in the diagram, give a same homomorphism.)

A $\mathfrak{G}$-module A is said to *split* when there is an additive subgroup X (which is not necessarily a ($\mathfrak{G}$-)submodule) of A such that $A = \sum_{s \in \mathfrak{G}} sX$ (direct). For instance $\mathbf{Z}[\mathfrak{G}]$ splits. For $\mathbf{Z}[\mathfrak{G}] = \sum_{s \in \mathfrak{G}} \mathbf{Z}s = \sum_{s \in \mathfrak{G}} s(\mathbf{Z}e)$ (direct).

THEOREM 2.1. *If A splits, then $\mathfrak{N}(\mathfrak{G}; A) = \{0\}$.*

To prove this, let $a \in A$ and $a = \sum_{s \in \mathfrak{G}} sx_s$ $(x_s \in X)$. Then $ta = \sum_s tsx_s = \sum_s sx_{t^{-1}s}$.

If here $a \in A^{\mathfrak{G}}$, then $ta = a$ and $x_s = x_{t^{-1}s}$ for all $s, t \in \mathfrak{G}$, whence $x_s = x_e$ for all $s \in \mathfrak{G}$ and $a = \sum_s s x_e = \sigma x_e$. Thus $A^{\mathfrak{G}} = \sigma A$, which proves our theorem.

LEMMA 2.1. *If A, B are $\mathfrak{G}$-modules and if A splits, so do $A \otimes B$ and $B \otimes A$.*

For, $A \otimes B = \sum_s sX \otimes B$ (direct) $= \sum_s sX \otimes sB$ (direct)
$= \sum_s s(X \otimes B)$ (direct). Similarly, $B \otimes A = \sum_s s(B \otimes X)$.

Now, we see easily

LEMMA 2.2. *If $A = \sum_\lambda A_\lambda$ (direct), $B = \sum_\mu B_\mu$ (direct) are $\mathfrak{G}$-modules (or merely additive groups) and ι_λ, ι'_λ are injection maps of A_λ, B_λ* into *A, B respectively. Then the mappings $\iota_\lambda \otimes \iota'_\mu$ of $A_\lambda \otimes B_\mu$ into $A \otimes B$ are monomorphic and*

$$A \otimes B = \sum_{\lambda, \mu} (\iota_\lambda \otimes \iota'_\mu)(A_\lambda \otimes B_\mu) \quad (direct).$$

Let next A, B, B' be $\mathfrak{G}$-modules (or additive groups), $\mathbf{I}$ be the identity map of A, and φ be a homomorphism of B into B'. Let H be the kernel of φ, and ι be the injection map of H into B. From lemma 2.2 we deduce easily.

LEMMA 2.3. *If either a) A has a base (over $\mathbf{Z}$), or b) B is a direct sum $H+K$ (direct), the injection map $\mathbf{I} \otimes \iota : A \otimes H \to A \otimes B$ is monomorphic and its image $(\mathbf{I} \otimes \iota)(A \otimes H)$ is the kernel of $\mathbf{I} \otimes \varphi$, in case of b) we have indeed*

$$A \otimes B = (\mathbf{I} \otimes \iota)(A \otimes H) + (\mathbf{I} \otimes \iota')(A \otimes K) \quad (direct)$$

where ι' is the injection map of K into B.

Now, let $\mathfrak{G}$ be a finite group and $\mathbf{Z}[\mathfrak{G}]$ be its group ring over the ring $\mathbf{Z}$ of rational integers; we shall often denote $\mathbf{Z}[\mathfrak{G}]$ by Z. Set $\sigma = \sum_{s \in \mathfrak{G}} s$ as before. Let $I = I[\mathfrak{G}]$ be the set of elements x of Z such that $\sigma x = 0$; I is a $\mathfrak{G}$-module. Further, if $x = \sum_{s \in \mathfrak{G}} \nu(s) s$ $(\nu(s) \in \mathbf{Z})$ is an element of Z, then $\sigma x = \sum_s \nu(s) \sigma s$ $= (\sum_s \nu(s))\sigma$. So I is the kernel of the homomorphism $x \to \chi(x) = \sum_{s \in \mathfrak{G}} \nu(s)$ of Z onto $\mathbf{Z}$ and we have the exact sequence

$$0 \to I \to Z \to \mathbf{Z} \to 0.$$

The homomorphisms are also $\mathfrak{G}$-homomorphisms if we consider $\mathbf{Z}$ as a $\mathfrak{G}$-module on which $\mathfrak{G}$ operates trivially; observe that $\chi(sx) = \chi(x)$ $(s \in \mathfrak{G})$.

On the other hand, $\mathbf{Z}\sigma$ is an ideal of Z. Set $J = Z/\mathbf{Z}\sigma$. As $\mathbf{Z}\sigma$ is ($\mathfrak{G}$-) isomorphic to $\mathbf{Z}$, by the correspondence $\nu\sigma \leftrightarrow \nu$ $(\nu \in \mathbf{Z})$. we have the exact sequence

$$0 \to \mathbf{Z} \to Z \to J \to 0.$$

For $s \in \mathfrak{G}$, let $\bar{s}$ be the residue class (mod $\mathbf{Z}\sigma$) of s in J. We have $\sum_{s\in\mathfrak{G}} \bar{s} = 0$ and $\bar{e} = -\sum_{s \neq e} \bar{s}$. $J = \sum_{s\in\mathfrak{G}} \mathbf{Z}\bar{s} = \sum_{s\neq e} \mathbf{Z}\bar{s}$, and the set $\{\bar{s} \mid s \neq e\}$ form a base of J. For, if $\sum_{s\neq e} \nu(s)\bar{s} = 0$, then $\sum_{s\neq e} \nu(s)s = \kappa\sigma = \sum_s \kappa s$ $(\kappa \in \mathbf{Z})$. Here necessarily $\kappa = 0$, as we see on comparing the coefficients of e, and thus all $\nu(s) = 0$. Further, $\sum_s \nu(s)\bar{s} = 0$ if and only if all ν are equal. For $\sum_s \nu(s)\bar{s} = \sum_{s\neq e} (\nu(s) - \nu(e))\bar{s}$.

LEMMA 2.4. *The* ($\mathfrak{G}$-)*module* Add$(I, \mathbf{Z})$ *of additive mapping of* I *into* $\mathbf{Z}$ *is* ($\mathfrak{G}$-)*isomorphic to* J. *Similarly* Add$(J, \mathbf{Z}) \cong I$.

To prove the lemma, let $x = \sum_{s\in\mathfrak{G}} \nu(s)\bar{s}$ be an element of J. $s \to \nu(s)$ gives an additive map of Z onto $\mathbf{Z}$. Let ν' be its restriction to I. Then ν' is determined by x. For, if $x = \sum_{s\in\mathfrak{G}} \nu(s)\bar{s} = \sum_{s\in\mathfrak{G}} \mu(s)\bar{s}$, there exists $k \in \mathbf{Z}$ such that $\mu(s) = \nu(s) + k$ for all s, and we see easily $\mu' = \nu'$. Now, if $\nu' = 0$, then $\nu(s) - \nu(e) = \nu'(s-e) = 0$ and $x = 0$. Thus $x \to \nu'$ is a monomorphism of J into Add$(I, \mathbf{Z})$. It is an epimorphism (whence an isomorphism). For, if $\varphi \in$ Add$(I, \mathbf{Z})$, then φ is the image of $x \in J$ with $x = \sum_{s\in\mathfrak{G}} \varphi(s-e)\bar{s}$. The isomorphism thus obtained is an $\mathfrak{G}$-isomorphism, because, if $x = \sum \nu(s)\bar{s}$, we have $tx = \sum \nu(s)\overline{ts} = \sum \mu(s)\bar{s}$ with $\mu(s) = \nu(t^{-1}s)$ and $\mu = t\nu$, $\mu' = t\nu'$. The isomorphism Add$(J, \mathbf{Z}) \cong I$ can be obtained similarly if we associate with $y = \sum_{s\in\mathfrak{G}} \lambda(s)s \in I$ $(\sum \lambda(s) = 0)$ the additive map of J into $\mathbf{Z}$ given by $\bar{s} \to \lambda(s)$.

§ 3. THE ALGEBRA $\mathfrak{H}$

Let $\mathfrak{G}$ be a finite group. Then we have associated to $\mathfrak{G}$ two modules $I = I[\mathfrak{G}]$, $J = J[\mathfrak{G}]$. For any $r > 0$, we denote by J_r (respectively: I_r) the tensor product of r modules identical to J (respectively: I); we set $J_0 = I_0 = \mathrm{Z}$ (considered as a $\mathfrak{G}$-module on which $\mathfrak{G}$ operates trivially). According to our conventions of identification, we have

$$J_r \otimes J_{r'} = J_{r+r'} \qquad I_r \otimes I_{r'} = I_{r+r'}$$

for all $r \geqq 0$, $r' \geqq 0$.

We introduce now a $\mathfrak{G}$-module $\mathfrak{H}$ which is the direct sum of all modules $J_p \otimes I_q$ $(0 \leqq p,\ q < \infty)$. We set

$${}^{p,q}\mathfrak{H} = J_p \otimes I_q.$$

Thus,

$${}^{p,0}\mathfrak{H} = J_p;\quad {}^{1,0}\mathfrak{H} = J;\quad {}^{0,q}\mathfrak{H} = I_q;\quad {}^{0,1}\mathfrak{H} = I,\quad {}^{0,0}\mathfrak{H} = \mathrm{Z}.$$

Let p, q, p', q' be integers $\geqq 0$. Then there is an isomorphism

$$\iota_{p,q,p',q'} : {}^{p,q}\mathfrak{H} \otimes {}^{p',q'}\mathfrak{H} \to {}^{p+p',q+q'}\mathfrak{H}$$

which maps $(u \otimes v) \otimes (u' \otimes v')$ upon $(u \otimes u') \otimes (v \otimes v')$ if $u \in J_p$, $v \in I_q$, $u' \in J_{p'}$, $v' \in I_{q'}$. We define a bi-linear mapping $(w, w') \to w \square w'$ of $\mathfrak{H} \times \mathfrak{H}$ into $\mathfrak{H}$ by the formulas

$$w \square w' = \iota_{p,q,p',q'}(w \otimes w') \quad (w \in {}^{p,q}\mathfrak{H},\ w' \in {}^{p',q'}\mathfrak{H}).$$

This defines a multiplication in $\mathfrak{H}$. We have

$$(u \otimes v) \square (u' \otimes v') = (u \otimes u') \otimes (v \otimes v')$$

if $u \in J_p$, $v \in I_p$, $u' \in J_{p'}$, $v' \in I_{q'}$; it follows immediately that our multiplication is associative. If $s \in \mathfrak{G}$, then we have

$$s(w \square w') = (sw) \square (sw') \quad (w,\ w' \in \mathfrak{H}).$$

We shall now define a mapping $\theta : \mathfrak{H} \to \mathfrak{H}$ in the following manner. Let p, q be $\geqq 0$; consider the mapping

$$(u\otimes v)\to\sum_{s\in\mathfrak{G}}(u\otimes\bar{s})\otimes((s-e)\otimes v)=u\otimes\Big(\sum_{s\in\mathfrak{G}}\bar{s}\otimes(s-e)\Big)\otimes v$$

(where $\bar{s}$ is the residue class of s modulo $Z\sigma$) of $J_p\otimes I_q$ into $J_{p+1}\otimes I_{q+1}$. This mapping is obviously bi-additive. As such it defines an additive mapping ${}^{p,q}\theta$: ${}^{p,q}\boxplus\to{}^{p+1,q+1}\boxplus$. We define θ to be the additive mapping which extends all ${}^{p,q}\theta$. This mapping θ is actually a homomorphism. For we have, if $t\in\mathfrak{G}$,

$$t\sum_{s\in\mathfrak{G}}\bar{s}\otimes(s-e)=\sum_{s\in\mathfrak{G}}\overline{ts}\otimes(ts-t)=\sum_{s\in\mathfrak{G}}\overline{ts}\otimes(ts-e)$$

as follows from the fact that $\sum_{s\in\mathfrak{G}}\overline{ts}=0$. It follows immediately that $\sum_{s\in\mathfrak{G}}\bar{s}\otimes(s-e)$ is $\mathfrak{G}$-invariant, and therefore that θ is a homomorphism.

We shall now define a mapping ${}^{p,q}S$ of ${}^{p+1,q+1}\boxplus$ into ${}^{p,q}\boxplus$, the *trace mapping*. The group $Z\otimes Z$ has a base composed of the elements $s\otimes t$, $s,t\in\mathfrak{G}$; let φ be the additive mapping of $Z\otimes Z$ into $\mathbf{Z}$ defined by $\varphi(s\otimes t)=0$ if $s\neq t$, $\varphi(s\otimes s)=1$. Then φ is obviously $\mathfrak{G}$-linear. We have $\varphi(\sigma\otimes s)=1$ for every $s\in\mathfrak{G}$, whence $\varphi(\sigma\otimes y)=0$ for every $y\in I$. It follows immediately that φ defines a linear mapping

$${}^{0,0}S: J\otimes I\to\mathbf{Z};$$

indeed we have seen in §2 that $\mathrm{Add}(I,\mathbf{Z})\cong J$ and $\mathrm{Add}(J,\mathbf{Z})\cong I$. We may write ${}^{p+1,q+1}\boxplus=J_p\otimes(J\otimes I)\otimes I_q$; then it is clear that there exists a $\mathfrak{G}$-linear map ${}^{p,q}S$: ${}^{p+1,q+1}\boxplus\to{}^{p,q}\boxplus$ such that

$${}^{p,q}S(u\otimes(x\otimes y)\otimes v)={}^{0,0}S(x\otimes y)\cdot u\otimes v$$

if $u\in J_p$, $x\in J$, $y\in I$, $v\in I_q$. This is the trace mapping.

Let n be the order of $\mathfrak{G}$. Then it follows immediately from the definitions that

$$\boxed{{}^{p,q}S(\theta(w))=(n-1)w}$$

for every $w\in{}^{p,q}\boxplus$.

For any $p\geqq 0$, we denote by Π_p the group of permutations of the set $\{1,\dots,p\}$. Let ϖ be in Π_p and ϖ' in Π_q; then there exists an automorphism $\omega(\varpi,\varpi')$ of ${}^{p,q}\boxplus$ which maps $x(1)\otimes\cdots\otimes x(p)\otimes y(1)\otimes\cdots\otimes y(q)$ upon $x(\varpi^{-1}(1))\otimes\cdots\otimes x(\varpi^{-1}(p))\otimes y(\varpi'^{-1}(1))\otimes\cdots\otimes y(\varpi'^{-1}(q))$ whenever $x(i)\in J$ $(1\leqq i\leqq p)$, $y(j)\in I$ $(1\leqq j\leqq q)$. It is clear that $\omega(\varpi_1\varpi_2,\varpi_1'\varpi_2')=\omega(\varpi_1,\varpi_1')\,\omega(\varpi_2,\varpi_2')$ if $\varpi_i\in\Pi_p$, $\varpi_i'\in\Pi_q$, $i=1,2$.

Let u be in J_p and v in I_q, u' in $J_{p'}$, v' in $I_{q'}$. Then

$$\theta((u \otimes v) \square (u' \otimes v')) = \sum_{s \in \mathfrak{G}} (u \otimes u' \otimes \bar{s}) \otimes ((s-e) \otimes v \otimes v')$$
$$(u \otimes v) \square \theta(u' \otimes v') = \sum_{s \in \mathfrak{G}} (u \otimes u' \otimes \bar{s}) \otimes (v \otimes (s-e) \otimes v')$$
$$\theta(u \otimes v) \square (u' \otimes v') = \sum_{s \in \mathfrak{G}} (u \otimes \bar{s} \otimes u') \otimes ((s-e) \otimes v \otimes v').$$

It follows that, for $w \in {}^{p,q}\boxplus$, $w' \in {}^{p',q'}\boxplus$, we have

$$\theta(w \square w') = \omega(1, \pi'_{q+1})\, w \square \theta(w') = \omega(\pi_{p'+1}, 1)\, \theta(w) \square w'$$

where 1 is the unit permutation, π'_{q+1} is an element of $\Pi_{q+q'+1}$ which permutes cyclically the first $q+1$ indices and leaves the last q' fixed, while $\pi_{p'+1}$ is an element of $\Pi_{p+p'+1}$ which leaves the first p indices fixed and permutes cyclically the last $p'+1$ indices.

§4. THE MODULE 早(A)

Let $\mathfrak{G}$ be a finite group and A a $\mathfrak{G}$-module. We set

$$\text{早}(A) = \text{田} \otimes A \qquad {}^{p,q}\text{早}(A) = {}^{p,q}\text{田} \otimes A$$

whence $\text{早}(A) = \sum_{p,q \geqq 0} {}^{p,q}\text{早}(A)$ (direct).

Then 早(A) is a $\mathfrak{G}$-module. Moreover, since 田 has a structure of algebra, 早(A) has a structure of 田-module, whose external law of composition is defined by

$$w \square (w' \otimes a) = (w \square w') \otimes a \quad (w,\ w' \in \text{田},\ a \in A).$$

It is clear that

$$s(w \square u) = sw \square su \quad (w \in \text{田},\ u \in \text{早}(A)).$$

If λ is any $\mathfrak{G}$-linear mapping of ^{p,q}田 into ${}^{p',q'}$田, then there is a $\mathfrak{G}$-linear mapping λ_A of ^{p,q}早(A) into ${}^{p',q'}$早(A) such that

$$\lambda_A(w \otimes a) = \lambda(w) \otimes a \quad (w \in {}^{p,q}\text{田},\ a \in A).$$

Thus, to ${}^{p,q}\theta$, ${}^{p,q}S$, there correspond $\mathfrak{G}$-linear maps

$${}^{p,q}\theta_A :\ {}^{p,q}\text{早}(A) \to {}^{p+1,q+1}\text{早}(A);\quad {}^{p,q}S_A :\ {}^{p+1,q+1}\text{早}(A) \to {}^{p,q}\text{早}(A)$$

such that

$${}^{p,q}S_A({}^{p,q}\theta_A(u)) = (n-1)u \quad (u \in {}^{p,q}\text{早}(A))$$

if n is the order of $\mathfrak{G}$. Moreover, if Π_p is the permutation group of the set $\{1, \ldots, p\}$, then we have a representation $(\varpi, \varpi') \to \omega_A(\varpi, \varpi')$ of $\Pi_p \times \Pi_q$ by $\mathfrak{G}$-linear automorphisms of ^{p,q}早(A).

Let M be any $\mathfrak{G}$-module. For any $m \in M$, set

$$\Delta(m) = \sum_{s \in \mathfrak{G}} \bar{s} \otimes sm \in J \otimes M.$$

Then Δ is an additive (but not $\mathfrak{G}$-linear) map of M into $J \otimes M$.

LEMMA 4.1. *If M is a $\mathfrak{G}$-module, and $\sum_{s \in \mathfrak{G}} \bar{s} \otimes m(s) = x$ an element of $J \otimes M$, then a necessary and sufficient condition for x to be 0 is that $m(s) = m(e)$ for all $s \in \mathfrak{G}$.*

Since $\sum_{s\in\mathfrak{G}}\bar{s}=0$, we may write $x=\sum_{s\neq e}\bar{s}\otimes(m(s)-m(e))$, and lemma 4.1 follows from the fact that the element $\bar{s}$, $s\neq e$, *form a base of* J.

It follows that the kernel of Δ is the set $M^{\mathfrak{G}}$ of invariant element of M. On the other hand, we have $\Delta(m)=\sigma(\bar{e}\otimes m)$, whence $\Delta(M)\subset\sigma(J\otimes M)$. Conversely, if $s\in\mathfrak{G}$ and $m\in M$, then $\sigma(\bar{s}\otimes m)=\sigma s^{-1}(\bar{s}\otimes m)=\sigma(\bar{e}\otimes s^{-1}m)=\Delta(s^{-1}m)$; it follows that $\Delta(M)=\sigma(J\otimes M)$.

We apply this to the case where $M=\text{早}(A)$. Then

$$J\otimes M=\sum_{p,q\geqq 0}J\otimes J_p\otimes J_q\otimes A=\sum_{p,q\geqq 0}J_{p+1}\otimes I_q\otimes A\subset\text{早}(A)$$

and Δ gives rise to an additive mapping d_A: $\text{早}(A)\to\text{早}(A)$. It is clear that $d_A({}^{p,q}\text{早}(A))=\sigma({}^{p-1,q}\text{早}(A))$ and that the kernel of d_A is $(\text{早}(A))^{\mathfrak{G}}$. Since $(\text{早}(A))^{\mathfrak{G}}$ contains $\sigma(\text{早}(A))$, we have $d_A^2=0$. If $w\in\text{田}$, $a\in A$, then

$$d_A(w\otimes a)=\sum_{s\in\mathfrak{G}}(\bar{s}\,\square\,sw)\otimes sa.$$

It follows immediately that

$$d_A(\theta_A(u))=\theta_A(d_Au)\qquad u\in{}^{p,q}\text{早}(A)\tag{4.1}$$

$$d_A({}^{p,q}S_A(u))={}^{p+1,q}S_A(d_Au)\qquad u\in{}^{p+1,q+1}\text{早}(A)\tag{4.2}$$

$$d_A(\omega_A(\tilde{\omega},\tilde{\omega}')u)=\omega_A(1\cup\tilde{\omega},\tilde{\omega}')d_Au\quad(\tilde{\omega}\in\Pi_p,\ \tilde{\omega}'\in\Pi_q)\tag{4.3}$$

where $1\cup\tilde{\omega}$ is the permutation of $\{1,\ldots,p+1\}$ which leaves 1 fixed and maps $i+1$ upon $\tilde{\omega}(i)+1$ $(i=1,\ldots,p)$.

Let f be a homomorphism of A into a $\mathfrak{G}$-module B. Then there is a homomorphism of the $\mathfrak{G}$-module $\text{早}(A)$ into $\text{早}(B)$ which maps $w\otimes a$ upon $w\otimes f(a)$ for any $w\in\text{田}$. We shall denote this homomorphism by $\hat{f}$. It is clear that it is also a homomorphism for the structures of 田-modules of $\text{早}(A)$ and $\text{早}(B)$. It follows immediately from the definitions that

$$\begin{cases}\hat{f}\circ\theta_A=\theta_B\circ\hat{f}\quad \hat{f}\circ{}^{p,q}S_A={}^{p,q}S_B\circ\hat{f}\quad \hat{f}\circ\omega_A(\tilde{\omega},\tilde{\omega}')=\omega_B(\tilde{\omega},\tilde{\omega}')\circ\hat{f}\\ \hat{f}\circ d_A=d_B\circ\hat{f}.\end{cases}\tag{4.4}$$

If g is a homomorphism of B into a third $\mathfrak{G}$-module C, then

$$\widehat{g\circ f}=\hat{g}\circ\hat{f}.$$

THEOREM 4.1. *Let* $0\longrightarrow A\xrightarrow{f}B\xrightarrow{g}C\longrightarrow 0$ *be an exact sequence of homomorphisms of* $\mathfrak{G}$*-modules. Then the sequence*

$$0\longrightarrow\text{早}(A)\xrightarrow{\hat{f}}\text{早}(B)\xrightarrow{\hat{g}}\text{早}(C)\longrightarrow 0$$

is exact.

Since J and I are free additive groups, the same is true of J_p, of I_q, of $J_p \otimes I_q$ and finally of 田. Theorem 4.1 then follows from a well known property of tensor products.

Let A and B be $\mathfrak{G}$-modules. There is an isomorphism j of

$$早(A) \otimes 早(B) = (田 \otimes A) \otimes (田 \otimes B)$$

with $(田 \otimes 田) \otimes (A \otimes B)$ which maps $(w \otimes a) \otimes (w' \otimes b)$ upon $(w \otimes w') \otimes (a \otimes b)$ if $w, w' \in 田$, $a \in A$, $b \in B$. On the other hand, the multiplication μ in 田 defines a homomorphism of $田 \otimes 田$ into 田, which maps $w \otimes w'$ upon $w \square w'$. This gives rise to a homomorphism $\mu_{1 \otimes B}$: $(田 \otimes 田) \otimes (A \otimes B) \to 早(A \otimes B)$ which maps $(w \otimes w') \otimes (a \otimes b)$ npon $(w \square w') \otimes (a \otimes b)$. We set

$$M_{A,B} = \mu_{1 \otimes B} \circ j$$

this is a homomorphism of $早(A) \otimes 早(B)$ into $早(A \otimes B)$, and it is clear that

$$M_{A,L}({}^{p,q}早(A) \otimes {}^{p',q'}早(B)) = {}^{p+p',q+q'}早(A \otimes B).$$

Let x be in ${}^{p,q}早(A)$, y in ${}^{p',q'}早(B)$. Then it follows from the formulas established in §3 that

$$\theta_{A \otimes B}(M_{A,B}(x \otimes y)) = \omega_{A \otimes B}(1, \pi'_{q+1}) M_{A,B}(x \otimes \theta_B(y)) \tag{4.5}$$
$$= \omega_{A \otimes B}(\pi_{p'+1}, 1) M_{A,B}(\theta_A(x) \otimes y)$$

where $\pi_{p'+1} \in \Pi_{p+p'+1}$, leaves the first p indices fixed and permutes cyclically the last $p'+1$, while $\pi'_{q+1} \in \Pi_{q+q'+1}$, permutes cyclically the first $q+1$ indices and leaves the others fixed.

If $\varpi \in \Pi_r$, $\varpi_1 \in \Pi_s$, we denote by $\varpi \cup \varpi_1$ the element of Π_{r+s} which coincides with ϖ on $\{1, \ldots, r\}$ and which maps $r+i$ upon $r+\varpi_1(i)$ $(1 \leqq i \leqq s)$. Then it is clear that

$$M_{A,B}(\omega_A(\varpi, \varpi') x \otimes \omega_B(\varpi_1, \varpi'_1) y)$$
$$= \omega_{A \otimes B}(\varpi \cup \varpi_1, \varpi' \cup \varpi'_1) M_{A,B}(x \otimes y)$$

if $\varpi \in \Pi_p$, $\varpi' \in \Pi_q$, $\varpi_1 \in \Pi_{p'}$, $\varpi'_1 \in \Pi_q$.

Theorem 4.2. *Let x be any element of* $早(A)$ *and y an invariant element of* $早(B)$. *Then we have*

$$d_{A \otimes B} M_{A,B}(x \otimes y) = M_{A,B}(d_A x \otimes y). \tag{4.6}$$

It will be sufficient to consider the case where x is of the form $w \otimes a$ $w \in \text{田}$, $a \in A$; set $y = \sum_{i-1}^{h} w_i' \otimes b_i$, $w_i' \in \text{田}$, $b_i \in B$. Then $d_{A \otimes B} M_{A,B}(x \otimes y)$ $= \sum_{s \in \mathfrak{G}} \sum_{i=1}^{h} (\bar{s} \square sw \square sw_i) \otimes (sa \otimes sb_i)$. But we have by assumption

$$\sum_{i=1}^{h} sw_i' \otimes sb_i = \sum_{i=1}^{h} w_i' \otimes b_i$$

whence $\sum_{i=1}^{h} (\bar{s} \square sw \square sw_i') \otimes sb_i = \sum_{i-1}^{h} (\bar{s} \square sw \square w_i') \otimes b_i$. It follows immediately that

$$d_{A \otimes B} M_{A,B}(x \otimes y) = \sum_{s \in \mathfrak{G}} \sum_{i=1}^{h} (\bar{s} \square sw \square w_i') \otimes (sa \otimes b_i) = M_{A,P}(d_A x \otimes y).$$

Now, let u and v be homomorphisms of A and B into $\mathfrak{G}$-modules A' and B' respectively. Then it follows immediately from the definitions that

$$M_{A', B'} \circ (\hat{u} \otimes \hat{v}) = \widehat{u \otimes v} \circ M_{A,B}. \tag{4.7}$$

Let A, B, C be $\mathfrak{G}$-modules. Then we have, if $x \in \text{早}(A)$, $y \in \text{早}(B)$, $z \in \text{早}(C)$,

$$M_{A \otimes B, C}(M_{A,B}(x \otimes y), z) = M_{A, B \otimes C}(x, M_{B,C}(y \otimes z)) \tag{4.8}$$

as one verifies immediately by considering the case where $x = u \otimes a$, $y = v \otimes b$, $z = w \otimes c$, $u, v, w \in \text{田}$, $a \in A$, $b \in B$, $c \in C$.

§5. THE COHOMOLOGY GROUPS

Let $\mathfrak{G}$ be a finite group and A a $\mathfrak{G}$-module. Then we set

$$H'(A) = \mathfrak{N}(\mathfrak{G}\,;\,\text{早}(A)) \qquad {}^{p,q}H(A) = \mathfrak{N}(\mathfrak{G}\,;\,{}^{p,q}\text{早}(A)),$$

whence

$$H'(A) = \sum_{p,q \geqq 0} {}^{p,q}H(A) \quad \text{(direct)}.$$

The group ${}^{p,q}H(A)$ is called the *cohomology group of type* (p, q) *of* A.

Let p be >0; then $({}^{p,q}\text{早}(A))^{\mathfrak{G}}$ is the kernel of the mapping induced by d_A on ${}^{p,q}\text{早}(A)$, while $\sigma({}^{p,q}\text{早}(A))$ is the image of the restriction of d_A to ${}^{p-1,q}\text{早}(A)$. Thus, if we denote by ${}^{p,q}\mathfrak{z}$ the kernel of d_A in ${}^{p,q}\text{早}(A)$,

$${}^{p,q}H(A) = {}^{p,q}\mathfrak{z}_A / d_A({}^{p-1,q}\text{早}(A)) \quad (p>0)$$

THEOREM 5.1. *If n is the order of the group $\mathfrak{G}$, then we have $n\zeta = 0$ for every $\zeta \in H'(A)$.*

For, if $u \in (\text{早}(A))^{\mathfrak{G}}$, then $nu = \sigma u \in \sigma\text{早}(A)$.

THEOREM 5.2. *Let the $\mathfrak{G}$-module A be the direct sum $\sum_{i\in I} A_i$ of a family $(A_i)_{i\in I}$ of submodules. Then we have, for every $p \geqq 0$, $q \geqq 0$,*

$${}^{p,q}H(A) \cong \sum_{i\in I} {}^{p,q}H(A_i).$$

For we have $\text{早}(A) = \text{田} \otimes \sum_{i\in I} A_i = \sum_{i\in I} \text{田} \otimes A_i$ (direct); it is clear that $(\text{早}(A))^{\mathfrak{G}} = \sum_{i\in I} (\text{早}(A_i))^{\mathfrak{G}}$, $\sigma\text{早}(A) = \sum_{i\in I} \sigma\text{早}(A_i)$, which proves the theorem.

THEOREM 5.3. *If A is a finitely generated $\mathfrak{G}$-module, then each ${}^{p,q}H(A)$ is a finite group.*

If $\{a_1, \ldots, a_h\}$ is a set of generators of A as a $\mathfrak{G}$-module, then the elements sa_i, $s \in \mathfrak{G}$, $1 \leqq i \leqq h$ form a set of generators of A as an additive group. Since ${}^{p,q}\text{田}$ has a finite base (as an additive group), ${}^{p,q}\text{早}(A)$ is a finitely generated additive group; so is every subgroup of ${}^{p,q}\text{早}(A)$, and, in particular, $({}^{p,q}\text{早}(A))^{\mathfrak{G}}$. It follows immediately that ${}^{p,q}H(A)$ is finitely generated; making use of theorem 5.1, we conclude that ${}^{p,q}H(A)$ is finite.

THEOREM 5.4. *Let n be the order of $\mathfrak{G}$. Let A be a $\mathfrak{G}$-module which satisfies either one of the following conditions: a) for every $a \in A$, there is a unique $a' \in A$ such that $na' = a$; b) A splits. Then $H'(A) = \{0\}$.*

Assume first that condition a) is satisfied. Since 田 is a free additive group, we may conclude that, for every $u \in$ 早(A), there is a unique $u' \in$ 早(A) such that $nu' = u$. If $u \in ($早$(A))^{\mathfrak{G}}$, then $n(su' - u') = 0$ for $s \in \mathfrak{G}$, whence $su' = u'$, and therefore $u = \sigma u'$; this proves that $H'(A) = \{0\}$. If A splits, then so does 早$(A) =$ 田 $\otimes A$, whence $H'(A) = \mathfrak{N}(\mathfrak{G},$ 早$(A)) = \{0\}$.

Let p, q be $\geqq 0$. Then the mappings ${}^{p,q}\theta_A$, ${}^{p,q}S_A$, $\omega_A(\varpi, \varpi')$ (where $\varpi \in \Pi_p$, $\varpi' \in \Pi_q$) gives rise to mappings

$$
\begin{aligned}
{}^{p,q}\theta_A^{\mathfrak{N}} &: {}^{p,q}H(A) \to {}^{p+1,q+1}H(A) \\
{}^{p,q}S_A^{\mathfrak{N}} &: {}^{p+1,q+1}H(A) \to {}^{p,q}H(A) \\
\omega_A^{\mathfrak{N}}(\varpi, \varpi') &: {}^{p,q}H(A) \to {}^{p,q}H(A).
\end{aligned}
$$

From the formula $(S_A \circ \theta_A)(u) = (n-1)u$, $u \in {}^{p,q}$早(A) and from theorem 5.1, it follows immediately that

$$({}^{p,q}S_A^{\mathfrak{N}} \circ {}^{p,q}\theta_A^{\mathfrak{N}})(\zeta) = -\zeta$$

for $\zeta \in {}^{p,q}H(A)$, which proves that ${}^{p,q}\theta_A^{\mathfrak{N}}$ is a monomorphism. We shall see a little later that it is actually an isomorphism.

Let f be a homomorphism of A into a $\mathfrak{G}$-module B. Then $\hat{f}$ is a homomorphism of 早(A) into 早(B), and $\hat{f}^{\mathfrak{N}}$ is an additive mapping of $H'(A)$ into $H'(B)$. *We shall denote this mapping by f^*.* It is clear that

$$f^*({}^{p,q}H(A)) \subset {}^{p,q}H(B).$$

If g is a homomorphism of B into a third $\mathfrak{G}$-module C, then

$$(g \circ f)^* = g^* \circ f^*.$$

Now, let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of homomorphisms of $\mathfrak{G}$ modules. Then we shall associate to this exact sequence an additive mapping δ of $H'(C)$ into $H'(A)$. Let z be in $($早$(C))^{\mathfrak{G}}$; since $\hat{g}$ is an epimorphism, there is a $y \in$ 早(B) such that $\hat{g}(y)$

$= z$. We have $\hat{g}(d_B y) = d_C z = 0$ since $z \in (\mathfrak{F}(C))^{\mathfrak{G}}$. Since the kernel of $\hat{g}$ is the image of $\hat{f}$, we may write $d_B y = \hat{f}(x)$, $x \in \mathfrak{F}(A)$. We have $\hat{f}(d_A x) = d_B^2 y = 0$, whence $d_A x = 0$ since $\hat{f}$ is a monomorphism, and $x \in (\mathfrak{F}(A))^{\mathfrak{G}}$. Let ξ be the class of x in $H'(A)$; then we shall see that ξ depends only on the class ζ of z in $H'(C)$. Let z' be an element of $(\mathfrak{F}(C))^{\mathfrak{G}}$ such that $z' - z \in \sigma(\mathfrak{F}(C))$, and let y' be an element of $\mathfrak{F}(B)$ shch that $\hat{g}(y') = z'$. Set $z' - z = \sigma w$, $w \in \mathfrak{F}(C)$, and let $v \in \mathfrak{F}(B)$ be such that $\hat{g}(v) = w$. Then $\hat{g}(\sigma v) = \sigma w$, and $\hat{g}(y' - y - \sigma v) = 0$. It follows that $y' - y - \sigma v = \hat{f}(u)$, with some $u \in \mathfrak{F}(A)$. Since σv is $\mathfrak{G}$-invariant, $d_B(\sigma v) = 0$, and $d_B y' = d_B y + d_B \hat{f}(u) = \hat{f}(x + d_A u)$. Since $d_A u \in \sigma\mathfrak{F}(A)$, our assertion is proved. Set $\xi = \delta(\zeta)$; then δ is obviously an additive mapping of $H'(C)$ into $H'(A)$, which maps ${}^{p,q}H(C)$ into ${}^{p+1,q}H(A)$.

We shall see that, for any $p \geqq 0$, $q \geqq 0$, the sequence

$${}^{p,q}H(A) \xrightarrow{f^*} {}^{p,q}H(B) \xrightarrow{g^*} {}^{p,q}H(C) \xrightarrow{\delta} {}^{p+1,q}H(A) \xrightarrow{f} {}^{p+1,q}H(B)$$

is exact.

Since $g \circ f = 0$, we have $g^* \circ f^* = 0$. Let conversely η be in the kernel of g^* and let y be a representative of η in $(\mathfrak{F}(B))^{\mathfrak{G}}$. Then $\hat{g}(y) = \sigma w$ with some $w \in \mathfrak{F}(C)$; writing w in the form $\hat{g}(v)$ for some v in $\mathfrak{F}(B)$, we have $\hat{g}(y - \sigma v) = 0$, and $y - \sigma v$, which is a representative of η, may be written in the form $\hat{f}(x)$, $x \in \mathfrak{F}(A)$. Since $\hat{f}$ is a monomorphism and $\hat{f}(x)$ is $\mathfrak{G}$-invariant, x is itself $\mathfrak{G}$-invariant, whence $\eta \in f^*(H'(A))$.

Let now z be in $(\mathfrak{F}(C))^{\mathfrak{G}}$, and let us use the same notation as above in the definition of δ. If $\zeta \in g^*(H'(B))$, then we may assume that $z = \hat{g}(y)$ with some $y \in (\mathfrak{F}(B))^{\mathfrak{G}}$; we then have $d_B y = 0$, $x = 0$, whence $\delta \circ g^* = 0$. Assume conversely that $\delta(\zeta) = 0$. Then we may write $x = \sigma x'$, with some $x' \in {}^{p+1,q}\mathfrak{F}(A)$, whence $x = d_A x''$ with some $x'' \in {}^{p,q}\mathfrak{F}(A)$. We have $d_B y = \hat{f}(d_A x'') = d_B(\hat{f}(x''))$, and therefore $y - \hat{f}(x'') \in (\mathfrak{F}(B))^{\mathfrak{G}}$. Since $\hat{g}(y - \hat{f}(x'')) = \hat{g}(y) = z$, we have $\zeta \in g^*({}^{p,q}H(A))$.

Still using the same notation as above, we see that $\hat{f}(x) \in d_B({}^{p,q}\mathfrak{F}(B)) = \sigma({}^{p+1,q}\mathfrak{F}(B))$, whence $f^* \circ \delta = 0$. Let conversely $\xi \in {}^{p+1,q}H(A)$ belong to the kerenel of f^*, and let x' be a representative for ξ. Then $\hat{f}(x') \in \sigma({}^{p+1,q}\mathfrak{F}(B)) = d_B({}^{p,q}\mathfrak{F}(B))$; write $\hat{f}(x') = d_B y'$, $y' \in {}^{p,q}\mathfrak{F}(B)$. We have $d_C \hat{g}(y') = \hat{g}(\hat{f}(x')) = 0$, whence $\hat{g}(y') = z' \in (\mathfrak{F}(C))^{\mathfrak{G}}$. If ζ is the class of z' in ${}^{p,q}H(C)$, it is clear that $\xi = \delta\zeta$. Our assertion is thereby proved.

THEOREM 5.5. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & {\scriptstyle u}\downarrow & & {\scriptstyle v}\downarrow & & {\scriptstyle w}\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of homomorphisms of $\mathfrak{G}$*-modules, and let* p, q *be integers* $\geqq 0$. *Assume that the two horizontal lines of our diagram are exact, and let* δ, δ' *be two mappings* ${}^{p,q}H(C) \to {}^{p+1,q}H(A)$, ${}^{p,q}H(C') \to {}^{p+1,q}H(A')$ *associated to our exact sequences. Then the diagram*

$$\begin{array}{ccccccccc} {}^{p,q}H(A) & \xrightarrow{f^*} & {}^{p,q}H(B) & \xrightarrow{g^*} & {}^{p,q}H(C) & \xrightarrow{\delta} & {}^{p+1,q}H(A) & \xrightarrow{f^*} & \\ {\scriptstyle u^*}\downarrow & & {\scriptstyle v^*}\downarrow & & {\scriptstyle w^*}\downarrow & & {\scriptstyle u^*}\downarrow & & \\ {}^{p,q}H(A') & \xrightarrow{f'^*} & {}^{p,q}H(B') & \xrightarrow{g'^*} & {}^{p,q}H(C') & \xrightarrow{\delta'} & {}^{p+1,q}H(A') & \xrightarrow{f'^*} & \end{array}$$

$$\begin{array}{ccccc} \xrightarrow{f^*} & {}^{p+1,q}H(B) & \xrightarrow{g^*} & {}^{p+1,q}H(C) \\ & {\scriptstyle v^*}\downarrow & & {\scriptstyle w^*}\downarrow \\ \xrightarrow{f'^*} & {}^{p+1,q}H(B') & \xrightarrow{g'^*} & {}^{p+1,q}H(C') \end{array}$$

is commutative and its lines are exact.

We know already that the horizontal lines of this diagram are exact, and that $v^* \circ f^* = (v \circ f)^* = (f' \circ u)^* = f'^* \circ u^*$, $w^* \circ g^* = g'^* \circ v^*$. It remains only to prove that $u^* \circ \delta = \delta' \circ w^*$. Let ζ be in ${}^{p,q}H(C)$, and z a representative of ζ in $(\text{早}(C))^{\mathfrak{G}}$. Write $z = \hat{g}(y)$, $y \in \text{早}(B)$, $d_B y = \hat{f}(x)$, $x \in (\text{早}(A))^{\mathfrak{G}}$, whence $x \in \delta(\zeta)$, $\hat{u}(x) \in (u^* \circ \delta)(\zeta)$. Set $z' = \hat{w}(z)$, $y' = \hat{v}(y)$; then $\hat{g}'(y') = z'$, $d_{B'} y' = \hat{v}(d_B y) = (\hat{v} \circ \hat{f})(x) = \hat{f}'(\hat{u}(x))$, whence $\hat{u}(x) \in \delta'(w^*(\zeta))$, which proves the theorem.

COROLLARY 1. *Let* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *be an exact sequence of homomorphisms of* $\mathfrak{G}$*-modules, and let* p, q *be integers* $\geqq 0$. *If* ${}^{p,q}H(A) = {}^{p+1,q}H(A) = \{0\}$, *then* g^* *induces an isomorphism of* ${}^{p,q}H(B)$ *with* ${}^{p,q}H(C)$. *If* ${}^{p,q}H(B) = {}^{p+1,q}H(B) = \{0\}$, *then* δ *induces an isomorphism of* ${}^{p,q}H(C)$ *with* ${}^{p+1,q}H(A)$. *If* ${}^{p,q}H(C) = {}^{p+1,q}H(C) = \{0\}$, *then* f^* *induces an isomorphism of* ${}^{p+1,q}H(A)$ *with* ${}^{p+1,q}H(B)$.

This follows immediately from the fact that the lines of our diagram are exact sequences.

COROLLARY 2. *Let* $\mathbf{R}$ *be the additive group of real numbers, and* $\mathbf{R}^* = \mathbf{R}/\mathbf{Z}$.

Considering $\mathbf{R}$ *and* $\mathbf{R}^*$ *as* $\mathfrak{G}$*-modules on which* $\mathfrak{G}$*-operates trivially, the exact sequence* $0 \to \mathbf{Z} \to \mathbf{R} \to \mathbf{R}^* \to 0$ *defines an isomorphism* $\delta : {}^{p,q}H(\mathbf{R}^*) \cong {}^{p+1,q}H(\mathbf{Z})$.

This follows from our cor. 1 since $H'(\mathbf{R}) = \{0\}$ by theorem 5.4.

The $\mathfrak{G}$-modules $I = I[\mathfrak{G}]$ and $J = J[\mathfrak{G}]$ were introduced in §2. We have the exact sequences

$$0 \to I \to Z \to \mathbf{Z} \to 0$$
$$0 \to \mathbf{Z} \to Z \to J \to 0$$

of $\mathfrak{G}$-homomorphisms. Since Z, I, J, $\mathbf{Z}$ are free additive groups, we have exact sequences

$$0 \to I \otimes A \to Z \otimes A \to A \to 0; \; 0 \to A \to Z \otimes A \to J \otimes A \to 0$$

(where A is $\mathfrak{G}$-module). The module Z splits; the same is therefore true of $Z \otimes A$, whence $H'(Z \otimes A) = \{0\}$. Thus, the mapping δ associated to the first one of our exact sequences induces (for every $p \geqq 0$, $q \geqq 0$) an isomorphism $\delta : {}^{p,q}H(A) \to {}^{p+1,q}H(I \otimes A)$. But we have ${}^{p+1,q}\text{早}(I \otimes A) = J_{p+1} \otimes I_q \otimes I \otimes A = {}^{p+1,q+1}\text{早}(A)$, whence ${}^{p+1,q}H(I \otimes A) = {}^{p+1,q+1}H(A)$, and δ induces an isomorphism

$${}^{p,q}\delta : {}^{p,q}H(A) \to {}^{p+1,q+1}H(A).$$

On the other hand, ${}^{p,q}\theta_A^{\mathfrak{N}}$ is also an additive mapping of ${}^{p,q}H(A)$ into ${}^{p+1,q+1}H(A)$; we shall compare it to ${}^{p,q}\delta$. Let $x \in ({}^{p,q}\text{早}(A))^{\mathfrak{G}}$, and let f, g be the mappings of the exact sequence $0 \longrightarrow I \otimes A \xrightarrow{f} Z \otimes A \xrightarrow{g} A \longrightarrow 0$. Set $x = \sum_{i=1}^{h} w_i \otimes a_i$, $w_i \in {}^{p,q}\text{田}$, $a_i \in A$; then we have $x = \hat{g}(y)$, $y = \sum_{i=1}^{h} w_i \otimes (e \otimes a_i)$ and

$$d_B y = \sum_{s \in \mathfrak{G}} \sum_{i=1}^{h} \bar{s} \otimes s w_i \otimes s \otimes s a_i, \quad (B = Z \otimes A).$$

Write $w_i = \sum_{j=1}^{k} u_{ij} \otimes v_{ij}$, $u_{ij} \in J_p$, $v_{ij} \in I_q$. Denote by ϖ the permutation of $\{1, \ldots, p+1\}$ which transforms $p+1$ into 1 and i into $1+i$ $(1 \leqq i \leqq p)$, and by ϖ' the permutation of $\{1, \ldots, q+1\}$ which transforms 1 into $q+1$ and $1+j$ into j $(1 \leqq j \leqq q)$. Then we have $\bar{s} \otimes u_{ij} \otimes v_{ij} \otimes s = \omega(\varpi, \varpi') \cdot u_{ij} \otimes \bar{s} \otimes s \otimes v_{ij}$. Then

$$d_B y = \hat{f}(\omega_A(\varpi, \varpi')(\theta_A(\sum_{i=1}^{h} w_i \otimes a_i)))$$

and

$${}^{p,q}\delta = \omega_A^{\mathfrak{N}}(\varpi, \varpi') \circ {}^{p,q}\theta_A^{\mathfrak{N}}.$$

THEOREM 5.6. *For any* $p \geqq 0$, $q \geqq 0$, ${}^{p,q}\theta_A^{\mathfrak{R}}$ *is an isomorphism of* ${}^{p,q}H(A)$ *with* ${}^{p+1,q+1}H(A)$, and ${}^{p,q}S_A^{\mathfrak{R}}$ *is an isomorphism of* ${}^{p+1,q+1}H(A)$ *with* ${}^{p,q}H(A)$.

The first assertion follows from the formula we have derived just above and from the fact that $\omega_A(\varpi, \varpi')$ is an automorphism. The second assertion follows from the first and from the formula $({}^{p,q}S_1^{\mathfrak{R}} \circ {}^{p,q}\theta_1^{\mathfrak{R}})(\zeta) = -\zeta$.

Now we prove

THEOREM 5.7. *Let* p, q *be integers* $\geqq 0$, ϖ *a permutation of* $\{1, \ldots, p\}$ *and* ϖ' *a permutation of* $\{1, \ldots, q\}$. *Let* $\varepsilon(\varpi)$, $\varepsilon(\varpi')$ *be the signatures of these permutations. Then we have* $\omega_1^{\mathfrak{R}}(\varpi, \varpi')\xi = \varepsilon(\varpi)\varepsilon(\varpi')\xi$ *for any* $\xi \in {}^{p,q}H(A)$.

Let x be in $({}^{p,q}\text{早}(A))^{\mathfrak{G}}$; denote by $\varpi \cup 1$ the permutation of $\{1, \ldots, p+2\}$ which extends ϖ and which leaves $p+1$, $p+2$ fixed, and by $1 \cup \varpi'$ the permutation of $\{1, \ldots, q+2\}$ which leaves 1, 2 fixed and maps $2+j$ upon $2+\varpi'(j)$ $(1 \leqq j \leqq q)$. Then it is clear that

$$({}^{p+1,q+1}\theta_A \circ {}^{p,q}\theta_A)(\omega_A(\varpi, \varpi')x) = \omega_A(\varpi \cup 1, 1 \cup \varpi')^{p+1,q+1}\theta_A \circ {}^{p,q}\theta_A(x)$$

and that $\varpi \cup 1$ has the same signature as ϖ, while $1 \cup \varpi'$ has the same signature as ϖ'. Since ${}^{p+1,q+1}\theta_A^{\mathfrak{R}} \circ {}^{p,q}\theta_A^{\mathfrak{R}}$ is an isomorphism of ${}^{p,q}H(A)$ with ${}^{p+2,q+2}H(A)$, we see that it will be sufficient to prove the theorem under the assumption that $p \geqq 2$, $q \geqq 2$. Let Π_p and Π_q be the permutation groups of $\{1, \ldots, p\}$ and $\{1, \ldots, q\}$. Then we know that $(\varpi, \varpi') \to \omega_A^{\mathfrak{R}}(\varpi, \varpi')$ is a representation of $\Pi_p \times \Pi_q$ by automorphisms of ${}^{p,q}H(A)$. It will therefore be sufficient to prove our formula in the following two case: a) ϖ exchanges $p-1$ and p and leaves $1, \ldots, p-2$ fixed; $\varpi' = 1$; b) $\varpi = 1$, ϖ' exchanges 1 and 2 and leaves $3, \ldots, q$ fixed. Since ${}^{p-1,q-1}\theta_A^{\mathfrak{R}} \circ {}^{p-2,q-2}\theta_A^{\mathfrak{R}}$ is an isomorphism, any $\xi \in {}^{p,q}H(A)$ may be represented by an element x of the form

$$x = ({}^{p-1,q-1}\theta_A \circ {}^{p-2,q-2}\theta_A)(x')$$

with $x' \in ({}^{p-2,q-2}\text{早}(A))^{\mathfrak{G}}$. If $x' = \sum_{i=1}^{h} u_i \otimes v_i \otimes a_i$, with $u_i \in J_{p-2}$, $v_i \in I_{q-2}$, then

$$x = \sum_{i=1}^{h} \sum_{s \in \mathfrak{G}} \sum_{t \in \mathfrak{G}} u_i \otimes \bar{s} \otimes \bar{t} \otimes (t-e) \otimes (s-e) \otimes v_i \otimes a_i,$$

and, in case a)

$$\omega_A(\varpi, \varpi')x = \sum_{i=1}^{h} \sum_{s,t \in \mathfrak{G}} u_i \otimes \bar{t} \otimes \bar{s} \otimes (t-e) \otimes (s-e) \otimes v_i \otimes a_i.$$

We have

$$({}^{p-2,q-2}S_{A} \circ {}^{p-1,q-1}S_{A})(x) = (n-1)^2 x'$$
$$({}^{p-2,q-2}S_{A} \circ {}^{p-1,q-1}S_{A})(\omega_{A}(\tilde{\omega}, \tilde{\omega}')x) = (n-1)x'$$

and the sum of these two elements is $(n-1)nx' = (n-1)\sigma x'$. It follows that $({}^{p-2,q-2}S_A^{\mathfrak{N}} \circ {}^{p-1,q-1}S_A^{\mathfrak{N}})(\xi + \omega_A^{\mathfrak{N}}(\tilde{\omega}, \tilde{\omega}')\xi) = 0$. Since ${}^{p-2,q-2}S_A^{\mathfrak{N}} \circ {}^{p-1,q-1}S_A^{\mathfrak{N}}$ is an isomorphism, $\xi + \omega_A^{\mathfrak{N}}(\tilde{\omega}, \tilde{\omega}')\xi = 0$, which proves the theorem in case a). The proof in case b) can be carried out exactly in the same way.

Let A and B be $\mathfrak{G}$-modules. We have difined above a homomorphism

$$M_{A,B} : \text{早}(A) \otimes \text{早}(B) \rightarrow \text{早}(A \otimes B).$$

It is clear that $M_{A,B}$ maps $(\text{早}(A))^{\mathfrak{G}} \otimes (\text{早}(B))^{\mathfrak{G}}$ into $(\text{早}(A \otimes B))^{\mathfrak{G}}$. If $x \in \text{早}(A)$, $y \in (\text{早}(B))^{\mathfrak{G}}$, then

$$\sigma M_{A,B}(x \otimes y) = M_{A,B}(\sum_{s \in \mathfrak{G}} sx \otimes sy) = M_{A,B}(\sigma x \otimes y)$$

and similarly, if $x \in (\text{早}(A))^{\mathfrak{G}}$, $y \in \text{早}(B)$, $\sigma M_{A,B}(x \otimes y) = M_{A,B}(x \otimes \sigma y)$. It follows immediately that, if $x \in (\text{早}(A))^{\mathfrak{G}}$, $y \in (\text{早}(B))^{\mathfrak{G}}$, then the class of $M_{A,B}(x \otimes y)$ in $H'(A \otimes B)$ depends only on the classes ξ of x in $H'(A)$ and η of y in $H'(B)$; therefore, $M_{A,B}$ defines an additive mapping

$$M_{A,B}^{\mathfrak{N}} : H'(A) \otimes H'(B) \rightarrow H'(A \otimes B).$$

Let C be a third $\mathfrak{G}$-module. By a *paring* of A and B to C is meant a bi-additive mapping φ of $A \times B$ into C with the property that $\varphi(sa, sb) = s\varphi(a, b)$ for all $s \in \mathfrak{G}$, $a \in A$, $b \in B$. To any such pairing is associated a homomorphism Φ of $A \otimes B$ into C. We shall denote by φ^* the mapping

$$\varphi^* = \Phi^{\natural} \circ M_{A,B}^{\mathfrak{N}}$$

of $H'(A) \otimes H'(B)$ into $H'(C)$.

It is clear that φ^* maps ${}^{p,q}H(A) \otimes {}^{p',q'}H(B)$ into ${}^{p+p',q+q'}H(C)$.

THEOREM 5.8. *Let A, B, C, A', B', C', be $\mathfrak{G}$-modules, u a homomorphism of A' into A, v a homomorphism of B' into B, w a homomorphism of C into C' and φ a pairing of A and B to C. Set $\varphi'(a', b') = w \cdot \varphi(u \cdot a', v \cdot b')$; φ' is therefore a pairing of A', B'* to *C'. Let ξ be in $H'(A')$, η in $H'(B')$; then*

$$\varphi'^*(\xi \otimes \eta) = w^* \cdot \varphi^*(u^*(\xi) \otimes v^*(\eta)).$$

Let Φ, Φ' be the homomorphisms $\Phi : A \otimes B \rightarrow C$, $\Phi' : A' \otimes B' \rightarrow C'$ associated to φ, φ'. We then have

$$\Phi' = w \circ \Phi \circ (u \otimes v)$$

whence $\varphi'^{*} = w^{*} \circ \Phi^{*} \circ (u \otimes v)^{*} \circ M^{\mathfrak{N}}_{A',B'}$. Let x be a representative for ξ in (早(A'))$^{\mathfrak{G}}$ and y a representative for η in (早(B'))$^{\mathfrak{G}}$. We know that

$$\widehat{u \otimes v}(M_{A',B'}(x \otimes y)) = M_{A,B}(\hat{u}(x) \otimes \hat{v}(y))$$

(cf. formula (4.7)). It follows that

$$(u \otimes v)^{*}(M^{\mathfrak{N}}_{A',B'}(\xi \otimes \eta)) = M^{\mathfrak{N}}_{A,B}(u^{*}(\xi) \otimes v^{*}(\eta)),$$

and theorem 5.8 follows immediately.

THEOREM 5.9. *Let A_1, A_2, A_3, B_1, B_2, C be $\mathfrak{G}$-modules, φ_1 a pairing of A_1, A_2 to B_1, ψ_1 a pairing of B_1, A_3 to C, φ_2 a pairing of A_2, A_3 to B_2, ψ_2 a pairing of A_1, B_2 to C. Assume that $\psi_1(\varphi_1(a_1, a_2), a_3) = \psi_2(a_1, \varphi_2(a_2, a_3))$ whenever $a_i \in A_i$ $(i = 1, 2, 3)$. Then we have*

$$\psi_1^{*}(\varphi_1^{*}(\xi_1 \otimes \xi_2) \otimes \xi_3) = \psi_2^{*}(\xi_1 \otimes \varphi_2^{*}(\xi_2 \otimes \xi_3))$$

whenever $\xi_i \in H'(A_i)$, $i = 1, 2, 3$.

Let Φ_1 be the mapping $A_1 \otimes A_2 \to B_1$ associated to φ_1. Then the formula $\lambda(u, a_3) = \psi_1(\Phi_1(u), a_3)$ defines a pairing of $A_1 \otimes A_2$ and A_3 to C. Since $\varphi_1^{*}(\xi_1 \otimes \xi_2) = (\Phi_1^{*} \circ M^{\mathfrak{N}}_{A_1,A_2})(\xi_1 \otimes \xi_2)$, it follows from theorem 5.8 that

$$\psi_1^{*}(\varphi_1^{*}(\xi_1 \otimes \xi_2) \otimes \xi_3) = \lambda^{*}(M^{\mathfrak{N}}_{A_1,A_2}(\xi_1 \otimes \xi_2) \otimes \xi_3).$$

Let Λ be the mapping $A_1 \otimes A_2 \otimes A_3 \to C$ associated to λ. Then

$$\psi_1^{*}(\varphi_1^{*}(\xi_1 \otimes \xi_2) \otimes \xi_3) = \Lambda^{*} \circ M^{\mathfrak{N}}_{A_1 \otimes A_2, A_3}(M^{\mathfrak{N}}_{A_1,A_2}(\xi_1 \otimes \xi_2) \otimes \xi_3).$$

We have $\Lambda(a_1 \otimes a_2 \otimes a_3) = \psi_1(\varphi_1(a_1, a_2), a_3) = \psi_2(a_1, \varphi_2(a_2, a_3))$, and Λ is also associated to the pairing of A_1 and $A_2 \otimes A_3$ to C which maps (a_1, v) upon $\psi_2(a_1, \Phi_2(v))$ $(a_1 \in A_1,\ v \in A_2 \otimes A_3)$. It follows that

$$\psi_2^{*}(\xi_1 \otimes \varphi_2^{*}(\xi_2 \otimes \xi_3)) = \Lambda^{*} \circ M^{\mathfrak{N}}_{A_1, A_2 \otimes A_3}(\xi_1 \otimes M^{\mathfrak{N}}_{A_2,A_3}(\xi_2 \otimes \xi_3)).$$

We have proved that $M_{A_1 \otimes A_2, A_3}(M_{A_1,A_2}(x_1 \otimes x_2) \otimes x_3)$ is equal to $M_{A_1, A_2 \otimes A_3}(x_1 \otimes M_{A_2,A_3}(x_2 \otimes x_3))$ whenever $x_i \in$ 早(A_i), $i = 1, 2, 3$. It follows immediately that

$$M^{\mathfrak{N}}_{A_1, A_2 \otimes A_3}(\xi_1 \otimes M^{\mathfrak{N}}_{A_2,A_3}(\xi_2 \otimes \xi_3)) = M^{\mathfrak{N}}_{A_1 \otimes A_2, A_3}(M^{\mathfrak{N}}_{A_1,A_2}(\xi_1 \otimes \xi_2) \otimes \xi_3),$$

which proves theorem 5.9.

THEOREM 5.10 *Let $0 \longrightarrow A_1 \xrightarrow{f} A_2 \xrightarrow{g} A_3 \longrightarrow 0$ be an exact sequence of homomorphisms of $\mathfrak{G}$-modules, and let δ be the corresponding mapping of $H'(A_3)$ into $H'(A_1)$. Let B be a $\mathfrak{G}$-module, and $\mathbf{I}$ the identity mapping of B onto itself. If the sequence $0 \longrightarrow A_1 \otimes B \xrightarrow{f\otimes \mathbf{I}} A_2 \otimes B \xrightarrow{g \otimes \mathbf{I}} A_3 \otimes B \longrightarrow 0$ is exact, let Δ be the corresponding mapping of $H'(A_3 \otimes B)$ into $H'(A_1 \otimes B)$. Then we have $M^{\mathfrak{N}}_{A_1, B}(\delta\xi_3 \otimes \eta) = \Delta M^{\mathfrak{N}}_{A_3, B}(\xi_3 \otimes \eta)$ if $\xi_3 \in H'(A_3)$, $\eta \in H'(B)$. If the sequence $0 \longrightarrow B \otimes A_1 \xrightarrow{\mathbf{I}\otimes f} B \otimes A_2 \xrightarrow{\mathbf{I}\otimes g} B \otimes A_3 \longrightarrow 0$ is exact, let Δ' be the corresponding mapping of $H'(B \otimes A_3)$ into $H'(B \otimes A_1)$. Then we have $M^{\mathfrak{N}}_{B, A_1}(\eta \otimes \delta\xi_3) = (-1)^{p'} \Delta' M_{B, A_3}(\eta \otimes \xi_3)$ if $\xi_3 \in {}^{p,q}H(A)$, $\eta \in {}^{p',q'}H'(B)$.*

Let x_3 be a representative for ξ_3 in $(\mathfrak{F}(A_3))^{\mathfrak{G}}$ and y a representative for η in $H'(B)$. Write $x_3 = \hat{g}(v)$, $v \in \mathfrak{F}(A_2)$, and $d_{A_2} v = \hat{f}(x_1)$, whence $x_1 \in \delta(\xi_3)$. The element $M_{A_3, B}(x_3 \otimes y)$ is a representative for $M^{\mathfrak{N}}_{A_3, B}(\xi_3 \otimes \eta)$ and is equal to $\widehat{g \otimes \mathbf{I}}\,(M_{A_2, B}(v \otimes y))$ by formula (4.7). We have

$$d_{A_2 \otimes B}(M_{A_2, B}(v \otimes y)) = M_{A_2, B}(d_B v \otimes y)$$

by formula (4.6). The right side is equal to $\widehat{f \otimes \mathbf{I}}(x_1 \otimes y)$. It follows that $x_1 \otimes y$ is a representative for $\Delta(M^{\mathfrak{N}}_{A_3, B}(\xi_3 \otimes \eta))$. But it is also obviously a representative for $M^{\mathfrak{N}}_{A_1, B}(\delta\xi_3 \otimes \eta)$, which proves the first assertion of the theorem. To prove the second assertion, we shall first establish a formula. Let A, B be any $\mathfrak{G}$-modules, then there is an isomorphism P of $A \otimes B$ with $B \otimes A$ which maps $a \otimes b$ upon $b \otimes a$ ($a \in A$, $b \in B$). Now, let ξ be in ${}^{p,q}H(A)$ and η in ${}^{p',q'}H(B)$. We shall prove that

$$P^{*} \cdot M^{\mathfrak{N}}_{A, B}(\xi \otimes \eta) = (-1)^{pp'+qq'} M^{\mathfrak{N}}_{B, A}(\eta \otimes \xi) \tag{5.1}$$

Let u be in J_p, v in I_q, u' in $J_{p'}$, v' in $I_{q'}$, $x = u \otimes v \otimes a$, $y = u' \otimes v' \otimes b$, with $a \in A$, $b \in B$. Then we have $M_{A,B}(x \otimes y) = (u \otimes u') \otimes (v \otimes v') \otimes (a \otimes b)$, whose image under $\hat{P}$ is $(u \otimes u') \otimes (v \otimes v') \otimes (b \otimes a)$. On the other hand, we have $M_{B,A}(y \otimes x) = (u' \otimes u) \otimes (v' \otimes v) \otimes (b \otimes a)$; it follows that

$$\hat{P} \circ M_{A,B} = \omega_{B \otimes A}(\varpi, \varpi') \circ M_{B,A}$$

where ϖ is the permutation of $\{1, \ldots, p+p'\}$ which maps i upon $p'+i$ if $i \leqq p$, $p+i$ upon i if $i \leqq p'$, while ϖ' is the permutation of $\{1, \ldots, q+q'\}$ which maps j upon $q'+j$ if $j \leqq q$, $q+j$ upon j if $j \leqq q'$. The signatures of ϖ, ϖ' are obviously $(-1)^{pp'}$ and $(-1)^{qq'}$ respectively, whence, by theorem 5.7,

$$P^{\sim}\circ M^{\mathfrak{N}}_{A,B} = (-1)^{pp'+qq'} M^{\mathfrak{N}}_{B,A}$$

which proves (5.1). Making use of this formula, it is easy to deduce the second assertion of theorem 5.10 from the first.

THEOREM 5.11. *Let* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *and* $0 \longrightarrow C' \xrightarrow{g'} B' \xrightarrow{f'} A' \longrightarrow 0$ *be exact sequences of homomorphisms of* $\mathfrak{G}$-*modules. Let* D *be a* $\mathfrak{G}$-*module, and let* α *be a pairing of* A, A' *to* D, β *a pairing of* B, B' *to* D *and* γ *a pairing of* C, C' *to* D *with the properly that* $\alpha(a, f'(b')) = \beta(f(a), b')$ *for* $a \in A$, $b' \in B'$ *and* $\beta(b, g'(c')) = \gamma(g(b), c')$ *for* $b \in B$, $c' \in C'$. *Let* δ *be the mapping* $H'(C) \to H'(A)$ *associated to our first exact sequence and* δ' *the mapping* $H'(A') \to H'(C')$ *associated to our second exact sequence. If* $\zeta \in H'(C)$, $\xi' \in H'(A')$, *then we have*

$$\alpha^*(\delta\zeta \otimes \xi') = -\gamma^*(\zeta \otimes \delta'\xi').$$

Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be the mappings

$$\mathfrak{a}:\ A\otimes A' \to D;\quad \mathfrak{b}:\ B\otimes B' \to D;\quad \mathfrak{c}:\ C\otimes C' \to D$$

associated to the mappings α, β, γ. Then $\hat{\mathfrak{a}} \circ M_{A,A'}$ is a homomorphism of $\text{早}(A) \otimes \text{早}(A')$ into $\text{早}(D)$, $\hat{\mathfrak{b}} \circ M_{B,B'}$ is a homomorphism of $\text{早}(B) \otimes \text{早}(B')$ into $\text{早}(D)$ and $\hat{\mathfrak{c}} \circ M_{C,C'}$ is a homomorphism of $\text{早}(C) \otimes \text{早}(C')$ into $\text{早}(D)$. We have

$$\alpha^* = (\hat{\mathfrak{a}} \circ M_{A,A'})^{\mathfrak{N}},\ \beta^* = (\hat{\mathfrak{b}} \circ M_{B,B'})^{\mathfrak{N}},\ \gamma^* = (\hat{\mathfrak{c}} \circ M_{C,C'})^{\mathfrak{N}}.$$

We want to show that

$$\hat{\mathfrak{a}} \circ M_{A,A'}(x \otimes \hat{f}'(y')) = \hat{\mathfrak{b}} \circ M_{B,B'}(\hat{f}(x) \otimes y') \qquad \text{if } x \in \text{早}(A),\ y' \in \text{早}(B').$$

It is sufficient to prove this in the case where $x = w \otimes a$, $y' = w' \otimes b'$, $w, w' \in \text{田}$, $a \in A$, $b' \in B'$. We then have $\hat{\mathfrak{a}} \circ M_{A,A'}(x \otimes \hat{f}'(y')) = w \square w' \cdot \alpha(a, f'(b'))$, $\hat{\mathfrak{b}} \circ M_{B,B'} (\hat{f}(x) \otimes y') = w \square w' \beta(f(a), b')$, which proves our assertion.

This being said, let $z \in (\text{早}(C))^{\mathfrak{G}}$ be a representative for ζ, and let $y \in \text{早}(B)$ be such that $\hat{g}(y) = z$. Then we may write, for $s \in \mathfrak{G}$, $sy - y = \hat{f}(x_s)$, $x_s \in \text{早}(A)$. We have $d_B y = \sum_{s\in\mathfrak{G}} \bar{s} \square sy = \sum_{s\in\mathfrak{G}} \bar{s} \square (sy - y) = \hat{f}(x)$, with $x = \sum_{s\in\mathfrak{G}} \bar{s} \square x_s$, and x belongs to $\delta\zeta$. Similarly, let x' be a representative for ξ'; write $x' = \hat{f}'(y')$, $y' \in \text{早}(B')$ and $sy' - y' = \hat{g}'(z'_s)$, with $z'_s \in \text{早}(C')$; then $z' = \sum_{s\in\mathfrak{G}} \bar{s} \square z'_s$ is a representative for $\delta'\xi'$. The element $\alpha^*(\delta\zeta \otimes \xi')$ is represented by the element $\hat{\mathfrak{a}} \cdot M_{A,A'}(x \otimes x')$, which is

$$\sum_{s\in\mathfrak{S}} \hat{\mathfrak{a}}(\bar{s}\,\square\, M_{A,A'}(x_s\otimes x')) = \sum_{s\in\mathfrak{S}} \bar{s}\,\square\,\hat{\mathfrak{a}}(M_{A,A'}(x_s\otimes \hat{f}'(y'))).$$

Since $\hat{f}(x_s) = sy - y$, we have

$$\hat{\mathfrak{a}}\cdot M_{A,A'}(x_s\otimes\hat{f}'(y')) = \hat{\mathfrak{b}}\cdot M_{B,B'}((sy-y)\otimes y').$$

A similar argument shows that $\gamma^*(\zeta\otimes\delta'\xi')$ is represented by

$$\sum_{s\in\mathfrak{S}} \bar{s}\,\square\,\hat{\mathfrak{b}}\cdot M_{B,B'}(y\otimes(sy'-y')).$$

Now, we observe that $\hat{\mathfrak{b}}\cdot M_{B,B'}((sy-y)\otimes(y'-sy'))=0$ because $sy-y=\hat{f}(x_s)$, $\hat{f}'(y'-sy')=0$. Thus, we may write

$$\hat{\mathfrak{b}}\cdot M_{B,B'}((sy-y)\otimes y') = \hat{\mathfrak{b}}\cdot M_{B,B'}((sy-y)\otimes sy')$$

and the element $\alpha^*(\delta\zeta\otimes\xi')+\gamma^*(\zeta\otimes\delta'\xi')$ is represented by

$$\sum_{s\in\mathfrak{S}} \bar{s}\,\square\,\hat{\mathfrak{b}}\cdot M_{B,B'}(sy\otimes sy' - y\otimes y').$$

If we set $\hat{\mathfrak{b}}\cdot M_{B,B'}(y\otimes y') = p$, this is $\sum_{s\in\mathfrak{S}} \bar{s}\,\square\,(sp-p) = \sigma(\bar{e}\,\square\, p)$. It follows that $\alpha^*(\delta\zeta\otimes\xi')+\gamma^*(\zeta\otimes\delta'\xi')=0$.

Let $0\longrightarrow A\xrightarrow{f} B\xrightarrow{g} C\longrightarrow 0$ be an exact sequence of homomorphisms of $\mathfrak{S}$-modules, and let p, q be $\geqq 0$. Let δ be the mapping $H^r(C)\to H^r(A)$ associated to our exact sequence. Then we shall prove that

$$\text{(5.2)}\qquad {}^{p+1,q}\theta_A^{\mathfrak{N}}(\delta(\zeta)) = \delta({}^{p,q}\theta_C^{\mathfrak{N}}(\zeta))$$

for any $\zeta\in{}^{p,q}H(C)$. Let z be a representative for ζ in $(\mathfrak{F}^r(C))^{\mathfrak{S}}$. Write $y=\hat{g}(z)$ with some $y\in\mathfrak{F}(B)$, and $d_B y=\hat{f}(x)$, $x\in(\mathfrak{F}(A))^{\mathfrak{S}}$. Then we have $\hat{g}({}^{p,q}\theta_B(y)) = {}^{p,q}\theta_C(z)$ by the first formula (4.4). On the other hand, we have $d_B({}^{p,q}\theta_B(y)) = {}^{p+1,q}\theta_B(d_B y)$ by formula (4.1), and this is $\hat{f}({}^{p+1,q}\theta_A(x))$, which proves that ${}^{p+1,q}\theta_A(x)$ is a representative for $\delta({}^{p,q}\theta_C^{\mathfrak{N}}(\zeta))$; formula (5.2) is thereby proved.

Let φ be a pairing of the $\mathfrak{S}$-modules A and B to the $\mathfrak{S}$-module C. Then we have for $\xi\in{}^{p,q}H(A)$, $\eta\in{}^{p',q'}H(B)$,

$$\text{(5.3)}\qquad \begin{cases} \varphi^*(\theta_A^{\mathfrak{N}}(\xi)\otimes\eta) = (-1)^{p'}\theta_C^{\mathfrak{N}}\varphi^*(\xi\otimes\eta)\\ \varphi^*(\xi\otimes\theta_B^{\mathfrak{N}}(\eta)) = (-1)^{q}\theta_C^{\mathfrak{N}}\varphi^*(\xi\otimes\eta).\end{cases}$$

For, it follows from formula (4.5) and theorem 5.7, and from the fact that a cyclic permutation of $r+1$ letters has signature $(-1)^r$, that

$$M_{A,B}^{\mathfrak{N}}(\theta_A^{\mathfrak{N}}(\xi)\otimes\eta) = (-1)^{p'}\theta_{A\otimes B}^{\mathfrak{N}} M_{A,B}^{\mathfrak{N}}(\xi\otimes\eta)$$
$$M_{A,B}^{\mathfrak{N}}(\xi\otimes\theta_B^{\mathfrak{N}}(\eta)) = (-1)^{q}\theta_{A\otimes B}^{\mathfrak{N}} M_{A,B}^{\mathfrak{N}}(\xi\otimes\eta).$$

It follows immediately that, if $\xi \in {}^{p+1,q+1}H(A)$, $\eta \in {}^{p',q'}H(B)$, then

$$\varphi^*({}^{p,q}S_A^{\mathfrak{N}}(\xi) \otimes \eta) = (-1)^{p'} \cdot {}^{p+p',q+q'}S_C^{\mathfrak{N}}\varphi^*(\xi \otimes \eta) \tag{5.4}$$

while, if $\xi \in {}^{p,q}H(A)$, $\eta \in {}^{p'+1,q'+1}H(B)$, then

$$\varphi^*(\xi \otimes {}^{p',q'}S_B^{\mathfrak{N}}(\eta)) = (-1)^{q} \cdot {}^{p+p',q+q'}S_C^{\mathfrak{N}}\varphi^*(\xi \otimes \eta). \tag{5.5}$$

We shall set

$$\begin{aligned} {}^{r}H(A) &= {}^{r,0}H(A) \qquad \text{if } r \geqq 0 \\ {}^{r}H(A) &= {}^{0,-r}H(A) \qquad \text{if } r < 0. \end{aligned}$$

The group ${}^{r}H(A)$ is then called the r-th *cohomology group* of A; the direct sum $\sum_{-\infty}^{+\infty}{}^{r}H(A)$ is called the *cohomology group* of A and is denoted by $H(A)$. To every homomorphism f of A into a $\mathfrak{G}$-module B, there is associated an additive mapping

$$f^* : H(A) \to H(B)$$

and we have $(g \circ f)^* = g^* \circ f^*$ if g is a homomorphism of B into a $\mathfrak{G}$-module C. Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of homomorphisms of $\mathfrak{G}$-modules. Let δ be the associated mapping of $H'(C)$ into $H'(A)$. Then, if $r \geqq 0$, δ induces a mapping ${}^{r}\delta$ of ${}^{r}H(C)$ into ${}^{r+1}H(A)$. If $r<0$, then δ maps ${}^{r}H(C)$ into ${}^{1,-r}H(A)$. But ${}^{0,-r-1}\theta_A^{\mathfrak{N}}$ is an isomorphism of ${}^{r+1}H(A)$ with ${}^{1,-r}H(A)$. It follows that there is a mapping, which we denote by ${}^{r}\delta$, of ${}^{r}H(C)$ into ${}^{r+1}H(C)$. We shall denote by δ the mapping of $H(A)$ into itself which extends all mappings ${}^{r}\delta$.

THEOREM 5.12. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & {\scriptstyle u}\downarrow & & {\scriptstyle v}\downarrow & & {\scriptstyle w}\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of homomorphisms of $\mathfrak{G}$-modules whose horizontal lines are exact sequences. Then the diagram

$$\begin{array}{ccccccccc}
H(A) & \xrightarrow{f} & H(B) & \xrightarrow{g} & H(C) & \xrightarrow{\delta} & H(A) & \xrightarrow{f} & H(B) \\
u \big\downarrow & & v \big\downarrow & & w \big\downarrow & & u \big\downarrow & & v \big\downarrow \\
H(A') & \xrightarrow{f'} & H(B') & \xrightarrow{g'} & H(C') & \xrightarrow{\delta'} & H(A') & \xrightarrow{f'} & H(B')
\end{array}$$

is commutative, and its horizontal lines are exact sequences.

This follows immediately from theorem 5.5 and from formula (5.2) above.

Functional representation

Any element $u \in {}^{p,q}\text{早}(A)$ may be written in the form $\sum_{s_1, \ldots, s_p, t_1, \ldots, t_q \in \mathfrak{G}} \bar{s}_1 \otimes \ldots \otimes \bar{s}_p \otimes t_1 \otimes \ldots \otimes t_q \cdot F(s_1, \ldots, s_p, t_1, \ldots, t_q)$ where F is a mapping of the product $\mathfrak{G}^p \times \mathfrak{G}^q$ of $p+q$ copies of $\mathfrak{G}$ into A. We shall say that F is a *functional representative* of u. Not every function F on $\mathfrak{G}^p \times \mathfrak{G}^q$ is representative for an element of ${}^{p,q}\text{早}(A)$; for F must satisfy the following condition (which is also obviously sufficient): if one of the last q arguments runs over all elements of $\mathfrak{G}$, the $p+q-1$ others being kept fixed, the sum of the values assumed by F is O. On the other hand, two distinct functions F and F' may be representative for the same element of ${}^{p,q}\text{早}(A)$: the condition for that is that $F'-F$ can be represented in the form $G_1 + \ldots + G_p$, where $G_i(s_1, \ldots, s_p, t_1, \ldots, t_q)$ does not depend on s_i.

Let F be representative for the element $u \in {}^{p,q}\text{早}(A)$, and let $s \in \mathfrak{G}$. Then it is clear that a representative for su is the function

$$(s_1, \ldots, s_p, t_1, \ldots, t_q) \rightarrow sF(s^{-1}s_1, \ldots, s^{-1}s_p, s^{-1}t_1, \ldots, s^{-1}t_q).$$

If $u \in ({}^{p,q}\text{早}(A))^{\mathfrak{G}}$, then we shall say that a functional representative F for u is also a *functional representative* for the element of ${}^{p,q}H(A)$ represented by u.

Let f be a homomorphism of A into a $\mathfrak{G}$-module B. If a function F is a functional representative for an element $\xi \in {}^{p,q}H(A)$, then it is clear that $f \circ F$ is a functional representative for $f^*(\xi)$.

Let φ be a pairing of the $\mathfrak{G}$-modules A and B to a $\mathfrak{G}$-module C. Let ξ be in ${}^{p,q}H(A)$ and η in ${}^{p',q'}H(B)$; let F and G be functional representatives for ξ and η. Then the function

$$\begin{aligned}
&(s_1, \ldots, s_p, s_{p+1}, \ldots, s_{p+p'}, t_1, \ldots, t_q, t_{q+1}, \ldots, t_{q+q'}) \\
&\rightarrow \varphi(F(s_1, \ldots, s_p, t_1, \ldots, t_q), G(s_{p+1}, \ldots, s_{p+p'}, t_{q+1}, \ldots, t_{q+q'}))
\end{aligned}$$

is obviously a functional representative for $\varphi^*(\xi \otimes \eta)$.

§6. DETERMINATION OF SOME COHOMOLOGY GROUPS

Let $\mathfrak{G}$ be a finite group, and A a $\mathfrak{G}$-module. Then we have

$$^0H(A) = {}^{0,0}H(A) = \mathfrak{N}(\mathfrak{G}\ ;\ A).$$

In order to determine $^{-1}H(A)$, we introduce the additive mapping $\varphi : I \otimes A \to A$ defined by

$$\varphi(\sum_{s \in \mathfrak{G}} s \otimes a(s)) = a(e) \quad (\text{where } \sum a(s) = 0).$$

In order for $x = \sum_{s \in \mathfrak{G}} s \otimes a(s)$ to be in $(I \otimes A)^{\mathfrak{G}}$, we must have, for any $t \in \mathfrak{G}$,

$$\sum_{s \in \mathfrak{G}} s \otimes a(s) = \sum_{s \in \mathfrak{G}} ts \otimes ta(s) = \sum_{s \in \mathfrak{G}} s \otimes ta(t^{-1}s)$$

which gives the condition $a(s) = ta(t^{-1}s)$ $(s, t \in \mathfrak{G})$. This condition is easily seen to be equivalent to $a(s) = sa(e)$ for all $s \in \mathfrak{G}$, which implies that $\sigma\varphi(x) = 0$. We shall denote by $A_{\mathfrak{G}}$ the group of all $a \in A$ such that $\sigma a = 0$. If $a \in A_{\mathfrak{G}}$, then $\sum_{s \in \mathfrak{G}} s \otimes sa$ belongs to $(I \otimes A)^{\mathfrak{G}}$; thus, φ maps $(I \otimes A)^{\mathfrak{G}}$ onto $A_{\mathfrak{G}}$. Let now $y = \sum_{s \in \mathfrak{G}} s \otimes b(s)$ be any element of $I \otimes A$. Then $\sigma y = \sum_{s \in \mathfrak{G}} s \otimes \sum_{t \in \mathfrak{G}} tb(t^{-1}s)$, where $\varphi(\sigma y) = \sum_{t \in \mathfrak{G}} tb(t^{-1})$. Since $\sum_{t \in \mathfrak{G}} b(t) = 0$, this may be written in the form

$$\varphi(\sigma y) = \sum_{t \in \mathfrak{G}} (tb(t^{-1}) - b(t^{-1})).$$

We shall denote by $[IA]$ the additive group generated by all $tb - b$, $t \in \mathfrak{G}$, $b \in A$; then φ maps $\sigma(I \otimes A)$ into $[IA]$. Let conversely $x = \sum_{s \in \mathfrak{G}} s \otimes sa$ be an element of $(I \otimes A)^{\mathfrak{G}}$ (with $a \in A_{\mathfrak{G}}$) such that $\varphi(x) \in [IA]$. It is then clear that we may write $a = \sum_{t \in \mathfrak{G}} (tb(t^{-1}) - b(t^{-1}))$, with $b(t^{-1}) \in A$, $\sum_{t \in \mathfrak{G}} b(t^{-1}) = 0$. Thus, $\varphi(x - \sigma \sum_{s \in \mathfrak{G}} s \otimes b(s)) = 0$; since $x - \sigma \sum_{s \in \mathfrak{G}} s \otimes b(s) \in (I \otimes A)^{\mathfrak{G}}$, this implies $x = \sigma \sum_{s \in \mathfrak{G}} s \otimes b(s)$. Moreover, we see in the same way that φ maps $\sigma(I \otimes A)$ onto $[IA]$. It follows that

$$\boxed{^{-1}H(A) = {}^{0,1}H(A) \cong A_{\mathfrak{G}}/[IA]}\ .$$

We shall now determine $^1H(A)$. This group is isomorphic to $^0H(J \otimes A)$.

An element $x \in J \otimes A$ may be uniquely written in the form $\sum_{s \in \mathfrak{G}} \bar{s} \otimes a(s)$, where $\alpha : s \to a(s)$ is a mapping *of* $\mathfrak{G}$ into A such that $a(e) = 0$. We have, for $t \in \mathfrak{G}$,

$$tx = \sum_{s \in \mathfrak{G}} \overline{ts} \otimes ta(s) = \sum_{s \in \mathfrak{G}} \bar{s} \otimes ta(t^{-1}s) = \sum_{s \in \mathfrak{G}} \bar{s} \otimes (ta(t^{-1}s) - ta(t^{-1})).$$

Thus, a necessary and sufficient condition for x to be in $(J \otimes A)^{\mathfrak{G}}$ is that $ta(t^{-1}s) - ta(t^{-1}) = a(s)$, a condition which may be written in the form

$$a(ts) = a(t) + ta(s) \quad (s, t \in \mathfrak{G}).$$

The mappings $s \to a(s)$ which satisfy this condition are called the *crossed homomorphisms* of $\mathfrak{G}$ into A. It is clear that $a(e) = 0$ for any crossed homomorphism $s \to a(s)$. We have

$$\sigma x = \sum_{s \in \mathfrak{G}} \bar{s} \otimes (\sum_{t \in \mathfrak{G}} ta(t^{-1}s) - ta(t^{-1})).$$

If we set $b = \sum_{t \in \mathfrak{G}} ta(t^{-1})$, then $\sum_{t \in \mathfrak{G}} ta(t^{-1}s) = sb$, and

$$\sigma x = \sum_{s \in \mathfrak{G}} \bar{s} \otimes (sb - b).$$

A crossed homomorphism which is of the form $s \to sb - b$, for some $b \in A$, is said to *split*. Thus we have proved

THEOREM 6.1. *The group* ${}^1H(A)$ *is isomorphic to the factor group of the group of all crossed homomorphisms of* $\mathfrak{G}$ *into A by the group of splitting crossed homomorphisms.*

COROLLARY 1. *If* $\mathfrak{G}$ *operates trivially on A, then* ${}^1H(A)$ *is isomorphic to the group of all homomorphisms of* $\mathfrak{G}$ *into A.*

COROLLARY 2. *Let* L/K *be a normal separable extension of finite degree of a field K, and* $\mathfrak{G}$ *its Galois group. Consider the multiplicative group* L^* *of elements* $\neq 0$ *in L as a* $\mathfrak{G}$*-module. Then* ${}^1H(\mathfrak{G}\ ;\ L^*) = \{0\}$.

This follows immediately from E. Noether's theorem.

Consider now the case where A is the group $\mathbf{Z}$, considered as a $\mathfrak{G}$-module on which $\mathfrak{G}$ operates trivially. We have $\mathbf{Z}^{\mathfrak{G}} = \mathbf{Z}$, $\sigma\mathbf{Z} = n\mathbf{Z}$, where n is the order of $\mathfrak{G}$. Thus

$$\boxed{{}^{0,0}H(\mathbf{Z}) = {}^0H(\mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}}$$

The group $\mathbf{Z}_{\mathfrak{G}}$ is $\{0\}$, whence

$$\boxed{{}^{0,1}H(\mathbf{Z}) = {}^{-1}H(\mathbf{Z}) = \{0\}}$$

Since $\mathbf{Z}$ has no element $\neq 0$ of finite order and $\mathfrak{G}$ is finite, there is no homomorphism $\neq 0$ of $\mathfrak{G}$ into $\mathbf{Z}$, whence

$$\boxed{{}^{1,0}H(\mathbf{Z}) = {}^{1}H(\mathbf{Z}) = \{0\}}$$

By corollary 2 to theorem 5.5, the group ${}^2H(\mathbf{Z})$ is isomorphic to ${}^1H(\mathbf{R}^*)$; on the other hand, we have defined a canonical isomorphism of ${}^1H(\mathbf{R}^*)$ with the group of all homomorphisms of $\mathfrak{G}$ into $\mathbf{R}^*$. The latter group will be denoted by Char $\mathfrak{G}$, and its elements will be called the *characters* of $\mathfrak{G}$. Let $\mathfrak{G}'$ be the commutator subgroup of $\mathfrak{G}$; since $\mathbf{R}^*$ is abelian, we have $\mathrm{Char}\,\mathfrak{G} \cong \mathrm{Char}\,\mathfrak{G}/\mathfrak{G}'$, and it is well known that $\mathrm{Char}\,\mathfrak{G}/\mathfrak{G}' \cong \mathfrak{G}/\mathfrak{G}'$. Thus

$$\boxed{{}^{2,0}H(\mathbf{Z}) = {}^{2}H(\mathbf{Z}) \cong \mathrm{Char}\,(\mathfrak{G}/\mathfrak{G}') \cong \mathfrak{G}/\mathfrak{G}'}$$

To a character χ of $\mathfrak{G}$ there is associated the element of ${}^1H(\mathbf{R}^*)$ represented by the element $\sum_{t\in\mathfrak{G}} \bar{t} \otimes \chi(t)$ *of* 早$(\mathbf{R}^*)$. Let us determine the corresponding element of ${}^2H(\mathbf{Z})$. Let χ_0 be a mapping of $\mathfrak{G}$ into $\mathbf{R}$ such that, for any $s \in \mathfrak{G}$, $\chi_0(s)$ belongs to the chass $\chi(s)$ modulo $\mathbf{Z}$. Then we have first to construct the element $\sum_{s\in\mathfrak{G}} \bar{s} \otimes s(\sum_{t\in\mathfrak{G}} \bar{t} \otimes \chi_0(t))$ of 早$(\mathbf{R})$; this is $\sum_{s\ t\in\mathfrak{G}} \bar{s} \otimes \bar{t} \otimes \chi_0(s^{-1}t)$. Set

$$c_\chi(s, t) = \chi_0(s^{-1}t) - \chi_0(s^{-1}) - \chi_0(t) \in \mathbf{Z}.$$

Since $\sum_{s\in\mathfrak{G}} \bar{s} = 0$, we have $\sum_{s,\, t\in\mathfrak{G}} \bar{s} \otimes \bar{t} \otimes \chi_0(s^{-1}) = \sum_{s\ t\in\mathfrak{G}} \bar{s} \otimes \bar{t} \otimes \chi_0(t) = 0$, and $\sum_{s,\, t\in\mathfrak{G}} \bar{s} \otimes \bar{t} \otimes \chi_0(s^{-1}t) = \sum_{s,\, t\in\mathfrak{G}} \bar{s} \otimes \bar{t} \otimes c_\chi(s, t)$. Thus, *the element of* ${}^2H(\mathbf{Z})$ *which corresponds to* χ *is represented by the element*

$$\sum_{s,\, t\in\mathfrak{G}} c_\chi(s, t)\bar{s} \otimes \bar{t}$$

of J_2.

It can be proved in general that ${}^{-p}H(\mathbf{Z}) \cong {}^{p}H(\mathbf{Z})$ for any p. We shall prove here directly that ${}^{-2}H(\mathbf{Z}) \cong \mathfrak{G}/\mathfrak{G}'$. We have ${}^{-2}H(\mathbf{Z}) = {}^{-1}H(I \otimes \mathbf{Z}) = {}^{-1}H(I) \cong I_{\mathfrak{G}}/[II]$. It is clear that $I_{\mathfrak{G}} = I$. Let π be the mapping $s \to s - e$ of $\mathfrak{G}$ into I. We have, for $s, t \in \mathfrak{G}$, $\pi(st) = s(t-e) + s - e \equiv \pi(s) + \pi(t) \pmod{[II]}$. If we denote by $\bar{\pi}(s)$ the residue class of $\pi(s)$ mod $[II]$, then $\bar{\pi}$ is a homomorphism of $\mathfrak{G}$ into $I/[II]$. It is clear that $\pi(\mathfrak{G})$ is a set of generators of the additive group I; $\bar{\pi}$ is therefore an epimorphism. Since the elements $s-e$, $s\in\mathfrak{G}$, $s\neq e$, form a base of I, there is a homomorphism ω of I into the abelian group $\mathfrak{G}/\mathfrak{G}'$ which maps any $s-e$ upon the coset $\bar{s}$ of $\mathfrak{G}$ modulo $\mathfrak{G}'$; thus $\omega\circ\pi$ is the canonical mapping of $\mathfrak{G}$ onto $\mathfrak{G}/\mathfrak{G}'$, and its kernel is therefore $\mathfrak{G}'$. If $s, t\in\mathfrak{G}$, then $\omega(t(s-e))=\omega(ts-e)-\omega(t-e)=\overline{ts}-\bar{t}=\bar{s}$ (we note $\mathfrak{G}/\mathfrak{G}'$ additively); it follows that $\omega([II])=0$, and therefore that the kernel of $\bar{\pi}$ is $\mathfrak{G}'$, which shows that $\bar{\pi}$ defines an isomorphism $\bar{\pi}_1 : \mathfrak{G}/\mathfrak{G}'\cong {}^{-1}H(I)$. We may explicit this isomorphism as follows. In the isomorphism between $I/[II]$ and ${}^{-1}H(I)$, the element which corresponds to $s-e$ is the cohomology class of $\sum_{t\in\mathfrak{G}} t\otimes t(s-e)$. Thus, the element of ${}^{-2}H(\mathbf{Z})$ which corresponds to the coset (mod $\mathfrak{G}'$) of an $s\in\mathfrak{G}$ is represented by the element

$$\sum_{t\in\mathfrak{G}} t\otimes(ts-t)=\sum_{t\in\mathfrak{G}}(t-e)\otimes(ts-t).$$

Observe now that $M^{\mathfrak{N}}_{\mathbf{Z},\mathbf{Z}}$ induces a mapping of ${}^{+2}H(\mathbf{Z})\otimes{}^{-2}H(\mathbf{Z})$ into ${}^{2,2}H(\mathbf{Z})$. On the other hand ${}^{0,0}s^{\mathfrak{N}}_{\mathbf{Z}}\circ{}^{1,1}S^{\mathfrak{N}}_{\mathbf{Z}}$ is an isomorphism of ${}^{2,2}H(\mathbf{Z})$ with ${}^{0}H(\mathbf{Z})=\mathbf{Z}/n\mathbf{Z}$, where n is the order of $\mathfrak{G}$. Let μ be the mapping ${}^{0,0}S^{\mathfrak{N}}_{\mathbf{Z}}\circ{}^{1,1}S^{\mathfrak{N}}_{\mathbf{Z}}\circ M^{\mathfrak{N}}_{\mathbf{Z},\mathbf{Z}}$ of ${}^{+2}H(\mathbf{Z})\otimes{}^{-2}H(\mathbf{Z})$ into $\mathbf{Z}/n\mathbf{Z}$. Let χ be a character of $\mathfrak{G}$ and s an element of $\mathfrak{G}$; denote by $\xi(\chi)$ the element of ${}^{2}H(\mathbf{Z})$ which corresponds to χ (by the isomorphism established above) and by $\eta(s)$ the element of ${}^{-2}H(\mathbf{Z})$ which corresponds to the coset of s modulo $\mathfrak{G}'$. We shall compute $\mu(\xi(\chi)\otimes\eta(s))$. We have to determine the value of

$$\begin{aligned}&{}^{0,0}S\circ{}^{1,1}S\cdot\sum_{u,v,t\in\mathfrak{G}} c_\chi(u,v)\bar{u}\otimes\bar{v}\otimes t\otimes(ts-t)\\ &={}^{0,0}S\sum_{u,t\in\mathfrak{G}} c_\chi(u,t)\bar{u}\otimes(ts-t)=\sum_{t\in\mathfrak{G}}(c_\chi(ts,t)-c_\chi(t,t)).\end{aligned}$$

We have, with the notation used above

$$c_\chi(ts,t)-c_\chi(t,t)=\chi_0(s^{-1})-\chi_0(s^{-1}t^{-1})-\chi_0(t)-[\chi_0(e)-\chi_0(t^{-1})-\chi_0(t)]$$

and the value of our expression is $n(\chi_0(s^{-1})-\chi_0(e))\equiv -n\chi_0(s)$ (mod $n\mathbf{Z}$), since $\chi_0(e)\in\mathbf{Z}$. Thus

$$\boxed{\mu(\xi(\chi)\otimes\eta(s))=-n\chi(s)} \tag{6.1}$$

where $n\chi(s)$ is the class of $n\chi_0(s)$ modulo $n\mathbf{Z}$.

Let A be a $\mathfrak{G}$-module which at the same time a ring, the operators of $\mathfrak{G}$ being automorphisms of the ring structure of A. Then the multiplication μ in

A is a pairing of A and A to A. It defines a mapping μ : $H'(A) \otimes H'(A) \to H'(A)$, and this mapping defines in turn a bi-additive law of composition in $H'(A)$. It follows immediately from theorem 5.9 that this law of composition is associative. Thus, $H'(A)$ has a structure of ring.

In particular, $\mathbf{Z}$ is a ring; therefore $H'(\mathbf{Z})$ has a structure of ring. Let A be any $\mathfrak{G}$-module. Then we have $A \otimes \mathbf{Z} = A$, and the mapping $(a, \nu) \to \nu a (a \in A, \nu \in \mathbf{Z})$ is a pairing of A and $\mathbf{Z}$ to A. This pairing defines a mapping of $H'(A) \otimes H'(\mathbf{Z})$ into $H'(A)$, namely the mapping $M^{\mathfrak{N}}_{A,\mathbf{Z}}$; this in turn defines an external law of composition between elements of $H'(A)$ and of $H'(\mathbf{Z})$, with values in $H'(A)$. It follows immediately from 5.9, that this external law of composition defines on $H'(A)$ a structure of $H'(\mathbf{Z})$-right module.

Denote by 1^+ the residue class of 1 modulo $n\mathbf{Z}$; this is an element of ${}^{0,0}H(\mathbf{Z})$. We have $M_{A,\mathbf{Z}}(x \otimes 1) = x$ for any $x \in \mathfrak{H}(A)$, whence

$$M^{\mathfrak{N}}_{A,\mathbf{Z}}(\xi \otimes 1^+) = \xi \quad (\xi \in H'(A)).$$

It follows that, if ν^+ is an element of order n, equal to the order of $\mathfrak{G}$, in ${}^0H(\mathbf{Z})$, then $\xi \to M^{\mathfrak{N}}_{A,\mathbf{Z}}(\xi \otimes \nu^+)$ is an automorphism of $H'(A)$; for ν^+ is then obviously invertible in the ring $H'(\mathbf{Z})$.

THEOREM 6.2. *Let r be $\geqq 0$, and let ν be an element of order n equal to the order of $\mathfrak{G}$ in ${}^{r,r}H(\mathbf{Z})$. Then $\xi \to M^{\mathfrak{N}}_{A,\mathbf{Z}}(\xi \otimes \nu)$ induces an isomorphism of ${}^{p,q}H(A)$ with ${}^{p+r,q+r}H(A)$ (for any $p \geqq 0$, $q \geqq 0$).*

We have just seen that this is true if $r = 0$. Assume that $r > 0$ and that our statement is true for $r-1$. We may write $\nu = {}^{r-1,r-1}\theta^{\mathfrak{N}}_{\mathbf{Z}}(\nu_1)$, where ν_1 is of order n in ${}^{r-1,r-1}H(\mathbf{Z})$. We have

$$M_{A,\mathbf{Z}}(\xi \otimes \nu) = (-1)^q \theta^{\mathfrak{N}}_A \cdot M_{A,\mathbf{Z}}(\xi \otimes \nu_1)$$

by formula (5.3). Since $\theta^{\mathfrak{N}}_A$ is an isomorphism, it follows immediately that our assertion is true for r.

Cohomology of cyclic groups

THEOREM 6.3. *Let $\mathfrak{G}$ be a cyclic group. Then we have*

$${}^rH(A) \cong {}^{r+2}H(A)$$

for every integer r.

Let s be a generator of $\mathfrak{G}$. Consider the mapping $z \to (s-e)z$ of $\mathbf{Z}[\mathfrak{G}]$ into itself. Since $\mathfrak{G}$ is commutative, this mapping is a homomorphism of $\mathfrak{G}$-modules. We have $(s-e)s^k \in I[\mathfrak{G}]$ for every k; conversely, for any k, we may write $s^k - e = (s-e)z_k$, $z_k \in \mathbf{Z}[\mathfrak{G}]$, whence $(s-e)\mathbf{Z}[\mathfrak{G}] = I[\mathfrak{G}]$. Let n be the order of $\mathfrak{G}$. Then $(s-e)\sum_{k=0}^{n-1} \nu_k s^k = \sum_{k=0}^{n-1} (\nu_k - \nu_{k+1}) s^{k+1}$, where we have set $\nu_n = \nu_0$. It follows immediately that the kernel of our mapping is $\mathbf{Z}\sigma$, whence $I \cong J$. Thus, we have $J_{p+2} \otimes I_q \otimes A \cong J_{p+1} \otimes I \otimes I_q \otimes A = J_{p+1} \otimes I_{q+1} \otimes A$, and ${}^{p+2,q}H(A) \cong {}^{p+1,q+1}H(A) \cong {}^{p,q}H(A)$, which proves the theorem.

We shall give later an other proof of this theorem, based on a different principle.

§7. THE RESTRICTION MAPPING

We shall denote by $\mathfrak{H}$ a subgroup of the group $\mathfrak{G}$. Any $\mathfrak{G}$-module may therefore be considered as an $\mathfrak{H}$-module.

It is clear that we may consider the group algebra $Z[\mathfrak{H}]$ of $\mathfrak{H}$ as a subalgebra of $Z[\mathfrak{G}]$; we then have $I[\mathfrak{H}]\subset I[\mathfrak{G}]$. On the other hand, there is a "natural" additive mapping of $Z[\mathfrak{G}]$ onto $Z[\mathfrak{H}]$ which maps t upon itself if $t\in\mathfrak{H}$, s upon 0 if $s\notin\mathfrak{H}$. This mapping maps $\sigma_{\mathfrak{G}}=\sum_{s\in\mathfrak{G}} s$ upon $\sigma_{\mathfrak{H}}=\sum_{t\in\mathfrak{H}} t$, and therefore defines a *natural* mapping $\varphi : J[\mathfrak{G}]\to J[\mathfrak{H}]$.

By a *normal mapping* of $\boxplus[\mathfrak{G}]$ into $\boxplus[\mathfrak{H}]$, we shall mean a homomorphism Φ of the algebra structure of $\boxplus[\mathfrak{G}]$ *onto* that of $\boxplus[\mathfrak{H}]$ which satisfies the following conditions: Φ is a homomorphism for the structures of $\mathfrak{H}$-modules; for any $p\geqq 0$, $q\geqq 0$, Φ maps ${}^{p,q}\boxplus[\mathfrak{G}]$ onto ${}^{p,q}\boxplus[\mathfrak{H}]$; Φ induces the identity mapping on the submodule $I[\mathfrak{H}]$ of $I[\mathfrak{G}]$; Φ induces the natural mapping φ on $J[\mathfrak{G}]$

THEOREM 7.1. *There exists at least one normal mapping of* $\boxplus[\mathfrak{G}]$ *into* $\boxplus[\mathfrak{H}]$; *if* Φ *is any such mapping, then the kernel of* Φ *splits.*

Let $\mathfrak{H}s_i$ ($i=1, \dots, m$; $s_1=e$, the unit element) be the distinct cosets of $\mathfrak{G}$ modulo $\mathfrak{H}$. Let X be the subgroup of $I[\mathfrak{G}]$ generated by the elements s_i-e $(2\leqq i\leqq m)$. The elements $t-e$ $(t\in\mathfrak{H}, t\neq e)$, $ts_i-t=t(s_i-e)$ $(t\in\mathfrak{H}, i>1)$ clearly form a base of $I[\mathfrak{G}]$. This shows that $I[\mathfrak{G}]$ is the direct sum of $I[\mathfrak{H}]$ and of the module $U_I=\sum_{t\in\mathfrak{H}} tX$, which splits. Let α be the mapping of $I[\mathfrak{G}]$ onto $I[\mathfrak{H}]$ which coincides with the identity on $I[\mathfrak{H}]$ and maps U_I upon $\{0\}$. If $p\geqq 0$, $q\geqq 0$, let ${}^{p,q}\Phi$ be the mapping $\varphi\otimes\dots\otimes\varphi\otimes\alpha\otimes\dots\otimes\alpha$ (p factors φ and q factors α) of ${}^{p,q}\boxplus[\mathfrak{G}]$ onto ${}^{p,q}\boxplus[\mathfrak{H}]$, and let Φ be the mapping which extends all ${}^{p,q}\Phi$. Then Φ is obviously a normal mapping. Now, let Φ be any normal mapping. The kernel U_I' of the restriction of Φ to $I[\mathfrak{G}]$ is clearly isomorphic to U_I, and therefore splits; the kernel K of the restriction of Φ to $J[\mathfrak{G}]$ is the kernel of φ. We shall see that this module splits. Denote by $\bar{s}$ the residue class of s in $J[\mathfrak{G}]$ (if $s\in\mathfrak{G}$); then we see immediately that K is generated as an additive group by the elements $\sum_{t\in\mathfrak{H}}\bar{t}$, $\overline{ts_i}$ $(t\in\mathfrak{H}, i>1)$, whose sum is 0, therefore the elements $\overline{ts_i}$ $(t\in\mathfrak{H}, i>1)$ form a base of K, and $K=\sum_{t\in\mathfrak{H}} tY$ (direct), where $Y=\sum_{i=2}^{m}\mathbf{Z}\bar{s}_i$. The kernel of Φ is clearly the direct sum of the tensor product of U'_l by some $\mathfrak{H}$-module and of the tensor product of K by some module. Since the tensor product of any splitting module by any module splits, theorem 7.1 is proved

Let A be an $\mathfrak{H}$-module, and $\mathbf{I}_A$ the identity map of A onto itself. If Φ is a normal mapping of $\mathfrak{T}[\mathfrak{G}]$ onto $\mathfrak{T}[\mathfrak{H}]$, then $\Phi\otimes\mathbf{I}_A$ is a homomorphism Φ_A of the $\mathfrak{H}$-module $\mathfrak{T}[\mathfrak{G}]\otimes A$ onto $\mathfrak{F}(\mathfrak{H}\,;A)$ whose kernel $\mathfrak{K}_A$ splits. The exact sequence $0\rightarrow\mathfrak{K}_1\rightarrow\mathfrak{T}[\mathfrak{G}]\otimes A\rightarrow\mathfrak{F}(\mathfrak{H}\,;A)\rightarrow 0$ therefore defines an isomorphism $\Phi_A^{\mathfrak{N}}:\mathfrak{N}(\mathfrak{H}\,;\mathfrak{T}[\mathfrak{G}]\otimes A)\cong H'(\mathfrak{H}\,;A)$. Thus we have proved:

THEOREM 7.2. *Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$ and A an $\mathfrak{H}$-module. Then we have ${}^{p,q}H(\mathfrak{H}\,;A)\cong\mathfrak{N}(\mathfrak{H}\,;{}^{p,q}\mathfrak{T}[\mathfrak{G}]\otimes A)$ for any $p\geqq 0$, $q\geqq 0$.*

Moreover, the isomorphism $\Phi_A^{\mathfrak{N}}$ does not depend on the choice of Φ. In order to prove this, we observe that $J[\mathfrak{G}]$ is the direct sum of the kernel K of φ and of an $\mathfrak{H}$-module V; for, using the notation of the proof of theorem 7.1, let $y=\sum_{i=1}^{m}\bar{s}_i$, and let V be the additive group generated by the elements ty, $t\in\mathfrak{H}$. The element $\varphi(ty)$ is the residue class of t in $J[\mathfrak{H}]$, and $\sum_{t\in\mathfrak{H}}ty=0$, which shows that φ induces an isomorphism of V with $J[\mathfrak{H}]$. Let ψ be the reciprocal isomorphism of $J[\mathfrak{H}]$ with V. Then there is an isomorphism Ψ of the $\mathfrak{H}$-module $\mathfrak{T}[\mathfrak{H}]$ with a submodule of $\mathfrak{T}[\mathfrak{G}]$ which maps $x_1\otimes\ldots\otimes x_p\otimes y_1\otimes\ldots\otimes y_q$ upon $\psi(x_1)\otimes\ldots\otimes\psi(x_p)\otimes y_1\otimes\ldots\otimes y_q$ if $x_i\in J[\mathfrak{H}]$, $1\leqq i\leqq p$, $y_j\in I[\mathfrak{H}]$, $1\leqq j\leqq q$.

If Φ is any normal mapping, then $\Phi\circ\Psi$ is the identity mapping of $\mathfrak{T}[\mathfrak{H}]$. Set $\Psi_A=\Psi\otimes\mathbf{I}_A$; then $\Phi_A^{\mathfrak{N}}$ is the reciprocal of the mapping $\Psi_A^{\mathfrak{N}}$, which proves that this mapping does not depend on the choice of Φ.

Moreover, since $\Phi_A\circ\Psi_A$ is the identity mapping, we see that any element of $(\mathfrak{F}(\mathfrak{H}\,;A))^{\mathfrak{H}}$ is the image under Φ_A of an element of $(\mathfrak{F}(\mathfrak{G}\,;A))^{\mathfrak{H}}$.

Now, let M be any $\mathfrak{G}$-module. It is clear that $M^{\mathfrak{H}}\supset M^{\mathfrak{G}}$. We have $\sigma_{\mathfrak{G}}M\subset\sigma_{\mathfrak{H}}M$; for, if $\mathfrak{H}s_i(i=1,\ldots,m)$ are the distinct cosets of $\mathfrak{G}$ modulo $\mathfrak{H}$, then $\sigma_{\mathfrak{G}}x=\sigma_{\mathfrak{H}}(\sum_{i=1}^{m}s_ix)$ $(x\in M)$. This gives rise to an additive mapping

$$\rho(M):\mathfrak{N}(\mathfrak{G}\,;M)\rightarrow\mathfrak{N}(\mathfrak{H}\,;M).$$

If A is a $\mathfrak{G}$-module, we set

$$r_A=r_A(\mathfrak{G}\,;\mathfrak{H})=\Phi_A^{\mathfrak{N}}\circ\rho(\mathfrak{F}(A));$$

r_A is an additive mapping of $H'(\mathfrak{G}\,;A)$ into $H'(\mathfrak{H}\,;A)$, which is called the *restriction mapping.* It is clear that r_A maps ${}^{p,q}H(\mathfrak{G}\,;\,A)$ into ${}^{p,q}H(\mathfrak{H}\,;\,A)$.

Let again M be any $\mathfrak{G}$-module, and let $s_i\mathfrak{H}(1 \leqq i \leqq m,\ s_1 = e)$ be the distinct cosets of $\mathfrak{G}$ modulo $\mathfrak{H}$. Let x be in $M^{\mathfrak{H}}$; then $x' = \sum_{i=1}^{m} s_i x$ belongs to $M^{\mathfrak{G}}$ and does not depend on the choice of the representatives s_i for the cosets $s_i\mathfrak{H}$. For, let s be in $\mathfrak{G}$; then we may write $ss_i = s_{\varpi(i)}t_i$, ϖ being a permutation of $\{1, \ldots, m\}$ and $t_i \in \mathfrak{H}$; it follows that $sx' = x'$. On the other hand, we have $s_i x = s_i tx$ for $t \in \mathfrak{H}$, which proves our second assertion. If $x = \sigma_{\mathfrak{H}} y$ belongs to $\sigma_{\mathfrak{H}} M$, then $x' = \sigma_{\mathfrak{G}} y$ belongs to $\sigma_{\mathfrak{G}} M$. This gives rise to an additive mapping

$$P(M) : \mathfrak{N}(\mathfrak{H}\,;\,M) \to \mathfrak{N}(\mathfrak{G}\,;\,M).$$

We set

$$R_A = R_A(\mathfrak{H}\,;\,\mathfrak{G}) = P(\text{早}(A)) \circ (\Phi_A^{\mathfrak{N}})^{-1}.$$

R_A is an additive mapping of $H'(\mathfrak{H}\,;\,A)$ into $H'(\mathfrak{G}\,;\,A)$; it is clear that R_A maps ${}^{p,q}H(\mathfrak{H}\,;\,A)$ into ${}^{p,q}H(\mathfrak{G}\,;\,A)$. We shall call R_A the *injection mapping.*

THEOREM 7.3. *Let m be the index of $\mathfrak{H}$ in $\mathfrak{G}$. Then we have, for any $\xi \in H'(\mathfrak{G}\,;\,A)$, $R_A(r_A(\xi)) = m\xi$.*

It is sufficient to prove that $(P(M) \circ \rho(M))(\mu) = m\mu$ if $\mu \in \mathfrak{N}(\mathfrak{G}\,;\,M)$, M being any $\mathfrak{G}$-module. Let x be a representative for μ in $M^{\mathfrak{G}}$; then, with the notation used above, x is also *a* representative for $\rho(M) \cdot \mu$, and $\sum_{i=1}^{m} s_i x = mx$ is a representative for $(P(M) \circ \rho(M))(\mu)$.

COROLLARY. *Let A be a $\mathfrak{G}$-module and p, q integers $\geqq 0$. Assume that ${}^{p,q}H(\mathfrak{H}\,;\,A) = \{0\}$ for every Sylow subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Then we have ${}^{p,q}H(\mathfrak{G}\,;\,A) = \{0\}$.*

Let $n = q_1 \ldots q_n$ be the order of $\mathfrak{G}$, each q_i being a power of a prime p_i, with $p_i \neq p_j$ for $i \neq j$. For each i, there is a Sylow subgroup $\mathfrak{H}_i$ of index n/q_i of $\mathfrak{G}$. Let ξ be in ${}^{p,q}H(\mathfrak{G}\,;\,A)$; then, considering the subgroup $\mathfrak{H}_i$, it follows immediately from theorem 7.3 that $(n/q_i)\xi = 0$. But the numbers n/q_i are relatively prime as a whole; it follows that $\xi = 0$.

THEOREM 7.4. *Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$ and $\mathfrak{K}$ a subgroup of $\mathfrak{H}$. Let A be a $\mathfrak{G}$-module; denote by $r_A(\mathfrak{H})$, $r_A(\mathfrak{K})$ the restriction mapping from $H'(\mathfrak{G}\,;\,A)$ to $H'(\mathfrak{H}\,;\,A)$ and $H'(\mathfrak{K}\,;\,A)$, by $R_A(\mathfrak{H})$ and $R_A(\mathfrak{K})$ the injection mappings from $H'(\mathfrak{H}\,;\,A)$ and $H'(\mathfrak{K}\,;\,A)$ into $H'(\mathfrak{G}\,;\,A)$, by $r'_A(\mathfrak{K})$ the restriction mapping from*

$H'(\mathfrak{H}\ ;\ A)$ to $H'(\mathfrak{K}\ ;\ A)$ and by $R'_A(\mathfrak{K})$ the injection mapping from $H'(\mathfrak{K}\ ;\ A)$ to $H'(\mathfrak{H}\ ;\ A)$. Then we have

$$r_A(\mathfrak{K}) = r'_A(\mathfrak{K}) \circ r_A(\mathfrak{H})\ ;\ R_A(\mathfrak{K}) = R_A(\mathfrak{H}) \circ R'_A(\mathfrak{K}).$$

Let Φ be a normal mapping of $\boxplus[\mathfrak{G}]$ into $\boxplus[\mathfrak{H}]$ and Ψ a normal mapping of $\boxplus[\mathfrak{H}]$ into $\boxplus[\mathfrak{K}]$. Then $\Psi\circ\Phi$ is a homomorphism of $\boxplus[\mathfrak{G}]$ into $\boxplus[\mathfrak{K}]$ relatively to the structures of algebras and $\mathfrak{K}$-modules, and coincides with the identity on $I[\mathfrak{K}]$. If $s\in\mathfrak{G}$, then clearly, $\Psi\circ\Phi$ maps $\bar{s}$ upon 0 if s is not in $\mathfrak{K}$ and upon the residue class of s in $J[\mathfrak{K}]$ if $s\in\mathfrak{K}$. It follows that $\Psi\circ\Phi$ is a normal mapping. If $\mathbf{I}_A$ is the identity mapping of A, then $(\Psi\circ\Phi)\otimes\mathbf{I}_A = (\Psi\otimes\mathbf{I}_A)\circ(\Phi \otimes\mathbf{I}_A)$. The first of our formulas follows immediately from this. Now, let ζ be an element of $H'(\mathfrak{K}\ ;\ A)$, and let w be an element of $(\mathfrak{F}(\mathfrak{G}\ ;\ A))^{\mathfrak{K}}$ such that $(\Psi\circ\Phi)(w)$ represents ζ. Let $s_i\mathfrak{H}$ $(1\leqq i\leqq m)$ be the distinct cosets of $\mathfrak{G}$ modulo $\mathfrak{H}$ and $t_k\mathfrak{K}$ $(1\leqq k\leqq n)$ the distinct cosets of $\mathfrak{H}$ modulo $\mathfrak{K}$; then the cosets of $\mathfrak{G}$ modulo $\mathfrak{K}$ are the $s_i t_k\mathfrak{K}$, $1\leqq i\leqq m$, $1\leqq k\leqq n$. Set $w' = \sum_{k=1}^{n} t_k w$; then $\Phi(w') = \sum_{k=1}^{n} t_k\Phi(w)$ is a representative for $R'_A(\mathfrak{K})\cdot\zeta$; moreover, w' is clearly $\mathfrak{H}$-invariant, and $\sum_{i=1}^{m} s_i w'$ is therefore a representative for $R_A(\mathfrak{H})\circ R'_A(\mathfrak{K})\cdot\zeta$. But this element is $\sum_{i=1}^{m}\sum_{k=1}^{n} s_i t_k w$ and is therefore a representative for $R_A(\mathfrak{K})\cdot\zeta$, which proves the second formula.

Let φ be a pairing of the $\mathfrak{G}$-modules A, B to a $\mathfrak{G}$-module C. Then φ defines mapping $\varphi^*_{\mathfrak{G}} : H'(\mathfrak{G}\ ;\ A)\otimes H'(\mathfrak{G}\ ;\ B)\to H'(\mathfrak{G}\ ;\ C)$ and $\varphi^*_{\mathfrak{H}} : H'(\mathfrak{H}\ ;\ A) \otimes H'(\mathfrak{H}\ ;\ B)\to H'(\mathfrak{H}\ ;\ C)$. We propose to prove the formula

$$\text{(7.1)}\qquad \boxed{r_C\varphi^*_{\mathfrak{G}}(\xi\otimes\eta) = \varphi^*_{\mathfrak{H}}(r_A(\xi)\otimes r_B(\eta))\qquad (\xi\in H'(\mathfrak{G}\ ;\ A),\ \eta\in H'(\mathfrak{G}\ ;\ B))}$$

There are associated to φ a mapping φ_0 of $A\otimes B$ into C, a mapping $\hat{\varphi}_0^{\mathfrak{G}}$ of $\mathfrak{F}(\mathfrak{G}\,;A\otimes B)$ into $\mathfrak{F}(\mathfrak{G}\ ;\ C)$ and a mapping $\hat{\varphi}_0^{\mathfrak{H}}$ of $\mathfrak{F}(\mathfrak{H}\ ;\ A\otimes B)$ into $\mathfrak{F}(\mathfrak{H}\ ;\ C)$. On the other hand, we have mappings $M^{\mathfrak{G}}_{A,B} : \mathfrak{F}(\mathfrak{G}\ ;\ A)\otimes\mathfrak{F}(\mathfrak{G}\ ;\ B)\to\mathfrak{F}(\mathfrak{G}\ ;\ A \otimes B)$ and $M^{\mathfrak{H}}_{A,B} : \mathfrak{F}(\mathfrak{H}\ ;\ A)\otimes\mathfrak{F}(\mathfrak{H}\ ;\ B)\to\mathfrak{F}(\mathfrak{H}\ ;\ A\otimes B)$. Denote by $\mathbf{I}_M$ the identity mapping of any module M. Take representative u for ξ in $(\mathfrak{F}(\mathfrak{G}\ ;\ A))^{\mathfrak{G}}$ and v for η in $(\mathfrak{F}(\mathfrak{G}\ ;\ B))^{\mathfrak{G}}$. Let Φ be a normal mapping of $\boxplus(\mathfrak{G})$ into $\boxplus(\mathfrak{H})$. Then $(\Phi\otimes\mathbf{I}_C)\hat{\varphi}_0^{\mathfrak{G}}M^{\mathfrak{G}}_{A,B}(u\otimes v)$ is a representative for $r_C\varphi^*_{\mathfrak{G}}(\xi\otimes\eta)$. This is obviously equal to $\hat{\varphi}_0^{\mathfrak{H}}(\Phi\otimes\mathbf{I}_{A\otimes B})M^{\mathfrak{G}}_{A,B}(u\otimes v)$; since Φ is a homomorphism for the algebra structures, we have

$$(7.2)\qquad \hat{\varphi}_0^{\mathfrak{H}}(\Phi\otimes\mathrm{I}_{A\otimes B})M_{A,B}^{\mathfrak{G}}(u\otimes v)=\hat{\varphi}_0^{\mathfrak{H}}M_{A,B}^{\mathfrak{H}}((\Phi\otimes\mathrm{I}_A)(u)\otimes(\Phi\otimes\mathrm{I}_B)(v))$$

and the right side is a representative for $\varphi_{\mathfrak{H}}^*(r_A(\xi)\otimes r_B(\eta))$, which proves (7.1).

Now, let ξ be an element of $H'(\mathfrak{G}\,;A)$ and η an element of $H'(\mathfrak{H}\,;B)$. We shall prove the formula

$$(7.3)\qquad \boxed{R_C\varphi_{\mathfrak{H}}^*(r_A(\xi)\otimes\eta)=\varphi_{\mathfrak{G}}^*(\xi\otimes R_B\eta)}$$

Let u be a representative for ξ in $(\mathfrak{F}(\mathfrak{G}\,;A))^{\mathfrak{G}}$ and v a representative for η in $(\mathfrak{F}(\mathfrak{H}\,;B))^{\mathfrak{H}}$. Defining φ_0, $\hat{\varphi}_0^{\mathfrak{G}}$, $\hat{\varphi}_0^{\mathfrak{H}}$, $M_{A,B}^{\mathfrak{G}}$, $M_{A,B}^{\mathfrak{H}}$ as above, $\varphi_{\mathfrak{H}}^*(r_A(\xi)\otimes\eta)$ is represented by the element $\hat{\varphi}_0^{\mathfrak{H}}M_{A,B}^{\mathfrak{H}}((\Phi\otimes\mathrm{I}_A)(u)\otimes v)$. We may write $v=(\Phi\otimes\mathrm{I}_B)(w)$, where w is an element of $(\mathfrak{F}(\mathfrak{G}\,;B))^{\mathfrak{H}}$. We then have

$$\begin{aligned}\hat{\varphi}_0^{\mathfrak{H}}M_{A,B}^{\mathfrak{H}}((\Phi\otimes\mathrm{I}_A)(u)\otimes v)&=\hat{\varphi}_0^{\mathfrak{H}}(\Phi\otimes\mathrm{I}_{A\otimes B})M_{A,B}^{\mathfrak{G}}(u\otimes w)\\&=(\Phi\otimes\mathrm{I}_C)\hat{\varphi}_0^{\mathfrak{G}}M_{A,B}^{\mathfrak{G}}(u\otimes w).\end{aligned}$$

Let $s_i\mathfrak{H}$ $(1\leqq i\leqq m)$ be the distinct cosets of $\mathfrak{G}$ modulo $\mathfrak{H}$. By definition of the mapping, $R_C\varphi_{\mathfrak{H}}^*(r_A(\xi)\otimes\eta)$ is represented by $\sum_{i=1}^m s_i\hat{\varphi}_0^{\mathfrak{G}}M_{A,B}^{\mathfrak{G}}(u\otimes w)=\sum_{i=1}^m\hat{\varphi}_0^{\mathfrak{G}}s_iM_{A,B}^{\mathfrak{G}}(u\otimes w)$. Since $s_iu=u$, we have $s_iM_{A,B}^{\mathfrak{G}}(u\otimes w)=M_{A,B}^{\mathfrak{G}}(u\otimes s_iw)$, and $R_C\varphi_{\mathfrak{H}}^*(r_A(\xi)\otimes\eta)$ is represented by $\hat{\varphi}_0^{\mathfrak{G}}M_{A,B}^{\mathfrak{G}}(u\otimes\sum_{i=1}^m s_iw)$. But $\sum_{i=1}^m s_iw$ is a representative of $R_B\eta$, and formula (7.3) is thereby proved.

Let ξ be an element of ${}^{p,0}H(\mathfrak{G}\,;A)$ and let F be a functional representative for ξ; this is a mapping of $\mathfrak{G}^p$ into A. *The restriction of F to $\mathfrak{H}^p$ is a functional representative for $r_A(\xi)$.* For, ξ is represented by the element $u=\sum_{s_1,\ldots,s_p\in\mathfrak{G}}\bar{s}_1\otimes\ldots\otimes\bar{s}_p\otimes F(s_1,\ldots,s_p)$. Let Φ be a normal mapping of $\boxplus[\mathfrak{G}]$ into $\boxplus[\mathfrak{H}]$; then $\Phi(\bar{s}_1\otimes\ldots\otimes\bar{s}_p)$ is 0 if $s_1,\ldots,s_p$ are not all in $\mathfrak{H}$ and is $(\bar{s}_1)_{\mathfrak{H}}\otimes\ldots\otimes(\bar{s}_p)_{\mathfrak{H}}$ if $s_1,\ldots,s_p\in\mathfrak{H}$, where $(\bar{s}_i)_{\mathfrak{H}}$ is the residue class of s_i in $J[\mathfrak{H}]$. Thus

$$\Phi(u)=\sum_{s_1,\ldots,s_p\in\mathfrak{H}}(\bar{s}_1)_{\mathfrak{H}}\otimes\ldots\otimes(\bar{s}_p)_{\mathfrak{H}}\otimes F(s_1,\ldots,s_p)$$

which proves our assertion.

The transfer mapping. Let $\mathfrak{G}$ be a finite group and $\mathfrak{H}$ a subgroup of $\mathfrak{G}$. We have established in §6 isomorphisms of ${}^2H(\mathfrak{G}\,;\mathbf{Z})$ with Char $\mathfrak{G}$ and of ${}^2H(\mathfrak{H}\,;\mathbf{Z})$ with Char $\mathfrak{H}$. Thus the injection mapping $R_{\mathbf{Z}}$ defines an additive mapping of ${}^2H(\mathfrak{H}\,;\mathbf{Z})$ into ${}^2H(\mathfrak{G}\,;\mathbf{Z})$. We propose now to explicit this mapping. Let χ be a character of $\mathfrak{H}$; let χ_0 be a mapping of $\mathfrak{H}$ into $\mathbf{R}$ such that $\chi(s)$ is, for any $s \in \mathfrak{H}$, the residue class of $\chi_0(s)$ modulo $\mathbf{Z}$. We may obviously assume that $\chi_0(e)=0$. Set $c_\chi(s,t)=\chi_0(s^{-1}t)-\chi_0(s^{-1})-\chi_0(t)(s,t\in\mathfrak{H})$; then the element $\xi(\chi)$ of ${}^2H(\mathfrak{H}\,;\mathbf{Z})$ which corresponds to χ is represented by the element $\sum_{s,t\in\mathfrak{H}} c_\chi(s,t)\bar{s}_{\mathfrak{H}}\otimes\bar{t}_{\mathfrak{H}}=u$ (if $s\in\mathfrak{H}$, $\bar{s}_{\mathfrak{H}}$ is the residue class of s in $J[\mathfrak{H}]$). Let $s_i\mathfrak{H}$ $(1\leq i\leq m;\ s_1=e)$ be the distinct coset of $\mathfrak{G}$ modulo $\mathfrak{H}$; then there is a homomorphism Ψ of $\mathbb{H}[\mathfrak{H}]$ into $\mathbb{H}[\mathfrak{G}]$ (relatively to the structures of algebras and of $\mathfrak{H}$-modules) which maps $\bar{s}_{\mathfrak{H}}$ upon $\sum_i \overline{ss_i^{-1}}$ (where $\overline{ss_i^{-1}}$ is the class of ss_i^{-1} in $J[\mathfrak{G}]$; cf. the proof given above that $J[\mathfrak{G}]$ is the direct sum of the kernel of φ and of an $\mathfrak{H}$-module V). We have

$$\Psi(u)=\sum_{s,t\in\mathfrak{H}}\sum_{i,j=1}^{m} c_\chi(s,t)\,\overline{ss_i^{-1}}\otimes\overline{ts_j^{-1}}$$

and $R_{\mathbf{Z}}\xi(\chi)$ is represented by

$$v=\sum_{k=1}^{m}\sum_{s,t\in\mathfrak{H}}\sum_{i,j-1}^{m} c_\chi(s,t)\,\overline{s_k ss_i^{-1}}\otimes\overline{s_k ts_j^{-1}}.$$

Let s' be any element of $\mathfrak{G}$. For any k, there exists exactly one index i such that $s_k^{-1}s's_i\in\mathfrak{H}$; *set* $s_k^{-1}s's_i=\gamma(k\,;\,s')$, and we have

$$v=\sum_{s',t'\in\mathfrak{G}}\Big(\sum_{k=1}^{m} c_\chi(\gamma(k,s'),\ \gamma(k,t'))\,\bar{s}'\otimes\bar{t}'.$$

Let χ' be the character of $\mathfrak{G}$ which corresponds to the element $R_{\mathbf{Z}}\xi(\chi)$. If $s'\in\mathfrak{G}$, let $\chi_0'(s')$ be a real number belonging to the class $\chi'(s')$ modulo $\mathbf{Z}$; we may assume that $\chi_0'(e)=0$. Set $c_{\chi'}(s',t')=\chi_0'(s'^{-1}t')-\chi_0'(s'^{-1})-\chi_0'(t')$, $v'=\sum_{s',t'\in\mathfrak{G}} c_{\chi'}(s',t')\bar{s}'\otimes\bar{t}'$. Then we have $v-v'=\sigma w$, with $w\in{}^{2,0}\mathbb{H}$. We may write $\sigma w=\Delta w_1$, where $w_1\in{}^{1,0}\mathbb{H}=J[\mathfrak{G}]$; write $w_1=\sum_{t'\in\mathfrak{G}}\nu(t')\bar{t}'$, where $\nu(t')\in\mathbf{Z}$ and we may assume $\nu(e)=0$. Then

$$\begin{aligned} v-v' &= \sum_{s'\in\mathfrak{G}}\bar{s}'\otimes s'w_1=\sum_{s',t'\in\mathfrak{G}}\nu(s'^{-1}t')\bar{s}'\otimes\bar{t}' \\ &= \sum_{s',t'\in\mathfrak{G}}(\nu(s'^{-1}t')-\nu(s'^{-1})-\nu(t'))\bar{s}'\otimes\bar{t}'. \end{aligned}$$

Set $C(s',t')=\sum_{k=1}^{m} c_\chi(\gamma(k,s'),\ \gamma(k,t'))$, $C'(s',t')=c_{\chi'}(s',t')$ and $W(s',t')=\nu(s'^{-1}t')-\nu(s'^{-1})-\nu(t')$. Then we have $\sum_{s',t'\in\mathfrak{G}}(C(s',t')-C'(s',t')-W(s',t'))\bar{s}'\otimes\bar{t}'=0$. It is clear that $c_\chi(e,s)=c_\chi(s,e)=0$ for every $s\in\mathfrak{H}$, $c_{\chi'}(e,s')=c_{\chi'}(s',e)=0$ for every $s'\in\mathfrak{G}$, $W(s',e)=W(e,s')=0$ for every $s'\in\mathfrak{G}$ and that $\gamma(k,e)=e$ for $1\leq k\leq m$. Thus $C(s',t')-C'(s',t')-W(s',t')=0$ if either s' or t' is e, and therefore $C(s', t') - C'(s', t') = W(s', t')$, whence $\sum_{s' \in \mathfrak{G}} C(s', t') - \sum_{s' \in \mathfrak{G}} C'(s', t') = \sum_{s' \in \mathfrak{G}} W(s', t')$. For every $s \in \mathfrak{H}$ and every k $(1 \leqq k \leqq m)$, there are exactly m elements $s' \in \mathfrak{G}$ such that $\gamma(k, s') = s$, namely the elements $s_k s s_i^{-1}$, $1 \leqq i \leqq m$. Thus, $\sum_{s' \in \mathfrak{G}} \chi_0(\gamma^{-1}(k, s')\gamma(k, t')) = m \sum_{s \in \mathfrak{H}} \chi_0(s^{-1}\gamma(k, t')) = m \sum_{s \in \mathfrak{H}} \chi_0(s^{-1})$. If n is the order of $\mathfrak{G}$, we have $\sum_{s' \in \mathfrak{G}} C(s', t') = -n \sum_{k=1}^{m} \chi_0(\gamma(k, t'))$. It is clear that $\sum_{s' \in \mathfrak{G}} C'(s', t') = -n\chi_0'(t')$, $\sum_{s' \in \mathfrak{G}} W(s', t') = -n\nu(t')$. Since $\nu(t')$ is an integer, we obtain

$$\chi'(t') = \sum_{k=1}^{m} \chi(\gamma(k, t')).$$

Denote by $\tau(t')$ the residue class modulo $\mathfrak{H}'$ of the product of the m elements $\gamma(k, t')$ $(1 \leqq k \leqq m)$, these elements being arranged in any order. Identifying Char $\mathfrak{G}$ to Char $\mathfrak{G}/\mathfrak{G}'$, we see that $\chi'(t') = \chi(\tau(t'))$. Now, χ' depends only on χ, not on the choice of the representatives s_i; and two elements of $\mathfrak{H}/\mathfrak{H}'$ to which every character of $\mathfrak{H}$ assigns the same value are equal. It follows that $\tau(t')$ does not depend on the choice of the representatives s_i. Moreover, since χ and χ' are characters, it is clear that $\tau(t_1' t_2') = \tau(t_1')\tau(t_2')$ for any t_1', $t_2' \in \mathfrak{G}$.

The homomorphism τ of $\mathfrak{G}$ into $\mathfrak{H}/\mathfrak{H}'$ is called the *transfer mapping.* It is clear that the kernel of τ contains the commutator subgroup $\mathfrak{G}'$ of $\mathfrak{G}$, and τ defines a homomorphism of $\mathfrak{G}/\mathfrak{G}'$ into $\mathfrak{H}/\mathfrak{H}'$; this homomorphism is also called the transfer mapping.

§8. THE LIFT MAPPING

Let $\mathfrak{H}$ be a normal subgroup of $\mathfrak{G}$. Then there exists an additive mapping $\mathfrak{l}$ of $\mathbf{Z}[\mathfrak{G}/\mathfrak{H}]$ into $\mathbf{Z}[\mathfrak{G}]$ which maps every element $s \in \mathfrak{G}/\mathfrak{H}$ upon the sum $\sum_{s \in s^*} s$ of the elements of the coset s. It is clear that $\mathfrak{l}$ is a homomorphism of $\mathfrak{G}$-modules ($\mathbf{Z}[\mathfrak{G}/\mathfrak{H}]$ being considered as a $\mathfrak{G}$-module on which $\mathfrak{H}$ operates trivially). Moreover, $\mathfrak{l}(\sigma_{\mathfrak{G}/\mathfrak{H}}) = \sigma_{\mathfrak{G}}$, which shows that $\mathfrak{l}$ defines a homomorphism $\mathfrak{l}_J$: $J[\mathfrak{G}/\mathfrak{H}] \to J[\mathfrak{G}]$. For any group $\mathfrak{G}$, we denote by $\boxplus^c[\mathfrak{G}]$ the subalgebra of $\boxplus[\mathfrak{G}]$ generated by 1 and $J[\mathfrak{G}]$, thus $\boxplus^c[\mathfrak{G}] = \sum_{i=0}^{\infty} J_p[\mathfrak{G}]$. The homomorphism $\mathfrak{l}_J$ may be extended to a homomorphism L of $\boxplus^c[\mathfrak{G}/\mathfrak{H}]$ into $\boxplus^c[\mathfrak{G}]$ which maps $x_1 \otimes \dots \otimes x_p$ upon $\mathfrak{l}_J(x_1) \otimes \dots \otimes \mathfrak{l}_J(x_p)$ if $x_i \in J[\mathfrak{G}/\mathfrak{H}]$ $(1 \leqq i \leqq p)$. Let A be any $\mathfrak{G}$-module, and $A^{\mathfrak{H}}$ the set of $\mathfrak{H}$-invariant elements of A. Then $A^{\mathfrak{H}}$ is a submodule of A; for, if $s \in \mathfrak{G}$, $t \in \mathfrak{H}$, $a \in A^{\mathfrak{H}}$, then $tsa = st'a = sa$ if $t' = s^{-1}ts \in \mathfrak{H}$, whence $sa \in A^{\mathfrak{H}}$. Since $\mathfrak{H}$ operates trivially on $A^{\mathfrak{H}}$, $A^{\mathfrak{H}}$ may be considered as a $\mathfrak{G}/\mathfrak{H}$-module. Let $\mathbf{I}_A$ be the identity map of $A^{\mathfrak{H}}$ into A; then

$$L_A = L \otimes \mathbf{I}_A$$

is a homomorphism of $\boxplus^c[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}}$ into $\boxplus^c[\mathfrak{G}] \otimes A$.

We shall prove that, for any $p > 0$, L_A maps $J_p[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}}$ into $\sigma_{\mathfrak{H}}(J_p[\mathfrak{G}] \otimes A)$. Consider first the case where $p = 1$. If we denote by s^* an element of $\mathfrak{G}/\mathfrak{H}$, by a an element of $A^{\mathfrak{H}}$, by $\overline{s^*}$ the image of s^* in $J[\mathfrak{G}/\mathfrak{H}]$, then we have $L_A(\overline{s^*} \otimes a) = \sum_{s \in s^*} \overline{s} \otimes a$, where $\overline{s}$ is the image of s in $J[\mathfrak{G}]$. If s_1 is any element of s^*, then $\sum_{s \in s^*} \overline{s} \otimes a = \sigma_{\mathfrak{H}}(\overline{s}_1 \otimes a)$, since $ta = a$ when $t \in \mathfrak{H}$; this proves our assertion when $p = 1$. Assume that $p > 1$ and that our assertion is proved for $p - 1$. Set $B = J_{p-1}[\mathfrak{G}] \otimes A$; then L_A maps $J_{p-1}[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}}$ into $\sigma_{\mathfrak{H}} B$, and, *a fortiori*, into $B^{\mathfrak{H}}$. On the other hand, it is clear that

$$L_A(x^* \otimes b^*) = L_B(x^* \otimes L_A(b^*)) \quad \text{if } x^* \in J[\mathfrak{G}/\mathfrak{H}],\ b^* \in J_{p-1}[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}}.$$

Our assertion being true for $p = 1$, $L_B(x^* \otimes L_A(b^*))$ is contained in $\sigma_{\mathfrak{H}}(J[\mathfrak{G}] \otimes B) = \sigma_{\mathfrak{H}}(J_p[\mathfrak{G}] \otimes A)$, which proves our assertion for p. Since L_A is a homomorphism for the structures of $\mathfrak{G}$-modules, it maps $(J_p[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}})^{\mathfrak{G}} = (J_p[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}})^{\mathfrak{G}/\mathfrak{H}}$ into $(J_p[\mathfrak{G}] \otimes A)^{\mathfrak{G}}$. It follows from what we have just proved that, for $p > 0$,

L_A maps $\sigma_{\mathfrak{G}/\mathfrak{H}}(J_p[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}})$ into $\sigma_{\mathfrak{G}/\mathfrak{H}}(\sigma_{\mathfrak{H}}(J_p[\mathfrak{G}] \otimes A))$, which is obviously $\sigma_{\mathfrak{G}}(J_p[\mathfrak{G}] \otimes A)$. It follows that L_A defines in a natural manner a mapping

$$\lambda_A : \mathfrak{N}(\mathfrak{G}/\mathfrak{H} ; J_p[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}}) \to \mathfrak{N}(\mathfrak{G} ; J_p[\mathfrak{G}] \otimes A).$$

This mapping of ${}^pH(\mathfrak{G}/\mathfrak{H} ; A^{\mathfrak{H}})$ into ${}^pH(\mathfrak{G} ; A)$ is called the *lift mapping*; it is only defined when $p > 0$.

THEOREM 8.1. *If $p \geqq 1$, then λ_A maps ${}^pH(\mathfrak{G}/\mathfrak{H} ; A^{\mathfrak{H}})$ into the kernel of the restriction map $r_A : {}^pH(\mathfrak{G} ; A) \to {}^pH(\mathfrak{H} ; A)$. If $p = 1$, then λ_A induces an isomorphism of ${}^1H(\mathfrak{G}/\mathfrak{H} ; A^{\mathfrak{H}})$ with the kernel of the restriction mapping r_A : ${}^1H(\mathfrak{G} ; A) \to {}^1H(\mathfrak{H} ; A)$.*

It follows from what was proved above that, for $p \geqq 1$,

$$\lambda_A({}^pH(\mathfrak{G}/\mathfrak{H} ; A^{\mathfrak{H}})) \subset (\sigma_{\mathfrak{H}}(J_p[\mathfrak{G}] \otimes A))^{\mathfrak{G}}/\sigma_{\mathfrak{G}}(J_p[\mathfrak{G}] \otimes A).$$

The right side is obviously in the kernel of the restriction mapping r_A.

Next, we shall prove that

$$(8.1) \qquad \sigma_{\mathfrak{H}}(J[\mathfrak{G}] \otimes A)/L_A(J[\mathfrak{G}/\mathfrak{H}] \otimes A^{\mathfrak{H}}) \cong \mathbf{Z}[\mathfrak{G}/\mathfrak{H}] \otimes (A/A^{\mathfrak{H}});$$

in this formula, $A/A^{\mathfrak{H}}$ is considered as a $(\mathfrak{G}/\mathfrak{H})$-module on which $\mathfrak{G}/\mathfrak{H}$ operates trivially, and the isomorphism is to be constructed as an isomorphism of $\mathfrak{G}/\mathfrak{H}$-modules. If $a(s) \in A$ for $s \in \mathfrak{G}$, then

$$\sigma_{\mathfrak{H}}(\sum_{s\in\mathfrak{G}} \bar{s} \otimes a(s)) = \sum_{s\in\mathfrak{G}} \sum_{t\in\mathfrak{H}} \overline{ts} \otimes ta(s) = \sum_{s\in\mathfrak{G}} \sum_{t\in\mathfrak{H}} \bar{s} \otimes ta(t^{-1}s)$$
$$= \sum_{s\in\mathfrak{G}} \bar{s} \otimes sb(s)$$

where $b(s) = \sum_{t\in\mathfrak{H}} (t^{-1}s)^{-1}a(t^{-1}s)$. If s^* is the coset of s modulo $\mathfrak{H}$, then $b(s) = \sum_{s'\in s^*} s'^{-1}a(s')$, which shows that $b(s)$ depends only on s^*; set $b(s) = b(s^*)$. Conversely, if $s^* \to b(s^*)$ is any mapping of $\mathfrak{G}/\mathfrak{H}$ into A, and if we set $b(s) = b(s^*)$ for $s \in s^*$, then $\sum_{s\in\mathfrak{G}} \bar{s} \otimes sb(s)$ belongs to $\sigma_{\mathfrak{H}}(J \otimes A)$; for, if $s^* \in \mathfrak{G}/\mathfrak{H}$ and $s_1 \in s^*$, then $\sum_{s\in s^*} \bar{s} \otimes sb(s) = \sigma_{\mathfrak{H}}(\bar{s}_1 \otimes s_1 b(s^*))$. Moreover, if $s^* \to b'(s^*)$ is any other mapping of $\mathfrak{G}/\mathfrak{H}$ into A, then a necessary and sufficient condition for $\sum \bar{s} \otimes sb(s)$ to be equal to $\sum \bar{s} \otimes sb'(s)$ is that $s(b'(s) - b(s))$ should not depend on s; since $b(s)$ and $b'(s)$ depend only on s^*, this implies that $b(s^*) - b'(s^*) \in A^{\mathfrak{H}}$. It follows that there is an additive mapping ω of $\sigma_{\mathfrak{H}}(J \otimes A)$ into $\mathbf{Z}[\mathfrak{G}/\mathfrak{H}] \otimes (A/A^{\mathfrak{H}})$ which maps any element of the form $\sum_{s\in\mathfrak{G}} \bar{s} \otimes sb(s^*)$ (where s^* is the coset of s) upon $\sum_{s^*\in\mathfrak{G}/\mathfrak{H}} s^* \otimes \bar{b}(s^*)$, where $\bar{b}(s^*)$ is the residue class of $b(s^*)$ modulo $A^{\mathfrak{H}}$. If $u \in \mathfrak{G}$, then $\omega(u\cdot \sum_{s\in\mathfrak{G}} \bar{s}\otimes sb(s^*)) = \omega(\sum_{s\in\mathfrak{G}} \bar{s}\otimes sb(u^{-1}s^*)) = u^*\cdot\omega(\sum_{s\in\mathfrak{G}} \bar{s}\otimes sb(s^*))$, which proves that ω is a homomorphism. Any element of $L_A(J[\mathfrak{G}/\mathfrak{H}]\otimes A^{\mathfrak{H}})$ is of the form $\sum_{s\in\mathfrak{G}} \bar{s}\otimes sb(s^*)$ with $b(s^*)\in A^{\mathfrak{H}}$, and is therefore mapped upon 0 under ω. Conversely, if $\sum_{s\in\mathfrak{G}} \bar{s}\otimes sb(s^*)$ is in the kernel of ω, then $b(s^*)\in A^{\mathfrak{H}}$, and our element is the image of $\sum_{s^*\in\mathfrak{G}/\mathfrak{H}} \bar{s}^*\otimes s^* b(s^*)$ under L_A. The isomorphism (8.1) is thereby proved.

It is clear that L_A is a monomorphism; thus we have an exact sequence

$$0\to J[\mathfrak{G}/\mathfrak{H}]\otimes A^{\mathfrak{H}} \xrightarrow{L_A} \sigma_{\mathfrak{H}}(J[\mathfrak{G}]\otimes A) \longrightarrow \mathbf{Z}[\mathfrak{G}/\mathfrak{H}]\otimes (A/A^{\mathfrak{H}}) \longrightarrow 0.$$

Since $\mathbf{Z}[\mathfrak{G}/\mathfrak{H}]\otimes (A/A^{\mathfrak{H}})$ splits, we see that the mapping L_A^* is an isomorphism

$$(8.2) \qquad L_A^* : H'(\mathfrak{G}/\mathfrak{H}\ ;\ J[\mathfrak{G}/\mathfrak{H}]\otimes A^{\mathfrak{H}}) \cong H'(\mathfrak{G}/\mathfrak{H}\ ;\ \sigma_{\mathfrak{H}}(J[\mathfrak{G}]\otimes A)).$$

In particular, λ_A induces an isomorphism of $\mathfrak{N}(\mathfrak{G}/\mathfrak{H}\ ;\ J[\mathfrak{G}/\mathfrak{H}]\otimes A^{\mathfrak{H}})$ with the submodule $\mathfrak{N}(\mathfrak{G}/\mathfrak{H}\ ;\ \sigma_{\mathfrak{H}}(J[\mathfrak{G}]\otimes A))$ of $\mathfrak{N}(\mathfrak{G}\ ;\ J[\mathfrak{G}]\otimes A)$. This submodule is obviously the kernel of the restriction map r_A of ${}^1H(\mathfrak{G}\ ;\ A) = \mathfrak{N}(\mathfrak{G}\ ;\ J[\mathfrak{G}]\otimes A)$ to ${}^1H(\mathfrak{H}\ ;\ A)$, and this proves the second assertion of theorem 8.1.

THEOREM 8.2. *Assume that* ${}^1H(\mathfrak{H}\ ;\ A) = \{0\}$. *Then* λ_A *induces an isomorphism of* ${}^2H(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ *with the kernel of the restriction map:*

$$r_A : {}^2H(\mathfrak{G}\ ;\ A) \to {}^2H(\mathfrak{H}\ ;\ A).$$

Let x_1^*, x_2^* be in $J[\mathfrak{G}/\mathfrak{H}]$ and $a\in A^{\mathfrak{H}}$; then we may write

$$L_A(x_1^*\otimes x_2^*\otimes a) = L_{J[\mathfrak{G}]\otimes A}(x_1^*\otimes L_A(x_2^*\otimes a)).$$

To the mapping L_A, considered as a mapping of $J[\mathfrak{G}/\mathfrak{H}]\otimes A^{\mathfrak{H}}$ into $(J[\mathfrak{G}]\otimes A)^{\mathfrak{H}}$, there corresponds a mapping μ_A of ${}^1H(\mathfrak{G}/\mathfrak{H}\ ;\ J[\mathfrak{G}/\mathfrak{H}]\otimes A^{\mathfrak{H}})$ into ${}^1H(\mathfrak{G}/\mathfrak{H}\ ;\ (J[\mathfrak{G}]\otimes A)^{\mathfrak{H}})$, and it is clear that $\lambda_A(\xi^*) = \lambda_{J[\mathfrak{G}]\otimes A}(\mu_A(\xi^*))$. Since ${}^1H(\mathfrak{H}\ ;\ A) = \{0\}$, we have $(J[\mathfrak{G}]\otimes A)^{\mathfrak{H}} = \sigma_{\mathfrak{H}}(J[\mathfrak{G}]\otimes A)$; therefore, it follows from the isomorphisms (8.2) that μ_A is an isomorphism. By theorem 8.1, applied to $J[\mathfrak{G}]\otimes A$, $\lambda_{J[\mathfrak{G}]\otimes A}$ induces an isomorphism of ${}^1H(\mathfrak{G}/\mathfrak{H}\ ;\ (J[\mathfrak{G}]\otimes A)^{\mathfrak{H}})$ with the kernel of the restriction map $r_{J\otimes A}$ of ${}^1H(\mathfrak{G}\ ;\ J[\mathfrak{G}]\otimes A)$ to ${}^1H(\mathfrak{H}\ ;\ J[\mathfrak{G}]\otimes A)$. We have ${}^1H(\mathfrak{G}\ ;\ J[\mathfrak{G}]\otimes A) = {}^2H(\mathfrak{G}\ ;\ A)$. To every normal mapping Φ of $\boxplus[\mathfrak{G}]$ into $\boxplus[\mathfrak{H}]$ there is associated an isomorphism $\Phi_A^{\mathfrak{N}}$ of ${}^1H(\mathfrak{H}\ ;\ J[\mathfrak{G}]\otimes A)$ with ${}^2H(\mathfrak{H}\ ;\ A)$, and it follows immediately from the definitions that $(\Phi_A^{\mathfrak{N}}\circ r_{J\otimes A})(\eta) = r_A(\eta)$ if $\eta\in {}^1H(\mathfrak{G}\ ;\ J[\mathfrak{G}]\otimes A) = {}^2H(\mathfrak{G}\ ;\ A)$; theorem 8.2 is thereby proved.

Let ξ^* be an element of ${}^pH(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ and let F^* be a functional representative for ξ^*. Denote by π the mapping of $\mathfrak{G}^p$ onto $(\mathfrak{G}/\mathfrak{H})^p$ which assigns to $(s_1, \ldots, s_p) \in \mathfrak{G}^p$ the element $(s_1^*, \ldots, s_p^*)$, where s_i^* is the coset of s_i modulo $\mathfrak{H}$. Then the function $F^* \circ \pi$, defined by

$$(F^* \circ \pi)(s_1, \ldots, s_p) = F^*(s_1^*, \ldots, s_p^*)$$

is a functional representative for $\lambda_A(\xi^*)$. For, it is clear that

$$L_A\Big(\sum_{s_1^*, \ldots, s_p^* \in \mathfrak{G}/\mathfrak{H}} \overline{s_1^*} \otimes \cdots \otimes \overline{s_p^*} \otimes F^*(s_1^*, \ldots, s_p^*)\Big)$$
$$= \sum_{s_1, \ldots, s_p \in \mathfrak{G}} s_1 \otimes \cdots \otimes s_p \otimes (F^* \circ \pi)(s_1, \ldots, s_p).$$

Using this fact, we establish immediately the following results:

THEOREM 8.3. *Let $\mathfrak{K}$ be a normal subgroup of $\mathfrak{G}$ contained in $\mathfrak{H}$. Denote by $\lambda_A(\mathfrak{H})$ and $\lambda_A(\mathfrak{K})$ the lift mappings from $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ and $H^c(\mathfrak{G}/\mathfrak{K}\ ;\ A^{\mathfrak{K}})$ into $H^c(\mathfrak{G}\ ;\ A)$ and by $\lambda'_A(\mathfrak{H})$ the lift mapping from $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ into $H^c(\mathfrak{G}/\mathfrak{K}\ ;\ A^{\mathfrak{K}})$ (where $\mathfrak{G}/\mathfrak{H}$ is identified to $(\mathfrak{G}/\mathfrak{K})/(\mathfrak{H}/\mathfrak{K})$). Then we have $\lambda_A(\mathfrak{H}) = \lambda_A(\mathfrak{K}) \circ \lambda'_A(\mathfrak{H})$.*

THEOREM 8.4. *Let $\mathfrak{G}'$ be a subgroup of $\mathfrak{G}$ and $\mathfrak{H}$ a normal subgroup of $\mathfrak{G}$ such that $\mathfrak{G}'\mathfrak{H} = \mathfrak{G}$; set $\mathfrak{H}' = \mathfrak{G}' \cap \mathfrak{H}$. Denote by r_A the restriction mapping from $H^c(\mathfrak{G}\ ;\ A)$ to $H^c(\mathfrak{G}'\ ;\ A)$, by λ_A the lift mapping from $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ into $H^c(\mathfrak{G}\ ;\ A)$, by λ'_A the lift mapping from $H^c(\mathfrak{G}'/\mathfrak{H}'\ ;\ A^{\mathfrak{H}'})$ into $H^c(\mathfrak{G}'\ ;\ A)$. Identifying canonically $\mathfrak{G}/\mathfrak{H}$ to $\mathfrak{G}'/\mathfrak{H}'$, denote by ι^* the mapping: $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}}) = H^c(\mathfrak{G}'/\mathfrak{H}'\ ;\ A^{\mathfrak{H}}) \to H^c(\mathfrak{G}'/\mathfrak{H}'\ ;\ A^{\mathfrak{H}'})$ which corresponds to the identity map $\iota : A^{\mathfrak{H}} \to A^{\mathfrak{H}'}$. Then we have $r_A \circ \lambda_A = \lambda'_A \circ \iota^*$.*

For, under our identification, the restriction to $\mathfrak{G}'^p$ of the mapping $\pi : \mathfrak{G}^p \to (\mathfrak{G}/\mathfrak{H})^p$ introduced above is the mapping $(s'_1, \ldots, s'_p) \to (s_1'^*, \ldots, s_p'^*)$, where $s'_i \in \mathfrak{G}'$ $(1 \leqq i \leqq p)$ and $s_i'^*$ is the coset of s'_i modulo $\mathfrak{H}'$.

THEOREM 8.5. *Let $\mathfrak{H}$ be a normal subgroup of $\mathfrak{G}$ and $\mathfrak{K}$ a subgroup of $\mathfrak{G}$ containing $\mathfrak{H}$. Denote by $r_A^{\mathfrak{K}}$ the restriction mapping from $H^c(\mathfrak{G}\ ;\ A)$ to $H^c(\mathfrak{K}\ ;\ A)$, by $r_A^{\mathfrak{G}/\mathfrak{H}}$ the restriction mapping from $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ to $H^c(\mathfrak{K}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$, by $\lambda_A^{\mathfrak{G}}$ the lift mapping from $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ to $H^c(\mathfrak{G}\ ;\ A)$ and by $\lambda_A^{\mathfrak{K}}$ the lift mapping from $H^c(\mathfrak{K}/\mathfrak{H}\ ;\ A^{\mathfrak{H}})$ to $H^c(\mathfrak{K}\ ;\ A)$. Then we have $\lambda_A^{\mathfrak{K}} \circ r_A^{\mathfrak{K}/\mathfrak{H}} = r_A^{\mathfrak{K}} \circ \lambda_A^{\mathfrak{G}}$.*

THEOREM 8.6. *Let φ be a pairing of the $\mathfrak{G}$-modules A and B to the $\mathfrak{G}$-module C, and let $\varphi^{\mathfrak{H}}$ be the restriction of φ to $A^{\mathfrak{H}} \times B^{\mathfrak{H}}$; this is a pairing of*

$A^{\mathfrak{H}}$ and $B^{\mathfrak{H}}$ to $C^{\mathfrak{H}}$. Then we have

$$\lambda_C(\varphi^{\mathfrak{H}})^*(\xi^* \otimes \eta^*) = \varphi^*(\lambda_A(\xi^*) \otimes \lambda_B(\eta^*))$$

$(\xi^* \in H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A^{\mathfrak{H}}),\ \eta^* \in H^c(\mathfrak{G}/\mathfrak{H}\ ;\ B^{\mathfrak{H}}))$, where λ_A, λ_B, λ_C are the lift mappings.

THEOREM 8.7. *Let f be a homomorphism of a $\mathfrak{G}$-module A into a $\mathfrak{G}$-module B; then f determines a mapping $f^*_{\mathfrak{G}}$ of $H^c(\mathfrak{G}\ ;\ A)$ into $H^c(\mathfrak{G}\ ;\ B)$ and its restriction to $A^{\mathfrak{H}}$ a mapping $f^*_{\mathfrak{G}/\mathfrak{H}}$ of $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A)$ into $H^c(\mathfrak{G}/\mathfrak{H} : B^{\mathfrak{H}})$. We have $f^*_{\mathfrak{G}}\lambda_A \cdot \xi^* = \lambda_B f^*_{\mathfrak{G}/\mathfrak{H}} \cdot \xi^*$ for any $\xi^* \in H^c(\mathfrak{G}/\mathfrak{H}\ ;\ A)$, where λ_A, λ_B are the lift mappings.*

§9. THE THEOREM OF TATE

LEMMA 9.1. *Let $\mathfrak{G}$ be a finite group and A a $\mathfrak{G}$-module. Assume that ${}^0H(\mathfrak{H}\ ;\ A)=\{0\}$ for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Then the conditions:*

A. ${}^1H(\mathfrak{H}\ ;\ A)=\{0\}$ *for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$.*

B. ${}^{-1}H(\mathfrak{H}\ ;\ A)=\{0\}$ *for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$.*

are equivalent to each other.

We prove this by induction on the order $[\mathfrak{G}]$ of $\mathfrak{G}$. There is nothing to prove if $[\mathfrak{G}]=1$. Assume that $[\mathfrak{G}]>1$ and that the lemma is true for every proper subgroup of $\mathfrak{G}$. If condition A (respectively B) is satisfied for $\mathfrak{G}$, then we have ${}^1H(\mathfrak{G}'\ ;\ A)=\{0\}$ (respectively: ${}^{-1}H(\mathfrak{G}'\ ;\ A)=\{0\}$) for every proper subgroup $\mathfrak{G}'$ of $\mathfrak{G}$. If the order of $\mathfrak{G}$ is not a power of a prime, then every Sylow subgroup of $\mathfrak{G}$ is $\neq\mathfrak{G}$, and it follows by the corollary to theorem 7.3 that ${}^{-1}H(\mathfrak{G}\ ;\ A)={}^1H(\mathfrak{G}\ ;\ A)=\{0\}$. Assume now that the order of $\mathfrak{G}$ is a power of a prime. Then $\mathfrak{G}$ has a normal subgroup $\mathfrak{G}'\neq\mathfrak{G}$ such that $\mathfrak{G}/\mathfrak{G}'$ is cyclic. Assume that condition A is satisfied; since ${}^1H(\mathfrak{G}\ ;\ A)={}^1H(\mathfrak{G}', A)=\{0\}$, it follows from theorem 8.1 that ${}^1H(\mathfrak{G}/\mathfrak{G}'\ ;\ A^{\mathfrak{G}'})=\{0\}$. Since $\mathfrak{G}/\mathfrak{G}'$ is cyclic, this implies that ${}^{-1}H(\mathfrak{G}/\mathfrak{G}'\ ;\ A^{\mathfrak{G}'})=\{0\}$ (by theorem 6.3). Let $a\in A$ be such that $\sigma_{\mathfrak{G}}a=0$; then $\sigma_{\mathfrak{G}/\mathfrak{G}'}(\sigma_{\mathfrak{G}'}a)=0$; since ${}^{-1}H(\mathfrak{G}/\mathfrak{G}'\ ;\ A^{\mathfrak{G}'})=0$, this implies that $\sigma_{\mathfrak{G}'}(a)$ is in the group spanned by the elements $b-tb$, $b\in A^{\mathfrak{G}'}$, $t\in\mathfrak{G}$: $\sigma_{\mathfrak{G}'}(a)=\sum_{i=1}^{m}(b_i-t_ib_i)$, $b_i\in A^{\mathfrak{G}'}$. But we have $A^{\mathfrak{G}'}=\sigma_{\mathfrak{G}'}A$, and we may write $b_i=\sigma_{\mathfrak{G}'}c_i$, $c_i\in A$, whence $\sigma_{\mathfrak{G}'}(a-\sum_{i=1}^{m}(c_i-tc_i))=0$. Since ${}^{-1}H(\mathfrak{G}'\ ;\ A)=\{0\}$, this implies that $a-\sum_{i=1}^{m}(c_i-tc_i)$ is in the group spanned by the elements $a'-s'a'$, $a'\in A$, $s'\in\mathfrak{G}'$; it follows immediately that a belongs to the group spanned by the elements $a''-sa''$, $a''\in A$, $s\in\mathfrak{G}$, whence ${}^{-1}H(\mathfrak{G}\ ;\ A)=\{0\}$. Assume conversely that condition B is satisfied. We shall prove that ${}^{-1}H(\mathfrak{G}/\mathfrak{G}'\ ;\ A^{\mathfrak{G}'})=\{0\}$. Let $a\in A^{\mathfrak{G}'}$ be such that $\sigma_{\mathfrak{G}/\mathfrak{G}'}a=0$. Since ${}^1H(\mathfrak{G}'\ ;\ A)=\{0\}$, we may write $a=\sigma_{\mathfrak{G}'}b$, $b\in A$, and we have $\sigma_{\mathfrak{G}}b=0$. Since ${}^{-1}H(\mathfrak{G}\ ;\ A)=\{0\}$, b is of the form $\sum_{i=1}^{m}(c_i-s_ic_i)$, $c_i\in A$, $s_i\in\mathfrak{G}$; thus $a=\sigma_{\mathfrak{G}'}b=\sum_{i=1}^{m}(\sigma_{\mathfrak{G}'}c_i-s_i\sigma_{\mathfrak{G}'}c_i)$. Since $\sigma_{\mathfrak{G}'}c_i\in A^{\mathfrak{G}'}$, it follows immediately that ${}^{-1}H(\mathfrak{G}/\mathfrak{G}' ; A^{\mathfrak{G}'}) = \{0\}$. Since $\mathfrak{G}/\mathfrak{G}'$ is cyclic, we have ${}^{1}H(\mathfrak{G}/\mathfrak{G}' ; A^{\mathfrak{G}'}) = \{0\}$, and, since ${}^{1}H(\mathfrak{G}' ; A) = \{0\}$, we have ${}^{1}H(\mathfrak{G} ; A) = \{0\}$ by theorem 8.1.

THEOREM 9.1. *Let $\mathfrak{G}$ be a finite group and A a $\mathfrak{G}$-module. Assume that, for some integer d, ${}^{d}H(\mathfrak{H} ; A) = {}^{d-1}H(\mathfrak{H} ; A) = \{0\}$ for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Then $H(\mathfrak{G} ; A) = \{0\}$.*

We prove by induction on l that ${}^{d+l}H(\mathfrak{H} ; A) = \{0\}$ for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$ and $l \geqq 0$. This is true for $l = 0$. Assume it is true for $0 \leqq l \leqq k$, where $k \geqq 0$. Then we have ${}^{d+k}H(\mathfrak{H} ; A) = {}^{d+k-1}H(\mathfrak{H} ; A) = \{0\}$. If $d + k \geqq 0$, set $B = J_{d+k}[\mathfrak{G}] \otimes A$; if $d + k < 0$, set $B = I_{-(d+k)}[\mathfrak{G}] \otimes A$. Then it follows from what we have proved in § 5 that, for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$, we have ${}^{d+k+m}H(\mathfrak{H} ; A) = {}^{m}H(\mathfrak{H} ; B)$ for every m. Thus we have ${}^{0}H(\mathfrak{H} ; B) = {}^{-1}H(\mathfrak{H} ; B) = \{0\}$; it follows by lemma 9.1 that ${}^{1}H(\mathfrak{H} ; B) = \{0\}$, whence ${}^{d+k+1}H(\mathfrak{H} ; A) = \{0\}$. Now we prove that ${}^{d-l}H(\mathfrak{H} ; A) = \{0\}$, for every $l \geqq 0$. This is true for $l = 0, 1$; assume that it is true for $0 \leqq l \leqq k$, *where* $k > 0$. If $d - k \geqq 0$, set $B = J_{d-k}[\mathfrak{G}] \otimes A$; if $d - k < 0$, set $B = I_{-(d-k)}[\mathfrak{G}] \otimes A$. Then we have ${}^{0}H(\mathfrak{H} ; B) = {}^{1}H(\mathfrak{H} ; B) = \{0\}$ for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$, whence ${}^{-1}H(\mathfrak{H} ; B) = \{0\}$ and ${}^{d-k-1}H(\mathfrak{H} ; A) = \{0\}$. Theorem 9.1 is thereby proved.

THEOREM 9.2. *Let $\mathfrak{G}$ be a finite group and A a $\mathfrak{G}$-module. Assume that the following conditions are satisfied: for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$, we have ${}^{1}H(\mathfrak{H} ; A) = \{0\}$ and ${}^{2}H(\mathfrak{H} ; A)$ is cyclic of the same order as $\mathfrak{H}$. Then, for any integer d, we have ${}^{d}H(\mathfrak{G} ; A) \cong {}^{d-2}H(\mathfrak{G} ; \mathbf{Z})$. Moreover, if ξ_0 is a generator of ${}^{2}H(\mathfrak{G} ; A)$, then $\zeta \to M^{\mathfrak{N}}_{\mathbf{Z}, A}(\zeta \otimes \xi_0)$ induces an isomorphism of ${}^{p,q}H(\mathfrak{G} ; \mathbf{Z})$ with ${}^{p+2,q}H(\mathfrak{G} ; A)$.*

Let $B = J_2[\mathfrak{G}] \otimes A$; then, for any subgroup $\mathfrak{H}$ of $\mathfrak{G}$, we have ${}^{-1}H(\mathfrak{H} ; B) = \{0\}$ and ${}^{0}H(\mathfrak{H} ; B)$ is cyclic of the same order as $\mathfrak{H}$. Let b_0 be an element of $B^{\mathfrak{G}} = ({}^{2,0}\underline{\mathrm{H}}(\mathfrak{G} ; A))^{\mathfrak{G}}$ belonging to the class ξ_0. From a $\mathfrak{G}$-module $F = \mathbf{Z}[\mathfrak{G}] + B$ which is the direct sum of $\mathbf{Z}[\mathfrak{G}]$ and B; since $b_0 \in B^{\mathfrak{G}}$, $\mathbf{Z}(\sigma + b_0)$ is a submodule of F. Set $E = F/\mathbf{Z}(\sigma + b_0)$. The canonical mapping of F onto E clearly maps B isomorphically onto a submodule B' of E and $\mathbf{Z}[\mathfrak{G}]$ onto a submodule Z' of E. We have $E = B' + Z'$, and $Z' \cap B'$ is $\mathbf{Z}\sigma'$, if σ' is the image of σ, whence $E/B' \cong J$. This shows that we have an exact sequence

$$0 \longrightarrow B \xrightarrow{f} E \xrightarrow{g} J[\mathfrak{G}] \longrightarrow 0.$$

We have $\sigma(e+b_0) = \sigma + nb_0 \equiv (n-1)b_0 \pmod{\mathbf{Z}(\sigma+b_0)}$, where n is the order of $\mathfrak{G}$. Let β_0 be the class of b_0 in ${}^0H(\mathfrak{G}\,;\,B)$, then $f^*_{\mathfrak{G}}((n-1)\beta_0) = 0$; since $n\beta_0 = 0$, we have $f^*_{\mathfrak{G}}(\beta_0) = 0$. Since β_0 generates ${}^0H(\mathfrak{G}\,;\,B)$, we have $f^*_{\mathfrak{G}}({}^0H(\mathfrak{G}\,;\,B)) = \{0\}$. Let $\mathfrak{H}$ be any subgroup of $\mathfrak{G}$, of index m; then $R_B(r_I(\beta_0)) = m\beta_0$ is of order n/m, which proves that $r_B(\beta_0)$ is of order $\equiv 0 \pmod{n/m}$. Since ${}^0H(\mathfrak{H}\,;\,B)$ is cyclic of order n/m, it is generated by $r_B(\beta_0)$. Since $f(b_0) \in \sigma_{\mathfrak{G}}E$, it is clear that $f^*_{\mathfrak{G}}(r_B(\beta_0)) = 0$, whence $f^*_{\mathfrak{G}}({}^0H(\mathfrak{H}\,;\,B)) = \{0\}$. On the other hand, we have ${}^0H(\mathfrak{H}\,;\,J[\mathfrak{G}]) \cong {}^0H(\mathfrak{H}\,;\,J[\mathfrak{H}]) \cong {}^1H(\mathfrak{H}\,;\,\mathbf{Z}) = \{0\}$. Making use of the exact sequence theorem, we conclude that ${}^0H(\mathfrak{H}\,;\,E) = \{0\}$ for every subgroup $\mathfrak{H}$ of $\mathfrak{G}$.

Let δ be the mapping $H'(\mathfrak{H}\,;\,J[\mathfrak{G}]) \to H'(\mathfrak{H}\,;\,B)$ associated to the exact sequence written above. Consider the exact sequence

$${}^{0,1}H(B) \xrightarrow{f^*} {}^{0,1}H(E) \xrightarrow{g^*} {}^{0,1}H(J) \xrightarrow{\delta} {}^{1,1}H(B) \xrightarrow{f^*} {}^{1,1}H(E)$$

We have just proved that ${}^{1,1}H(\mathfrak{H}\,;\,E) = \{0\}$; it follows that δ induces an epimorphism of ${}^{0,1}H(\mathfrak{H}\,;\,J[\mathfrak{G}])$ onto ${}^{1,1}H(\mathfrak{H}\,;\,B)$. The latter group is cyclic of the same order $[\mathfrak{H}]$ as $\mathfrak{H}$. On the other hand, ${}^{0,1}H(\mathfrak{H}\,;\,J[\mathfrak{G}]) \cong {}^{0,1}H(\mathfrak{H}\,;\,J[\mathfrak{H}]) \cong {}^{1,1}H(\mathfrak{H}\,;\,\mathbf{Z})$, and the latter group is likewise cyclic of order $[\mathfrak{H}]$. It follows that the epimorphism of ${}^{0,1}H(\mathfrak{H}\,;\,J[\mathfrak{G}])$ induced by δ is actually an isomorphism, and therefore that $g^*({}^{0,1}H(E)) = \{0\}$. Thus, f^* induces an epimorphism of ${}^{0,1}H(\mathfrak{H}\,;\,B)$. But the latter group is $\{0\}$. It follows that ${}^{-1}H(\mathfrak{H}\,;\,E) = {}^{0,1}H(\mathfrak{H}\,;\,E) = \{0\}$.

We conclude by theorem 9.1 that $H'(\mathfrak{G}\,;\,E) = \{0\}$ and therefore that δ induces an isomorphism of ${}^{p,q}H(\mathfrak{G}\,;\,J[\mathfrak{G}])$ with ${}^{p+1,q}H(\mathfrak{G}\,;\,B)$ for every p, q. But we know that ${}^{p,q}H(\mathfrak{G}\,;\,J[\mathfrak{G}]) \cong {}^{p+1,q}H(\mathfrak{G}\,;\,\mathbf{Z})$, whence ${}^{p+1,q}H(\mathfrak{G}, \mathbf{Z}) \cong {}^{p+1,q}H(\mathfrak{G}\,;\,B) \cong {}^{p+3,q}H(\mathfrak{G}\,;\,A)$. This being true for every $p \geqq 0$, $q \geqq 0$, we have ${}^dH(\mathfrak{G}\,;\,A) \cong {}^{d-2}H(\mathfrak{G}\,;\,\mathbf{Z})$.

Consider now the digram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B & \xrightarrow{f} & E & \xrightarrow{g} & J[\mathfrak{G}] & \longrightarrow & 0 \\
 & & u\uparrow & & v\uparrow & & w\uparrow & & \\
0 & \longrightarrow & \mathbf{Z} & \longrightarrow & \mathbf{Z}[\mathfrak{G}] & \longrightarrow & J[\mathfrak{G}] & \longrightarrow & 0
\end{array}$$

where the mappings are defined as follows: those of second line are the mappings of the exact sequence $0 \to \mathbf{Z} \to \mathbf{Z}[\mathfrak{G}] \to J[\mathfrak{G}] \to 0$ which we have already considered; we have $u(1) = -b_0$; v is the mapping induced on $\mathbf{Z}[\mathfrak{G}]$ by the canonical mapping $F = \mathbf{Z}[\mathfrak{G}] + B \to E$; w is the identity. We see immediately that this diagram is commutative. Let ∂' be the mapping: $H'(J[\mathfrak{G}]) \to H'(\mathbf{Z})$ induced by the second horizontal line. Then we have $u^{\sim} \circ \partial' = \partial \circ w = \partial$, which shows that u is an isomorphism $H'(\mathfrak{G} ; \mathbf{Z}) \to H'(\mathfrak{G} ; B)$. On the other hand, it follows immediately from the definition of u that $u(\zeta) = -M^{\mathfrak{R}}_{\mathbf{Z},F}(\zeta \otimes \beta_0)$. If $\zeta \in {}^{p,q}H(\mathfrak{G} ; \mathbf{Z})$ is the class of an element $z \in ({}^{p,q}\mathfrak{F}(\mathbf{Z}))^{\mathfrak{G}} = ({}^{p,q}\mathfrak{H})^{\mathfrak{G}}$, then $M_{\mathbf{Z},I}(\zeta \otimes \beta_0)$ is the class of $z \otimes b_0 \in J_p \otimes I_q \otimes J_2 \otimes A$. Write $b_0 = \sum_{i=1}^{n} x_i \otimes a_i$ $a_i \in A$, $x_i \in J_2$; then $M_{\mathbf{Z},A}(\zeta \otimes \xi_0)$ is represented by $\sum_{i=1}^{n} (z \square x_i) \otimes a_i$, which is deduced from $z \otimes b_0$ by a permutation automorphism. This proves the last assertion of theorem 9.2.

If $\mathfrak{G}$ is a cyclic group of order n, then the character group of $\mathfrak{G}/\mathfrak{G}'$ (i.e. of $\mathfrak{G}$) is cyclic of order n, which shows that ${}^{2,0}H(\mathfrak{G} ; \mathbf{Z})$ is cyclic of order n.

THEOREM 9.3. *Let $\mathfrak{G}$ be a cyclic group, and let ζ_1 be a generator of ${}^{2,0}H(\mathfrak{G} ; \mathbf{Z})$. Then, for any $\mathfrak{G}$-module A, $\xi \to M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \zeta_1)$ induces an isomorphism of ${}^{p,q}H(A)$ with ${}^{p+2,q}H(A)$ (for any $p \geqq 0$, $q \geqq 0$).*

Since every subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is cyclic, ${}^{0,2}H(\mathfrak{H} ; \mathbf{Z})$ is cyclic of the same order as $\mathfrak{H}$; moreover, we have ${}^{1}H(\mathfrak{H} ; \mathbf{Z}) = \{0\}$. It follows that $\zeta \to M^{\mathfrak{R}}_{\mathbf{Z},\mathbf{Z}}(\zeta_1 \otimes \zeta)$ induces an isomorphism of ${}^{0,2}H(\mathbf{Z})$ with ${}^{2,2}H(\mathbf{Z})$ (observe that $M^{\mathfrak{R}}_{\mathbf{Z},\mathbf{Z}}(\zeta_1 \otimes \zeta) = M^{\mathfrak{R}}_{\mathbf{Z},\mathbf{Z}}(\zeta \otimes \zeta_1)$ by formula (5.1)). The latter group is cyclic of order n equal to the order of $\mathfrak{G}$. Let $\zeta_1' \in {}^{0,2}H(\mathfrak{H} ; \mathbf{Z})$ be such that $M^{\mathfrak{R}}_{\mathbf{Z},\mathbf{Z}}(\zeta_1 \otimes \zeta_1') = \nu$ is of order n. We have $M^{\mathfrak{R}}_{A,\mathbf{Z}}(M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \zeta_1) \otimes \zeta_1') = M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \nu)$ (because $H'(A)$ is an $H'(\mathbf{Z})$-module), and $\xi \to M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \nu)$ induces an isomorphism of ${}^{p,q}H(A)$ with ${}^{p+2,q+2}H(A)$ (theorem 6.2). It follows immediately that $\xi \to M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \zeta_1)$ is a monomorphism. Let ξ' be any element of ${}^{p,q+2}H(A)$; then we may write $M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi' \otimes \zeta_1') = M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \nu)$ with some $\xi \in {}^{p,q}H(A)$. Set $\xi'' = M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi \otimes \zeta_1) - \xi'$; then $M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi'' \otimes \zeta_1') = 0$; since $M^{\mathfrak{R}}_{\mathbf{Z},\mathbf{Z}}(\zeta_1' \otimes \zeta_1) = \nu$, we have $M^{\mathfrak{R}}_{A,\mathbf{Z}}(\xi'' \otimes \nu) = 0$, whence $\xi'' = 0$; this completes the proof of theorem 9.3.

§10. HERBRAND'S LEMMA

Let $\mathfrak{G}$ be a cyclic group, and A a $\mathfrak{G}$-module. We know that I is isomorphic with J; let χ be an isomorphism of I with J. If $p \geqq 0$, $q \geqq 0$, there is an isomorphism $\chi_{p,q}$ of ${}^{p+1,q+1}\mathfrak{K}(A) = J_{p+1} \otimes I \otimes I_q \otimes A$ with ${}^{p+2,q}\mathfrak{K}(A) = J_{p+1} \otimes J \otimes I_q \otimes A$ which maps $u \otimes y \otimes v \otimes a$ upon $u \otimes \chi(y) \otimes v \otimes a$ if $u \in J_{p+1}$, $y \in I$, $v \in I_q$, $a \in A$. Then $\chi_{p,q}^{\mathfrak{N}} \circ \theta_A^{\mathfrak{N}}$ is an isomorphism ${}^{p,q}\kappa_A$ of ${}^{p,q}H(A)$ with ${}^{p+2,q}H(A)$. If f is a homomorphism of A into a $\mathfrak{G}$-module B, then, clearly,

$$f^* \circ \kappa_{p,q} = \kappa_{p,q} \circ f^* \tag{10.1}$$

We shall say that A is an *Herbrand module* if ${}^0H(A)$ and ${}^1H(A)$ are finite groups (which implies that ${}^pH(A)$ is finite for every p). If this is so, then the quotient of the order of ${}^0H(A)$ by that of ${}^1H(A)$ is called the *Herbrand quotient* of A.

THEOREM 10.1 *Let A be a $\mathfrak{G}$-module and B a submodule of A. Assume that A, B and A/B are Herbrand modules, and denote by $Q(A)$, $Q(B)$, $Q(A/B)$ their Herbrand quotients. Then we have*

$$Q(A) = Q(B)\,Q(A/B).$$

The exact sequence $0 \to B \to A \to A/B \to 0$ gives rise to an exact sequence

$$\begin{aligned} &{}^0H(B) \xrightarrow{f_1} {}^0H(A) \xrightarrow{f_2} {}^0H(A/B) \xrightarrow{f_3} {}^1H(B) \xrightarrow{f_4} {}^1H(A) \xrightarrow{f_5} {}^1H(A/B) \\ &\quad \xrightarrow{f_6} {}^2H(B) \xrightarrow{f_7} {}^2H(A). \end{aligned}$$

For each finite group H, we denote by $[H]$ the order of H; we denote by F_i the order of the image group of f_i. We then have

$$[{}^0H(A)] = F_1F_2,\ [{}^0H(A/B)] = F_2F_3,\ [{}^1H(B)] = F_3F_4,\ [{}^1H(A)] = F_4F_5,$$
$$[{}^1H(A/B)] = F_5F_6,\ [{}^2H(B)] = F_6F_7.$$

On the other hand, it follows immediately from formula (10.1) above that $F_7 = F_1$. Thus we have

$$[{}^0H(A)][{}^1H(B)][{}^1H(A/B)] = [{}^0H(A/B)][{}^1H(A)][{}^2H(B)].$$

Since $[{}^2H(B)] = [{}^0H(B)]$, theorem 10.1 is proved.

THEOREM 10.2. *Let A be a finite $\mathfrak{G}$-module. Then the Herbrand quotient of A is* 1.

We have a finite sequence $\{0\} = A_0 \subset A_1 \subset \ldots \subset A_h = A$ of submodules of A such that A_i/A_{i-1} is an irreducible $\mathfrak{G}$-module. Making use of theorem 10.1, we see that it suffices to consider the case where A itself is irreducible. Since $A^{\mathfrak{G}}$ is a submodule, we have either $A^{\mathfrak{G}} = A$ or $A^{\mathfrak{G}} = \{0\}$. If $A^{\mathfrak{G}} = A$, $\sigma A = A$, then we have $nA = A$, where n is the order of $\mathfrak{G}$, and, for every $a \in A$, there is a unique $a' \in A$ such that $na' = a$, whence ${}^0H(A) = {}^1H(A) = \{0\}$. If $A^{\mathfrak{G}} = A$, $\sigma A \neq A$, then $\sigma A = \{0\}$ because σA is a $\mathfrak{G}$-module, whence ${}^0H(A) \cong A$, ${}^{-1}H(A) \cong A$ and therefore ${}^1H(A) \cong A$. If $A^{\mathfrak{G}} = \{0\}$, then ${}^0H(A) = \{0\}$; moreover, if s is a generator of $\mathfrak{G}$, then the mapping $a \to (1-s)a$ is a monomorphism, and therefore an epimorphism, since A is finite; it follows that ${}^{-1}H(A) = \{0\}$, whence ${}^1H(A) = \{0\}$.

LEMMA 10.1. *Let $\mathfrak{G}$ be a cyclic group of prime order, and let V be a simple representation space of $\mathfrak{G}$ over the field $\mathbf{Q}$ of rational numbers. Then V is isomorphic either to $\mathbf{Q}$ (considered as a $\mathfrak{G}$-module on which $\mathfrak{G}$ operates trivially) or to $\mathbf{Q}\otimes J$.*

If x is $\neq 0$ in V, then V is spanned by the elements sx, $s \in \mathfrak{G}$. Let t be a generator of $\mathfrak{G}$. Then the polynomials $P[X]$ in a letter X with coefficients in $\mathbf{Q}$ such that $P(t)\cdot x = 0$ form an ideal $\mathfrak{P}$, which contains $X^p - 1$. This ideal is generated by a polynomial P_1 which divides $X^p - 1$. Were $P_1 = P_2P_3$ reducible (with P_2, P_3 of degrees $\neq 0$), then the set of $y \in V$ such that $P_2(t)\cdot y = 0$ would be a subspace and a submodule of V, different from V (since $P_2 \notin \mathfrak{P}$) and from $\{0\}$ (because it would contain $P_3(t)x$); this is impossible, which shows that P_1 is irreducible. Now, the only irreducible factors of $X^p - 1$ in $\mathbf{Q}[X]$ are $X-1$ and $1 + X + \ldots + X^{p-1}$. If $P_1 = k(X-1)$, then $sx = x$, $V \cong \mathbf{Q}$. If not, then $x, tx, \ldots, t^{p-2}x$ form a base of V, and $V \cong \mathbf{Q}\otimes J$ since $\sigma x = 0$.

THEOREM 10.3. *Let $\mathfrak{G}$ be a cyclic group of prime order p, and let A be a finitely generated $\mathfrak{G}$-module. Let α be the rank of A as an additive group, and β that of $A^{\mathfrak{G}}$. Then the Herbrand quotient of A is $p^{(p\beta-\alpha)/(p-1)}$.*

Set $V = \mathbf{Q}\otimes A$; then V is a finite dimensional representation space of $\mathfrak{G}$ over $\mathbf{Q}$. Since every representation of $\mathfrak{G}$ over $\mathbf{Q}$ is semi-simple, it follows from lemma 10.1 that $V = U_1 + \cdots + U_k + W_1 + \cdots + W_l$ (direct), where each U_i

is $\cong \mathbf{Q}$, while each W_j is $\cong \mathbf{Q}\otimes J$. Every element of V is of the form $q\otimes a$, $q\in \mathbf{Q}$, $a\in A$. It follows that we may take elements $u_1, \dots, u_k, w_1, \dots, w_l$ of A such that $\{u_i\}$ is a base of U_i $(1\leqq i\leqq k)$, and, for each $j\leqq l$, $(w_j, tw_j, \dots, t^{p-2}w_j)$ is a base of W_j (where t is a generator of $\mathfrak{G}$). We have $u_i\in A^{\mathfrak{G}}$, $w_j\in A_{\mathfrak{G}}$. Let B be the submodule of A spanned by $u_1, \dots, u_k$ and C_j the submodule spanned by the $t^h w_j$ $(0\leqq h\leqq p-2,\ 1\leqq j\leqq l)$. For any Herbrand module M, we denote by $Q(M)$ the Herbrand quotient of M. We have $B^{\mathfrak{G}}=B$, $\sigma B=pB$, $B_{\mathfrak{G}}=\{0\}$; it follows that ${}^0H(B)$ is of order p^k, and that ${}^{-1}H(B)={}^1H(B)=\{0\}$, whence $Q(B)=p^k$. We have $C^{\mathfrak{G}}=\{0\}$, whence ${}^0H(C)=\{0\}$. It is clear that $C_j\cong J$ under a mapping which assigns $\bar{s}$ to sw_j (for $s\in\mathfrak{G}$). Then ${}^{-1}H(C_j)\cong {}^{-1}H(J)\cong {}^0H(\mathbf{Z})$, which shows that ${}^{-1}H(C_j)$ is of order p; and that ${}^{-1}H(\sum_{j=1}^{l} C_j)$ is of order p^l. Thus we have $Q(\sum_{j=1}^{l} C_j)=p^{-l}$ and

$$Q(B+\sum_{j=1}^{l} C_j)=p^{k-l}.$$

Now, for every $a\in A$, there is a $\nu>0$ such that $\nu a\in B+\sum_{i=1}^{l} C_j$. For, we have $1\otimes a\in \sum_{i=1}^{k} U_i+\sum_{j=1}^{l} W_j$, which shows that there is an integer $\nu_1>0$ such that $1\otimes \nu_1 a=1\otimes a'$, $a'\in B+\sum_{j=1}^{l} C_j$. Since $1\otimes(\nu_1 a-a')=0$, $\nu_1 a-a'$ is of finite order, which proves our assertion. Since A is finitely generated, $A/(B+\sum_{j=1}^{l} C_j)$ is finite, and it follows from theorem 10.1, 10.2 that

$$Q(A)=Q(B+\sum_{j=1}^{l} C_j)=p^{k-l}.$$

On the other hand, it is clear that $\alpha=k+(p-1)l$. Since $\mathbf{Q}\otimes A^{\mathfrak{G}}\subset U_1+\cdots+U_k$, $B\subset A^{\mathfrak{G}}$, we have $\beta=k$. Theorem 10.3 is thereby proved.

§11. LOCAL COHOMOLOGY

Let K be a field which is algebraic of finite degree over the field of p-adic numbers, for some prime p, and let L/K be a normal extension of finite degree, of group $\mathfrak{G}$. We denote by L the group of elements $\neq 0$ of L, which we consider as a $\mathfrak{G}$-module, and by U the group of units of L.

Let $x \to \|x\|$ be a valuation of L which extends the p-adic valuation of the field of rational numbers. There is a number $\alpha > 0$ such that the condition $\|x\| \leqq \alpha$ implies the convergence in L of the series $\sum_{n=0}^{\infty}(n\,!)^{-1}x^n$. For, let $\nu(n)$ be the exponent of p in the prime factor decomposition of $n\,!$, and let $a = \|p\|^{-1}$; then $\|(n\,!)^{-1}x^n\| \leqq a^{\nu(n)}\alpha^n$. Now, an elementary computation gives

$$\nu(n) = \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] \leqq \sum_{k=1}^{\infty}\frac{n}{p^k} = \frac{n}{p-1}.$$

It will therefore be sufficient to take α so that $\|a^{1/p-1}\alpha\| < 1$. Having thus selected α, we set $\exp x = \sum_{n=0}^{\infty}(n\,!)^{-1}x^n$ (for $\|x\| < \alpha$), and we denote by M the additive group of all x such that $\|x\| < \alpha$. It is clear that $\alpha < 1$; the elements of M are therefore integers. Let x, y be in M; then

$$\exp(x+y) = \sum_{n=0}^{\infty}(n\,!)^{-1}\sum_{k+l=n}\frac{n\,!}{k\,!\,l\,!}x^k y^l.$$

The series $\sum_{k=0}^{\infty}\sum_{l=0}^{\infty}(k!)^{-1}(l!)^{-1}x^k y^l$ is convergent, because $(k!)^{-1}(l!)^{-1}x^k y^l$ tends to 0 as (k, l) tends to (∞, ∞). It follows that

$$\exp(x+y) = (\exp x)(\exp y).$$

The mapping $x \to \exp x$ is therefore a homomorphism $M \to L^*$. It is clear that

$$\exp(sx) = s\exp x \quad (s \in \mathfrak{G}).$$

We shall prove that $\exp M$ is a subgroup of finite index of U. If $\|x\| \leqq \alpha$, then $\|x^n\| < \|x\|$ for $n > 1$, whence $\|(\exp x) - 1\| = \|x\| < 1$, which proves that $\exp M \subset U$.

Let $\alpha_1 = \alpha > \alpha_2 > \cdots > \alpha_n > \cdots$ be the values $\neq 0$ and $\leqq \alpha$ taken by the function $x \to \|x\|$, and let U_n be the group of elements $u \in U$ such that $\|u-1\| \leqq \alpha_n$. If $u \in U_n$, then $u \equiv \exp(u-1) \pmod{U_{n+1}}$; it follows that $U_{n+1}(\exp M) \supset U_n$, and therefore, by induction, that $U_1 = U_{n+1}(\exp M)$ for every

n. This means that $\exp M$ is dense in U_1. On the other hand, it is clear that $x \to \exp x$ is a continuous homomorphism; since M is a compact additive group, $\exp M$ is compact and therefore closed, whence $U_1 = \exp M$.

By the theorem of the normal base, there is an $x_0 \in L$ such that the transforms of x_0 by the operations of $\mathfrak{G}$ form a base of L/K; and we may obviously assume that $x_0 \in M$. Let $\mathfrak{o}$ be the ring of integers of K; set $M' = \sum_{s \in \mathfrak{G}} \mathfrak{o}(sx_0)$. Then M' is a submodule of M. Moreover, M/M' is finite. In fact, it is well known that M, which is an ideal in the ring $\mathfrak{O}$ of integers of L, is a finitely generated $\mathfrak{o}$-module. Let $M = \mathfrak{o}x_1 + \dots + \mathfrak{o}x_h$, $x_i \in M$; since the elements $s_i x_0$ from a base of L over K, there is a $\nu \neq 0$ in $\mathfrak{o}$ such that $\nu x_i \in M'$ $(1 \leqq i \leqq h)$, whence $\nu M \subset M'$. On the other hand, νM is an ideal in $\mathfrak{O}$, which shows that $\mathfrak{O}/\nu M$, and therefore also $M/\nu M$, is finite. It follows that M/M' is finite, and the same is true of $(\exp M)/(\exp M')$. Now, it is clear that M' splits as a $\mathfrak{G}$-module; the same is therefore true of $\exp M'$. Thus we have proved:

LEMMA 11.1. *There is a submodule V of the group U of units in L which is of finite index in U and which splits as a $\mathfrak{G}$-module.*

Now we prove:

THEOREM 11.1. *The notation being as above, assume furthermore that $\mathfrak{G}$ is cyclic. Then ${}^0H(\mathfrak{G}\,;L^*)$ is of the same order as $\mathfrak{G}$. If L/K is not ramified, then $H'(\mathfrak{G}\,;U) = \{0\}$, if U is the group of units of L.*

By Hilbert's theorem 90, we have ${}^{-1}H(L^*) = \{0\}$, whence ${}^1H(L^*) = \{0\}$. Let V be a submodule of U with the property stated in Lemma 11.1. Then we have $H'(V) = \{0\}$, and the exact sequence $0 \to V \to L^* \to L^*/V \to 0$ gives rise to isomorphisms ${}^0H(L^*) \cong {}^0H(L^*/V)$, $\{0\} = {}^{-1}H(L^*) \cong {}^{-1}H(L^*/V)$. The group U/V is finite, and $(L^*/V)/(U/V) \cong L^*/U$. If π is an element of L of order 1 for the place of L, then every element of L^* is uniquely representable in the form $\pi^\nu u$, $u \in U$: it follows that $L^*/U \cong \mathbf{Z}$. Since U/V is finite, it follows immediately that L^*/V is an Herbrand module and has the same Herbrand quotient as $\mathbf{Z}$. Since ${}^0H(\mathbf{Z}) \cong \mathbf{Z}/n\mathbf{Z}$, ${}^{-1}H(\mathbf{Z}) = \{0\}$ (where n is the order of $\mathfrak{G}$), the Herbrand quotient of L^*/V is n. Since ${}^{-1}H(L^*/V) = \{0\}$, we see that ${}^0H(L^*/V)$ is of order n; and ${}^0H(L^*)$ is of order n. Now, assume that L/K is not ramified. Then we have ${}^{-1}H(U) = \{0\}$. For, let u be an element of U such that $N_{L/K}u = 1$. Then we may write $u = y^{1-s}$, where s is a generator of $\mathfrak{G}$ and $y \in L^*$.

Since L/K is not ramified, there is a $\pi \in K$ which is of order 1 at the place of L; we may write $y = \pi^k v$, $v \in U$, $k \in \mathbf{Z}$, whence $u = v^{1-s}$, which proves that ${}^{-1}H(U) = \{0\}$. The Herbrand quotient of U being 1, we have also ${}^{0}H(U) = \{0\}$, whence $H'(U) = \{0\}$.

THEOREM 11.2. *The notation being as above, the order of* ${}^{2}H(\mathfrak{G} ; L^*)$ *divides* $[L : K]$.

We proceed by induction on $[L : K]$. The theorem being obvious if $[L : K] = 1$, assume that it is true for all extensions of degrees $< [L : K]$. It is well known that $\mathfrak{G}$ is solvable; thus L contains an overfield L' of K such that L'/K is cyclic of prime degree. Let $\mathfrak{H}$ be the Galois group of L/L'. Since ${}^{1}H(\mathfrak{H} ; L^*) = \{0\}$, the kernel of the restriction mapping from ${}^{2}H(\mathfrak{G} ; L^*)$ to ${}^{2}H(\mathfrak{H} ; L^*)$ is isomorphic to ${}^{2}H(\mathfrak{G}/\mathfrak{H} ; L'^*)$ (theorem 8.2). The order of ${}^{2}H(\mathfrak{H} ; L^*)$ divides $[L : L']$ by the inductive assumption. Since $\mathfrak{G}/\mathfrak{H}$ is cyclic, ${}^{2}H(\mathfrak{G}/\mathfrak{H} ; L'^*)$ is isomorphic to ${}^{0}H(\mathfrak{G}/\mathfrak{H} ; L'^*)$ (theorem 6.3) which is of order $[L' : K]$ by theorem 11.1. It follows that ${}^{2}H(\mathfrak{G} ; L^*)$ has an order which divides $[L : L'][L' : K] = [L : K]$.

Now, let M_K be the set $M \cap \mathfrak{o}$; this is clearly an ideal in $\mathfrak{o}$, whose image under the mapping $x \to \exp x$ is a subgroup V_K of the group of units U_K of K. It is clear that $V_K = V \cap K$ is of finite index in U_K. Let q be any prime number, and Γ a cyclic group of order q which we consider as operating trivially on the various groups under consideration. The group ${}^{0}H(\Gamma ; M_K)$ is M_K/qM_K, and therefore isomorphic to $\mathfrak{o}/q\mathfrak{o}$. If w is the normalized valuation which defines the place of K, then $\mathfrak{o}/q\mathfrak{o}$ is of order $w(q)^{-1}$. The group ${}^{-1}H(\Gamma ; M_K)$ is $\{0\}$ because M_K has no element $\neq 0$ of finite order. Thus, M_K is an Herbrand module for Γ, whose Herbrand quotient is $w(q)^{-1}$. Since U_K/V_K is finite, and $K^*/U_K \cong \mathbf{Z}$, K^*/V_K is an Herbrand module for Γ, whose Herbrand quotient is the same as that of $\mathbf{Z}$, namely q. We conclude that K^* is an Herbrand module for Γ, with $qw(q)^{-1}$ as its Herbrand quotient. We have ${}^{0}H(\Gamma ; K^*) = K^*/(K^*)^q$, while ${}^{-1}H(\Gamma, K^*)$ is the group of elements of order q, i.e. of q-th roots of unity in K^*. Thus we have proved

THEOREM 11.3. *Let K be a finite algebraic extension of the field of p-adic numbers, p being a prime, and let q be any prime. Let K^* be the multiplicative group of numbers $\neq 0$ in K, and $(K^*)^q$ the group of q-th powers of K^*. Then*

$K^*/(K^*)^q$ is a finite group; denoting by w the normalized valuation which defines the place of K, $K^*/(K^*)^q$ is of order $q^2 w(q)^{-1}$ or $qw(q)^{-1}$ according as to whether K contains a primitive q-th root of unity or not.

COROLLARY. *The group $(K^*)^q$ is open in the topology of K^*.*

For we know that U_K, the group of units of K^*, is compact and open. Since $x \to x^q$ is a continuous mapping, U_K^q is compact, and therefore closed. But we have $U_K^q = U_K \cap (K^*)^q$; since $(K^*)^q$ is of finite index in K^*, U_K^q is of finite index in U_K, and therefore open, which proves the corollary.

§12. COHOMOLOGY IN THE IDÈLE GROUP

Let K be a field of algebraic numbers of finite degree, and let L/K be a finite normal extension of K, of Galois group $\mathfrak{G}$. Let J_L be the group of idèles of L, which has a structure of $\mathfrak{G}$-module.

THEOREM 12.1. *Let $\mathfrak{p}$ be a place of K, and let $J_L^{\mathfrak{p}}$ be the group of idèles of L whose components at all places not above $\mathfrak{p}$ are 1. Let $\mathfrak{P}$ be a place of L above $\mathfrak{p}$, and $\mathfrak{G}(\mathfrak{P})$ its decomposition group. Denote by $L_{\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of L and by $L_{\mathfrak{P}}^*$ the group of numbers $\neq 0$ in $L_{\mathfrak{P}}$, which is a $\mathfrak{G}(\mathfrak{P})$-module. Then ${}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}) \cong {}^{p,q}H(\mathfrak{G}(\mathfrak{P})\ ;\ L_{\mathfrak{P}}^*)$ for any $p \geqq 0$, $q \geqq 0$. Let $U_L^{\mathfrak{p}}$ be the group of idèles in $J_L^{\mathfrak{p}}$ whose components at all places above $\mathfrak{p}$ are units; if $\mathfrak{p}$ is not ramified in L, then ${}^{p,q}H(\mathfrak{G}\ ;\ U_L^{\mathfrak{p}}) = \{0\}$.*

Let $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_m$ be the distinct places of L above $\mathfrak{p}$; if $1 \leqq i \leqq m$, let J_L^i be the group of idèles whose components at all places $\neq \mathfrak{P}_i$ are 1. Then, if we write J_L additively, $J_L^{\mathfrak{p}} = \sum_{i=1}^{m} J_L^i$ (direct). We may select representatives s_i for the cosets $s_i\mathfrak{G}(\mathfrak{P})$ of $\mathfrak{G}$ module $\mathfrak{G}(\mathfrak{P})$ in such a way that $s_i J_L^1 = J_L^i$ $(1 \leqq i \leqq m)$, and $s_1 = e$. Set $M = 田 \otimes J_L^1$; then $早(J_L^{\mathfrak{p}}) = \sum_{i=1}^{m} s_i M$ (direct). Let φ be the mapping of M into $早(J_L^{\mathfrak{p}})$ defined by $\varphi(\mu) = \sum_{i=1}^{m} s_i \mu$ $(\mu \in M)$. We have $J_L^1 \cong L_{\mathfrak{P}}^*$, and we may consider M as a $\mathfrak{G}(\mathfrak{P})$-module. Let s be in $\mathfrak{G}$, and $ss_i = s_{\varpi(i,s)} t_i(s)$, $t_i(s) \in \mathfrak{G}(\mathfrak{P})$; then $i \to \varpi(i\ ;\ s)$ is a permutation of $\{1, \ldots, m\}$, and we have $s \cdot \sum_{i=1}^{m} s_i \mu_i = \sum_{i=1}^{m} s_{\varpi(i,s)} t_i(s) \mu_i$ $(\mu_i \in M,\ 1 \leqq i \leqq m)$. Thus, $\sum_{i=1}^{m} s_i \mu_i$ belongs to $(早(J_L^{\mathfrak{p}}))^{\mathfrak{G}}$ if and only if $\mu_{\varpi(i,s)} = t_i(s) \mu_i$ for all $s \in \mathfrak{G}$ and $1 \leqq i \leqq m$. We have $\varpi(1, s_i) = i$, $t_1(s_i) = e$, whence $\mu_i = \mu_1$. If $t \in \mathfrak{G}(\mathfrak{P})$, then $t_1(t) = t$, whence $t\mu_1 = \mu_1$, whence $\mu_1 \in M^{\mathfrak{G}(\mathfrak{P})}$, $\sum_{i=1}^{m} s_i \mu_i = \varphi(\mu_1)$. Conversely, we see immediately that, if $\mu \in M^{\mathfrak{G}(\mathfrak{P})}$, then $\varphi(\mu) \in (早(J_L^{\mathfrak{p}}))^{\mathfrak{G}}$; thus φ induces an isomorphism of $M^{\mathfrak{G}(\mathfrak{P})}$ with $(早(J_L^{\mathfrak{p}}))^{\mathfrak{G}}$. If $\mu \in M$, then $\varphi(\sigma_{\mathfrak{G}(\mathfrak{P})} \mu) = \sum_{i=1}^{m} \sum_{t \in \mathfrak{G}(\mathfrak{P})} s_i t \mu = \sigma_{\mathfrak{G}} \mu$. Conversely, if $\sum_{i=1}^{m} s_i \mu_i$ is any element of $早(J_L^{\mathfrak{p}})$ $(\mu_i \in M,\ 1 \leqq i \leqq m)$, then $\sigma_{\mathfrak{G}}(\sum_{i=1}^{m} s_i \mu_i) = \sum_{i=1}^{m} \sigma \mu_i = \varphi(\sigma_{\mathfrak{G}(\mathfrak{P})} \cdot \sum_{i=1}^{m} \mu_i)$, whence $\varphi(\sigma_{\mathfrak{G}(\mathfrak{P})} M) = \sigma_{\mathfrak{G}} 早(J_L^{\mathfrak{p}})$. It follows that $\mathfrak{N}(\mathfrak{G}(\mathfrak{P})\ ;\ M) \cong H'(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$. But $\mathfrak{N}(\mathfrak{G}(\mathfrak{P}),\ M)$ is isomorphic to $H'(\mathfrak{G}(\mathfrak{P})\ ;\ L_{\mathfrak{P}}^*)$ by theorem 7.2, which proves the first assertion. Let $U_{\mathfrak{P}}$ be the group of units of $L_{\mathfrak{P}}$, and $U'_{\mathfrak{P}}$ the image of $U_{\mathfrak{P}}$

in $\boxplus \otimes J^1_L$. Then $\varphi((U'_{\mathfrak{P}})^{\mathfrak{G}(\mathfrak{P})}) = (\boxplus(\mathfrak{G}\,;\, U^{\mathfrak{p}}_L))^{\mathfrak{G}}$, and we know that $H'(\mathfrak{G}(\mathfrak{P})\,;\, U_{\mathfrak{P}}) = \{0\}$ (theorem 11.1). Theorem 12.1 is thereby proved.

THEOREM 12.2. *Denote by $\lambda_{\mathfrak{p}}$ the homomorphism of J_L onto $J^{\mathfrak{p}}_L$ which assigns to every idèle $\mathfrak{a}$ the ldèle whose $\mathfrak{P}$-component is the same as that of $\mathfrak{a}$ if $\mathfrak{P}$ is above $\mathfrak{p}$, 1 in the opposite case. Let $\lambda^*_{\mathfrak{p}}$ be the corresponding mapping of $H'(\mathfrak{G}\,;\, J_L)$ into $H'(\mathfrak{G}\,;\, J^{\mathfrak{p}}_L)$. In order for an element $\xi \in H'(\mathfrak{G}\,;\, J_L)$ to be 0, it is necessary and sufficient that $\lambda^*_{\mathfrak{p}}(\xi) = 0$ for every place $\mathfrak{p}$ of K.*

The condition is obviously necessary. Assume that it is satisfied. We may obviously assume that $\xi \in {}^{p,q}H(\mathfrak{G}\,;\, J_L)$ for some $p \geqq 0$, $q \geqq 0$. Let $u = \sum_{i=1}^{h} w_i \otimes \mathfrak{a}_i$ be a representative for ξ in ${}^{p,q}\boxplus \otimes J_L$, the w_i's forming a base of the additive group ${}^{p,q}\boxplus$ and the $\mathfrak{a}_i$'s being idèles. Let E be a finite set of places of L containing all places ramified with respect to K and such that, for any place $\mathfrak{P}$ not in E, the $\mathfrak{P}$-components of all idèles $\mathfrak{a}_i$ $(1 \leqq i \leqq h)$ be units. Let E_K be the set of places of K below places in E. Then, if $\mathfrak{p} \notin E_K$, it follows from theorem 12.1 that $\sum_{i=1}^{h} w_i \otimes \lambda_{\mathfrak{p}}(\mathfrak{a}_i)$ may be written in the form $\sigma_{\mathfrak{G}}(\sum_{i=1}^{h} w_i \otimes \mathfrak{b}^{\mathfrak{p}}_i)$, with $\mathfrak{b}^{\mathfrak{p}}_i \in U^{\mathfrak{p}}_L$. If $\mathfrak{p} \in E_K$, then it follows from the assumption that $\lambda^*_{\mathfrak{p}}(\xi) = 0$ that $\sum_{i=1}^{h} w_i \otimes \lambda_{\mathfrak{p}}(\mathfrak{a}_i) = \sigma_{\mathfrak{G}}(\sum_{i=1}^{h} w_i \otimes \mathfrak{b}^{\mathfrak{p}}_i)$, $\mathfrak{b}^{\mathfrak{p}}_i \in J^{\mathfrak{p}}_L$. Since $\mathfrak{b}^{\mathfrak{p}}_i \in U^{\mathfrak{p}}_L$ if $\mathfrak{p} \notin E_K$, there exists, for each i, an idèle $\mathfrak{b}_i$ such that $\lambda_{\mathfrak{p}}(\mathfrak{b}_i) = \mathfrak{b}^{\mathfrak{p}}_i$ for every place $\mathfrak{p}$ of K. It is then clear that $u = \sigma_{\mathfrak{G}}(\sum_{i=1}^{h} w_i \otimes \mathfrak{b}_i)$, which proves the theorem.

Let $\mathfrak{a}$ be an idèle of K, and let $\mathfrak{p}$ be a place of K.

We shall say that $\mathfrak{a}$ is a local norm from L at $\mathfrak{p}$ if, $\mathfrak{P}$ being any place of L above $\mathfrak{p}$, the $\mathfrak{p}$-component $\mathfrak{a}_{\mathfrak{p}}$ of $\mathfrak{a}$ at $\mathfrak{p}$ is the norm from $L_{\mathfrak{P}}$ to $K_{\mathfrak{p}}$ of some element of $L_{\mathfrak{P}}$ (if this condition is satisfied for some $\mathfrak{P}$ above $\mathfrak{p}$, then it is clearly satisfied for any other). As a special case of theorem 12.2, we obtain, making use of theorem 12.1, the following

THEOREM 12.3. *In order for an idèle $\mathfrak{a}$ of K to be the norm (from L to K) of an idèle of L, it is sufficient that $\mathfrak{a}$ be local norm from L at every place $\mathfrak{p}$ of K.*

Moreover, $\mathfrak{a}$ will certainly be local norm at $\mathfrak{p}$ in either one of the following two cases: a) $\mathfrak{p}$ is not ramified in L and $\mathfrak{a}_{\mathfrak{p}}$ is a unit of the completion $K_{\mathfrak{p}}$ of K ; b) $\mathfrak{p}$ splits completely in L (i.e. the decomposition group of any place of L above $\mathfrak{p}$ reduces to $\{e\}$).

THEOREM 12.4. *Let p, q be integers $\geqq 0$; then ${}^{p,q}H(\mathfrak{G}\ ;\ J_L)$ is isomorphic to the direct sum $\sum_{\mathfrak{p}} {}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$, extended to all places of K. Let E be a set of places of L containing all places ramified with respect to K and all infinite places and moreover with the condition that $E^s = E$ for every $s \in \mathfrak{G}$, and E_K the set of places of K below places of E. Denote by J_L^E the group of idèles of L whose components at all places not in E are units. Then ${}^{p,q}H(\mathfrak{G}\ ;\ J_L^E)$ is isomorphic to the direct sum $\sum_{\mathfrak{p}\in E_K} {}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$.*

Using the same notation as in the proof of theorem 12.2, we observe that, for any $\eta \in {}^{p,q}H(J_L)$, we have $\lambda_{\mathfrak{p}}^*(\eta) = 0$ for almost all places $\mathfrak{p}$ of K. For, represent η by an element $\sum_{i=1}^{h} w_i \otimes \mathfrak{c}_i$, $\mathfrak{c}_i \in J_L$. Then there is a finite set F of places of L which contains all places ramified with respect to K and is such that, for each $\mathfrak{Q}$ not in F, the $\mathfrak{Q}$-components of $\mathfrak{c}_1, \ldots, \mathfrak{c}_h$ are units. If $\mathfrak{q}$ is a place of K not below a place of F, then $H'(\mathfrak{G}\ ;\ U_L^{\mathfrak{q}}) = \{0\}$, and conversely, $\lambda_{\mathfrak{q}}^*(\eta) = 0$. It follows that the formula $\Lambda(\eta) = \sum_{\mathfrak{p}} \lambda_{\mathfrak{p}}^*(\eta)$ defines an additive mapping of ${}^{p,q}H(\mathfrak{G}\ ;\ J_L)$ into $\sum_{\mathfrak{p}} {}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$. This mapping is a monomorphism by theorem 12.2. Let $\sum_{\mathfrak{p}} \zeta_{\mathfrak{p}}$ be any element of $\sum_{\mathfrak{p}} {}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$. For each $\mathfrak{p}$ select a representative $v_{\mathfrak{p}} = \sum_{i=1}^{h} w_i \otimes \mathfrak{z}_i^{(\mathfrak{p})}$ of $\zeta_{\mathfrak{p}}$ in $({}^{p,q}\boxplus \otimes J_L^{\mathfrak{p}})^{\mathfrak{G}}$; then we may assume that $\mathfrak{z}_i^{(\mathfrak{p})} = 1$ $(1 \leqq i \leqq h)$ for almost all $\mathfrak{p}$, since $\zeta_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$ (it should be remembered that 1 becomes 0 if we write $J_L^{\mathfrak{p}}$ additively!). It follows that there exist idèles $\mathfrak{z}_i$ such that $\lambda_{\mathfrak{p}}(\mathfrak{z}_i) = \mathfrak{z}_i^{\mathfrak{p}}$ for all $\mathfrak{p}$; it is clear that $\sum {}^{p,q}\boxplus \otimes \mathfrak{z}_i$ is in $(\boxplus(J_L))^{\mathfrak{G}}$ and represents a class ζ such that $\lambda_{\mathfrak{p}}^*(\zeta) = \zeta_{\mathfrak{p}}$ for all $\mathfrak{p}$, which proves that Λ is an isomorphism. Let $\lambda_{\mathfrak{p}}^{**}$ be the mapping ${}^{p,q}H(\mathfrak{G}\ ;\ J_L^E) \to {}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ induced by $\lambda_{\mathfrak{p}}$, and let Λ' be the mapping $\eta' \to \sum_{\mathfrak{p}\in E} \lambda_{\mathfrak{p}}^{**}(\eta')$ of ${}^{p,q}H(\mathfrak{G}\ ;\ J_L^E)$ into the direct sum $\sum_{\mathfrak{p}\in E} {}^{p,q}H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$. Assume first that $\Lambda'(\eta') = 0$. If $v' = \sum_{i=1}^{h} w_i \otimes \mathfrak{c}_i'$, $\mathfrak{c}_i' \in J_L^E$ is a representative of η', then, for $\mathfrak{p} \notin E$, $\sum_{i=1}^{h} w_i \otimes \lambda_{\mathfrak{p}}(\mathfrak{c}_i')$ is of the form $\sigma(\sum_{i=1}^{h} w_i \otimes \mathfrak{u}_i^{\mathfrak{p}})$, with $\mathfrak{u}_i^{\mathfrak{p}} \in U_L^{\mathfrak{p}}$, in virtue of theorem 12.1. If $\mathfrak{p} \in E$, then $\sum_{i=1}^{h} w_i \otimes \lambda_{\mathfrak{p}}(\mathfrak{c}_i') = \sigma(\sum_{i=1}^{h} w_i \otimes \mathfrak{u}_i^{\mathfrak{p}})$, with $\mathfrak{u}_i^{\mathfrak{p}} \in J_L^{\mathfrak{p}}$, since $\lambda_{\mathfrak{p}}^{**}(\eta') = 0$. There are idèles $\mathfrak{u}_i$ such that $\lambda_{\mathfrak{p}}(\mathfrak{u}_i) = \mathfrak{u}_i^{\mathfrak{p}}$ for all $\mathfrak{p}$, and these idèles are in J_L^E; we have $\sum_{i=1}^{h} w_i \otimes \mathfrak{c}_i' = \sigma(\sum_{i=1}^{h} w_i \otimes \mathfrak{u}_i)$, whence $\eta' = 0$, and Λ' is a monomorphism. We see immediately that it is also an epimorphism, which proves the second assertion of theorem 12.4.

COROLLARY. *The notation being as in theorem* 12.4, *we have* ${}^1H(\mathfrak{G}\ ;\ J_L^F) = {}^1H(\mathfrak{G}\ ;\ J_L) = \{0\}$.

In fact, ${}^1H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}) \cong {}^1H(\mathfrak{G}(\mathfrak{P}), L_{\mathfrak{P}}^*)$ if $\mathfrak{P}$ is a place above $\mathfrak{p}$. Our assertion therefore follows from corollary 2 to theorem 6.1.

§13. THE FIRST INEQUALITY

THEOREM 13.1. *Let K be a field of algebraic numbers of finite degree and L/K a cyclic extension of K of prime degree p, of Galois group $\mathfrak{G}$. Let $\mathfrak{C}_L$ be the group of idèle classes of L, considered as a $\mathfrak{G}$-module. Then $\mathfrak{C}_L$ is an Herbrand module, whose quotient of Herbrand is p.*

Let E be a finite set of places of L which satisfies the following conditions: a) E contains all infinite places and all places which are ramified with respect to K: b) every idèle class of L and K contains an idèle whose components at all places not in E are units. c) $E^s = E$ for every $s \in \mathfrak{G}$. Let P_L be the group of principal idèles and $P_L^F = J_L^F \cap P_L$. Then we have

$$\mathfrak{C}_L \cong J_L^E / P_L^F.$$

We shall denote by N the number of places in E and by n the number of places of K below the places of E. Above a place of K, there lies either 1 or p places of L; let n_1 be the number of places of K above which there lies exactly one place of E; then $N = n_1 + p(n - n_1)$. We use the notation of the last section. If $\mathfrak{p}$ is a place of K above which lie p distinct places of L, then, clearly, $^0H(J_L^{\mathfrak{p}}) = \{0\}$ (by theorem 12.1). If $\mathfrak{p}$ is a finite place of K above which there lies only one place of L, then it follows from theorems 11.1 and 12.1 that $^0H(J_L^{\mathfrak{p}})$ is of order p. The same is true if $\mathfrak{p}$ is infinite instead of being finite. For, we must then have $p = 2$, $\mathfrak{p}$ is real and the place $\mathfrak{P}$ of L above $\mathfrak{p}$ is imaginary. The field $K_{\mathfrak{p}}$ is the field of real numbers, while $L_{\mathfrak{P}}$ is the field of complex numbers, and only the real numbers >0 are norms (from $L_{\mathfrak{P}}$ to $K_{\mathfrak{p}}$) of complex numbers $\neq 0$. making use of the scholium to theorem 12.3, we see that $^0H(J_L^F)$ is a finite group of order p^{n_1}. On the other hand, we have $^{-1}H(J_L^F) = \{0\}$ (corollary to theorem 12.4).

We know that the group P_L^F is a finitely generated group of rank $N-1$. Let P_K be the group of principal idèles of K, and $P_K^F = P_L^F \cap P_K = (P_L^F)^{\mathfrak{G}}$; then we know that P_K^E is a finitely generated group of rank $n-1$. Therefore, it follows from theorem 10.3 that P_L^E is an Herbrand module, whose Herbrand quotient is $p^{(p(n-1)-N+1)/(p-1)} = p^{n_1-1}$.

We have ${}^{-1}H(P_L^F)=\{0\}$. For, let $x\in P_L^F$ be such that $N_{L/K}x=1$. Then we may write $x=y^{1-s}$, $y\in L^{\cdot}$, where s is a generator of $\mathfrak{G}$. Let ι be the canonical isomorphism of J_K with $J_L^{\mathfrak{G}}$. If $\mathfrak{P}$ is a place of L not in E, then the order of sy at $\mathfrak{P}$ is the same as that of y, since $y^{1-s}\in P_L^F$. It follows that the orders of y at all places conjugate of $\mathfrak{P}$ with respect to K are equal. On the other hand, $\mathfrak{P}$ is not ramified with respect to K from which it follows that there is an idèle $u\in J_K$ such that $\iota(u)$ is of order 1 at $\mathfrak{P}$; we may furthermore assume that the components of u at all places of K not below $\mathfrak{P}$ are 1. We conclude easily that $y=\iota(v)v'$, where v is an idèle of K and $v'\in J_L^F$. We may write $v=zv_1$, $z\in P_K$, $v_1\in J_K^F$, whence $y=zv''$, $v''\in J_L^F$. It follows that $v''\in J_L^F\cap P_L=P_L^F$ and $x=(v'')^{1-s}$, which proves our assertion.

It follows that ${}^0H(P_L^F)$ is of order p^{n_1-1}. To the isomorphism $\mathfrak{C}\cong J_L^F/P_L^F$, there corresponds an exact sequence

$$ {}^{-1}H(J_L^F)\to {}^{-1}H(\mathfrak{C})\to {}^0H(P_L^F)\to {}^0H(J_L^F)\to {}^0H(\mathfrak{C})\to {}^1H(P_L^F); $$

it follows immediately that ${}^{-1}H(\mathfrak{C})$ and ${}^0H(\mathfrak{C})$ are finite groups. By theorem 10.1, the Herbrand quotient of $\mathfrak{C}$ is

$$ p^{n_1}/p^{n_1-1}=p. $$

COROLLARY 1. *The group ${}^0H(\mathfrak{C})$ is of order $\equiv 0$ (mod p), and is of order p if and only if ${}^{-1}H(\mathfrak{C})=\{0\}$.*

COROLLARY 2. *There are infinitely many places of K which do not split in L.*

Assume the contrary, and let F be the set of places of K which do not split in L. Let $\mathfrak{A}$ be any idèle class of K, and $\mathfrak{a}$ an idèle in $\mathfrak{A}$. If $\mathfrak{p}\in F$, then K is everywhere dense in its $\mathfrak{p}$-adic completion $K\mathfrak{p}$. Since $(K_{\mathfrak{p}}^*)^p$ is open in $K_{\mathfrak{p}}^*$ (corollary to theorem 11.3), there is a number $x_{\mathfrak{p}}\neq 0$ in K such that $x_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}\in(K_{\mathfrak{p}}^*)^p$.

Morover, $x_{\mathfrak{p}}(K_{\mathfrak{p}}^*)^p$ being a neighbourhood of $x_{\mathfrak{p}}$ in $K_{\mathfrak{p}}$, it follows from the theorem of independence of valuations that there is a number $x\neq 0$ in K such that $x^{-1}x_{\mathfrak{p}}\in(K_{\mathfrak{p}}^*)^p$ for all $\mathfrak{p}\in F$. Set $\mathfrak{b}=x^{-1}\mathfrak{a}$; then $\mathfrak{b}$ belongs to $\mathfrak{A}$. For each $\mathfrak{p}\in F$, $\mathfrak{b}_{\mathfrak{p}}$ is a local norm from L because $\mathfrak{b}_{\mathfrak{p}}\in(K_{\mathfrak{p}}^*)^p$; if $\mathfrak{q}$ is a place of K not in F, then $\mathfrak{b}_{\mathfrak{q}}$ is a local norm of L because $\mathfrak{q}$ splits in L. It follows that $\mathfrak{b}\in N_{L/K}J_L$ (theorem 12.3), whence $\mathfrak{A}\in N_{L/K}\mathfrak{C}_L$ and $N_{L/K}\mathfrak{C}_L=\mathfrak{C}_K$, in contradiction with the fact that ${}^0H(\mathfrak{G}\,;\,\mathfrak{C}_L)$ is of order $\equiv 0$ (mod p).

§14. THE SECOND INEQUALITY

Let K be a field of algebraic numbers of finite degree, and let L/K be a cyclic extension of prime degree p, of group $\mathfrak{G}$. Then we propose to prove that ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ is of order exactly p. However, for technical reasons, we shall have to assume that K contains a primitive p-th root of unity. The group ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ is $\mathfrak{C}_K/N_{L/K}\mathfrak{C}_L$; we know already that its order is $\equiv 0 \pmod{p}$ (corollary 1 to theorem 13.1); it will therefore be sufficient to show that $N_{L/K}\mathfrak{C}_L$ is of index $\leqq p$ in $\mathfrak{C}_K$. Since L/K is cyclic of degree p, we may write

$$L = K(x_0^{1/p}),$$

where x_0 is a number $\neq 0$ in K. We denote by E a finite set of places of K which satisfies the following conditions:

a) E contains all infinite places of K and all places of K above the prime number p.

b) for any place $\mathfrak{p}$ not in E, x_0 is a unit in $K_\mathfrak{p}$ (the $\mathfrak{p}$-adic completion of K):

c) any class of idèles in K is represented by an idèle in J_K^F (where J_K^F is the group of idèles $\mathfrak{a}$ such that, for each place $\mathfrak{p}$ not in E, the $\mathfrak{p}$-component of $\mathfrak{a}$ is a unit in $K_\mathfrak{p}$).

It is clear that there exist set E with these properties. We denote by P_K the group of numbers $\neq 0$ in K, and we set $P_K^F = P_K \cap J_K^F$. If $\mathfrak{p}$ is a place of K not in E, then $\mathfrak{p}$ is not ramified in $K(x^{1/p})$. For, if x is not a p-th power in $K_\mathfrak{p}$, then the different of $x^{1/p}$ with respect to $K_\mathfrak{p}$ is px^{p-1}, and is a unit, because x is a unit in $K_\mathfrak{p}$ by assumption, and p is a unit in $K_\mathfrak{p}$ by condition a) above. Since $x_0 \in P_K^F$, it follows that no place outside E is ramified in L.

Moreover, if $x \in P_K^F$ and if $\mathfrak{p}$ is a place not in E, then every unit in $K_\mathfrak{p}$ is the norm from $K_\mathfrak{p}(x^{1/p})$ to $K_\mathfrak{p}$ of a unit of $K_\mathfrak{p}(x^{1/p})$ (by theorem 11.1). It follows immediately that the group U_K^F of idèles of K whose components at all places in E are 1 while their components at any place $\mathfrak{p} \notin E$ are units of $K_\mathfrak{p}$ is contained in $N_{L/K}J_L$. It is clear that the group J_K^p of p-th powers of idèles of K is contained in $N_{L/K}J_L$. Finally, let $\mathfrak{q}$ be a finite place of K not in E which splits in L (i.e. there are p distinct places of L above $\mathfrak{q}$). If $\mathfrak{u}_\mathfrak{q}$ is an idèle whose $\mathfrak{q}$-component is of order 1 while its other components are 1, then $\mathfrak{u}_\mathfrak{q} \in N_{L/K}J_L$.

We shall denote by $\mathfrak{E}$ the subgroup of $\mathfrak{C}_K$ generated by the classes of idèles belonging to U_K^Γ or to J_K^p, and by $\mathfrak{F}$ the group generated by $\mathfrak{E}$ and by the classes of the idèles $\mathfrak{u}_\mathfrak{q}$ defined above, for all finite places $\mathfrak{q}$ which split in L. Then $\mathfrak{F}\subset N_{L/K}\mathfrak{C}_L$, and we shall prove that $\mathfrak{F}$ is of index $\leqq p$ in $\mathfrak{C}_L$.

We shall compute the order of $\mathfrak{E}$. In order to do this, we shall first estimate the order of the group $J_K^\Gamma/J_K^\Gamma\cap(J_K^p\cdot U_K^\Gamma)=J_K^\Gamma/(J_K^\Gamma)^pU_K^\Gamma$. If $\mathfrak{a}\in J_K^\Gamma$, let $\varphi(\mathfrak{a})$ be the element of the group $\prod_{\mathfrak{p}\in\Gamma}K_\mathfrak{p}^*$ whose coordinates are the components of $\mathfrak{a}$ at the places $\mathfrak{p}\in E$. Then φ is an epimorphism of kernel U_K^Γ, and $\varphi((J_K^\Gamma)^pU_K^\Gamma)$ $=\prod_{\mathfrak{p}\in\Gamma}(K_\mathfrak{p}^*)^p$, whence

$$J_K^\Gamma/(J_K^F)^pU_K^F\cong\prod_{\mathfrak{p}\in\Gamma}K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^p.$$

If $\mathfrak{p}$ is finite, then we know that $K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^p$ is of order $p^2\|p\|_\mathfrak{p}^{-1}$, where $\|p\|_\mathfrak{p}$ is the value at p of the normalized valuation attached to $\mathfrak{p}$. Let $\mathbf{Q}$ be the field of rationals, and n the degree of $K/\mathbf{Q}$. Since all places above p are in E, we have

$$\prod_{\mathfrak{p}\in\Gamma,\ \mathfrak{p}\text{ finite}}\|p\|_\mathfrak{p}^{-1}=|N_{K/\mathbf{Q}}p|=p^n,$$

If $\mathfrak{p}$ is infinite, then $[K_\mathfrak{p}^*:(K_\mathfrak{p}^*)^p]$ is 1 if $\mathfrak{p}$ is imaginary. Now, $\mathfrak{p}$ can only be real if $p=2$, since K contains a primitive p-th root of unity; if $\mathfrak{p}$ is real, $[K_\mathfrak{p}^*:(K_\mathfrak{p}^*)^2]=2$. Let N be the number of all places in E and r the number of real infinite places of K. Then the number of finite places in E is $N-r$ $-\frac{1}{2}(n-r)$, and we have

$$[J_K^F:(J_K^F)^pU_K^F]=p^{2(N-r)-(n-r)}p^np^r=p^{2N}.$$

Every idèle class is represented by an idèle in J_K^F (by c) above), and $\mathfrak{E}$ is the group of classes represented by elements of $(J_K^F)^pU_K^F$; for, since $J_K=P_KJ_K^\Gamma$, we have $J_K^pU_K^F\subset P_K(J_K^F)^pU_K^E$. If an idèle $\mathfrak{a}\in J_K^F$ represents a class belonging to $\mathfrak{E}$, then there is an $\mathfrak{a}'\in(J_K^F)^pU_K^E$ such that $\mathfrak{a}=x\mathfrak{a}'$, $x\in P_K$; but $x=\mathfrak{a}\mathfrak{a}'^{-1}$ then belongs to P_K^F. Every element of $(P_K^F)^p$ belongs to $(J_K^F)^pU_K^F$; let

$$\delta=[P_K^F\cap(J_K^F)^pU_K^F:(P_K^F)^p].$$

Then the number of cosets of J_K^F represented by elements of P_K^F is $\delta^{-1}[P_K^E:(P_K^E)^p]$. Now, P_K^E is of rank $N-1$; it is the product of a free abelian group of rank $N-1$ by a finite group F consisting of all roots of unity in K.

Thus, F is cyclic of order $\equiv 0 \pmod{p}$, whence $[P_K^F : (P_K^F)^p] = p^N$ and

$$[\mathfrak{C}_K : \mathfrak{E}] = p^{2N}(\delta^{-1}p^N)^{-1} = \delta p^N.$$

We shall prove in a moment that $\delta = 1$.

Let T be the field obtained by adjunction to K of the p-th roots of all elements in P_K^F. Then we know that $L \subset T$, that no place of K outside E is ramified in T and that $[T : K] = [P_K^F : (P_K^F)^p] = p^N$; moreover, the Galois group of T/K is of type $(p, \ldots, p)$.

The Galois group of T/K is generated by N elements $s_1, \ldots, s_N$ of order p and we may assume that the Galois group of T/L is generated by $s_1, \ldots, s_{N-1}$; let T_i be the field of fixed elements of s_i $(1 \leqq i \leqq N)$. Then we have $K \subset T_i$ and T/T_i is cyclic of degree p. It follows from corollary 2 to theorem 13.1 that there exists for each i a place $\mathfrak{Q}_i$ of T_i which does not split in T and such that the place $\mathfrak{q}_i$ of K below $\mathfrak{Q}_i$ is not in E. We shall prove that, if Z/K is a cyclic extension of degree p such that the places of E all split in Z, then it is impossible that the places of K ramified in Z should occur only among $\mathfrak{q}_1, \ldots, \mathfrak{q}_N$. Assume the contrary. Let V_i be the group of units in the $\mathfrak{q}_i$-adic completion of K. For every $x \in P_K^F$, denote by $\mu_i(x)$ the residue class of the element $x \in V_i$ modulo V_i^p, and by $\mu(x)$ the element $(\mu_1(x), \ldots, \mu_N(x))$ of the group $\prod_{i=1}^{N} V_i/V_i^p$. If $\mu(x) = 1$, then x is a p-th power in each one of the fields $K_{\mathfrak{q}_i}$, which mean that $\mathfrak{q}_1, \ldots, \mathfrak{q}_N$ all split in $K(x^{1/p})$. But the decomposition group of $\mathfrak{q}_i$ in T contains s_i and is cyclic, because $\mathfrak{q}_i$, not being in E, is not ramified in T. This group is therefore generated by s_i, and the decomposition field of $\mathfrak{q}_i$ in T is T_i. Since $\mathfrak{q}_i$ splits in $K(x^{1/p})$, we have $K(x^{1/p}) \subset T_i$ $(1 \leqq i \leqq N)$. Since $s_1, \ldots, s_N$ generate the Galois group of T/K, this implies that $K(x^{1/p}) = K$, i.e. $x \in (P_K^F)^p$. The index of $(P_K^F)^p$ in P_K^F being p^N, we see that $\mu(P_K^F)$ is a group of order p^N. On the other hand, since $\mathfrak{q}_i$ is not above p, $[K_{\mathfrak{q}_i}^* : K_{\mathfrak{q}_i}^{*p}] = p^2$ by theorem 11.3. We have obviously $[K_{\mathfrak{q}_i}^* : V_i(K_{\mathfrak{q}_i}^*)^p] = p$; it follows that $V_i(K_{\mathfrak{q}_i}^*)^p/(K_{\mathfrak{q}_i}^*)^p$ is a group of order p. This group is isomorphic to $V_i/V_i \cap (K_{\mathfrak{q}_i}^*)^p = V_i/V_i^p$, which proves that $[V_i : V_i^p] = p$ and that $\prod_{i=1}^{N}[V_i : V_i^p] = p^N$. Thus, $\mu(P_K^E) = \prod_{i=1}^{N} V_i/V_i^p$. Now, let $\mathfrak{A}$ be any idèle class of K; then $\mathfrak{A}$ may be represented by an idèle $\mathfrak{a}_1 \in J_K^F$. Let $\bar{\mathfrak{a}}^{(i)}$ be the residue class modulo V_i^p of the $\mathfrak{q}_i$-component of $\mathfrak{a}_1$ $(1 \leqq i \leqq N)$; then there is an $x \in P_K^E$ such that $\mu_i(x) = \bar{\mathfrak{a}}^{(i)}$ $(1 \leqq i \leqq N)$. We have $\mathfrak{a} = x^{-1}\mathfrak{a}_1 \in \mathfrak{A}$ and $\mathfrak{a}_{\mathfrak{q}_i} \in V_i^p$ $(1 \leqq i \leqq N)$. If $\mathfrak{p} \in E$, then $\mathfrak{a}$ is local norm at $\mathfrak{p}$ from

Z because $\mathfrak{p}$ splits in Z. If $\mathfrak{q}$ is a place of K not in E but distinct from $\mathfrak{q}_1, \ldots, \mathfrak{q}_N$, then $\mathfrak{a}$ is local norm from Z at $\mathfrak{q}$ because $\mathfrak{a}_\mathfrak{q}$ is a unit and $\mathfrak{q}$ is not ramified in Z. Finally, $\mathfrak{a}$ is a local norm of Z at $\mathfrak{q}_i$ because $\mathfrak{a}_{\mathfrak{q}_i} \in V_i^p$. It follows from theorem 12.3 that $\mathfrak{a} \in N_{Z/K}J_Z$, whence $\mathfrak{A} \in N_{Z/K}\mathfrak{C}_Z$ and $\mathfrak{C}_K = N_{Z/K}\mathfrak{C}_Z$. But we know that $N_{Z/K}\mathfrak{C}_Z$ is of index $\equiv 0 \pmod{p}$ in $\mathfrak{C}_K$ (corollary 1 to theorem 13.1); we have therefore arrived at an impossibility.

Let $\mathfrak{u}_i$ be an idèle of K whose $\mathfrak{q}_i$-component is of order 1 at $\mathfrak{q}_i$ but whose other components are all 1, and let $\mathfrak{U}_i$ be the idèle class of $\mathfrak{u}_i$. We shall prove that the condition

$$\prod_{i=1}^{N} \mathfrak{U}_i^{e(i)} \in \mathfrak{E} \quad (e(i) \in \mathbf{Z})$$

implies $e(i) \equiv 0 \pmod{p}$ $(1 \leqq i \leqq N)$. In fact, assuming this condition satisfied, we have

$$\prod_{i=1}^{N} \mathfrak{u}_i^{e(i)} = z\mathfrak{a}^p\mathfrak{b} \quad z \in P_K,\ \mathfrak{a} \in J_K,\ \mathfrak{b} \in U_K^F.$$

Let $Z = K(z^{1/p})$. If $\mathfrak{p} \in E$, then we have $z = (\mathfrak{a}_\mathfrak{p}^{-1})^p \in (K_\mathfrak{p}^*)^p$, which shows that $\mathfrak{p}$ splits in Z. If $\mathfrak{q} \notin E$, $\mathfrak{q} \neq \mathfrak{q}_1, \ldots, \mathfrak{q}_N$, then we have $z = (\mathfrak{a}_\mathfrak{q}^{-1})^p \mathfrak{b}_\mathfrak{q}^{-1}$, and $K_\mathfrak{q}(z^{1/p}) = K_\mathfrak{q}(\mathfrak{b}_\mathfrak{q}^{1/p})$. But $\mathfrak{b}_\mathfrak{q}$ is a unit in $K_\mathfrak{q}$; since $\mathfrak{q}$ is not above p, we conclude that $K_\mathfrak{q}(z^{1/p})$ is not ramified over $K_\mathfrak{q}$, i.e. that $\mathfrak{q}$ is not ramified in Z. By the result derived above, we have $Z = K$, and z is a p-th power in K. But the order of z at $\mathfrak{q}_i$ is clearly $\equiv e(i) \pmod{p}$; it follows that $e(i) \equiv 0 \pmod{p}$, which proves our assertion. Moreover, the argument actually shows that the condition $z \in (J_K)^p U_K^F$ implies that z is a p-th power. This means that the number δ introduced above is 1, and that

$$\boxed{[\mathfrak{C}_K : \mathfrak{E}] = p^N} \tag{14.1}$$

Now, if $i \leqq N-1$, then $L \subset T_i$ and $\mathfrak{q}_i$ splits in L, whence $\mathfrak{U}_i \in N_{L/K}\mathfrak{C}_L$. It follows from our result that the group $\mathfrak{E}'$ generated by $\mathfrak{E}, \mathfrak{U}_1, \ldots, \mathfrak{U}_{N-1}$ contains $\mathfrak{E}$ as a subgroup of index p^{N-1}. Thus, $[\mathfrak{C}_K : N_{L/K}\mathfrak{C}_L]$, which divides $[\mathfrak{C}_K : \mathfrak{E}']$, is $\leqq p$, and our assertion is established.

THEOREM 14.1. *Let L/K be any normal extension of finite degree of the field K of algebraic numbers, and let $\mathfrak{G}$ be the Galois group of L/K. Then we have* ${}^1H(\mathfrak{G}\,;\,\mathfrak{C}_L) = \{0\}$.

We proceed by induction on the degree n of L/K. If $n=1$, the statement is obvious. Assume that $n>1$ and that the theorem is true for all extensions of degree $<n$. If $\mathfrak{G}$ is not of prime power order, then we have ${}^1H(\mathfrak{H}\ ;\ \mathfrak{C}_L)=\{0\}$ for every Sylow subgroup $\mathfrak{H}$ of $\mathfrak{G}$, and our assertion follows from the corollary to theorem 7.3. If $\mathfrak{G}$ is of prime power order. then it has a normal subgroup $\mathfrak{H}$ of prime index p, and it follows that ${}^1H(\mathfrak{G}\ ;\ \mathfrak{C}_L)\cong{}^1H(\mathfrak{G}/\mathfrak{H}\ ;\ (\mathfrak{C}_L)^{\mathfrak{H}})$ (theorem 8.1). If M is the field of invariants of $\mathfrak{H}$, then $(\mathfrak{C}_L)^{\mathfrak{H}}\cong\mathfrak{C}_M$, and M/K is of prime degree p. If $p<n$, then ${}^1H(\mathfrak{G}/\mathfrak{H}\ ;\ (\mathfrak{C}_L)^{\mathfrak{H}})=\{0\}$, and our assertion is true. Assume now that $n=p$; denote by K' and L' the fields obtained from K, L by adjunction of the p-th roots of unity, by $\mathfrak{G}'$ the Galois group of L'/K' and by $\mathfrak{K}$ that of L'/K. We have just proved that ${}^0H(\mathfrak{G}'\ ;\ \mathfrak{C}_{L'})$ is of order $\leqq p$; by corollary 1 to theorem 13.1, this implies that ${}^1H(\mathfrak{G}'\ ;\ \mathfrak{C}_{L'})=\{0\}$, and therefore, by theorem 8.1, that ${}^1H(\mathfrak{K}\ ;\ \mathfrak{C}_{L'})\cong{}^1H(\mathfrak{K}/\mathfrak{G}'\ ;\ \mathfrak{C}_{K'})$, where $\mathfrak{K}/\mathfrak{G}'$ is identified to the Galois group of K'/K. Now, $[K':K]$ divides $p-1$; it follows that ${}^1H(\mathfrak{K}/\mathfrak{G}'\ ;\ \mathfrak{C}_{K'})=\{0\}$ by our inductive assumption; thus we have ${}^1H(\mathfrak{K}\ ;\ \mathfrak{C}_{L'})=\{0\}$. The group $\mathfrak{G}$ is isomorphic to $\mathfrak{K}/\mathfrak{L}$, where $\mathfrak{L}$ is the Galois group of L'/L; therefore it follows from theorem 8.1, that ${}^1H(\mathfrak{G}\ ;\ \mathfrak{C}_L)=\{0\}$.

THEOREM 14.2. *Let L/K be any finite normal extension of the field K of algebraic numbers and $\mathfrak{G}$ its Galois group. Then the order of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ divides the degree $[L:K]$ of L/K.*

We proceed by induction on $[L:K]=n$. The theorem is obvious if $n=1$. Assume that $n>1$ and that the theorem is true for all extensions of degrees $<n$. Assume first that n is not a prime power. Let p be any prime divisor of n and $\mathfrak{H}$ a Sylow subgroup of $\mathfrak{G}$ whose order is a power of p. Let ${}^2H_p(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ be the group of elements of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ whose orders are powers of p. Then the restriction map r of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ to ${}^2H(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ maps ${}^2H_p(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ monomorphically. For, let n_p be the contribution of n to p. If ξ belongs to the kernel of r, then we have $(n/n_p)\xi=0$ (theorem 8.1). But n/n_p is prime to p; thus, if $\xi\in{}^2H_p(\mathfrak{G}:\mathfrak{C}_L)$, the condition $(n/n_p)\xi=0$ implies $\xi=0$. We conclude that ${}^2H_p(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ is of an order which divides n_p. This being true for any prime divisor of n, it is clear that the order of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C})$ divides n. Now assume that n is a power of a prime p. Then $\mathfrak{G}$ has a normal subgroup $\mathfrak{H}$ of index p, and the order of ${}^2H(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ divides n/p by the inductive assumption. On the other hand, since ${}^1H(\mathfrak{H}\ ;\ \mathfrak{C}_L)=\{0\}$ (theorem 14.1), the kernel of the

restriction map of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ to ${}^2H(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ is isomorphic to ${}^2H(\mathfrak{G}/\mathfrak{H}\ ;\ (\mathfrak{C}_L)^{\mathfrak{H}})$ $\cong {}^2H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_M)$, if M is the field of invariants of $\mathfrak{H}$. But $\mathfrak{G}/\mathfrak{H}$ is cyclic; it follows that ${}^2H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_M) \cong {}^0H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_M)$. Since ${}^{-1}H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_M) \cong {}^1H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_M)$ $=\{0\}$ (theorem 14.1), it follows from corollary 1 to theorem 13.1 that ${}^2H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_M)$ is of order p. We conclude that the order of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ divides $\frac{n}{p}\cdot p = n$.

§15. THE SYMBOL $\langle \mathfrak{A}, \chi \rangle$

Let K be a field of algebraic numbers of finite degree, and let L/K be a finite normal extension of K whose Galois group we denote by $\mathfrak{G}$. Then we have associated to every character χ of the group $\mathfrak{G}$ an element $\zeta(\chi)$ of ${}^2H(\mathbf{Z})$ (cf. §6). This element is defined as follows. For each $s \in \mathfrak{G}$, let $\chi_0(s)$ be a real number whose residue class (mod $\mathbf{Z}$) is $\chi(s)$; set

$$c_\chi(s, t) = \chi_0(s^{-1}t) - \chi_0(s^{-1}) - \chi_0(t) \in \mathbf{Z};$$

then $\zeta(\chi)$ is represented by the element

$$\sum_{s,\, t \in \mathfrak{G}} c_\chi(s, t) \bar{s} \otimes \bar{t} \in J_2[\mathfrak{G}].$$

Now, let $\mathfrak{A}$ be any element of $\mathfrak{C}_K$. We have ${}^0H(\mathfrak{G}\,;\,\mathfrak{C}_K) = \mathfrak{C}_K / N_{L/K}\mathfrak{C}_L$; let α be the class of $\mathfrak{A}$ module $N_{L/K}\mathfrak{C}_L$. We set

$$\langle \mathfrak{A}, \chi \rangle = M^{\mathfrak{M}}_{\mathfrak{C}_L, \mathbf{Z}}(\alpha \otimes \zeta(\chi)) \in {}^2H(\mathfrak{G}\,;\,\mathfrak{C}_K)$$

Then we have obviously,

(15.1) $$\langle \mathfrak{A}\mathfrak{A}', \chi \rangle = \langle \mathfrak{A}, \chi \rangle + \langle \mathfrak{A}', \chi \rangle \quad (\mathfrak{A}, \mathfrak{A}' \in \mathfrak{C}_K)$$

(15.2) $$\langle \mathfrak{A}, \chi + \chi' \rangle = \langle \mathfrak{A}, \chi \rangle + \langle \mathfrak{A}, \chi' \rangle \quad (\chi, \chi' \in \mathrm{Char}\,\mathfrak{G}).$$

Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$; we shall denote by $r_\mathfrak{H}$ the restriction map relative to this subgroup $\mathfrak{H}$. On the other hand, the restriction to $\mathfrak{H}$ of a character χ of $\mathfrak{G}$ is a character of $\mathfrak{H}$, which we shall denote by $r_\mathfrak{H}\chi$. We shall prove the formula

(15.3) $$\langle \mathfrak{A}, r_\mathfrak{H}\chi \rangle = r_\mathfrak{H}\langle \mathfrak{A}, \chi \rangle.$$

The notation being as above, $\mathfrak{A}$ is a representative of the element $r_\mathfrak{H}\alpha \in {}^0H(\mathfrak{H}\,;\,\mathfrak{C}_L)$. Taking formula (7.1) into account, we see that it will be sufficient to prove that $r_\mathfrak{H}\zeta(\chi) = \zeta(r_\mathfrak{H}\chi)$. Let Φ be a normal mapping of $\boxplus[\mathfrak{G}]$ into $\boxplus[\mathfrak{H}]$. If $s \in \mathfrak{G}$, $\Phi(\bar{s})$ is 0 if $s \notin \mathfrak{H}$, while, if $s \in \mathfrak{H}$, then $\Phi(\bar{s})$ is the residue class $\bar{s}_\mathfrak{H}$ of s in $J[\mathfrak{H}]$. Thus,

$$\Phi\Big(\sum_{s,\, t \in \mathfrak{G}} c_\chi(s, t) \bar{s} \otimes \bar{t}\Big) = \sum_{s,\, t \in \mathfrak{H}} c_\chi(s, t) \bar{s}_\mathfrak{H} \otimes \bar{t}_\mathfrak{H},$$

which proves that $r_\mathfrak{H}\zeta(\chi) = \zeta(r_\mathfrak{H}\chi)$.

Assume now that $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$, and denote by $\lambda_{\mathfrak{H}}$ the lift mapping from $\mathfrak{G}/\mathfrak{H}$ to $\mathfrak{G}$. Let χ^* be a character of $\mathfrak{G}/\mathfrak{H}$; denoting by s^* the coset of an $s\in\mathfrak{G}$ modulo $\mathfrak{H}$, the formula $\chi(s)=\chi^*(s^*)$ defines a character χ of $\mathfrak{G}$; we shall denote this character by $\lambda_{\mathfrak{H}}\chi^*$. We shall prove the formula

$$(15.4) \qquad \langle \mathfrak{A}, \lambda_{\mathfrak{H}}\chi^* \rangle = \lambda_{\mathfrak{H}}\langle \mathfrak{A}, \chi^* \rangle.$$

For any $s^*\in\mathfrak{G}/\mathfrak{H}$, let $\chi_0^*(s^*)$ be a real number whose residue class modulo $\mathbf{Z}$ is $\chi^*(s^*)$. Set $\chi_0(s)=\chi_0^*(s^*)$; then $\chi(s)$ is the residue class of $\chi_0(s)$ modulo $\mathbf{Z}$ (where $\chi=\lambda_{\mathfrak{H}}\chi^*$), and we have $c_\chi(s,t)=c_{\chi^*}(s^*,t^*)$. The idèle class $\mathfrak{A}$ is a representative of $\lambda_{\mathfrak{H}}\alpha$; taking theorem 8.6 into account, we see that it will be sufficient to prove that $\zeta(\chi)$ is $\lambda_{\mathfrak{H}}\zeta(\chi^*)$, where $\zeta(\chi^*)$ is the element of ${}^2H(\mathfrak{G}/\mathfrak{H};\mathbf{Z})$ associated to χ^*. The lift mapping has been defined by means of a homomorphism L of $\mathbb{H}^c[\mathfrak{G}/\mathfrak{H}]$ into $\mathbb{H}^c[\mathfrak{G}]$; if $\bar{s}^*$ is the class in $J[\mathfrak{G}/\mathfrak{H}]$ of the coset s^* of an $s\in\mathfrak{G}$ modulo $\mathfrak{H}$, then $L(\bar{s}^*)$ is $\sum_{u\in s^*}\bar{u}$. Therefore

$$L\Big(\sum_{s^*,\,t^*\in\mathfrak{G}/\mathfrak{H}} c_{\chi^*}(s^*,t^*)\,\bar{s}^*\otimes\bar{t}^*\Big)=\sum_{s,\,t\in\mathfrak{G}} c_\chi(s,t)\,\bar{s}\otimes\bar{t},$$

and formula (15.4) is proved.

THEOREM 15.1. *Let K be a field of algebraic numbers of finite degree and L/K a normal extension of K of finite degree; let $\mathfrak{G}$ be the Galois group of L/K. The set of elements $\mathfrak{A}\in\mathfrak{C}_K$ such that $\langle\mathfrak{A},\chi\rangle=0$ for every $\chi\in\mathrm{Char}\,\mathfrak{G}$ is $\bigcap_X N_{X/K}\mathfrak{C}_X$, where X/K runs over all cyclic extensions of K contained in L. If $\chi\in\mathrm{Char}\,\mathfrak{G}$ is such that $\langle\mathfrak{A},\chi\rangle=0$ for every $\mathfrak{A}\in\mathfrak{C}_K$, then $\chi=0$.*

Let χ be any character of $\mathfrak{G}$, and let $\mathfrak{H}$ be the subgroup of $\mathfrak{G}$ composed of the elements s such that $\chi(s)=0$. Then $\mathfrak{G}/\mathfrak{H}$ is cyclic of the same order m as χ, and χ may be written in the form $\lambda_{\mathfrak{H}}\chi^*$, where χ^* is a character of order m of $\mathfrak{G}/\mathfrak{H}$. Let X be the subfield of L corresponding to $\mathfrak{H}$. We know that $\alpha\to M_{\mathfrak{C}_X,\mathbf{Z}}(\alpha\otimes\zeta(\chi^*))$ induces an isomorphism of ${}^0H(\mathfrak{G}/\mathfrak{H};\mathfrak{C}_X)$ with ${}^2H(\mathfrak{G}/\mathfrak{H};\mathfrak{C}_X)$ (theorem 9.3). If $\mathfrak{A}$ is not in $N_{X/K}\mathfrak{C}_X$, then $\langle\mathfrak{A},\chi^*\rangle\neq 0$. We have $\langle\mathfrak{A},\chi\rangle=\lambda_{\mathfrak{H}}\langle\mathfrak{A},\chi^*\rangle$; and, since ${}^1H(\mathfrak{H};\mathfrak{C}_L)=\{0\}$, $\lambda_{\mathfrak{H}}$ is a monomorphism; it follows that $\langle\mathfrak{A},\chi\rangle\neq 0$. On the contrary, the condition $\mathfrak{A}\in N_{X/K}\mathfrak{C}_X$ implies $\langle\mathfrak{A},\chi\rangle=0$. Since every cyclic extension of K contained in L may be obtained by means of suitable character χ of $\mathfrak{G}$, the first assertion is proved. Assume now that χ is of prime order p; then X/K is of degree p, which implies ${}^0H(\mathfrak{G}/\mathfrak{H};\mathfrak{C}_X)\neq\{0\}$ and therefore that there is an $\mathfrak{A}\in\mathfrak{C}_K$ such that $\langle\mathfrak{A},\chi\rangle\neq 0$. If χ is any character

$\neq 0$, there is an integer $h>0$ such that $h\chi$ is of prime degree, and this proves the second assertion.

Let $\mathfrak{N}_L$ be the group $\bigcap_\lambda N_{\lambda/K}\mathfrak{C}_\lambda$ of theorem 15.1. If α is the residue class modulo $\mathfrak{N}$ of an element $\mathfrak{A}\in\mathfrak{C}_K$ and $\chi\in\operatorname{Char}\mathfrak{G}$, we set $\langle\alpha,\chi\rangle=\langle\mathfrak{A},\chi\rangle$. Then $(\alpha,\chi)\rightarrow\langle\alpha,\chi\rangle$ is a pairing of the groups $\mathfrak{C}_K/\mathfrak{N}$ and $\operatorname{Char}\mathfrak{G}$ to ${}^2H(\mathfrak{G}\,;\,\mathfrak{C}_L)$, and it follows from theorem 15.1 that this pairing is *regular*, i.e. a) if $\alpha\in\mathfrak{C}_K/\mathfrak{N}$, the condition $\langle\alpha,\chi\rangle=0$ for all $\chi\in\operatorname{Char}\mathfrak{G}$ implies that α is the neutral element; b) if $\chi\in\operatorname{Char}\mathfrak{G}$, then the condition $\langle\alpha,\chi\rangle=0$ for every $\alpha\in\mathfrak{C}_K/\mathfrak{N}$ implies that $\chi=0$.

§16. THE ARTIN SYMBOL FOR CYCLOTOMIC EXTENSIONS

Let K be a field of algebraic numbers. An extension L/K is called *cyclotomic* if it is contained in an extension of the form $K(z)$, z being a root of unity.

In order to study such extensions, we shall first consider the group $\mathfrak{C}_{\mathbf{Q}}$ of classes of idèles of the field $\mathbf{Q}$ of rational numbers. Let U be the group of idèles $\mathfrak{u}$ which satisfy the following conditions: a) for any prime number p, $\mathfrak{u}_p$ is a unit in the field of p-adic numbers; b) if $\mathfrak{p}$ is the infinite place of $\mathbf{Q}$, then $\mathfrak{u}_{\mathfrak{p}}>0$. The only units of $\mathbf{Q}$ being ± 1, it is clear that $U \cap P_{\mathbf{Q}}=\{1\}$. $P_{\mathbf{Q}}$ being the group of principal idèles. Now, let $\mathfrak{a}$ be any idèle of $\mathbf{Q}$; if p is a prime, let $e(\mathfrak{a}\ ;p)$ be the order of $\mathfrak{a}_{\mathfrak{p}}$ at p; and let $\varepsilon(\mathfrak{a})$ be $+1$ or -1 according as to whether $\mathfrak{a}_{\mathfrak{p}}$ is >0 or <0. If we set $r=\varepsilon(\mathfrak{a})\prod_p p^{e(\mathfrak{a}\ p)}$, then it is clear that $r^{-1}\mathfrak{a}\in U$. It follows immediately that every idèle class of $\mathbf{Q}$ has a unique representative in U, and that $\mathfrak{C}_{\mathbf{Q}}\cong U$.

Now, let z be an m-th root of unity, m being an integer >0, and let $\mathfrak{u}$ be any idèle in U. Let U_m be the group of idèles $\mathfrak{u}'\in U$ such that, for every prime p, $\mathfrak{u}'_p-1$ is of order at least equal to that of m at p. (this is no restriction if p does not divide m). Then it is clear that, for any $\mathfrak{u}\in U$, there is an integer u such that $\mathfrak{u}\equiv u \pmod{U_m}$; any such integer is prime to m, and two integers u, u' which satisfy this condition are congruent to each other mod m. Let z be any m-th root of unity; then we see that z^u depends only on $\mathfrak{u}$, not on the choice of the integer u. Moreover, z may also be considered as an m'-th root of unity if m' is a multiple of m; if u' is an integer such that $\mathfrak{u}\equiv u' \pmod{U_{m'}}$, then $z^{u'}=z^u$. We shall denote z^u by $z^{\mathfrak{u}}$; and if $\mathfrak{A}$ is any element in $\mathfrak{C}_{\mathbf{Q}}$, we set

$$z^{\mathfrak{A}}=z^{\mathfrak{u}}$$

where $\mathfrak{u}$ is the idèle in U belonging to $\mathfrak{A}$. The following facts are obvious:

1) we have $(zz')^{\mathfrak{A}}=z^{\mathfrak{A}}z'^{\mathfrak{A}}$ if z, z' are roots of unity;

2) we hava $z^{\mathfrak{A}\mathfrak{A}'}=(z^{\mathfrak{A}})^{\mathfrak{A}'}$ if $\mathfrak{A},\mathfrak{A}'\in\mathfrak{C}_{\mathbf{Q}}$

3) if z is a primitive root of unity, then so is $z^{\mathfrak{A}}$ (because, in the condition above, u is prime to m).

Let $Z/\mathbf{Q}$ be any cyclotomic extension of $\mathbf{Q}$; let z be a root of unity such that $Z \subset \mathbf{Q}(z)$, and let $\mathfrak{A} \in \mathfrak{G}_{\mathbf{Q}}$. Then it follows from 3) that there is an automorphism s of $\mathbf{Q}(z)/\mathbf{Q}$ which changes z into $z^{\mathfrak{A}^{-1}}$. The restriction of s to Z does not depend on the choice of z. For, let Z be contained in $\mathbf{Q}(z)$ and $\mathbf{Q}(z')$, where z, z' are roots of unity; then we may write $z = z''^k$, $z' = z''^{k'}$, where z'' is a root of unity. It follows, by 1), that $z^{\mathfrak{A}} = (z''^{\mathfrak{A}})^k$, $z'^{\mathfrak{A}} = (z''^{\mathfrak{A}})^{k'}$, which proves our assertion. We shall denote the restriction of s to Z by

$$(Z/\mathbf{Q}\ ;\ \mathfrak{A}).$$

If Z' is an intermediary field between $\mathbf{Q}$ and Z, then $(Z'/\mathbf{Q}\ ;\ \mathfrak{A})$ is the restriction of $(Z/\mathbf{Q}\ ;\ \mathfrak{A})$ to Z'. If $\mathfrak{A}$, $\mathfrak{A}'$ are in $\mathfrak{G}_K$, then $(Z/\mathbf{Q}\ ;\ \mathfrak{A}\mathfrak{A}') = (Z/\mathbf{Q}\ ;\ \mathfrak{A}) \cdot (Z/\mathbf{Q}\ ;\ \mathfrak{A}')$.

Let K be any field of algebraic numbers, L a finite normal extension of K, $\mathfrak{P}$ a finite place of L and $\mathfrak{p}$ the place of K below $\mathfrak{P}$. Denote by f the degree of $\mathfrak{P}$ with respect to K, by $P_{\mathfrak{p}}$ the residue field of $\mathfrak{p}$ and by $P_{\mathfrak{P}}$ that of $\mathfrak{P}$. Then $P_{\mathfrak{P}}/P_{\mathfrak{p}}$ is a cyclic extension of degree f. If we denote by $N\mathfrak{p}$ the absolute norm of $\mathfrak{p}$, then the Galois group of $P_{\mathfrak{P}}/P_{\mathfrak{p}}$ is generated by an operation which changes every $\xi \in P_{\mathfrak{P}}$ into $\xi^{N\mathfrak{p}}$. Every operation of the decomposition group $\mathfrak{G}(\mathfrak{P})$ of $\mathfrak{P}$ defines in a natural manner an automorphism of the extension $P_{\mathfrak{P}}/P_{\mathfrak{p}}$. It is well known that the resulting homomorphism of $\mathfrak{G}(\mathfrak{P})$ into the Galois group of $P_{\mathfrak{P}}/P_{\mathfrak{p}}$ is an epimorphism, and is even an isomorphism if $\mathfrak{P}$ is not ramified with respect to K. In the latter case, $\mathfrak{G}(\mathfrak{P})$ is therefore generated by an operation s such that

$$sx \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

for every $x \in L$ which is integral at $\mathfrak{P}$. This operation is called the *Frobenius automorphism* and is denoted by $(L/K\ ;\ \mathfrak{P})$. If s is any operation of the Galois group of L/K, then $(L/K\ ;\ s\mathfrak{P}) = s(L/K\ ;\ \mathfrak{P})\, s^{-1}$; thus, if L/K is abelian, then $(L/K\ ;\ \mathfrak{P})$ depends only on the place $\mathfrak{p}$ of K below $\mathfrak{P}$, and is then denoted by $(L/K\ ;\ \mathfrak{p})$. It should be remembered that this symbol is only defined when $\mathfrak{p}$ is not ramified in L.

Now, let $\mathfrak{P}$ be an infinite place of L and $\mathfrak{p}$ the place of K below $\mathfrak{P}$. If $\mathfrak{p}$ is real and $\mathfrak{P}$ imaginary, the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$ of K may be identified to the field of real numbers and the $\mathfrak{P}$-adic completion $L_{\mathfrak{P}}$ of L to the field of complex numbers. The restriction to L of the unique automorphism distinct from the identity of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is denoted by $(L/K\ ;\ \mathfrak{P})$; this operation is called the *Frobenius automorphism.* If L/K is abelian, we see as above that this automorphism depends only on $\mathfrak{p}$; it is then denoted by $(L/K\ ;\ \mathfrak{p})$.

Let m be an integer >0. We shall say that an idele $\mathfrak{a}$ of the field K is $\equiv 1 \pmod{\tilde{m}}$ if the following conditions are satisfied: for every place $\mathfrak{p}$ above a prime divisor of m, the order of $\mathfrak{a}_{\mathfrak{p}}-1$ (at $\mathfrak{p}$) is at least equal to that of m; for every real infinite place $\mathfrak{p}$, we have $\mathfrak{a}_{\mathfrak{p}}>0$. Let $\mathfrak{a}$ be any idele. If $\mathfrak{p}$ is a place at which the order of m is >0, then the elements $x_{\mathfrak{p}}\in K_{\mathfrak{p}}$ such that $x_{\mathfrak{p}}\equiv 1$ $(\mathrm{mod}\ m\mathfrak{o}_{\mathfrak{p}})$, (where $\mathfrak{o}_{\mathfrak{p}}$ is the ring of integers of $K_{\mathfrak{p}}$) form an open subgroup of $K_{\mathfrak{p}}$. Making use of the theorem of independence of valuations, we see that there is an $x\in P_K$ such that $x^{-1}\mathfrak{a}\equiv 1 \pmod{\tilde{m}}$. Thus, every idèle class is representable by an idèle $\equiv 1 \pmod{\tilde{m}}$.

Now, let z be an m-th root of unity. Let $\mathfrak{p}$ be a finite place of K which is not above a prime divisor of m, and let $\mathfrak{a}$ be an idèle of K which is $\equiv 1$ (mod $\tilde{m}$) and which is such that $\mathfrak{a}_{\mathfrak{q}}$ is a unit in $K_{\mathfrak{q}}$ for every finite place $\mathfrak{q}\neq\mathfrak{p}$ of K. Let a be the order of $\mathfrak{a}_{\mathfrak{q}}$.

Then we shall prove that *the restriction of* $(K(z)/K\ ;\ \mathfrak{p})^a$ *to* $\mathbf{Q}(z)$ *is* $(\mathbf{Q}(z)\ ;\ N_{K/\mathbf{Q}}(\mathfrak{A}))$, *if* $\mathfrak{A}$ *is the class of* $\mathfrak{a}$. In fact, it is clear that $N_{K/\mathbf{Q}}\mathfrak{a}$ is $\equiv 1$ $(\mathrm{mod}\ \tilde{m})$ in $J_{\mathbf{Q}}$ and is of the form $p^{af}\mathfrak{u}$, where f is the absolute degree of $\mathfrak{p}$ and $\mathfrak{u}$ is in the group denoted above by U. Thus we have $\mathfrak{u}^{-1}\equiv p^{af} \pmod{m}$ and $(\mathbf{Q}(z)\ ;\ N_{K/\mathbf{Q}}(\mathfrak{A}))$ changes z into z^{ap^f}. On the other hand, we have

$$(K(z)/K\ ;\ \mathfrak{p})\cdot z\equiv z^{p^f}\quad (\mathrm{mod}\ \mathfrak{P})$$

if $\mathfrak{P}$ is a place of $K(z)$ above $\mathfrak{p}$. But $(K(z)/K\ ;\ \mathfrak{p})\cdot z$ is a power z^k of z; since the order of m at $\mathfrak{P}$ is 0, the congruence $z^k\equiv z^{p^f}$ (mod $\mathfrak{P}$) implies $z^k=z^{p^f}$; thus, $(K(z)/K\ ;\ \mathfrak{p})^a$ changes z into z^{ap^f}, which proves the assertion made above.

Now, let z be an m-th root of unity, and $\mathfrak{A}$ any idèle class in $\mathfrak{C}_K$. Let $\mathfrak{a}$ be an idèle of $\mathfrak{A}$ which is $\equiv 1 \pmod{\tilde{m}}$. Then it is obviously possible to represent $\mathfrak{a}$ in the form $\mathfrak{a}_1\cdots\mathfrak{a}_h$, where each $\mathfrak{a}_i$ is $\equiv 1 \pmod{\tilde{m}}$ and has the property that there is at most one finite place of K at which $\mathfrak{a}_i$ is not a unit (if there is one, then the order of m at this place is 0). Making use of the result proved above, we conclude that there is an automorphism (and, obviously, only one) of $K(z)/K$ whose restriction to $\mathbf{Q}(z)$ is $(\mathbf{Q}(z)\ ;\ N_{K/\mathbf{Q}}\mathfrak{A})$. We shall denote this automorphism by $(K(z)/K\ ;\ \mathfrak{A})$. Let Z/K be any cyclotomic extension of K. Then there is a root of unity z such that $Z\subset K(z)$; the restriction of

$(K(z)/K\,;\,\mathfrak{A})$ to Z does not depend on the choice of z. For, if $Z\subset K(z)$, $Z\subset K(z')$, then there is a root of unity z'' such that $K(z)\subset K(z'')$, $K(z')\subset K(z'')$, and $(K(z)/K, \mathfrak{A})$, $(K(z')/K\,;\,\mathfrak{A})$ are restrictions of $(K(z'')/K\,;\,\mathfrak{A})$. We shall denote the restriction of $(K(z)/K\,;\,\mathfrak{A})$ to Z by $(Z/K\,;\,\mathfrak{A})$. Then we have obviously the following results;

1) *If Z' is an intermediary field between K and Z, then $(Z'/K\,;\,\mathfrak{A})$ is the restriction of $(Z/K\,;\,\mathfrak{A})$ to Z'.*

2) *If $\mathfrak{A}$, $\mathfrak{A}'$ are in $\mathfrak{C}_K$, then $(Z/K\,;\,\mathfrak{A}\mathfrak{A}')=(Z/K\,;\,\mathfrak{A})\cdot(Z/K\,;\,\mathfrak{A}')$;*

3) *Let Z be contained in $K(z)$, where z is an m-th root of unity. Let $\mathfrak{a}$ be an idèle $\equiv 1 \pmod{\tilde{m}}$ such that there is at most one finite place $\mathfrak{p}$ at which $\mathfrak{a}_\mathfrak{p}$ is not a unit; denote by a the order of $\mathfrak{a}$ at $\mathfrak{p}$, and by $\mathfrak{A}$ the class of $\mathfrak{a}$; then $(Z/K\,;\,\mathfrak{A})=(Z/K\,;\,\mathfrak{p})^a$.*

The last assertion follows from the obvious fact that $(Z/K\,;\,\mathfrak{p})$ is the restriction of $(K(z)/K\,;\,\mathfrak{p})$ to Z.

3′) *Let $\mathfrak{p}$ be an infinite place of K. Let $\mathfrak{a}$ be an idèle of K whose components at all places $\neq\mathfrak{p}$ are 1, and let $\mathfrak{A}$ be the idèle class of $\mathfrak{a}$. Then $(Z/K\,;\,\mathfrak{A}) =(Z/K\,;\,\mathfrak{p})^a$ where a is determined as follows: $a=0$ if $\mathfrak{p}$ is real and $\mathfrak{a}_\mathfrak{p}>0$; $a=1$ if $\mathfrak{p}$ is real and $\mathfrak{a}_\mathfrak{p}<0$; $a=0$ if $\mathfrak{p}$ is imaginary.*

Let p_∞ be the unique place at infinity of $\mathbf{Q}$; set $\mathfrak{b}=N_{K/\mathbf{Q}}\mathfrak{a}$. Then the components of $\mathfrak{b}$ at all places $\neq p_\infty$ of $\mathbf{Q}$ are 1, and its component at p_∞ is >0 if $\mathfrak{p}$ is imaginary or if $\mathfrak{p}$ is real and $\mathfrak{a}_\mathfrak{p}>0$, but is <0 if $\mathfrak{p}$ is real and $\mathfrak{a}_\mathfrak{p}<0$. Let z be an m-th root of unity such that $Z\subset K(z)$. If $\mathfrak{b}_{p_\infty}>0$, then we have $\mathfrak{b}\equiv 1 \pmod{U_m}$, whence $(Z/K\,;\,\mathfrak{A})=e$ (the unit element). If $\mathfrak{b}_{p_\infty}<0$, then $-\mathfrak{b}\in U_m$, and $(K(z)/K\,;\,\mathfrak{A})$ changes z into its imaginary conjugate z^{-1}, whence $(Z/K\,;\,\mathfrak{A}) =(Z/K\,;\,\mathfrak{p})$.

4) *Let K' be an extension of finite degree of K, and $\mathfrak{A}'$ an element of $\mathfrak{C}_{K'}$; then $(Z/K\,;\,N_{K'/K}\mathfrak{A}')$ is the restriction to Z of $(Z'/K\,;\,\mathfrak{A}')$.*

For, if $Z=K(z)$, z being a root of unity, the restriction of $(K(z)/K\,;\, N_{K'/K}\mathfrak{A}')$ and $(K'(z)/K'\,;\,\mathfrak{A}')$ to $\mathbf{Q}(z)$ are both equal to $(\mathbf{Q}(z)/\mathbf{Q}\,;\,N_{K'/\mathbf{Q}}\mathfrak{A}')$.

THEOREM 16.1. *Let Z/K be a cyclotomic extension. Then $\mathfrak{A}\to(Z/K\,;\,\mathfrak{A})$ is an epimorphism of $\mathfrak{C}_K$ on the Galois group of Z/K, whose kernel contains $N_{Z/K}\mathfrak{C}_Z$.*

Let Z' be the field of elements of Z left fixed by all operations $(Z/K\ ;\ \mathfrak{A})$, $\mathfrak{A}\in\mathfrak{C}_K$. Assume that $Z\subset K(z)$, z an m-th root of unity, and let $\mathfrak{p}$ be a finite place of K at which the order of m is 0. Let $\mathfrak{a}$ be an idèle whose $\mathfrak{p}$-component is of order 1 and whose other components are 1; it follows from 3) that $(Z/K\ ;\ \mathfrak{A})=(Z/K\ ;\ \mathfrak{p})$, if $\mathfrak{A}$ is the class of $\mathfrak{a}$. Thus, $(Z/K\ ;\ \mathfrak{p})$ *leaves the elements of Z'* invariant, which means that $\mathfrak{p}$ splits in Z'. Were $Z'\neq K$, then Z' would contain a cyclic extension Z''/K of prime degree of K, and almost all places of K would split in Z'': this is impossible by the corollary 2 to theorem 13.1. Thus $Z'=K$, and the mapping $\mathfrak{A}\rightarrow(Z/K\ ;\ \mathfrak{A})$ is an epimorphism. That its kernel contains $N_{Z/K}\mathfrak{C}_Z$ follows immediately from 4), applied to the case $K'=Z$.

COROLLARY 1. *Let Z/K be a cyclic cyclotomic extension of K. Then ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)$ is isomorphic to $\mathfrak{G}$, if $\mathfrak{G}$ is the Galois group of Z/K.*

Let n be the order of $\mathfrak{G}$. It follows from theorem 16.1 that $\mathfrak{G}$ is isomorphic to a factor group of ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)=\mathfrak{C}_K/N_{Z/K}\mathfrak{C}_Z$. Since $\mathfrak{G}$ is cyclic, ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)$ is isomorphic to ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)$, and the latter group is of order $\leqq n$ by theorem 14.2; this proves the corollary.

COROLLARY 2. *If Z/K is a cyclic cyclotomic extension, then the kernel of the mapping $\mathfrak{A}\rightarrow(Z/K\ ;\ \mathfrak{A})$ is $N_{Z/K}\mathfrak{C}_Z$.*

In fact, ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)\cong{}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)$ is isomorphic to $\mathfrak{G}$ by corollary 1, and corollary 2 follows immediately from theorem 16.1.

Let Z/K be a cyclic cyclotomic extension of degree n, and let s be a generator of the Galois group $\mathfrak{G}$ of Z/K. Let $\mathfrak{A}$ be an idèle class of K such that $(Z/K\ ;\ \mathfrak{A})=s$. Let χ be the character of $\mathfrak{G}$ such that $\chi(s)$ is the class of $1/n$ modulo $\mathbf{Z}$. Set

$$\langle\mathfrak{A},\chi\rangle=\xi.$$

Then ξ does not depend on the choice of s. For, replace s by another generator $s'=s^k$; if $\chi'(s')$ is the class of $1/n$ modulo $\mathbf{Z}$, then $k\chi'=\chi$. On the other hand, we have $(Z/K\ ;\ \mathfrak{A}^k)=s'$, and $\langle\mathfrak{A}^k,\chi'\rangle=k\langle\mathfrak{A},\chi'\rangle=\langle\mathfrak{A},k\chi'\rangle=\langle\mathfrak{A},\chi\rangle$, which proves our assertion.

The cohomology class $\xi\in{}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)$ defined by the formula given above is called the canonical class of the extension Z/K. It is obviously of order n, and it generates ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_Z)$.

THEOREM 16.2. *Let K'/K be a finite extension of the field K and Z/K a cyclic cyclotomic extension of K, whose canonical class we denote by $\xi_{Z/K}$. Set $K''=K'\cap Z$; denote by $\mathfrak{G}$ and $\mathfrak{H}$ the Galois group of Z/K and Z/K'', and by m the degree of K'/K''. Let $r_{\mathfrak{H}}$ be the restriction map of $H'(\mathfrak{G}\,;\,\mathfrak{C}_Z)$ to $H'(\mathfrak{H}\,;\,\mathfrak{C}_Z)$ and ι^* the mapping of $H'(\mathfrak{H}\,;\,\mathfrak{C}_Z)$ into $H'(\mathfrak{H}\,;\,\mathfrak{C}_{ZK'})$ induced by the identity map $\iota:\mathfrak{C}_Z\to\mathfrak{C}_{ZK'}$. ($\mathfrak{H}$ being identified to the Galois group ZK'/K'). Then $\iota^* r_{\mathfrak{H}}\xi_{Z/K}=m\xi_{ZK'/K'}$, where $\xi_{ZK'/K'}$ is the canonical class of ZK'/K'.*

Let s be a generator of $\mathfrak{G}$, n the order of $\mathfrak{G}$, χ a character of $\mathfrak{G}$ such that $\chi(s)$ is the class of $1/n$ modulo $\mathbf{Z}$ and $\mathfrak{A}$ an idèle class of K such that $(Z/K\,;\,\mathfrak{A})=s$, whence $\xi_{Z/K}=\langle\mathfrak{A},\chi\rangle$. Then $r_{\mathfrak{H}}\xi_{Z/K}=\langle\mathfrak{A},r_{\mathfrak{H}}\chi\rangle$. Let h be the smallest exponent such that $s^h\in\mathfrak{H}$; then s^h generates $\mathfrak{H}$, and is the restriction to Z of an automorphism s' of ZK'/K'; $(r_{\mathfrak{H}}\chi)(s')$ is the class of $1/(n/h)$ modulo $\mathbf{Z}$, and $[ZK'\,:\,K']=n/h$. It is clear that $\iota^* r_{\mathfrak{H}}\xi_{Z/K}$ is the element of ${}^2H(\mathfrak{H}\,;\,\mathfrak{C}_{ZK'})$ represented by the symbol $\langle\mathfrak{A},r_{\mathfrak{H}}\chi\rangle$ when we consider $\mathfrak{A}$ as an element of $\mathfrak{C}_{K'}$ and $r_{\mathfrak{H}}\chi$ as a character of the Galois group of ZK'/K'.

The restriction of $(ZK'/K'\,;\,\mathfrak{A})$ to Z is $(Z/K\,;\,N_{K'/K}\mathfrak{A})=(Z/K\,;\,\mathfrak{A}^{mh})=s^{mh}$, whence $(ZK'/K'\,;\,\mathfrak{A})=s'^m$. It follows that $\iota^* r_{\mathfrak{H}}\xi_{Z/K}=m\xi_{ZK'/K'}$.

THEOREM 16.3. Let *Z, Z' be cyclic extensions of K of respective degrees n and n'; denote by $\xi_{Z/K}$ and $\xi_{Z'/K}$ their canonical classes. Let ν, ν' be integers >0 such that $n/n'=\nu/\nu'$; denote by λ_Z (respectively: $\lambda_{Z'}$) the lift mapping from the Galois group of Z/K (respectively: Z'/K) to that of ZZ'/K. Then $\lambda_Z\nu\xi_{Z/K}=\lambda_{Z'}\nu'\xi_{Z'/K}$.*

We can find generators s_Z, $s_{Z'}$ of the Galois groups of Z/K, Z'/K which have the same restriction to $Z\cap Z'$; this being the case, there is an automorphism s of ZZ'/K whose restrictions to Z and Z' are s_Z and $s_{Z'}$. Let $\mathfrak{A}$ be an idèle class of K such that $(ZZ'/K\,;\,\mathfrak{A})=s$ (cf. theorem 16.1). Then we have $(Z/K\,;\,\mathfrak{A})=s_Z$, $(Z'/K\,;\,\mathfrak{A})=s_{Z'}$. Let χ (respectively: χ') be a character of the Galois group of Z/K (resp: of Z'/K) such that $\chi(s_Z)$ (resp: $\chi'(s_{Z'})$) is the class of $1/n$ (resp: $1/n'$) modulo $\mathbf{Z}$. Then $\lambda_Z\xi_{Z/K}=\langle\mathfrak{A},\lambda_Z\chi\rangle$, $\lambda_{Z'}\xi_{Z'/K}=\langle\mathfrak{A},\lambda_{Z'}\chi'\rangle$, and

$$\nu\lambda_Z\xi_{Z/K}-\nu'\lambda_{Z'}\xi_{Z'/K}=\langle\mathfrak{A},\,\nu\lambda_Z\chi-\nu'\lambda_{Z'}\chi'\rangle.$$

We have $(\nu\lambda_Z\chi)(s)=\left[\frac{\nu}{n}\right]$, $(\nu'\lambda_{Z'}\chi')(s)=\left[\frac{\nu'}{n'}\right]$, where $[\rho]$ denotes the class of

ρ modulo 1. If follows that $(\nu\lambda_Z\chi - \nu'\lambda_{Z'}\chi')(s) = 0$. Let S be the field left invariant by s; then $\nu\lambda_Z\chi - \nu'\lambda_{Z'}\chi'$ may be witten in the form $\lambda_S\chi''$, where χ'' is a character of the group of S/K, and λ_S is the lift mapping from the group of S/K to that of ZZ'/K. It follows that

$$\langle \mathfrak{A}, \nu\lambda_Z\chi - \nu'\lambda_{Z'}\chi'\rangle = \lambda_S\langle \mathfrak{A}, \chi''\rangle$$

(formula (15.4)). If t is a generator of the Galois group of ZZ'/Z, then s and t clearly generate the group of ZZ'/K, which shows that S/K is cyclic. Since $(ZZ'/K, \mathfrak{A}) = s$, we have $(S/K, \mathfrak{A}) = e$ (the identity). This shows that $\mathfrak{A} \in N_{S/K}\mathfrak{C}_S$, whence $\langle \mathfrak{A}, \chi''\rangle = 0$, which proves theorem 16.3.

COROLLARY. *The notation being as in theorem* 16.3, *assume furthermore that* $Z' \subset Z$. *Then the lift from the Galois group of* Z'/K *to that of* Z/K *of* $\xi_{Z'/K}$ *is* $n/n' \cdot \xi_{Z/K}$.

THEOREM 16.4. *Let* K *be a field of algebraic numbers of finite degree,* $\mathfrak{p}$ *a finite place of* K *and* n *an integer* >0. *Then there exists a cyclic cyclotomic extension* Z/K *with the following properties:* $\mathfrak{p}$ *is not ramified in* Z, *and, if* $\mathfrak{P}$ *is a place of* Z *above* $\mathfrak{p}$, *then* $\mathfrak{P}$ *is of degree* n *with respect to* K.

Let $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of K. It is well known that the unramified extension of degree n of $K_\mathfrak{p}$ may be generated by adjunction to $K_\mathfrak{p}$ of a root of unity z. Then $\mathfrak{p}$ is not ramified in $K(z)$, and $(K(z)/K\ ;\ \mathfrak{p}) = s$ is of order n. By a well known theorem, there exists a character χ of the Galois group $\mathfrak{G}$ of $K(z)/K$ such that $\chi(s)$ is of order n. Let $\mathfrak{H}$ be the group of elements $t \in \mathfrak{G}$ such that $\chi(t) = 1$. Then $\mathfrak{G}/\mathfrak{H}$ is cyclic; let Z be the corresponding cyclic cyclotomic extension of K. Then $(Z/K\ ;\ \mathfrak{p})$ is the restriction of $(K(z)/K\ ;\ \mathfrak{p})$ to Z, and is therefore of order n; Z therefore has the property stated in theorem 16.4.

§17. CANONICAL CLASSES

We shall use in what follows the following notation. If L/K is a finite normal extension of the field K of algebraic numbers, $\mathfrak{G}$ the Galois group of L/K, $\mathfrak{H}$ a subgroup of $\mathfrak{G}$ and L' the subfield of L attached to $\mathfrak{H}$, we shall denote by $r_{K\to L'}$ the restriction mapping of $H^r(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ to $H^r(\mathfrak{H}\ ;\ \mathfrak{C}_L)$, by $R_{L'\to K}$ the mapping $R_{\mathfrak{C}_L}$ of $H^r(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ into $H^r(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ which was defiend in §7; if L' is normal over K, we shall identify its Galois group over K with $\mathfrak{G}/\mathfrak{H}$, and we shall denote by $\lambda_{L'\to L}$ the lift mapping of $H^c(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_{L'})$ into $H^c(\mathfrak{G}\ ;\ \mathfrak{C}_L)$. The restriction of this mapping to ${}^2H(\mathfrak{G}/\mathfrak{H}\ ;\ \mathfrak{C}_{L'})$ is an isomorphism of this group with the kernel of the mapping of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ induced by $r_{K\to L'}$, as follows from the fact that ${}^1H(\mathfrak{H}\ ;\ \mathfrak{C}_L)=\{0\}$ and from theorem 8.2.

Let K be a field of algebraic numbers of finite degree and L/K a finite normal extension of degree n of K. There exists a cyclic cyclotomic extension Z/K of K whose degree νn is $\equiv 0 \pmod n$ (theorem 16.4). Let $\xi_{Z/K}$ be its canonical class. The class $r_{K\to L}\lambda_{Z\to LZ}\xi_{Z/K}$ is $m\xi_{ZL/L}$ (theorem 16.2), where $m=[L:L\cap Z]$ and $\xi_{ZL/L}$ is the canonical class of ZL/L. On the other hand, we have $[ZL:L]=[Z:Z\cap L]=n\nu[Z\cap L:K]^{-1}=m\nu$; thus, the order of $\xi_{ZL/L}$ is $m\nu$, and $r_{K\to L}\lambda_{Z\to LZ}\cdot\nu\xi_{Z/K}=0$. It follows that we may write

$$\lambda_{Z\to LZ}\nu\xi_{Z/K}=\lambda_{L\to LZ}\xi$$

where ξ is a uniquely determined element of ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$, $\mathfrak{G}$ denoting the Galois group of L/K. We shall see that ξ does not depend on the choice of Z. Let Z'/K be any cyclic cyclotomic extension of degree $\nu' n$ divisible by n. Making use of theorem 8.3, we have

$$\lambda_{L\to LZZ'}\xi=\lambda_{LZ\to LZZ'}\lambda_{Z\to LZ}\nu\xi_{Z/K}=\lambda_{ZZ'\to LZZ'}(\lambda_{Z\to ZZ'}\nu\xi_{Z/K}).$$

Similarly, if $\lambda_{L\to LZ'}\xi'=\lambda_{Z'\to LZ'}\nu'\xi_{Z'/K}$, $\xi_{Z'/K}$ being the canonical class of Z'/K, then

$$\lambda_{L\to LZZ'}\xi'=\lambda_{ZZ'\to LZZ'}(\lambda_{Z'\to ZZ'}\nu'\xi_{Z'/K}).$$

But we have $\lambda_{Z\to ZZ'}\nu\xi_{Z/K}=\lambda_{Z'\to ZZ'}\nu'\xi_{Z'/K}$ by theorem 16.3. Since $\lambda_{L\to LZZ'}$ is a monomorphism, we have $\xi=\xi'$.

If L/K is cyclic and cyclotomic, then ξ is obviously the canonical class of

L/K (take $L=Z$!). In general, we shall call ξ the canonical class of L/K and denote it by $\xi_{L/K}$.

THEOREM 17.1. *Let K be a field of algebraic numbers of finite degree and L/K a normal finite extension of K; we denote by $\mathfrak{G}$ the Galois group of L/K, and by n the order of $\mathfrak{G}$. Then the canonical class $\xi_{L/K}$ is of order n and generates ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$.*

The notation being as above, $\nu\xi_{Z/K}$ is of order $n\nu/\nu=n$; it follows that $\xi=\xi_{L/K}$ is of order n. Since ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ is of order $\leqq n$ (theorem 14.2), it is generated by $\xi_{L/K}$.

THEOREM 17.2. *The notation being as in theorem* 17.1, *let further p and q be integers $\geqq 0$. Then $\zeta \to M^{\mathfrak{N}}_{\mathfrak{C}_L,\mathbf{Z}}(\xi_{L/K}\otimes\zeta)$ induces an isomorphism of ${}^{p,q}H(\mathfrak{G}\ ;\ \mathbf{Z})$ with ${}^{p+2,q}H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$. The group $\mathfrak{C}_K/N_{L/K}\mathfrak{C}_L$ is isomorphic to $\mathfrak{G}/\mathfrak{G}'$, where $\mathfrak{G}'$ is the commutator subgroup of $\mathfrak{G}$.*

If $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$, then $\mathfrak{H}$ is the Galois group of L/L', where L' is the invariant field of $\mathfrak{H}$. We know that ${}^1H(\mathfrak{H}\ ;\ \mathfrak{C}_L)=\{0\}$ and that ${}^2H(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ is cyclic of the same order as $\mathfrak{H}$. Thus the first assertion follows from theorem 9.2. In particular, $\mathfrak{C}_K/N_{L/K}\mathfrak{C}_L={}^{0,0}H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$, which is isomorphic to ${}^{2,2}H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$, is isomorphic to ${}^{0,2}H(\mathfrak{G}\ ;\ \mathbf{Z})$, i.e. to $\mathfrak{G}/\mathfrak{G}'$ (cf. § 6).

THEOREM 17.3. *The notation being as above, let further L'/K be a finite normal extension containing L/K; if $h=[L\ :\ L']$, we have*

$$\lambda_{L\to L'}\xi_{L/K}=h\xi_{L'/K}.$$

Let $n=[L\ ;\ K]$, whence $[L'\ :\ K]=nh$. Let Z/K be a cyclic cyclotomic extension of K of degree $\nu nh\equiv 0 \pmod{nh}$. Then we have $\lambda_{L'\to L'Z}\lambda_{L\to L'}\xi_{L'K} =\lambda_{LZ\to L'Z}\lambda_{L\to LZ}\xi_{L/K}=\lambda_{Z\to L'Z}\nu h\xi_{Z/K}$ (theorem 8.3), while $\lambda_{L'\to L'Z}\xi_{L'/K}=\lambda_{Z\to L'Z}\nu\xi_{Z/K}$. Theorem 17.3 then follows from the fact that $\lambda_{L'\to L'Z}$ induces a monomorphism of ${}^2H(\mathfrak{G}'\ ;\ \mathfrak{C}_{L'})$, where $\mathfrak{G}'$ is the Galois group of L'/K.

THEOREM 17.4. *The notation being as above, let further K'/K be an extension of finite degree of K; set $m=[K'\ :\ K'\cap L]$. Denote by $\mathfrak{H}$ the Galois group of LK'/K', which we identify to that of $L/L\cap K'$. Let ι^* be the mapping: ${}^2H(\mathfrak{H}\ ;\ \mathfrak{C}_L)\to{}^2H(\mathfrak{H}\ ;\ \mathfrak{C}_{LK'})$ associated to the identity map $\iota:\mathfrak{C}_L\to\mathfrak{C}_{LK'}$. Then we have*

$$\iota^* r_{K\to L\cap K'}\xi_{L/K}=m\xi_{LK'/K'}.$$

We first consider the case where $K' \subset L$, in which case the formula to be proved becomes

$$r_{K \to K'} \xi_{L/K} = \xi_{L/K'}.$$

Let Z/K be a cyclic cyclotomic extension of degree $n\nu$ of K, where $n = [L : K]$. We have $\lambda_{L \to LZ} r_{K \to K'} \xi_{LK} = r_{K \to K'} \lambda_{L \to LZ} \xi_{L/K}$ (theorem 8.5), and this is

$$r_{K \to K'} \lambda_{Z \to LZ} \nu \xi_{Z/K} = r_{K' \cap Z \to K'} r_{K \to K' \cap Z} \lambda_{Z \to LZ} \nu \xi_{Z/K}$$

(theorem 7.4). We have $r_{K \to K' \cap Z} \lambda_{Z \to LZ} \nu \xi_{Z/K} = \lambda_{Z \to LZ} r_{K \to K' \cap Z} \nu \xi_{Z/K}$ (theorem 8.5), and $r_{K \to K' \cap Z} \xi_{Z/K} = \xi_{Z/K' \cap Z}$ (theorem 16.2). The Galois group of $LZ/K' \cap Z$ is generated by those of LZ/K' and of LZ/Z. Denote by $\mathfrak{Z}$ the Galois group of $K'Z/K'$, which we identify to that of $Z/K' \cap Z$, and by ι_1^* the mapping: ${}^2H(\mathfrak{Z}\,;\,\mathfrak{C}_Z) \to {}^2H(\mathfrak{Z}\,;\,\mathfrak{C}_{K'Z})$ associated to the injection map $\iota_1 : \mathfrak{C}_Z \to \mathfrak{C}_{K'Z}$. Making use of theorem 8.4, we have

$$r_{K' \cap Z \to K'} \lambda_{Z \to LZ} \nu \xi_{Z/K' \cap Z} = \lambda_{K'Z \to LZ} \nu \iota_1^* \xi_{Z'K' \cap Z}.$$

On the other hand, $\iota_1^* \xi_{Z/K' \cap Z} = [K' : K' \cap Z] \xi_{K'Z/K'}$ by theorem 16.2. Thus $\lambda_{K'Z \to LZ} \nu \iota_1^* \xi_{Z/K' \cap Z} = \nu [LZ : K'Z][K' : K' \cap Z] \xi_{LZ/K'}$ by theorem 17.3 above. We have $[K' : K' \cap Z] = [K'Z : Z]$, and therefore $[LZ : K'Z][K' : K' \cap Z] = [LZ : Z]$, and

$$\lambda_{L \to LZ} r_{K \to K'} \xi_{L/K} = \nu [LZ : Z] \xi_{LZ/K'}.$$

We have $[LZ : K] = [LZ : L][L : K] = [LZ : Z] \nu [L : K]$, whence $\nu [LZ : Z] = [LZ : L]$; since $[LZ : L] \xi_{LZ/K'} = \lambda_{L \to LZ} \xi_{L/K'}$ (theorem 17.3), we see that

$$\lambda_{L \to LZ} (r_{K \to K'} \xi_{L/K}) = \lambda_{L \to LZ} \xi_{L/K'}$$

whence $r_{K \to K'} \xi_{L/K} = \xi_{L/K'}$.

We consider now the general case. Let K''/K be a finite normal extension containing K'/K. We have $r_{K \to L \cap K'} \xi_{L/K} = \xi_{L/L \cap K'}$ by the result just proved. The Galois group of $K''L/L \cap K'$ is generated by those of $K''L/L$ and of $K''L/K'$. Therefore,

$$\lambda_{K'L \to K''L} \iota^* \xi_{L/L \cap K'} = r_{L \cap K' \to K'} \lambda_{L \to K''L} \xi_{L/L \cap K'}$$

by theorem 8.4. This is equal to $r_{L \cap K' \to K'} [K''L : L] \xi_{K''L/L \cap K'}$ by theorem 17.3, and therefore to $[K''L : L] \xi_{K''L/K'}$ by the result established in the first part of the proof. But

$$
\begin{aligned}
[K''L : L]\xi_{K''L/K'} &= [K'L : L][K''L : K'L]\xi_{K''L/K'} \\
&= [K'L : L]\lambda_{K'L\to K''L}\xi_{K'L/K'}
\end{aligned}
$$

by theorem 17.3. Since $m=[K'L : L]$, theorem 17.4 is thereby proved.

§18. THE RECIPROCITY MAPPING

We shall use the same convention of notation as in §17. Moreover, if χ is a character of the Galois group of a finite Galoisian extension L/K, and if $K \subset K' \subset L$, we shall denote by $r_{K \to K'}\chi$ the restriction of χ to the Galois group of L/K'. If L'/K is a finite Galoisian extension of L/K, we shall denote by $\lambda_{L \to L'}\chi$ the character of the Galois group of L'/K which assigns to every element s of this group the value $\chi(s_L)$, s_L being the restriction of s to L. Finally, for any finite group $\mathfrak{G}$, we shall identify Char $\mathfrak{G}$ to Char $\mathfrak{G}/\mathfrak{G}'$, where $\mathfrak{G}'$ is the commutator subgroup of $\mathfrak{G}$.

Let L/K be a finite normal extension of a field K of algebraic numbers of finite degree, and let $\mathfrak{G}$ be its Galois group. Denote by $\xi_{L/K}$ the canonical class of L/K. Then every $\eta \in {}^2H(\mathfrak{G}\,;\,\mathfrak{C}_L)$ may be written in the form $k\xi_{L/K}$, where k is an integer whose residue class modulo $n\mathbf{Z}$ is uniquely determined (where n is the order of $\mathfrak{G}$). Let $\left[\frac{k}{n}\right]$ be the residue class of k/n modulo $\mathbf{Z}$; then $\eta \to [k/n]$ is an isomorphism ρ of ${}^2H(\mathfrak{G}\,;\,\mathfrak{C}_L)$ with a subgroup of $\mathbf{R}^*$. If $\mathfrak{A} \in \mathfrak{C}_K$, $\chi \in$ Char $\mathfrak{G}$, then $\langle \mathfrak{A}, \chi \rangle$ is an element of ${}^2H(\mathfrak{G}\,;\,\mathfrak{C}_L)$. Set

$$\langle \mathfrak{A}, \chi \rangle^* = \rho(\langle \mathfrak{A}, \chi \rangle).$$

Then $(\mathfrak{A}, \chi) \to \langle \mathfrak{A}, \chi \rangle^*$ is a pairing of $\mathfrak{C}_K$ and Char $\mathfrak{G}$ to $\mathbf{R}^*$. The mapping $\chi \to \langle \mathfrak{A}, \chi \rangle^*$ is a character of the group Char $\mathfrak{G}$; it follows that there exists a uniquely determined element $\bar{s} \in \mathfrak{G}/\mathfrak{G}'$ such that $\langle \mathfrak{A}, \chi \rangle^* = \chi(\bar{s})$ for every $\chi \in$ Char $\mathfrak{G}$. We set

$$\bar{s} = (L/K\,;\,\mathfrak{A})^*.$$

If A_L/K is the largest abelian extension of K contained in L, then $\mathfrak{G}/\mathfrak{G}'$ is the Galois group of A_L/K and $(L/K\,;\,\mathfrak{A})^*$ is an automorphism of A_L/K.

Let L'/K be a finite normal extension of K containing L/K. Then we have $A_L \subset A_{L'}$, and we shall see that $(L/K\,;\,\mathfrak{A})^*$ is the restriction of $(L'/K\,;\,\mathfrak{A})^*$ to A_L. Let χ be any character of $\mathfrak{G}$; write $\langle \mathfrak{A}, \chi \rangle = k\xi_{L/K}$, whence $\chi((L/K\,;\,\mathfrak{A})^*) = \left[\frac{k}{n}\right]$. We have

$$\langle \mathfrak{A}, \lambda_{L \to L'}\chi \rangle = \lambda_{L \to L'}\langle \mathfrak{A}, \chi \rangle = k[L' : L]\xi_{L/K}.$$

We have $k[L' : L][L' : K]^{-1} = \frac{k}{n}$, whence $\langle \mathfrak{A}, \lambda_{L\to L'}\chi\rangle^* = \langle \mathfrak{A}, \chi\rangle^*$, and

$$(\lambda_{L\to L'}\chi)((L'/K\ ;\ \mathfrak{A})^*) = \chi((L/K\ ;\ \mathfrak{A})^*).$$

This being true for every $\chi \in \mathrm{Char}\,\mathfrak{G}$, it is clear that $(L/K\ ;\ \mathfrak{A})^*$ is the restriction of $(L'/K\ ;\ \mathfrak{A})^*$ to A_L.

Now, we shall see that $(L/K\ ;\ \mathfrak{A})^* = (L/K\ ;\ \mathfrak{A})$ in case L/K is a cyclotomic extension. Consider first the case where L/K is cyclic; let s_1 be a generator of its Galois group $\mathfrak{G}$, and χ, the character of $\mathfrak{G}$ such that $\chi(s_1) = \left[\frac{1}{n}\right]$, n being the order of $\mathfrak{G}$. Let $\mathfrak{A}_1$ be an idèle class such that $(L/K\ ;\ \mathfrak{A}_1) = s_1$, whence $\langle \mathfrak{A}_1, \chi\rangle = \xi_{L/K}$. Set $(L/K\ ;\ \mathfrak{A}) = s_1^k$; then $(L/K\ ;\ \mathfrak{A}\mathfrak{A}_1^{-k}) = e$, whence $\mathfrak{A}\mathfrak{A}_1^{-k} \in N_{L/K}\mathfrak{C}_L$ and $\langle \mathfrak{A}, \chi\rangle = \langle \mathfrak{A}_1^k, \chi\rangle = k\xi_{L/K}$. It follows that $\chi((L/K\ ;\ \mathfrak{A})^*) = \left[\frac{k}{n}\right] = \chi(s_1^k)$, which proves our assertion in this case. In the general case, we may assert that $(L/K\ ;\ \mathfrak{A})$ and $(L/K\ ;\ \mathfrak{A})^*$ have the same restriction to any subfield X of L which is cyclic over K, whence $(L/K\ ;\ \mathfrak{A}) = (L/K\ ;\ \mathfrak{A})^*$.

Thus, there is no inconvenient in denoting in general the element $(L/K\ ;\ \mathfrak{A})$ by $(L/K\ ;\ \mathfrak{A})$. The mapping $\mathfrak{A} \to (L/K\ ;\ \mathfrak{A})$ is called the *reciprocity mapping* for L/K.

THEOREM 18.1. *Let K be a field of algebraic numbers of finite degree and L/K a finite normal extension of K, whose Galois group we denote by $\mathfrak{G}$. Then the reciprocity mapping for L/K is an epimorphism of $\mathfrak{C}_K$ on $\mathfrak{G}/\mathfrak{G}'$ (where $\mathfrak{G}'$ is the commutator subgroup of $\mathfrak{G}$) whose kernel is $N_{L/K}\,\mathfrak{C}_L$.*

Let $\mathfrak{N}$ be the intersection of all groups $N_{X/K}\mathfrak{C}_X$, where X/K runs over all cyclic extensions of K contained in L/K. Then it follows from theorem 15.1 that the pairing $(\mathfrak{A}, \chi) \to \langle \mathfrak{A}, \chi\rangle^*$ defines a regular pairing of $\mathfrak{C}_K/\mathfrak{N}$ and $\mathrm{Char}\,\mathfrak{G}$ to $\mathbf{R}^*$. By a well known theorem, this implies that $\mathfrak{C}_K/\mathfrak{N}$ is isomorphic to $\mathrm{Char}\,(\mathrm{Char}\,\mathfrak{G}) \cong \mathfrak{G}/\mathfrak{G}'$; more precisely, $(L/K\ ;\ \mathfrak{A})$ depends only on the class α of $\mathfrak{A}$ modulo $\mathfrak{N}$, and, if we set $(L/K\ ;\ \alpha) = (L/K\ ;\ \mathfrak{A})$, then $\alpha \to (L/K\ ;\ \alpha)$ is an isomorphism of $\mathfrak{C}_K/\mathfrak{N}$ with $\mathfrak{G}/\mathfrak{G}'$. But $\mathfrak{N}$ obviously contains $N_{L/K}\mathfrak{C}_L$, and $\mathfrak{C}_K/N_{L/K}\mathfrak{C}_L \cong \mathfrak{G}/\mathfrak{G}'$ by theorem 17.2. It follows that $\mathfrak{N} = N_{L/K}\mathfrak{C}_L$, and theorem 18.1 is proved.

THEOREM 18.2. *Let the notation be as above and let L'/K be a finite normal extension containing L/K. Let A_L and $A_{L'}$ be the maximal abelian extensions contained in L/K and L'/K. Then, for any $\mathfrak{A} \in \mathfrak{C}_K$, $(L/K\ ;\ \mathfrak{A})$ is the restriction* *of* $(L'/K\ ;\ \mathfrak{A})$ *to* A_L.

This has been proved above.

THEOREM 18.3. *Let the notation be as above, and let* K' *be an intermediary field between* K *and* L; *denote by* $\mathfrak{H}$ *the Galois group of* L/K'. *Let* $\mathfrak{A}$ *be in* $\mathfrak{C}_K$; *then* $(L/K'\ ;\ \mathfrak{A})$ *is the image of* $(L/K\ ;\ \mathfrak{A})$ *under the transfer mapping from* $\mathfrak{G}/\mathfrak{G}'$ *to* $\mathfrak{H}/\mathfrak{H}'$ *(where* $\mathfrak{G}'$ *and* $\mathfrak{H}'$ *are the commutator subgroups of* $\mathfrak{G}$ *and* $\mathfrak{H}$*).*

Let χ be any element of Char $\mathfrak{H}$, and α the class of $\mathfrak{A}$ in ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$. Then the class of $\mathfrak{A}$ in ${}^0H(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ is $r_{K\to K'}\,\alpha$.

Let $\zeta(\chi)$ be the element of ${}^2H(\mathfrak{H}\ ;\ \mathbf{Z})$ which corresponds to the character χ, and let χ' be the character of $\mathfrak{G}$ which corresponds to $R_{\mathbf{Z}}\zeta(\chi)$, where $R_{\mathbf{Z}}$ is the injection map: ${}^2H(\mathfrak{H}\ ;\ \mathbf{Z}) \to {}^2H(\mathfrak{G}\ ;\ \mathbf{Z})$. Then we have $R_{K'\to K}M^{\mathfrak{N}}_{\mathfrak{C}_L,\mathbf{Z}}(r_{K\to K'}\,\alpha\otimes\zeta(\chi)) = M^{\mathfrak{N}}_{\mathfrak{C}_L,\mathbf{Z}}(\alpha\otimes R_{\mathbf{Z}}\zeta(\chi))$ by formula (7.3). Thus, we have

$$R_{K'\to K}\langle\mathfrak{A},\chi\rangle = \langle\mathfrak{A},\chi'\rangle.$$

Set $\langle\mathfrak{A},\chi\rangle = k\xi_{L/K'} = kr_{K\to K'}\xi_{L/K}$ (theorem 17.4). We have $R_{K'\to K}r_{K\to K'}\xi_{L/K} = [K : K']\xi_{L/K}$ (theorem 7.3), whence $\langle\mathfrak{A},\chi'\rangle = [K : K']k\xi_{L/K}$, and $\chi'((L/K\ ;\mathfrak{A})) = \chi((L/K'\ ;\ \mathfrak{A}))$. On the other hand, we have $\chi'(\bar{s}) = \chi(\tau(\bar{s}))$ if τ is the transfer map. It follows that $(L/K'\ ;\ \mathfrak{A}) = \tau((L/K\ ;\ \mathfrak{A}))$.

THEOREM 18.4. *Let* K' *be any extension of finite degree of* K *and let* $\mathfrak{A}$ *be an idèle class of* K'. *Then the restriction of* $(LK'/K'\ ;\ \mathfrak{A})$ *to* A_L *(the largest abelian overfield of* K *in* L*) is* $(L/K\ ;\ N_{K'/K}\mathfrak{A})$.

Let K''/K be a finite normal extension of K containing K'/K. Then $(LK'/K'\ ;\ \mathfrak{A})$ is the restriction of $(LK''/K'\ ;\ \mathfrak{A})$ to the largest abelian extension of K' contained in LK' (theorem 18.2). It follows that it will be sufficient to consider the case where $K'\subset L$. Let $\mathfrak{H}$ be Galois group of L/K' and α the element of ${}^0H(\mathfrak{H}\ ;\ \mathfrak{C}_L)$ represented by $\mathfrak{A}$. Then the element of ${}^0H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ represented by $N_{K'/K}\mathfrak{A}$ is clearly $R_{K'\to K}\alpha$. Let χ be any character of $\mathfrak{G}$, and let $\xi(\chi)$ be the corresponding element of ${}^2H(\mathfrak{G}\ ;\ \mathbf{Z})$. Then it follows immediately from formula (7.3), that

$$R_{K'\to K}M^{\mathfrak{N}}_{\mathfrak{C}_L,\mathbf{Z}}(\alpha\otimes r_{K\to K'}\xi(\chi)) = M^{\mathfrak{N}}_{\mathfrak{C}_L,\mathbf{Z}}(R_{K'\to K}\alpha\otimes\xi(\chi)).$$

The element $r_{K\to K'}\xi(\chi)$ is the one which corresponds to the restriction χ' of χ to $\mathfrak{H}$. Thus we have $R_{K'\to K}\langle\mathfrak{A},\chi'\rangle = \langle N_{K'/K}\mathfrak{A},\chi\rangle$.

We have seen in the proof of theorem 18.3 that $R_{K'\to K}\hat{\xi}_{L/K'}=[K':K]\hat{\xi}_{L/K}$. Thus, if $\langle\mathfrak{A},\chi'\rangle=k\hat{\xi}_{L/K'}$, we have $\langle N_{K'/K}\mathfrak{A},\chi\rangle=k[K:K']\hat{\xi}_{L/K}$, whence $\chi'((L/K';\mathfrak{A}))=\chi((L/K;N_{K'/K}\mathfrak{A}))$. Since χ' is the restriction of χ to $\mathfrak{H}$, the left side is $\chi(s)$, where s is the restriction of $(L/K';\mathfrak{A})$ to A_L; thus we have $s=(L/K;N_{K'/K}\mathfrak{A})$.

If $\mathfrak{a}$ is any idèle in K and $\mathfrak{A}$ the idèle class of $\mathfrak{a}$, we set

$$(L/K;\mathfrak{a})=(L/K;\mathfrak{A}).$$

§ 19. THE NORM RESIDUE SYMBOL

Let K be a field of algebraic numbers of finite degree. If $\mathfrak{p}$ is any place of K, we denote by $K_{\mathfrak{p}}$ the $\mathfrak{p}$-adic completion of K and by $K_{\mathfrak{p}}^*$ the multiplicative group of elements $\neq 0$ of $K_{\mathfrak{p}}$. If L/K is a finite normal extension of K, we shall donote by $LK_{\mathfrak{p}}/K$ a composite extension of $K_{\mathfrak{p}}/K$ and L/K; this extension is determined up to isomorphism. If $\mathfrak{P}$ is any place of L above $\mathfrak{p}$, then $LK_{\mathfrak{p}}$ is isomorphic to the $\mathfrak{P}$-adic completion of L. We shall denote by $(LK_{\mathfrak{p}})^*$ the group of elements $\neq 0$ in $LK_{\mathfrak{p}}$. The extension $LK_{\mathfrak{p}}/K_{\mathfrak{p}}$ is normal, and its Galois group is isomorphic to the decomposition group of $\mathfrak{P}$.

We denote by $J_L^{\mathfrak{p}}$ the group of idèles of L whose components at all places not above $\mathfrak{p}$ are 1. If $\mathfrak{G}$ is the Galois group of L/K, J_L is a $\mathfrak{G}$-module, and $J_L^{\mathfrak{p}}$ a submodule of J_L. The identity map of $J_L^{\mathfrak{p}}$ into J_L, followed by the canonical mapping of J_L onto $\mathfrak{C}_L$, gives a $\mathfrak{G}$-module homomorphism $\iota_{\mathfrak{p}}$ of $J_L^{\mathfrak{p}}$ into $\mathfrak{C}_L$. and $\iota_{\mathfrak{p}}$ defines a mapping $\iota_{\mathfrak{p}}^*$ of $H'(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ into $H'(\mathfrak{G}\ ;\ \mathfrak{C}_L)$.

THEOREM 19.1. *Set $n=[L:K]$, $n(\mathfrak{p})=[LK_{\mathfrak{p}}:K_{\mathfrak{p}}]$. Then $n/n(\mathfrak{p})\xi_{L/K}$ belongs to the image of ${}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ under $\iota_{\mathfrak{p}}^*$.*

If $\mathfrak{p}$ is finite, then there exists a cyclic cyclotomic extension Z/K which satisfies the following conditions: $\mathfrak{p}$ is not ramified in Z, and $N(\mathfrak{p})=[ZK_{\mathfrak{p}}:K_{\mathfrak{p}}]$ is divisible by $n(\mathfrak{p})$. If $\mathfrak{p}$ is infinite, set $Z=K(i)$, where $i^2=-1$; then it is still true that $N(\mathfrak{p})=[ZK_{\mathfrak{p}}:K_{\mathfrak{p}}]$ is divisible by $n(\mathfrak{p})$. We denote by $\mathfrak{Z}$ the Galois group of Z/K. The decomposition group of $\mathfrak{p}$ in Z/K is generated by the operation $(Z/K\ ;\ \mathfrak{p})$ of order $N/N(\mathfrak{p})$ (where N is the order of $\mathfrak{Z}$); we may therefore write $(Z/K\ ;\ \mathfrak{p})=s^{N/N(\mathfrak{p})}$, where s is a generator of $\mathfrak{Z}$. If $\mathfrak{p}$ is finite, let $\mathfrak{a}$ be an idèle of K whose $\mathfrak{p}$-component is of order 1 at $\mathfrak{p}$ and whose other components are 1; if $\mathfrak{p}$ is infinite real, let $\mathfrak{a}$ be an idèle of K whose $\mathfrak{p}$-component is -1 and whose other components are 1; if $\mathfrak{p}$ is infinite complex, set $\mathfrak{a}=1$. Let $\mathfrak{A}$ be the idèle class of $\mathfrak{a}$; then we have $(Z/K\ ;\ \mathfrak{A})=(Z/K\ ;\ \mathfrak{p})$ (cf. 3) and 3′), § 16). Let χ be the character of $\mathfrak{Z}$ such that $\chi(s)$ is the class of $1/N$ modulo $\mathbf{Z}$. Since $\chi((Z/K,\ \mathfrak{A}))$ is the class of $(N/N(\mathfrak{p}))1/N$ modulo $\mathbf{Z}$, we have $\langle\mathfrak{A},\chi\rangle = N/N(\mathfrak{p})\xi_{Z/K}$. Let α be the class of $\mathfrak{A}$ in ${}^0H(\mathfrak{Z}\ ;\ \mathfrak{C}_Z)$ and $\zeta(\chi)$ the element of ${}^2H(\mathfrak{Z}\ ;\ \mathbf{Z})$ which corresponds to the character χ; then we have

$$\langle \mathfrak{A}, \chi \rangle = M^{\mathfrak{N}}_{\mathfrak{C}_L, \mathbf{Z}}(\alpha \otimes \zeta(\chi)) = N/N(\mathfrak{p})\,\xi_{L/K}.$$

Let Γ be the Galois group of LZ/K; set $M = [LZ : Z]$. Denote by α' the class of $\mathfrak{A}$ in ${}^0H(\Gamma ; \mathfrak{C}_{LZ})$, whence $\alpha' = \lambda_{Z\to LZ}\,\alpha$. Let ζ' be the image of $\zeta(\chi)$ under the lift mapping from ${}^2H(\mathfrak{Z} ; \mathbf{Z})$ to ${}^2H(\Gamma ; \mathbf{Z})$. We have $\lambda_{Z\to LZ}\,\xi_{L/K} = M\xi_{LZ/K}$ (theorem 17.3). Making use of theorem 8.6, we have $MN/N(\mathfrak{p})\,\xi_{LZ/K} = M^{\mathfrak{N}}_{\mathfrak{C}_{LZ}, \mathbf{Z}}(\alpha' \otimes \zeta')$. If u is a representative of ζ' in $(J_2[\Gamma])^\Gamma$, then $MN/N(\mathfrak{p})\,\xi_{LZ/K}$ is represented by $\mathfrak{A} \otimes u$. Since $u \in (J_2[\Gamma])^\Gamma$ and $\mathfrak{a} \in J^{\mathfrak{p}}_K = (J^{\mathfrak{p}}_{LZ})^\Gamma$, $\mathfrak{a} \otimes u$ is in $(J^{\mathfrak{p}}_{LZ} \otimes J_2[\Gamma])^\Gamma$, and represents a certain cohomology class $\eta \in {}^2H(\Gamma ; J^{\mathfrak{p}}_{LZ})$. It is clear that

$$\iota^*_{\mathfrak{p}}\eta = MN/N(\mathfrak{p})\,\xi_{LZ/K}.$$

We shall prove that the restriction of $N(\mathfrak{p})/n(\mathfrak{p})\,\eta$ to the Galois group $\mathfrak{H}$ of LZ/L is 0. If β is the class of $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})}$ in ${}^0H(\mathfrak{H} ; J^{\mathfrak{p}}_{LZ})$, then the restriction of $N(\mathfrak{p})/n(\mathfrak{p})\eta$ to $\mathfrak{H}$ is $M^{\mathfrak{N}}_{J^{\mathfrak{p}}_{LZ}, \mathbf{Z}}(\beta \otimes \zeta'')$, where ζ'' is the restriction of ζ' to $\mathfrak{H}$ (formula (7.1)). It will therefore be sufficient to prove that $\beta = 0$, i.e. that $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})}$ belongs to $N_{LZ/L}J^{\mathfrak{p}}_{LZ}$. Assume first that $\mathfrak{p}$ is finite. Let $\mathfrak{P}_L$ be any place of L above $\mathfrak{p}$, and e its ramification index with respect to K; the order of $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})}$ at $\mathfrak{P}_L$ is therefore $eN(\mathfrak{p})/n(\mathfrak{p})$. On the other hand, the largest unramified extension of $K_{\mathfrak{p}}$ in $LK_{\mathfrak{p}}$ is of degree $n(\mathfrak{p})/e$ over $K_{\mathfrak{p}}$, and is therefore contained in $ZK_{\mathfrak{p}}/K_{\mathfrak{p}}$, since $ZK_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified of degree $N(\mathfrak{p})$ divisible by $n(\mathfrak{p})$. Since $ZK_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified, its intersection with $LK_{\mathfrak{p}}/K_{\mathfrak{p}}$ is the largest unramified extension of $K_{\mathfrak{p}}$ in $LK_{\mathfrak{p}}$, and $LZK_{\mathfrak{p}}/LK_{\mathfrak{p}}$ is of degree $N(\mathfrak{p})/(n(\mathfrak{p})/e) = eN(\mathfrak{p})/n(\mathfrak{p})$; moreover, this extension is unramified. It follows that the $\mathfrak{P}_L$-component of $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})}$ is in $N_{LZK_{\mathfrak{p}}/LK_{\mathfrak{p}}}(LZK_{\mathfrak{p}})^*$. This being true for every place $\mathfrak{P}_L$ of L above $\mathfrak{p}$, $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})}$ belongs to $N_{LZ/L}J^{\mathfrak{p}}_{LZ}$ (theorem 12.3).

In the case where $\mathfrak{p}$ is infinite and $N(\mathfrak{p})/n(\mathfrak{p}) = 2$, we have $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})} = 1$. Assume that $N(\mathfrak{p}) = n(\mathfrak{p})$; if $\mathfrak{p}$ is real, then $N(\mathfrak{p}) = 2$ by our definition of Z, whence $n(\mathfrak{p}) = 2$, and the places of L above $\mathfrak{p}$ are imaginary; the same conclusion is valid if $\mathfrak{p}$ is imaginary. It follows immediately that $\mathfrak{a}^{N(\mathfrak{p})/n(\mathfrak{p})} \in N_{LZ/LZ}J^{\mathfrak{p}}_{LZ}$.

If $\mathfrak{P}_{LZ}$ is any place of LZ above $\mathfrak{p}$ and $\mathfrak{H}(\mathfrak{P}_{LZ})$ the decomposition group of $\mathfrak{P}_{LZ}$ with respect to LZ, then ${}^1H(\mathfrak{H}(\mathfrak{P}_{LZ}) ; (LZ)^*_{\mathfrak{P}_{LZ}}) = \{0\}$. Therefore, it follows from theorem 12.1 that ${}^1H(\mathfrak{H} ; J^{\mathfrak{p}}_{LZ}) = \{0\}$. Making use of theorem 8.2, we see that we may write

$$N(\mathfrak{p})/n(\mathfrak{p})\,\eta = \lambda(\eta')$$

where λ is the lift mapping from ${}^2H(\mathfrak{G} ; J^{\mathfrak{p}}_L)$ to ${}^2H(\Gamma ; J^{\mathfrak{p}}_{LZ})$, $\mathfrak{G} = \Gamma/\mathfrak{H}$ being the

Galois group of L/K. It follows that $N(\mathfrak{p})/n(\mathfrak{p})\,\iota_{\mathfrak{p}}^{*}\eta = \lambda_{L\to LZ}(\iota_{\mathfrak{p}}^{*}\eta')$ (theorem 8.7). The left side is $MN/n(\mathfrak{p})\,\xi_{LZ/K} = n/n(\mathfrak{p})\,\lambda_{L\to LZ}\,\xi_{L/K}$ (theorem 17.3) since $[LZ : L]$ MN/n. Thus we have

$$\lambda_{L\to LZ}(n/n(\mathfrak{p})\,\xi_{L/K} - \iota_{\mathfrak{p}}^{*}\eta') = 0$$

whence $n/n(\mathfrak{p})\,\xi_{L/K} = \iota_{\mathfrak{p}}^{*}\eta'$, which proves theorem 19.1.

If $\mathfrak{a}$ is any idèle in K and $\mathfrak{A}$ the class of $\mathfrak{a}$, we set

$$(L/K\ ;\ \mathfrak{a}) = (L/K\ ;\ \mathfrak{A}).$$

If $\mathfrak{p}$ is a place of K and $x\in K_{\mathfrak{p}}^{*}$, denote by $\mathfrak{a}^{\mathfrak{p}}(x)$ the idèle whose $\mathfrak{p}$-component is x and whose other components are 1; we set

$$\left(\frac{x,\ L/K}{\mathfrak{p}}\right) = (L/K\ ;\ \mathfrak{a}^{\mathfrak{p}}(x))$$

THEOREM 19.2. *Let K be a field of algebraic numbers of finite degree and L/K a finite normal extension of K. Denote by $\mathfrak{p}$ a place of K and by $\mathfrak{Z}$ the decomposition group of $\mathfrak{p}$ in A_L/K, where A_L is the largest abelian extension contained in L. Then $x \to \left(\frac{x,\ L/K}{\mathfrak{p}}\right)$ is an epimorphism of $K_{\mathfrak{p}}^{*}$ on $\mathfrak{Z}$, whose kernel is $N_{LK_{\mathfrak{p}}/K_{\mathfrak{p}}}(LK_{\mathfrak{p}})^{*}$.*

Let T be the decomposition field of $\mathfrak{p}$ in the extension A_L/K; then $\mathfrak{Z}$ is the Galois group of A_L/T, and $\mathfrak{p}$ splits completely in T. It follows that, if $x\in K_{\mathfrak{p}}^{*}$, then $\mathfrak{a}^{\mathfrak{p}}(x)$ may be written in the form $N_{T/K}\mathfrak{b}$, where $\mathfrak{b}$ is an idèle of T. We have $\left(\frac{x,\ L/K}{\mathfrak{p}}\right) = (A_L/T\ ;\ \mathfrak{b})\in\mathfrak{Z}$ by theorem 18.4. Let T' be the field of elements of A_L which are left invariant by all elements of the form $\left(\frac{x,\ L/K}{\mathfrak{p}}\right)$, $x\in K_{\mathfrak{p}}^{*}$. Then T' contains T, and we wish to prove that $T' = T$. Let $\mathfrak{p}_T$ be a place of T above $\mathfrak{p}$, and $\mathfrak{b}$ an idèle of T whose components at every place $\neq \mathfrak{p}_T$ are 1. Then $N_{T/K}\mathfrak{b}$ is of the form $\mathfrak{a}^{\mathfrak{p}}(x)$, with some $x\in K_{\mathfrak{p}}^{*}$; it follows that $(A_L/T\ ;\ \mathfrak{b})$ belongs to the Galois group of A_L/T', whence $(T'/T\ ;\ \mathfrak{b}) = e$ (the neutral element). Assume for a moment that $T' \neq T$; then T'/T contains a cyclic extension T''/T of prime degree of T, whose Galois group we denote by $\mathfrak{T}$. Since T is the decomposition field of $\mathfrak{p}$ in A_L/K, there is only one place of T'' above $\mathfrak{p}_T$; therefore, it follows from theorem 19.1 that the canonical class $\xi_{T''/T}$ may be written in the form $\iota_{\mathfrak{p}_T}^{*}(\eta)$, where η is an element of ${}^{2}H(\mathfrak{T}\ ;\ J_{T''}^{\mathfrak{p}_T})$. Let ζ be a generator of ${}^{2}H(\mathfrak{T}\ ;\ \mathbf{Z})$; then η may be written in the form $M^{\mathfrak{N}}_{J_{T''}^{\mathfrak{p}_T},\mathbf{Z}}(\beta\otimes\zeta)$, where β is an element of ${}^{0}H(\mathfrak{T}\ ;\ J_{T''}^{\mathfrak{p}_T})$. Thus we have

$$\xi_{T''/T} = M^{\mathfrak{N}}_{\mathfrak{G}_T, \mathrm{Z}}(\iota^*_{\mathfrak{p}T}\beta \otimes \zeta).$$

If $\mathfrak{b} \in J_T^{\mathfrak{p}T}$ is a representative of β, then the idèle class $\mathfrak{B}$ of $\mathfrak{b}$ is a representative of $\iota^*_{\mathfrak{p}T}\beta$. Since $(T''/T\,;\,\mathfrak{B}) = (T''/T\,;\,\mathfrak{b}) = e$, we have $\mathfrak{B} \in N_{T''/T}\mathfrak{C}_{T'}$, and $\iota^*_{\mathfrak{p}T}\beta = 0$, whence $\xi_{T'/T} = 0$, which brings a contradiction. This proves that $T' = T$ and that $x \to \left(\frac{x,\, L/K}{\mathfrak{p}}\right)$ is an epimorphism on $\mathfrak{Z}$.

Assume now that $\left(\frac{x,\, L/K}{\mathfrak{p}}\right) = e$. Denote by $\mathfrak{P}$ some place of L above $\mathfrak{p}$ and by T_0 the decomposition field of $\mathfrak{P}$ in the extension L/K. Among all subfields X of L containing T_0 such that $x \in N_{XK_\mathfrak{p}/K_\mathfrak{p}}(XK_\mathfrak{p})^*$, select one, which we now call X, of maximal degree. Let $\mathfrak{p}(X)$ be the place of X below $\mathfrak{P}$; then we may write $\mathfrak{a}^{\mathfrak{p}}(x) = N_{X/K}\,\mathfrak{a}^{\mathfrak{p}(X)}(y)$, where y is an element of $X_{\mathfrak{p}(X)}$ whose norm with respect to $K_\mathfrak{p}$ is x. We wish to prove that $X = L$. Assuming for a moment that this is not the case, let Y/X be a cyclic extension of prime degree q of X contained in L/X (there exists such an extension because the Galois group of L/X is a subgroup of the decomposition group of $\mathfrak{P}$ and is therefore solvable). The decomposition group of $\mathfrak{p}(X)$ in the extension Y/X is the whole Galois group $\mathfrak{Y}$ of Y/X. Therefore, it follows from what we have already proved that $u \to \left(\frac{u,\, Y/X}{\mathfrak{p}(X)}\right)$ is an epimorphism of $X^*_{\mathfrak{p}(X)}$ on $\mathfrak{Y}$; the kernel of this epimorphism is therefore of index q. This kernel clearly contains $N_{YX_{\mathfrak{p}(X)}/X_{\mathfrak{p}(X)}}(YX_{\mathfrak{p}(X)})^*$; but we know that the latter group is of index q in $X^*_{\mathfrak{p}(X)}$; it is therefore exactly the kernel of our epimorphism. Now, we have $e = (L/K\,;\,\mathfrak{a}^{\mathfrak{p}}(x)) = (L/X\,;\,\mathfrak{a}^{\mathfrak{p}(X)}(y))$ (theorem 18.4). It follows that $(Y/X,\, \mathfrak{a}^{\mathfrak{p}(X)}(y)) = \left(\frac{y,\, Y/X}{\mathfrak{p}(X)}\right) = e$, and therefore that y is the norm with respect to $X_{\mathfrak{p}(X)}$ of an element of $(YX_{\mathfrak{p}(X)})^*$, whence $x \in N_{YK_\mathfrak{p}/K_\mathfrak{p}}(YK_\mathfrak{p})^*$, in contradiction with the definition of X. Theorem 19.2 is thereby proved.

The symbol $\left(\frac{x,\, L/K}{\mathfrak{p}}\right)$ is accordingly called the *norm residue symbol.* It has the following formal properties which follow immediately from the corresponding properties of the reciprocity mapping:

1. Let L'/K be a finite normal extension of K containing L/K; if $x \in K_\mathfrak{p}$, then $\left(\frac{x, L/K}{\mathfrak{p}}\right)$ is the restriction of $\left(\frac{x, L'/K}{\mathfrak{p}}\right)$ to the maximal abelian extension of K contained in L/K.

2. Let K' be an intermediary field between K and L; denote by $\mathfrak{G}$ and $\mathfrak{H}$ the Galois group of L with respect to K and K', and by $\mathfrak{G}'$ and $\mathfrak{H}'$ their com-

mutator subgroups; let x be in $K_{\mathfrak{p}}$; then $\Pi_{\mathfrak{p}'}\left(\frac{x, L/K'}{\mathfrak{p}'}\right)$ (the product being extended to all places $\mathfrak{p}'$ of K' above $\mathfrak{p}$) *is the image of $\left(\frac{x, L/K}{\mathfrak{p}}\right)$ under the transfer mapping of $\mathfrak{G}/\mathfrak{G}'$ into $\mathfrak{H}/\mathfrak{H}'$.*

3. Let K'/K be a finite extension of K, $\mathfrak{p}'$ a place of K' above $\mathfrak{p}$ and x' an element of $K'_{\mathfrak{p}'}$; then the restriction of $\left(\frac{x', L'/K'}{\mathfrak{p}'}\right)$ to the largest abelian extension of K contained in A_L/K is $\left(\frac{N_{K'_{\mathfrak{p}'}/K_{\mathfrak{p}}}x', L/K}{\mathfrak{p}}\right)$.

THEOREM 19.3. *Assume that $\mathfrak{p}$ is finite and not ramified in L. Let x be an element of $K_{\mathfrak{p}}^*$, and a the order of x at $\mathfrak{p}$. Let A_L/K be the largest abelian extension of K in L/K. Then $\left(\frac{x, L/K}{\mathfrak{p}}\right) = (A_L/K\,;\,\mathfrak{p})^a$.*

Let Z/K be a cyclic cyclotomic extension of K in which $\mathfrak{p}$ is not ramified and such that $[ZK_{\mathfrak{p}} : K_{\mathfrak{p}}]$ is divisible by $[LK_{\mathfrak{p}} : K_{\mathfrak{p}}]$. Then $\mathfrak{p}$ is not ramified in LZ; let $\mathfrak{P}_{LZ}$ be a place of LZ above $\mathfrak{p}$. Its decomposition group is generated by $(LZ/K\,;\,\mathfrak{P}_{LZ})$. If $\mathfrak{P}_L$, $\mathfrak{P}_Z$ are the places of L, Z below $\mathfrak{P}_{LZ}$, then the restrictions of $(LZ/K\,;\,\mathfrak{P}_{LZ})$ to L and Z are $(L/K\,;\,\mathfrak{P}_L)$ and $(Z/K\,;\,\mathfrak{P}_Z) = (Z/K\,;\,\mathfrak{p})$. The operation $\left(\frac{x, LZ/K}{\mathfrak{p}}\right)$ is the restriction to the maximal abelian extension ZA_L/K of K contained in LZ/K of an operation s of the decomposition group of $\mathfrak{P}_{LZ}$; write $s = (LZ/K\,;\,\mathfrak{P}_{LZ})^h$. The restriction of s to Z is $\left(\frac{x, Z/K}{\mathfrak{p}}\right) = (Z/K\,;\,\mathfrak{p})^a$ (cf. 3), §16); thus $(Z/K\,;\,\mathfrak{p})^a = (Z/K\,;\,\mathfrak{p})^h$, whence $a \equiv h \pmod{[ZK_{\mathfrak{p}} : K_{\mathfrak{p}}]}$, since $(Z/K\,;\,\mathfrak{p})$ is of order $[ZK_{\mathfrak{p}} ; K_{\mathfrak{p}}]$. The restriction of $\left(\frac{x, LZ/K}{\mathfrak{p}}\right)$ to A_L is $\left(\frac{x, L/K}{\mathfrak{p}}\right)$, while that of $(LZ/K\,;\,\mathfrak{P}_{LZ})$ is $(A_L/K\,;\,\mathfrak{p})$. Since $h \equiv a \pmod{[LK_{\mathfrak{p}} : K_{\mathfrak{p}}]}$ and $(A_L/K\,;\,\mathfrak{p})$ is of order $[LK_{\mathfrak{p}} : K_{\mathfrak{p}}]$, theorem 19.3 is proved.

THEOREM 19.4. *Let $\mathfrak{a}$ be any idèle of K. Then there are only a finite number of places $\mathfrak{p}$ of K such that $\left(\frac{\mathfrak{a}_{\mathfrak{p}}, L/K}{\mathfrak{p}}\right) \neq e$, and we have*

$$(L/K\,;\,\mathfrak{a}) = \Pi_{\mathfrak{p}}\left(\frac{\mathfrak{a}_{\mathfrak{p}}, L/K}{\mathfrak{p}}\right),$$

the product being extended to all places $\mathfrak{p}$ of K.

Let E be a finite set of places of K containing all infinite places, all places ramified in L and all finite places $\mathfrak{p}$ such that $\mathfrak{a}_{\mathfrak{p}}$ is not a unit. Then we have $\left(\frac{\mathfrak{a}_{\mathfrak{p}}, L/K}{\mathfrak{p}}\right) = e$ for all $\mathfrak{p} \notin E$ by theorem 11.1. Write

$$\mathfrak{a} = \left(\prod\nolimits_{\mathfrak{p} \in F} \mathfrak{a}^{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})\right) \mathfrak{b},$$

where $\mathfrak{b}$ is an idèle. Then we have $\mathfrak{b}_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in E$, while, if $\mathfrak{q} \notin E$, then $\mathfrak{b}_{\mathfrak{q}}$ is a unit. It follows that $\mathfrak{b} \in N_{L/K} J_L$, whence $(L/K\,;\,\mathfrak{b}) = e$ and $(L/K\,;\,\mathfrak{a}) = \prod_{\mathfrak{p} \in F} (L/K\,;\,\mathfrak{a}^{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}}))$; theorem 19.4 follows immediately from this.

COROLLARY. *If x is any number $\neq 0$ in K, we have*

$$\prod\nolimits_{\mathfrak{p}} \left(\frac{x,\, L/K}{\mathfrak{p}}\right) = e.$$

§20. DETERMINATION OF CERTAIN COHOMOLOGY GROUPS

We use the same notation as in the preceding section. If $\mathfrak{G}$ is the Galois group of L/K, we know that

$$^2H(\mathfrak{G}\ ;\ J_L) \cong \sum_{\mathfrak{p}} {}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}) \quad \text{(direct)},$$

the sum being extended to all places $\mathfrak{p}$ of K (theorem 12.4). Let $\mathfrak{P}$ be a place of L above a place $\mathfrak{p}$ of K, and let $\mathfrak{G}(\mathfrak{P})$ be its decomposition group. Then we know that ${}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}) \cong {}^2H(\mathfrak{G}(\mathfrak{P})\ ;\ L_{\mathfrak{P}}^*)$ (theorem 12.1), and that the order of this group divides $n(\mathfrak{p}) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. On the other hand, if $n = [L : K]$, then $\iota_{\mathfrak{p}}^*({}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}))$ contains $n/n(\mathfrak{p})\xi_{L/K}$, which is of order $n(\mathfrak{p})$. This proves the following result:

THEOREM 20.1 *For any place $\mathfrak{p}$ of K, the group ${}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ is cyclic of order equal to $n_{\mathfrak{p}} = [LK_{\mathfrak{p}} : K_{\mathfrak{p}}]$; the mapping $\iota_{\mathfrak{p}}^*$ of this group into ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ is a monomorphism.*

Let ξ be an element of ${}^2H(\mathfrak{G}\ ;\ J_L)$; Let $\sum_{\mathfrak{p}} \xi_{\mathfrak{p}}$ be the corresponding element of $\sum_{\mathfrak{p}} {}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$. Then, for each $\mathfrak{p}$, we may write $\iota_{\mathfrak{p}}^*(\xi_{\mathfrak{p}}) = kn/n(\mathfrak{p}) \cdot \xi_{L/K}$, where k is an integer whose residue class modulo $n(\mathfrak{p})$ is uniquely determined. The residue class modulo $\mathbf{Z}$ of $k/n(\mathfrak{p})$ is called the *$\mathfrak{p}$-invariant of ξ*, and is denoted by $\rho_{\mathfrak{p}}(\xi)$. We have proved

THEOREM 20.2. *An element ξ of ${}^2H(\mathfrak{G}\ ;\ J_L)$ is uniquely determined by its $\mathfrak{p}$-invariants for all places $\mathfrak{p}$. If $n(\mathfrak{p}) = [LK\mathfrak{p} : K_{\mathfrak{p}}]$, then $n(\mathfrak{p})\rho_{\mathfrak{p}}(\xi) = 0$. Conversely, let there be given for each $\mathfrak{p}$ an element $\rho_{\mathfrak{p}} \in \mathbf{R}^*$ such that $n(\mathfrak{p})\rho_{\mathfrak{p}} = 0$; assume that only a finite number of the elements $\rho_{\mathfrak{p}}$ are $\neq 0$. Then there exists a $\xi \in {}^2H(\mathfrak{G}\ ;\ J_L)$ such that $\rho_{\mathfrak{p}}(\xi) = \rho_{\mathfrak{p}}$ for every $\mathfrak{p}$.*

Consider now the exact sequence

$$\{1\} \longrightarrow P_L \xrightarrow{\iota} J_L \xrightarrow{\pi} \mathfrak{C}_L \longrightarrow \{1\}.$$

It gives rise to an exact sequence

$$^1H(\mathfrak{G}\ ;\ \mathfrak{C}_L) \xrightarrow{\delta} {}^2H(\mathfrak{G}\ ;\ P_L) \xrightarrow{\iota^*} {}^2H(\mathfrak{G}\ ;\ J_L) \xrightarrow{\pi^*} {}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L).$$

We know that ${}^1H(\mathfrak{G}\ ;\ \mathfrak{C}_L)=\{0\}$; thus ι^* induces an isomorphism of ${}^2H(\mathfrak{G}\ ;\ P_L)$ with the kernel of π^*. Let ξ be any element of ${}^2H(\mathfrak{G}\ ;\ J_L)$, and let $\sum_{\mathfrak{p}}\xi_{\mathfrak{p}}$ be the element of $\sum_{\mathfrak{p}}{}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ which corresponds to ξ. Then it is clear that $\pi^*(\xi)=\sum_{\mathfrak{p}}\iota_{\mathfrak{p}}^*(\xi_{\mathfrak{p}})$. Write $\iota_{\mathfrak{p}}^*(\xi_{\mathfrak{p}})=k_{\mathfrak{p}}\xi_{L/K}$, where $k_{\mathfrak{p}}$ is an integer and $k_{\mathfrak{p}}=0$ for almost all $\mathfrak{p}$. Then $\pi^*(\xi)=(\sum_{\mathfrak{p}}k_{\mathfrak{p}})\xi_{L/K}$. This is 0 if and only if $\sum_{\mathfrak{p}}k_{\mathfrak{p}}$ is divisible by $n=[L:K]$; since $\rho_{\mathfrak{p}}(\xi)$ is the class of $k_{\mathfrak{p}}/n$ modulo $\mathbf{Z}$, we obtain the following results.

THEOREM 20.3. *Let π^* be the mapping: ${}^2H(\mathfrak{G}\ ;\ J_L)\rightarrow{}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ which corresponds to the canonical mapping $\pi : J_L\rightarrow\mathfrak{C}_L$. Then the kernel of π^* is isomorphic to ${}^2H(\mathfrak{G}\ ;\ P_L)$ and is composed of all elements $\xi\in{}^2H(\mathfrak{G}\ ;\ J_L)$ the sum of whose invariant is* 0.

Next, we observe that ${}^3H(\mathfrak{G}\ ;\ J_L)=\{0\}$. For, this group is isomorphic to $\sum_{\mathfrak{p}}{}^3H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ (direct); and, using the same notation as above, ${}^3H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}})$ is isomorphic to ${}^3H(\mathfrak{G}(\mathfrak{P})\ ;\ L_{\mathfrak{P}}^*)$. Let $\mathfrak{H}$ be any subgroup of $\mathfrak{G}(\mathfrak{P})$; this is the Galois group of L/K', where K' is an intermediary field between K and L which contains the field of decomposition of $\mathfrak{P}$. The group $\mathfrak{H}$ is the decomposition group of $\mathfrak{P}$ in the extension L/K'. Making use of the result established above, we see that ${}^2H(\mathfrak{H}\ ;\ L_{\mathfrak{P}}^*)$ is cyclic of the same order as $\mathfrak{H}$. Moreover, ${}^1H(\mathfrak{H}\ ;\ L_{\mathfrak{P}}^*)=\{0\}$. Making use of Tate's theorem (theorem 9.2), we see that ${}^3H(\mathfrak{G}(\mathfrak{P})\ ;\ L_{\mathfrak{P}}^*)\cong{}^1H(\mathfrak{G}(\mathfrak{P})\ ;\ \mathbf{Z})=\{0\}$, which proves our assertion.

This being said, we have an exact sequence

$$ {}^2H(\mathfrak{G}\ ;\ J_L)\xrightarrow{\pi^*}{}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)\xrightarrow{\delta}{}^3H(\mathfrak{G}\ ;\ P_L)\xrightarrow{\iota^*}{}^3H(\mathfrak{G}\ ;\ J_L)\ ; $$

since ${}^3H(\mathfrak{G}\ ;\ J_L)=\{0\}$, we see that ${}^3H(\mathfrak{G}\ ;\ P_L)$ is $\delta({}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L))$ and isomorphic to ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)/\pi^*({}^2H(\mathfrak{G}\ ;\ J_L))$. The group ${}^2H(\mathfrak{G}\ ;\ \mathfrak{C}_L)$ being cyclic, we see that ${}^3H(\mathfrak{G}\ ;\ P_L)$ is cyclic and is generated by $\delta(\xi_{L/K})$. The group $\pi^*({}^2H(\mathfrak{G}\ ;\ J_L))$ is the sum of the groups $\iota_{\mathfrak{p}}^*({}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}))$, and $\iota_{\mathfrak{p}}^*({}^2H(\mathfrak{G}\ ;\ J_L^{\mathfrak{p}}))$ is generated by $n/n(\mathfrak{p})\xi_{L/K}$, where $n(\mathfrak{p})=[LK_{\mathfrak{p}}\ ;\ K_{\mathfrak{p}}]$. It follows that $\pi^*({}^2H(\mathfrak{G}\ ;\ J_L))$ is generated by $m\xi_{L/K}$, where m is the H.C.D. of the numbers $n/n(\mathfrak{p})$. Thus we obtain

THEOREM 20.4. *The group ${}^3H(\mathfrak{G}\ ;\ P_L)$ is cyclic of order equal to the H.C.D. of the numbers $n/n(\mathfrak{p})$, where $n=[L:K]$, $n(\mathfrak{p})=[LK_{\mathfrak{p}}:K_{\mathfrak{p}}]$. It is generated by $\delta(\xi_{L/K})$, where δ is the mapping which corresponds to the exact sequence*

$1 \to P_L \to J_L \to \mathfrak{C}_L \to 1.$

We know by Tate's theorem that ${}^{-1}H(\mathfrak{G}\ ;\ \mathfrak{C}_L) \cong {}^{-3}H(\mathfrak{G}\ ;\ \mathbf{Z})$. Thus we have

THEOREM 20.5. *The factor group of the group of idèle classes* $\mathfrak{A}$ *such that* $N_{L/k}\mathfrak{A}=1$ *by the group generated by the elements* $\mathfrak{B}^{1-s}$, $\mathfrak{B}\in\mathfrak{C}_L$, $s\in\mathfrak{G}$, *is isomorphic to* ${}^{-3}H(\mathfrak{G}\ ;\ \mathbf{Z})$.

If we consider the exact sequence

$${}^{-1}H(\mathfrak{G}\ ;\ \mathfrak{C}_L) \xrightarrow{\delta} {}^{0}H(\mathfrak{G}\ ;\ P_L) \xrightarrow{\iota^*} {}^{0}H(\mathfrak{G}\ ;\ J_L)$$

we obtain the following result:

THEOREM 20.6. *The group* $(P_k \cap N_{L/k}J_L)/N_{L/k}P_L$ *is isomorphic to a factor group of* ${}^{-3}H(\mathfrak{G}\ ;\ \mathbf{Z})$.

§ 21. THE EXISTENCE THEOREM

Let K be a field of algebraic numbers of finite degree. If L/K is any finite abelian extension of K, then $N_{L/K}\mathfrak{C}_L$ is a subgroup of index $[L:K]$ of $\mathfrak{C}_K$. If L'/K is a finite abelian extension containing L/K, then $N_{L/K}\mathfrak{C}_L$ is the group of all idèle classes $\mathfrak{A}$ such that $(L'/K, \mathfrak{A})$ belongs to the Galois group of L'/L, and, conversely, every element s of this group may be written in the form $(L'/K, \mathfrak{A})$ with some $\mathfrak{A}\in N_{L/K}\mathfrak{C}_L$; for, we may write $s=(L'/L, \mathfrak{B})$ for some $\mathfrak{B}\in\mathfrak{C}_L$, whence $s=(L'/K, N_{L/K}\mathfrak{B})$. It follows immediately that the knowledge of the group $N_{L/K}\mathfrak{C}_L$ determines L entirely. Now, we propose to determine what are the groups $N_{L/K}\mathfrak{C}_L$ relative to all abelian extensions L/K.

We have defined a topology in the group $\mathfrak{C}_K$. We shall see that $N_{L/K}\mathfrak{C}_L$ is always a closed subgroup of $\mathfrak{C}_K$. Select an infinite place $\mathfrak{P}$ of L and let $\mathfrak{p}$ be the place of K below $\mathfrak{P}$. Let x be any real number >0; denote by $\mathfrak{a}^{\mathfrak{P}}(x)$ the idèle of L whose $\mathfrak{P}$-component is x and whose other components are 1, and by $\mathfrak{A}^{\mathfrak{P}}(x)$ the class of $\mathfrak{a}^{\mathfrak{P}}(x)$; then we know that the classes $\mathfrak{A}^{\mathfrak{P}}(x)$ form a closed subgroup of $\mathfrak{C}_L$, isomorphic to the multiplicative group of real numbers >0, and that $\mathfrak{C}_L$ is the direct product of this group and of a compact group $\mathfrak{C}_L^0$. It is clear that the norm mapping is continuous; thus, $N_{L/K}\mathfrak{C}_L^0$ is a compact group. The norm of $\mathfrak{A}^{\mathfrak{P}}(x)$ with respect to K is the class of the idèle whose $\mathfrak{p}$-component is either x (if $[L_{\mathfrak{P}}:K_{\mathfrak{p}}]=1$) or x^2 (if $[L_{\mathfrak{P}}:K_{\mathfrak{p}}]=2$) and whose other components are 1; when x varies over $\mathbf{R}^+$, these classes run over a subgroup Γ of $\mathfrak{C}_K$ isomorphic to $\mathbf{R}^+$, and $\mathfrak{C}_K$ is the direct product of Γ with a compact group. We have $N_{L/K}\mathfrak{C}_L=(N_{L/K}\mathfrak{C}_L^0)\times\Gamma$, which proves that this group is closed. We propose now to prove the following converse result:

THEOREM 21.1 *If $\mathfrak{N}$ is any closed subgroup of finite index of $\mathfrak{C}_K$, then there exists a finite abelian extension L/K of K such that $\mathfrak{N}=N_{L/K}\mathfrak{C}_L$.*

We proceed by induction on the index ν of $\mathfrak{N}$. Assume that the theorem is proved for all subgroups of indices $<\nu$ (and for all fields K of algebraic numbers of finite degree). The theorem being obvious for $\nu=1$, we may assume that $\nu>1$. Assume first that ν is not a prime; then there is a subgroup $\mathfrak{N}'$ of $\mathfrak{C}_K$ such that $\mathfrak{N}'\supset\mathfrak{N}$, $\mathfrak{N}'\neq\mathfrak{C}_K$, $\mathfrak{N}'\neq\mathfrak{N}$. Since $\mathfrak{N}$ is closed of finite index, it is also open, and $\mathfrak{N}'$ is likewise open and closed. Let L'/K be the finite abelian extension such that $N_{L'/K}\mathfrak{C}_{L'} = \mathfrak{N}'$, and let $\mathfrak{N}_1$ be the group of idèle classes $\mathfrak{B}$ of L' such that $N_{L'/K}\mathfrak{B}\in\mathfrak{N}$. Denote by ν' the index of $\mathfrak{N}'$. Then the mapping $\mathfrak{B}\to N_{L'/K}\mathfrak{B}$ defines an isomorphism of $\mathfrak{B}/\mathfrak{N}_1$ with $\mathfrak{N}'/\mathfrak{N}$, and $\mathfrak{B}/\mathfrak{N}_1$ is of finite index ν/ν'. The norm mapping being continuous, it is clear that $\mathfrak{N}_1$ is closed. Since $\nu/\nu'<\nu$, there is an abelian extension L/L' such that $N_{L/L'}\mathfrak{C}_L=\mathfrak{N}_1$. Let P/K be a normal extension containing L. If s is any automorphism of P/K, then it is clear that $N_{sL/L'}\mathfrak{C}_{sL}=s\mathfrak{N}_1$. Since s induces an automorphism of L'/K, it follows immediately from the definition of $\mathfrak{N}_1$ that $s\mathfrak{N}_1=\mathfrak{N}_1$. Since sL is still abelian over L', we have $sL=L$, which shows that L/K is a normal extension. If $\mathfrak{M}\in\mathfrak{C}_L$, then we have $N_{L/K}\mathfrak{M}=N_{L'/K}(N_{L/L'}\mathfrak{M})\in N_{L'/K}\mathfrak{N}_1=\mathfrak{N}$. If A_L/K is the maximal abelian extension of K in L/K, then we know that $N_{L/K}\mathfrak{C}_L$ is of index $[A_L : K]$. Since $N_{L/K}\mathfrak{C}_L$ is contained in $\mathfrak{N}$, which is of index ν, we have $[A_L : K]\geqq\nu$. On the other hand, we have $[L : K]=[L : L'][L' : K]=\nu/\nu'\cdot\nu'=\nu$; it follows that $L=A_L$ and $N_{L/K}\mathfrak{C}_L=\mathfrak{N}$.

Consider now the case where $\mathfrak{N}$ is of prime index p. Let then K' be the field $K(z)$, where z is a primitive p-th root of unity, and let $\mathfrak{N}'$ be the group of idèle classes $\mathfrak{A}$ of K' such that $N_{K'/K}\mathfrak{A}\in\mathfrak{N}$. Then $\mathfrak{C}_{K'}/\mathfrak{N}'$ is isomorphic to $N_{K'/K}\mathfrak{C}_{K'}/(\mathfrak{N}\cap N_{K'/K}\mathfrak{C}_{K'})$, and $N_{K'/K}\mathfrak{C}_{K'}$ is a subgroup of $\mathfrak{C}_K$ whose index is equal to $[K' : K]$, which divides $p-1$. It follows immediately that $\mathfrak{N}'$ is of index p in $\mathfrak{C}_{K'}$. Since $\mathfrak{N}\cap N_{K'/K}\mathfrak{C}_{K'}$ is of index $p\cdot[K' : K]$ in $\mathfrak{C}_K$, the same argument as above, applied to K' instead of L', shows that, if there exists an abelian extension X/K' such that $N_{X/K'}\mathfrak{C}_X=\mathfrak{N}'$, then X/K is abelian and $N_{X/K}\mathfrak{C}_X=\mathfrak{N}\cap N_{K'/K}\mathfrak{C}_{K'}$. Then, if L is the subfield of X which corresponds by the Galois theory to the group of elements $(X/K,\mathfrak{A})$, for $\mathfrak{A}\in\mathfrak{N}$, we have $N_{L/K}\mathfrak{C}_L=\mathfrak{N}$.

Thus we are reduced to the case where $\mathfrak{N}$ is of prime index p and where K contains a primitive p-th root of unity; $\mathfrak{N}$ then contains $\mathfrak{C}_K^p$. If E is a finite set of places of K containing all infinite places, denote by U^E the set of idèles $\mathfrak{a}$ which satisfy the following conditions: we have $\mathfrak{a}_\mathfrak{p}=1$ for every $\mathfrak{p}\in E$, and, if $\mathfrak{q}$ is a place not in E, then $\mathfrak{a}_\mathfrak{q}$ is a unit in the $\mathfrak{q}$-adic completion $K_\mathfrak{q}$ of K. Let $\mathfrak{U}_K^E$ be the group of idèle classes represented by elements of U^E. We assert that we may select E in such a way that $\mathfrak{U}_K^E\subset\mathfrak{N}$. It is clear that U^E is always a compact group, and that the intersection of all groups U^E contains only 1. On the other hand, $\mathfrak{N}$ being open, the same is true of the group N of idèles whose classes belong to $\mathfrak{N}$. Thus, there are a finite number of sets E such that the intersection of the corresponding sets U^F is contained in N. Since $U^\Gamma \cap U^{\Gamma'} = U^{\Gamma \cup F'}$, our assertion is established. It follows that we can find a finite set E of places of K which satisfies the following conditions: a) E contains all infinite places and all places above the prime number p; b) every idèle class of K contains an idèle whose components at all places not in E are units; c) the group $\mathfrak{U}^\Gamma$ is contained in $\mathfrak{N}$. Let N be the number of places in E. Then we have established in §14 that $\mathfrak{C}_K/\mathfrak{C}_K^p\mathfrak{U}^\Gamma$ is of order p^N (cf. formula (14.1)). Let P_K^Γ be the group of numbers of K whose orders at all places not in E are 0; we have seen in §14 that $P_K^F/(P_K^F)^p = p^N$. Let T be the field obtained by adjunction to K of the p-th roots of all numbers in P_K^F; T/K is therefore an abelian extension of degree p^N. If $\mathfrak{q}$ is a place not in E, then $\mathfrak{q}$ is not ramified in T; for, if $x \in P_K^F$, then x is a unit at $\mathfrak{q}$ and $\mathfrak{q}$ is not above p. Thus, $\mathfrak{q}$ is not ramified in T; $TK_\mathfrak{q}/K_\mathfrak{q}$ is therefore a cyclic extension and this extension is of degree p, since the Galois group of T/K is of type $(p, \ldots, p)$. It follows that every unit of $K_\mathfrak{q}$ is the norm of an element of $TK_\mathfrak{q}$, and therefore that every idèle in U^Γ belongs to $N_{T/K}J_T$, whence $\mathfrak{U}^F \subset N_{T/K}\mathfrak{C}_T$. If $\mathfrak{A}$ is an idèle class in K, then $(T/K, \mathfrak{A})^p = e$ since the Galois group of T/K is of type $(p, \ldots, p)$; thus, we have $(T/K\,;\,\mathfrak{A}^p) = e$ and $\mathfrak{A}^p \in N_{T/K}\mathfrak{C}_T$. It follows that $\mathfrak{C}_K^p\mathfrak{U}^F \subset N_{T/K}\mathfrak{C}_T$. But $\mathfrak{C}_K^p\mathfrak{U}^F$ and $N_{T/K}\mathfrak{C}_T$ are both of index p^N in $\mathfrak{C}_K$. These two groups are therefore equal. Let L be the subfield of T left invariant by the operations $(T/K\,;\,\mathfrak{A})$ for $\mathfrak{A} \in \mathfrak{N}$; then it is clear that $N_{L/K}\mathfrak{C}_L = \mathfrak{N}$, which completes the proof of theorem 21.1.