Tôhoku Math. Journ.
33 (1981), 35-63.

SOME ARITHMETICAL APPLICATIONS OF GROUPS $H^q(R, G)$

AKIRA HATTORI

(Received May 8, 1979)

In a preceding paper [8] we defined a series of abelian groups $H^q(R, G)$ for a commutative ring R and a group G acting on R. If G is finite and R is Galois over the fixed subring R_0 of R, then $H^1(R, G) \simeq$ Pic (R_0) (the Picard group of R_0), and $H^2(R, G) \simeq \mathrm{Br}(R/R_0)$ (the Brauer group of Azumaya algebras over R_0 split by R). We have constructed two long exact sequences, one of which generalizes the exact sequence of Chase, Harrison and Rosenberg [2]. In [8, §6] we considered extensions of integer rings of algebraic number fields, and showed that these groups are intimately related to arithmetically important Galois cohomology groups. For instance, the above-mentioned exact sequence reduces to that of Iwasawa [12] in the case of unramified extensions. As a continuation, we shall deal, in the present paper, with some number-theoretical problems which fit to cohomological approach by making use of our groups $H^q(R, G)$, whereas in [8] our main objective lied in the study of the Brauer groups of rings.

These groups $H^q(R, G)$ are defined in [8] by means of something like the group cohomology with values in the category $\mathscr{P}\!ic(S)$. Similar method is applied to Amitsur cohomology in [9], and a systematic treatment of this construction is given by Ulbrich [20] in the most general form. Moreover, there is another approach to this type of construction due to Villamayor and Zelinsky [21]. These works deal with quite general cases, and are of rather abstract character. However, when dealing with integral domains (or orders in commutative algebras), we can argue more concretely in terms of invertible ideals as is mentioned on [8, p. 12]. In the first three sections, we shall develop new simpler foundations for groups $H^q(R, G)$ along this line, which are not quite general, but are sufficient for most applications. This is the method of mapping cones, and we realize that an exact sequence of aforementioned type was established in the general form by MacLane on the occasion of his study of infinite abelian groups [17]. In §1 we deal with two basic exact sequences in the general setting, and in §2 the case of group cohomology. For finite groups we define the reduced groups $\hat{H}^q$ as in the theory of group cohomology. In §3 we further specialize to Galois cohomology and arrive at the groups $\boldsymbol{H}^q(R, G)$ and $\hat{\boldsymbol{H}}^q(R, G)$.

From §4 onward, we restrict ourselves to algebraic number fields. Then, as was already observed in [8], groups $\hat{\boldsymbol{H}}^q(R, G)$ are in close connection with cohomology groups of idèle class groups, and this fact is the basis for most applications of groups $\hat{\boldsymbol{H}}^q(R, G)$. As one of such applications we give a proof to an old theorem of Iwasawa [11] on the class number of cyclotomic-type extensions. In §5 and §6 we treat the Hasse norm principle and the problem of genera in non-cyclic extensions. These problems are recently studied by several authors (e.g., [3], [4], [5], [6], [19]), and we shall reproduce some of their results as well as some classical results by our method. In §7 we consider cyclotomic fields, and treat cohomological results of Iwasawa [13], [14] in this manner. Not that this way of approach really improves on the existing one which is direct and is not difficult. Yet it will be of some interest to deal with the matter more in the spirit of [12], thereby affirming a suggestion at the end of that paper.

In a short Appendix at the end of the paper we derive one of the exact sequences of Hochschild and Serre [10] by the method of mapping cones.

In a subsequent paper we shall deal with Amitsur-type groups of integer rings of algebraic number fields ([9a]).

1. Mapping cones. 1.1. By a complex we mean a cochain complex $C = \{C^q, \delta^q \ (q \in \boldsymbol{Z})\}$ of abelian groups. To a morphism (of degree 0) of complexes $f\colon A \to B$ one associates the *mapping cone* $C(f)$ which is defined as follows:

$$C(f) = \{C^q, \delta^q\}\ , \quad C^q = A^{q+1} \times B^q\ , \quad \delta(a, b) = (-\delta a, fa + \delta b)\ .$$

We have an exact sequence

$$0 \to B \to C(f) \to A_\# \to 0\ , \tag{1.1}$$

where $A_\#$ is A with degree raised by 1, i.e.,

$$A_\#^q = A^{q+1}\ , \quad \delta_\#^q a = -\delta^{q+1} a \qquad (\text{for } a \in A_\#^q)\ .$$

For definiteness we fix the morphisms of (1.1) as follows: $B^q \to C^q(f)$ to be the natural embedding $B^q \to C^q$, while $C^q(f) \to A_\#^q$ to be the projection: $(a, b) \mapsto a$. The short exact sequence (1.1) gives rise to the cohomology exact sequence

$$\cdots \to H^q(A) \to H^q(B) \to H^q(C(f)) \to H^{q+1}(A) \to \cdots\ , \tag{1.2}$$

which is natural in $f: A \to B$ in the following sense. If we mean by a morphism $\varphi: (f: A \to B) \to (f': A' \to B')$ a pair of $\varphi_A: A \to A'$ and $\varphi_B: B \to B'$ such that $\varphi_B f = f'\varphi_A$, then φ defines homomorphisms $\varphi^q: H^q(C(f)) \to H^q(C(f'))$ such that the following diagram is commutative

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^q(B) & \longrightarrow & H^q(C(f)) & \longrightarrow & H^{q+1}(A) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & H^q(B') & \longrightarrow & H^q(C(f')) & \longrightarrow & H^{q+1}(A') & \longrightarrow & \cdots . \end{array}$$

We shall call (1.2) the *first exact sequence* associated to f.

LEMMA 1.1. *If $f: A \to B$ is monomorphic, there is a morphism $g: C(f) \to \operatorname{coker} f \simeq B/A$, which yields the following commutative diagram:*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^q(B) & \longrightarrow & H^q(C(f)) & \longrightarrow & H^{q+1}(A) & \longrightarrow & \cdots \\ & & \| & & \downarrow{\scriptstyle H^q(g)} & & \| & & \\ \cdots & \longrightarrow & H^q(B) & \longrightarrow & H^q(B/A) & \xrightarrow{-\Delta} & H^{q+1}(A) & \longrightarrow & \cdots . \end{array}$$

It follows that $H^q(g)$ is an isomorphism for every q.

PROOF. g is given by the map $(a, b) \mapsto b \pmod{A}$.

REMARK. The inverse map $H^q(\operatorname{coker} f) \to H^q(C(f))$ is given as follows. Let $b(\operatorname{mod} A)$ be in the kernel of δ. Then there is a such that $\delta b = -fa$. The class of (a, b) is just the element of $H^q(C(f))$ corresponding to the class of $b(\operatorname{mod} A)$.

Similarly we have

LEMMA 1.2. *If f is epimorphic, there is a morphism $(\ker f)_\# \to C(f)$, which yields the following isomorphism of cohomology exact sequences:*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^q(B) & \longrightarrow & H^{q+1}(\ker f) & \longrightarrow & H^{q+1}(A) & \longrightarrow & \cdots \\ & & \| & & \downarrow\wr & & \| & & \\ \cdots & \longrightarrow & H^q(B) & \longrightarrow & H^q(C(f)) & \longrightarrow & H^{q+1}(A) & \longrightarrow & \cdots . \end{array}$$

$(\ker f)_\# \to C(f)$ is given by $a \mapsto (a, 0)$. The inverse map $H^q(C(f)) \to H^{q+1}(\ker f)$ is given as follows. Let $\delta(a, b) = 0$ for $(a, b) \in C(f)$. Then $\delta a = 0, fa = -\delta b$. If $b = fa_1$, then $a + \delta a_1$ is a cocycle in $\ker f$, and its cohomology class is the image of the class of (a, b).

Important is the following exact sequence, which, in this general form, was found by MacLane [17].

THEOREM 1.3. *Concerning the exact sequence of complexes*

$$0 \to \ker f \to A \xrightarrow{f} B \to \operatorname{coker} f \to 0 \tag{1.3}$$

we have the following long exact sequence

(1.4) $$\cdots \to H^{q+1}(\ker f) \xrightarrow{\alpha} H^q(C(f)) \xrightarrow{\beta} H^q(\operatorname{coker} f) \xrightarrow{\gamma} H^{q+2}(\ker f) \to \cdots$$

which is natural in f.

In [17, Theorem 4], two sequences (1.2) and (1.4) are embedded in a 'braid diagram'. The direct proof of Theorem is not difficult, and is left to the reader. The following gives an alternative proof.

Let

$$g: X \to Y, \qquad h: Y \to Z$$

be morphisms of complexes. The mapping cone construction yields two exact sequences:

$$0 \to Y \to C(g) \to X_\sharp \to 0$$
$$0 \to Z_b \to C(h)_b \to Y \to 0,$$

where the subscript b means the lowering of degree by 1. Combining them, we have a four term exact sequence:

$$0 \to Z_b \to C(h)_b \xrightarrow{F} C(g) \to X_\sharp \to 0 .$$

This F, in turn, gives rise to the following exact sequence of mapping cones:

(1.5) $$0 \to C(g) \to C(F) \to C(h) \to 0 .$$

On the other hand, we have $C(hg)$ for the composite map $hg: X \to Z$.

LEMMA 1.4. *$C(F)$ is chain equivalent to $C(hg)$.*

PROOF. F consists of the following maps F^q:

$$F^q: Y^q \times Z^{q-1} \to X^{q+1} \times Y^q; \qquad (y, z) \mapsto (0, y) .$$

Hence the complex $C(F)$ is defined as follows:

$$C^q(F) = C^{q+1}(h)_b \times C^q(g) = (Y^{q+1} \times Z^q) \times (X^{q+1} \times Y^q)$$
$$\delta[(y, z), (x, y')] = [(-\delta y, hy + \delta z), (-\delta x, gx + \delta y' + y)] .$$

We define the following maps:

$$\varphi^q: C^q(F) \to C^q(hg): [(y, z), (x, y')] \mapsto (x, hy' - z)$$
$$\psi^q: C^q(hg) \to C^q(F): (x, z) \mapsto [(-gx, -z), (x, 0)] .$$

Then we can easily verify that these maps commute with δ and that they satisfy

$$I = \varphi^q\psi^q, \quad \text{and} \quad I - \psi^q\varphi^q = \delta s + s\delta ,$$

where the homotopy $s^q: C^q(F) \to C^{q-1}(F)$ is defined by

$$s^q: [(y, z), (x, y')] \mapsto [(y', 0), (0, 0)] .$$

This proves Lemma 1.4.

The following corollary to Lemma 1.4 will be of some interest.

COROLLARY 1.5. *We have the following long exact sequence*:

$$\cdots \to H^q(C(g)) \to H^q(C(hg)) \to H^q(C(h)) \to H^{q+1}(C(g)) \to \cdots .$$

Proof of Theorem 1.3 is now immediate. We have only to decompose the given f as $A \overset{g}{\twoheadrightarrow} Y \overset{h}{\rightarrowtail} B$, and apply Lemmas 1.1 and 1.2 to the above exact sequence.

We call the sequence (1.4) the *second exact sequence* associated to f. By the definition of various maps, α, β, γ of this sequence are given as follows.

α takes the class of $a \in \ker f$ to that of $(a, 0) \in C(f)$.

β takes the class of $(a, b) \in C(f)$ to that of $-b (\operatorname{mod} fA)$.

γ takes the class of $b (\operatorname{mod} fA)$ to that of δa, where $a \in A$ is such that $\delta b = -fa$.

1.2. We return to the commutative square

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \varphi_A} & & \downarrow{\scriptstyle \varphi_B} \\ A' & \xrightarrow{f'} & B' . \end{array} \tag{1.6}$$

We call

$$Y = \{(a', b) \in A' \times B \mid f'a' = \varphi_B b\}/\{(\varphi_A a, fa), a \in A\}$$

the *center* of the diagram, and denote by $[a', b]$ the class containing (a', b). (1.6) is extended to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & \operatorname{coker} f & \longrightarrow 0 \\ & & \downarrow{\scriptstyle \varphi_K} & & \downarrow{\scriptstyle \varphi_A} & & \downarrow{\scriptstyle \varphi_B} & & \downarrow{\scriptstyle \varphi_C} & \\ 0 & \longrightarrow & \ker f' & \longrightarrow & A' & \xrightarrow{f'} & B' & \longrightarrow & \operatorname{coker} f' & \longrightarrow 0 . \end{array} \tag{1.6'}$$

Denoting by $A' \times_{B'} B$ the pullback of f' and φ_B and by $A' \times^A B$ the pushout of φ_A and f, we have three sequences:

$$0 \to A \to A' \times_{B'} B \to Y \to 0 \tag{1.7}$$

$$0 \to Y \to A' \times^A B \to B' \to 0 \tag{1.8}$$

$$0 \to \ker f \xrightarrow{\varphi_K} \ker f' \to Y \to \operatorname{coker} f \xrightarrow{\varphi_C} \operatorname{coker} f' \to 0 , \tag{1.9}$$

where $\ker f' \to Y$ is the map $a' \mapsto [a', 0]$ and $Y \to \operatorname{coker} f$ is the map

$[a', b] \mapsto b(\mathrm{mod}\, fA)$. (1.7) is exact at A if and only if (1.9) is exact at $\ker f$, and (1.8) is exact at B' if and only if (1.9) is exact at $\operatorname{coker} f'$. The other parts of the three sequences are always exact. The verification of the exactness is easy. For example, let $Y \ni [a', b] \mapsto 0$. This means that $b = fa$ $(a \in A)$. Then $a' - \varphi a \in \ker f'$ and its image in Y is $[a' - \varphi a, 0] = [a', b]$.

EXAMPLE. If φ_A is the identity $A \to A$, then $Y \simeq \ker \varphi_B$.

The following is the mapping cone version of [8, Theorem 2] and [9, Theorem 6.1].

THEOREM 1.6. *If φ_K is injective and φ_C is surjective in* (1.6′), *we have the following long exact sequence*:

$$(1.10) \qquad \cdots \to H^q(Y) \xrightarrow{\psi} H^q(C(f)) \xrightarrow{\varphi} H^q(C(f')) \xrightarrow{\chi} H^{q+1}(Y) \xrightarrow{\psi} H^{q+1}(C(f)) \to \cdots ,$$

where φ is the map induced by (1.6), *and χ, ψ are defined below.*

PROOF. (1) *The definition of maps.* First assume the injectivity of φ_K and define ψ as follows. Let $\delta[a', b] = 0$ for $[a', b] \in Y^q$. By assumption, there is a unique $a \in A^{q+1}$, such that $\delta a' = \varphi a$, $\delta b = fa$, and we have $\delta a = 0$. Then $(a, -b) \in C^q(f)$ satisfies $\delta(a, -b) = (-\delta a, fa - \delta b) = 0$. If $a' = \varphi a_1$, $b = fa_1$, then $a = \delta a_1$, and the corresponding element of $C(f)$ is $(\delta a_1, -fa_1) = \delta(-a_1, 0)$. Hence the cohomology class of $(a, -b)$ is well-defined. Since we have $a = 0$ for $[\delta a', \delta b]$, we get a map $\psi\colon H^q(Y) \to H^q(C(f))$.

Next assume the surjectivity of φ_C and define χ as follows. Let $(a', b') \in C^q(f')$, and $b' = f'a'_1 - \varphi b_1$ with $a'_1 \in A'^q$, $b_1 \in B^q$. If $\delta(a', b') = 0$, then $f'a' = -\delta b' = -f'\delta a'_1 + \varphi\delta b_1$ so that $f'(a' + \delta a'_1) = \varphi(\delta b_1)$. If $b' = f'a'_2 - \varphi b_2$ with another $a'_2 \in A'^q$, $b_2 \in B^q$, then $f'(a'_1 - a'_2) = \varphi(b_1 - b_2)$. Hence $(a' + \delta a'_1, \delta b_1) - (a' + \delta a'_2, \delta b_2) = \delta(a'_1 - a'_2, b_1 - b_2)$. This means that the cohomology class of $(a' + \delta a'_1, \delta b_1)$ in $H^{q+1}(A' \times_{B'} B)$ is well-determined. Moreover, the image of $\delta(a', b')$ is verified to be the class 0. Hence we have $H^q(C(f')) \to H^{q+1}(A' \times_{B'} B)$. Followed by the map induced from $A' \times_{B'} B \to Y$, this provides the desired map χ.

(2) *The proof of exactness at $H^q(C(f))$.* First, $\varphi\psi[a', b] = (\varphi a, -\varphi b) = \delta(-a', 0)$. Conversely, let $\varphi(a, b) = \delta(a', b')$ for $(a, b) \in Z^q(C(f))$, i.e., $\varphi a = -\delta a'$, $\varphi b = f'a' + \delta b'$. By the surjectivity of φ_C, $b' = f'a'_1 + \varphi b_1$ with $a'_1 \in A'^{q-1}$, $b_1 \in B^{q-1}$. Then we observe that $(a' + \delta a'_1, b - \delta b_1) \in (A' \times_{B'} B)^q$. Since $\delta(a' + \delta a'_1, b - \delta b_1) = -(\varphi a, fa)$ by $\delta b = -fa$, we have $-[a' + \delta a'_1, b - \delta b_1] \in Z^q(Y)$ and this is mapped by ψ to $(a, b - \delta b_1) = (a, b) - \delta(0, b_1)$.

Exactness at $H^q(C(f'))$. First, $\chi\varphi(a, b) = [\varphi a, -\delta b] = [\varphi a, fa] = 0$. Let

$\chi(a', b') = [a' + \delta a_1', \delta b_1] = \delta[a_2', b_2]$ with some $a_2' \in A'^q$, $b_2 \in B^q$ such that $f'a_2' = \varphi b_2$, where a_1', b_1 are as in the definition of χ. This means that there is $a \in A^{q+1}$ such that $a' + \delta a_1' = \varphi a + \delta a_2'$, $\delta b_1 = fa + \delta b_2$. Then $\varphi\delta a = \delta a' = 0$ and $f\delta a = 0$ so that $\delta a = 0$ by the injectivity of φ_K. Since $-fa = \delta(b_2 - b_1)$, we have $(a, b_2 - b_1) \in Z^q(C(f))$. Now,

$$(a', b') - \varphi(a, b_2 - b_1) = (\delta(a_2' - a_1'), b' - \varphi(b_2 - b_1)) = \delta(a_1' - a_2', 0)$$

by $b' = f'a_1' - \varphi b_1$ and $f'a_2' = \varphi b_2$. This shows that the cohomology class of (a', b') is in the image of φ.

Exactness at $H^{q+1}(Y)$. First, $\psi\chi(a', b') = (a, -\delta b_1)$, where a is determined by the conditions $\varphi a = \delta(a' + \delta a_1') = 0$, $fa = \delta(\delta b_1) = 0$, i.e., $a = 0$. Hence $\psi\chi(a', b') = \delta(0, -b_1)$. Let, conversely, $\psi[a', b] = (a, -b) = \delta(a_1, b_1)$ with $(a_1, b_1) \in C^q(f)$, where a is as in the definition of ψ. This means that $-a = \delta a_1$ and $-b = fa_1 + \delta b_1$. Since $f'(a' + \varphi a_1) = \varphi b + \varphi f a_1 = -\delta(\varphi b_1)$, we have $(a' + \varphi a_1, \varphi b_1) \in Z^q(C(f'))$, and the cohomology class of this element is mapped by χ to the class of

$$[a' + \varphi a_1, -\delta b_1] = [a', b] + [\varphi a_1, f a_1] = [a', b] .$$

REMARK. The exact sequence which we have just established may be viewed as a compositum of the following two parts. 1° We have the following commutative diagram

$$\begin{array}{ccccccc}
A & = & A & \xrightarrow{\varphi_A} & A' & \longrightarrow & A' \times^A B \\
\downarrow \alpha & & \downarrow f & & \downarrow f' & & \downarrow \beta \\
A' \times_{B'} B & \longrightarrow & B & \xrightarrow{\varphi_B} & B' & = & B'
\end{array}$$

which yields a sequence of mapping cones:

$$C(\alpha) \to C(f) \to C(f') \to C(\beta) .$$

Under the assumption of the injectivity of φ_K and the surjectivity of φ_C, the resulting sequence

$$H^q(C(\alpha)) \to H^q(C(f)) \to H^q(C(f')) \to H^q(C(\beta))$$

is exact. 2° Since α is injective and β is surjective, we have, by Lemmas 1.1 and 1.2, the following diagram

$$\begin{array}{ccc}
H^q(C(f')) \to & H^q(C(\beta)) & \\
& \wr & \\
& H^{q+1}(Y) & \\
& \wr & \\
& H^{q+1}(C(\alpha)) & \to H^{q+1}(C(f))
\end{array}$$

and also this is exact.

Consider in particular the following square:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \| & & \downarrow \\ A & \xrightarrow{f'} & 0\,. \end{array}$$

In this case, we can identify Y with B (cf. the above Example), and $C(f')$ with $A_{\#}$ obviously. We can easily verify that if we identify Y with B by the correspondence $[a, b] \mapsto -b$, then the sequence (1.10) precisely coincides with the sequence (1.2). Therefore (1.10) may be viewed as a generalization of (1.2), so that we shall call (1.10) likewise the *first exact sequence* (associated to $f \xrightarrow{\varphi} f'$).

Now, the situation is symmetric in rows and columns of the square. Indeed, φ_K is injective if and only if $\ker \varphi_A \to \ker \varphi_B$ is injective, and φ_C is surjective if and only if $\operatorname{coker} \varphi_A \to \operatorname{coker} \varphi_B$ is surjective. Hence we have the first exact sequence also for the pair of φ_A and φ_B. Combining this with the former, we obtain the following

PROPOSITION 1.7. *Under the assumption of Theorem* 1.6, *we have the following diagram which is exact and commutative except at the asterisked square which is anti-commutative, where unnamed sequences are those of* (1.2).

$$\begin{array}{ccccccccccc}
 & & \vdots & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H^{q-1}(A) & \longrightarrow & H^{q-1}(B) & \longrightarrow & H^{q-1}(C(f)) & \longrightarrow & H^q(A) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\varphi} & & \downarrow & & \\
\cdots & \longrightarrow & H^{q-1}(A') & \longrightarrow & H^{q-1}(B') & \longrightarrow & H^{q-1}(C(f')) & \longrightarrow & H^q(A') & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & * & \downarrow{\scriptstyle\chi} & & \downarrow & & \\
\cdots & \longrightarrow & H^{q-1}(C(\varphi_A)) & \xrightarrow{\varphi} & H^{q-1}(C(\varphi_B)) & \xrightarrow{\chi} & H^q(Y) & \xrightarrow{\psi} & H^q(C(\varphi_A)) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\psi} & & \downarrow & & \\
\cdots & \longrightarrow & H^q(A) & \longrightarrow & H^q(B) & \longrightarrow & H^q(C(f)) & \longrightarrow & H^{q+1}(A) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

The verification of the commutativity is straightforward.

Next we examine the interrelation between the first and the second exact sequences. Observe the following diagram with Y at the center.

$$\begin{array}{ccccccccccccc}
 & & & & & & 0 & & & & & & \\
 & & & & & & \downarrow & & & & & & \\
0 & \longrightarrow & \ker f & \xrightarrow{\varphi_K} & \ker f' & \longrightarrow & X & \longrightarrow & 0 & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & & & \\
0 & \longrightarrow & A & \longrightarrow & A' \times_{B'} B & \longrightarrow & Y & \longrightarrow & A' \times^{A} B & \longrightarrow & B' & \longrightarrow & 0 \\
 & & & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 0 & \longrightarrow & Z & \longrightarrow & \operatorname{coker} f & \xrightarrow{\varphi_C} & \operatorname{coker} f' & \longrightarrow & 0 \\
 & & & & & & \downarrow & & & & & & \\
 & & & & & & 0 & & & & & &
\end{array}$$

where $X = \operatorname{coker} \varphi_K$ and $Z = \ker \varphi_C$. Two short exact sequences (1.7), (1.8) are connected in the middle row of this diagram, while the exact sequence (1.9) is decomposed into three short exact sequences displayed in 'Z' form.

PROPOSITION 1.8. *The following diagram is exact and commutative except at the asterisked square which is anti-commutative, where unnamed sequences are those derived from the short exact sequences in the above diagram.*

$$\begin{array}{ccccccccccc}
 & & \vdots & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H^q(\ker f) & \xrightarrow{\alpha} & H^{q-1}(C(f)) & \xrightarrow{\beta} & H^{q-1}(\operatorname{coker} f) & \xrightarrow{\gamma} & H^{q+1}(\ker f) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow \varphi & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H^q(\ker f') & \xrightarrow{\alpha} & H^{q-1}(C(f')) & \xrightarrow{\beta} & H^{q-1}(\operatorname{coker} f') & \xrightarrow{\gamma} & H^{q+1}(\ker f') & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow \chi & & \downarrow & * & \downarrow & & \\
\cdots & \longrightarrow & H^q(X) & \longrightarrow & H^q(Y) & \longrightarrow & H^q(Z) & \longrightarrow & H^{q+1}(X) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow \psi & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H^{q+1}(\ker f) & \xrightarrow{\alpha} & H^q(C(f)) & \xrightarrow{\beta} & H^q(\operatorname{coker} f) & \xrightarrow{\gamma} & H^{q+2}(\ker f) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Proof is a routine work. Notice that the position of the anti-commutative square differs from that in [8, Proposition 4.1], as some of the maps are changed by sign.

2. $H^q(G, f)$ **and** $\hat{H}^q(G, f)$. Let G be a group, and $f: A \to B$ be a homomorphism of G-modules. For a G-chain complex C, f gives rise to a morphism of complexes $\mathrm{Hom}_G(C, A) \to \mathrm{Hom}_G(C, B)$. We denote the mapping cone of this morphism again by $C(f)$ (by abuse of notation). So we have an exact sequence of complexes:

$$0 \to \mathrm{Hom}_G(C, B) \to C(f) \to \mathrm{Hom}_G(C, A)_\# \to 0 . \tag{2.1}$$

This is natural in C and f. Namely, if $\varphi: C' \to C$ is a morphism of chain complexes, and $(f: A \to B) \to (f': A' \to B')$ is a morphism of G-homomorphisms, we have a naturally defined morphism $C(f) \to C'(f')$, which yields the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_G(C, B) & \longrightarrow & C(f) & \longrightarrow & \mathrm{Hom}_G(C, A)_\# & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}_G(C', B') & \longrightarrow & C'(f') & \longrightarrow & \mathrm{Hom}_G(C', A')_\# & \longrightarrow & 0 . \end{array}$$

Hence the cohomology exact sequence belonging to (2.1) is mapped to that for C', f'.

A chain equivalence between C and C' induces an isomorphism of $H^*(C(f))$ and $H^*(C'(f))$. Hence, the structure of the groups $H^q(C(f))$, where C is a $\boldsymbol{Z}G$-projective resolution of $\boldsymbol{Z}$, is independent of a particular choice of C. Denoting these groups by the notation $H^q(G, f)$, we have

PROPOSITION 2.1. *A G-homomorphism $f: A \to B$ canonically determines a series of groups $H^q(G, f)$ $(q \in \boldsymbol{Z})$, and we have the following (first and second) exact sequences:*

$$\cdots \to H^q(G, A) \to H^q(G, B) \to H^q(G, f) \to H^{q+1}(G, A) \to \cdots$$

$$\cdots \to H^{q+1}(G, \ker f) \to H^q(G, f) \to H^q(G, \operatorname{coker} f) \to H^{q+2}(G, \ker f) \to \cdots$$

which are natural in $f: A \to B$.

Notice that we have the group in dimension -1:

$$H^{-1}(G, f) = (\ker f)^G \tag{2.2}$$

(where M^G means the set of G-invariant elements of M). Therefore the initial part of the first exact sequence is as follows:

$$0 \to (\ker f)^G \to A^G \to B^G \to H^0(G, f) \to H^1(G, A) \to \cdots , \tag{2.3}$$

while the second exact sequence, after trivially isomorphic terms casted aside, begins with

$$(2.4)\qquad 0 \to H^1(G, \ker f) \to H^0(G, f) \to (\operatorname{coker} f)^G \to H^2(G, \ker f) \to \cdots .$$

We can treat more general cases (cf. [17, §4]), but we consider the group cohomology alone in this paper.

When G is *finite*, we can apply the same arguments to complete $\boldsymbol{Z}G$-resolutions of $\boldsymbol{Z}$. We use the notation $\hat{H}^q(G, f)$, if necessary, to denote $H^q(C(f))$ in the complete cohomology. If, in particular, G is finite cyclic, generated by σ, we can compute the cohomology groups of G by means of the complex

$$\cdots \longrightarrow \boldsymbol{Z}G \xrightarrow{N} \boldsymbol{Z}G \xrightarrow{\sigma-1} \boldsymbol{Z}G \longrightarrow \cdots .$$

Since all constructions are periodic of degree 2, we have

PROPOSITION 2.2. *If G is finite cyclic, there are isomorphisms $\hat{H}^q(G, f) \simeq \hat{H}^{q+2}(G, f)$ $(q \in \boldsymbol{Z})$, natural in f, such that both of the following diagrams are commutative*:

$$\begin{array}{ccccccc}
\cdots \to & \hat{H}^q(G, B) & \to & \hat{H}^q(G, f) & \to & \hat{H}^{q+1}(G, A) & \to \cdots \\
& \wr & & \wr & & \wr & \\
\cdots \to & \hat{H}^{q+2}(G, B) & \to & \hat{H}^{q+2}(G, f) & \to & \hat{H}^{q+3}(G, A) & \to \cdots
\end{array}$$

$$\begin{array}{ccccccc}
\cdots \to & H^{q+1}(G, \ker f) & \to & H^q(G, f) & \to & H^q(G, \operatorname{coker} f) & \to \cdots \\
& \wr & & \wr & & \wr & \\
\cdots \to & H^{q+3}(G, \ker f) & \to & H^{q+2}(G, f) & \to & H^{q+2}(G, \operatorname{coker} f) & \to \cdots .
\end{array}$$

We can equally define $H^q(G, f)$ for a topological group G and a continuous G-homomorphism $f: A \to B$ of topological G-modules. If G is *profinite* and A, B are discrete G-modules, $H^q(G, f)$ is the direct limit of $H^q(G/N, f^N)$ via suitably defined inflation maps, where N runs through open normal subgroups of G, and f^N denotes the map $A^N \to B^N$ induced by f on N-invariant elements.

Let $\gamma: H \to G$ be a group homomorphism. An additive homomorphism φ from a G-module A to an H-module A' will be called an operator homomorphism if it satisfies $\varphi(\gamma(\sigma)a) = \sigma\varphi(a)$ for $a \in A$, $\sigma \in H$, i.e., if it is an H-homomorphism when A is viewed as an H-module via γ. Let $f: A \to B$ (resp. $f': A' \to B'$) be a homomorphism of G-modules (resp. H-modules), and $\varphi = (\varphi_A, \varphi_B)$ be an operator morphism $f \to f'$. Further, let C (resp. C') be a projective resolution of $\boldsymbol{Z}$ over G (resp. over H). Then there is an operator morphism $C' \to C$, and this gives rise to the following diagram which is exact and commutative:

$$\begin{array}{ccccccccc} 0 \longrightarrow & \mathrm{Hom}_G(C, \ker f) & \longrightarrow & \mathrm{Hom}_G(C, A) & \xrightarrow{f_*} & \mathrm{Hom}_G(C, B) & \longrightarrow & \mathrm{Hom}_G(C, \mathrm{coker} f) & \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ 0 \longrightarrow & \mathrm{Hom}_H(C', \ker f') & \longrightarrow & \mathrm{Hom}_H(C', A') & \xrightarrow{f'_*} & \mathrm{Hom}_H(C', B') & \longrightarrow & \mathrm{Hom}_H(C', \mathrm{coker} f') & \longrightarrow 0 . \end{array}$$

By Theorem 1.6, if the kernel map is injective and the cokernel map is surjective, we have the following exact sequence with a suitable complex Y:

$$(2.5) \qquad \cdots \to H^q(Y) \to H^q(G, f) \to H^q(H, f') \to H^{q+1}(Y) \to \cdots .$$

If, in particular, $H = G$, we can take $C' = C$, and we have

PROPOSITION 2.3. *Assume that, for a commutative square* (1.6) *of G-modules,* $\ker f \to \ker f'$ *is injective and* $\mathrm{coker} f \to \mathrm{coker} f'$ *is surjective, and let Y be its center. Then we have the following exact sequence*:

$$(2.6) \qquad \cdots \to H^q(G, Y) \xrightarrow{\psi} H^q(G, f) \xrightarrow{\varphi} H^q(G, f') \xrightarrow{\chi} H^{q+1}(G, Y) \to \cdots .$$

3. **$\boldsymbol{H}^q(R, G)$ and $\hat{\boldsymbol{H}}^q(R, G)$.** Let R be an integral domain with the field of quotients K. We denote by $I(R)$ the group of invertible R-ideals of K, and by $\mathrm{Pic}(R)$ the factor group of $I(R)$ by the group of principal ideals. Let pr be the map which assigns to every non-zero element $a \in K^*$ $(=K - \{0\})$ the principal ideal $(a) = aR$. Then we have the following exact sequence:

$$(3.1) \qquad 0 \to U(R) \to K^* \xrightarrow{pr} I(R) \to \mathrm{Pic}(R) \to 0 ,$$

where $U(R)$ denotes the group of units of R.

Let K/k be a finite Galois extension with Galois group G, and assume that R is G-admissible. Then (3.1) is an exact sequence of G-modules, and we can apply to it the construction of §2. We define

$$(3.2) \qquad \boldsymbol{H}^q(R, G) = H^{q-1}(G, pr) .$$

Thus $\boldsymbol{H}^q(R, G)$ is computed as follows. Let C be any $\boldsymbol{Z}G$-projective resolution of $\boldsymbol{Z}$. Then, a q-'cochain' is a pair (F, f) of a q-cochain $f: C^q \to K^*$ and a $(q-1)$-cochain $F: C^{q-1} \to I(R)$; (F, f) is a 'cocycle' if f is a cocycle and $\delta F = (f^{-1})$, while it is a 'coboundary' if $f = \delta h^{-1}$ and $F = h\delta H$ for some (H, h). This is in accordance with the description of $\boldsymbol{H}^q$ given in [8, p. 12], where C is assumed to be the non-homogeneous standard complex of G. The main exact sequences of [8, Theorems 1 and 2] are, in the present case, obtained as a special case of Proposition 2.1.

THEOREM 3.1. *We have the following exact sequences*:

$$(3.3) \qquad \cdots \to H^q(G, K^*) \xrightarrow{\chi} H^q(G, I(R)) \xrightarrow{\psi} \boldsymbol{H}^{q+1}(R, G) \xrightarrow{\varphi} H^{q+1}(G, K^*) \to \cdots$$

$$(3.4) \qquad \cdots \to H^q(G, U(R)) \xrightarrow{\alpha} \boldsymbol{H}^q(R, G) \xrightarrow{\beta} H^{q-1}(G, \mathrm{Pic}\,(R)) \xrightarrow{\gamma} H^{q+1}(G, U(R)) \to \cdots .$$

Clearly we have

$$(3.5) \qquad \boldsymbol{H}^0(R, G) \simeq U(R_0)$$

where $R_0 = R \cap k$. By Hilbert's Theorem 90, the beginning part of (3.3) becomes

$$0 \to U(R_0) \to k^* \to I(R)^G \to \boldsymbol{H}^1(R, G) \to 0 .$$

Respecting the traditional terminology *ambiguous* for ideals which are invariant under G, we can state this as follows.

PROPOSITION 3.2. *$\boldsymbol{H}^1(R, G)$ is the group of k-equivalence classes of ambiguous K-ideals.*

We also have the modified (or reduced) groups

$$(3.6) \qquad \hat{\boldsymbol{H}}^q(R, G) = \hat{H}^{q-1}(G, pr)$$

for all dimensions $q \in \boldsymbol{Z}$, and Theorem 3.1 holds for these $\hat{\boldsymbol{H}}^q$ (and $\hat{H}^q$) as well.

The motivation for these groups lied primarily in the following fact which we shall quote without proof.

THEOREM 3.3 ([8, §5 and §7]). *If R is G-Galois over $R_0 = R \cap k$, we have*

$$\boldsymbol{H}^1(R, G) \simeq \mathrm{Pic}\,(R_0)\,, \qquad \hat{\boldsymbol{H}}^1(R, G) \simeq \mathrm{Pic}\,(R_0)/N_{R/R_0}(\mathrm{Pic}\,(R))$$
$$\boldsymbol{H}^2(R, G) \simeq \mathrm{Br}\,(R/R_0)\,,$$

where $\mathrm{Br}\,(R/R_0)$ *means the R-split part of the Brauer group of R_0.*

However, the main objective of the present paper is to utilize the groups $\boldsymbol{H}^q$ in case R/R_0 is non-Galois, namely admits ramification.

Let S be another integral domain, L its field of quotients, and H a finite group of automorphisms of L which maps S onto S. Let $\varphi: R \to S$ be an injective ring homomorphism, and $\gamma: H \to G$ a group homomorphism such that $\varphi(\gamma(\sigma)a) = \sigma(\varphi(a))$ for $a \in R$, $\sigma \in H$. We denote by the same φ the induced map $K \to L$. We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U(R) & \longrightarrow & K^* & \longrightarrow & I(R) & \longrightarrow & \mathrm{Pic}\,(R) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U(S) & \longrightarrow & L^* & \longrightarrow & I(S) & \longrightarrow & \mathrm{Pic}\,(S) & \longrightarrow & 0 \end{array}$$

and this gives rise to homomorphisms $\boldsymbol{H}^q(R, G) \to \boldsymbol{H}^q(S, H)$. Under suitable conditions, we have a long exact sequence connecting these groups (2.5). This happens e.g. in the case of completion with respect to a valuation, H being the decomposition group. In §4 and §7, we will exploit the quotient ring of R by a multiplicative subset to evade ramified primes.

4. The case of algebraic number fields. 4.1. Here and throughout the rest of paper, we consider algebraic number fields. So let K be a finite extension of $\boldsymbol{Q}$ and $R = R_K$ be the ring of integers of K. Let J_K be the idèle group of K. K^* is embedded in J_K as the group of principal idèles, and the factor group $C_K = J_K/K^*$ is the idèle class group. Further, let U_K be the group of unit idèles which is the direct product $U_K = U_0 \times U_\infty$, where U_0 is the product of all local unit groups $U_{\mathfrak{P}}$ for non-archimedean primes, and U_∞ is the product of completions of K at archimedean primes. Then J_K/U_K (resp. J_K/K^*U_K) is isomorphic to the ideal group $I(R)$ (resp. ideal class group Pic(R)), which we shall denote rather as I_K (resp. P_K) in what follows. Hence (3.1) is expressed in the following form:

$$0 \to E_K \to K^* \xrightarrow{pr} I_K \to P_K \to 0\,, \tag{4.1}$$

where E_K is the group of (global) units $U(R)$.

In some problems which we shall deal with in the following sections, it is more adequate to consider *narrow* ideal classes. So let U_K^+ be the group of totally positive unit idèles, i.e.,

$$U_K^+ = U_0 \times U_\infty^+\,, \quad \text{where} \quad U_\infty^+ = \prod_{\text{real } \mathfrak{P}} \boldsymbol{R}^+ \times \prod_{\text{complex } \mathfrak{P}} \boldsymbol{C}$$

where $\boldsymbol{R}^+$ denotes the group of positive real numbers, and put

$$I_K^+ = J_K/U_K^+\,, \qquad P_K^+ = J_K/K^*U_K^+\,,$$

the latter being the narrow ideal class group. The sequence (4.1) is modified to

$$0 \longrightarrow E_K^+ \longrightarrow K^* \xrightarrow{pr^+} I_K^+ \longrightarrow P_K^+ \longrightarrow 0\,, \tag{4.2}$$

where E_K^+ is the group of totally positive units of K.

Now let K/k be a finite Galois extension of degree n of algebraic number fields with Galois group G. We denote the groups $H^{q-1}(G, pr^+)$ (resp. $\hat{H}^{q-1}(G, pr)$) associated to (4.2) by $\boldsymbol{H}_+^q(R, G)$ (resp. $\hat{\boldsymbol{H}}_+^q(R, G)$). We deal mainly with modified groups, for which we have

PROPOSITION 4.1. *$\hat{\boldsymbol{H}}_+^q(R, G) \simeq \hat{\boldsymbol{H}}^q(R, G)$ for every $q \in \boldsymbol{Z}$.*

PROOF. Apply Proposition 2.3 to the square

$$\begin{array}{ccc} K^* & \xrightarrow{pr^+} & I_K^+ \\ \| & & \downarrow \\ K^* & \xrightarrow{pr} & I_K \end{array} .$$

In this case, $Y \simeq \ker(I_K^+ \to I_K) \simeq \prod_{\mathrm{real}\,\mathfrak{P}} \boldsymbol{R}/\boldsymbol{R}^+$. But, since the decomposition group of a real prime $\mathfrak{P}$ reduces to $\{1\}$, $\hat{H}^q(G, Y)$ is a product of several $\hat{H}^q(\{1\}, \boldsymbol{R}/\boldsymbol{R}^+) = 0$. Hence the homomorphism $\hat{H}^q(G, pr^+) \to \hat{H}^q(G, pr)$ is an isomorphism for every q.

By this proposition we use the notation $\hat{\boldsymbol{H}}^q$ instead of $\hat{\boldsymbol{H}}_+^q$ even when dealing with the construction concerning (4.2). Notice that unmodified groups $\boldsymbol{H}_+^q$ may differ from $\boldsymbol{H}^q$ for $q=0, 1$. Indeed, for $q=0$, we have $\boldsymbol{H}_+^0(R, G) \simeq E_k^+$ while $\boldsymbol{H}^0(R, G) \simeq E_k$. For $q=1$, $\boldsymbol{H}_+^1(R, G)$ is the cokernel of $k^* \to (I_K^+)^G$, while $\boldsymbol{H}^1(R, G)$ is the cokernel of $k^* \to I_K^G$. In particular, when K/k is unramified, we have $\boldsymbol{H}_+^1(R, G) \simeq P_k^+$ while $\boldsymbol{H}^1(R, G) \simeq P_k$.

The second exact sequence concerning (4.2) reads for modified cohomology

$$\cdots \to \hat{H}^q(G, E_K^+) \xrightarrow{\alpha} \hat{\boldsymbol{H}}^q(R, G) \xrightarrow{\beta} \hat{H}^{q-1}(G, P_K^+) \xrightarrow{\gamma} \hat{H}^{q+1}(G, E_K^+) \to \cdots . \tag{4.3}$$

As is remarked in [8, p. 18], this reduces to the exact sequence given by Iwasawa [12] in case K/k is an unramified extension, since in this case the map ω^q of (4.4) below is an isomorphism for every q.

[8, Proposition 6.1] is modified to

PROPOSITION 4.2. *We have the following commutative diagram with exact rows:*

(4.4)

$$\begin{array}{ccccccccc} \cdots \longrightarrow & \hat{H}^q(G, K^*) & \longrightarrow & \hat{H}^q(G, J_K) & \longrightarrow & \hat{H}^q(G, C_K) & \longrightarrow & \hat{H}^{q+1}(G, K^*) & \longrightarrow \cdots \\ & \| & & \downarrow w^q & & \downarrow \omega^q & & \| & \\ \cdots \longrightarrow & \hat{H}^q(G, K^*) & \xrightarrow{\chi} & \hat{H}^q(G, I_K^+) & \xrightarrow{\psi} & \hat{\boldsymbol{H}}^{q+1}(R, G) & \xrightarrow{-\varphi} & \hat{H}^{q+1}(G, K^*) & \longrightarrow \cdots \\ & \downarrow & & \| & & \downarrow * & & \downarrow & \\ \cdots \longrightarrow & \hat{H}^q(G, PI_K^+) & \longrightarrow & \hat{H}^q(G, I_K^+) & \longrightarrow & \hat{H}^q(G, P_K^+) & \longrightarrow & \hat{H}^{q+1}(G, PI_K^+) & \longrightarrow \cdots , \end{array}$$

where 1° the upper sequence is the cohomology exact sequence belonging *to* $0 \to K^* \to J_K \to C_K \to 0$, 2° *the middle sequence is the first exact sequence associated to* (4.2) *up to sign,* 3° *the lower sequence is the cohomology exact sequence belonging to* $0 \to PI_K^+ \to I_K^+ \to P_K^+ \to 0$, *where* $PI_K^+ = K^* U_K^+ / U_K^+ (\simeq K^*/E_K^+)$, *and* 4° *the compositum of* ω^q *with* $*$ *is the homomorphism induced by the natural map* $C_K \to P_K^+$.

PROOF. We have a commutative diagram of G-modules

$$\begin{array}{ccc} K^* & \xrightarrow{i} & J_K \\ \| & & \downarrow \\ K^* & \xrightarrow{pr^+} & I_K^+ \\ \downarrow & & \| \\ PI_K^+ & \xrightarrow{i'} & I_K^+ \end{array}$$

where i and i' are monomorphisms. Proposition 4.2 is immediate by the naturality of the first exact sequence together with Lemma 1.1.

The upper half of (4.4) is more important than the lower part, and we shall call this upper half the *basic diagram* for $\hat{\boldsymbol{H}}^q(R, G)$. As is experienced in [8], the following fact is useful:

(4.5) $\quad H^q$(*cokernels of basic diagram*) $\simeq H^{q+2}$(*kernels of basic diagram*).

As is well-known, the 1-cohomology $H^1(G, A)$ vanishes for $A = K^*$, J_K, C_K, I_K (hence also for I_K^+), and further $H^3(G, J_K) = 0$. Therefore the most interesting part of the basic diagram splits into two sections: One which will be studied in the next section (cf. (5.1)), and the following

$$(4.6) \qquad \begin{array}{ccccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & H^2(K^*) & \xrightarrow{i} & H^2(J_K) & \xrightarrow{j} & H^2(C_K) & \xrightarrow{\Delta} & H^3(K^*) \longrightarrow 0 \\ & & \downarrow & & \| & & \downarrow{\scriptstyle w^2} & & \downarrow{\scriptstyle \omega^2} & & \| \\ & & 0 \longrightarrow \boldsymbol{H}^2(R, G) & \xrightarrow{-\varphi} & H^2(K^*) & \xrightarrow{\chi} & H^2(I_K) & \xrightarrow{\psi} & \boldsymbol{H}^3(R, G) & \xrightarrow{-\varphi} & H^3(K^*) \; . \end{array}$$

We utilized this diagram in [8] in the case of unramified extensions to determine the structure of the Brauer group $\mathrm{Br}\,(R/R_0) \simeq \boldsymbol{H}^2(R, G)$. A similar computation is possible in the general case, only lacking being the interpretation for $\boldsymbol{H}^2$. Thus, let $S = \{\mathfrak{p}\}$ be the set of all (finite and infinite) primes of k which ramify in the extension K/k, and for $\mathfrak{p} \in S$ let $e_\mathfrak{p}$ be the ramification index and $G_\mathfrak{p}$ the decomposition group of one of the primes $\mathfrak{P}$ of K lying above $\mathfrak{p}$. Further let e be the least common multiple of all $e_\mathfrak{p}$ ($\mathfrak{p} \in S$). Since the map denoted j in (4.6) is the summation of Hasse local invariants, and since $H^2(G, C_K)$ is cyclic of order $n = [K:k]$ generated by the fundamental cohomology class, we obtain the following proposition by applying (4.5).

PROPOSITION 4.3. *Concerning the structure of* $\boldsymbol{H}^2$ *and* $\boldsymbol{H}^3$ *of a cyclic extension* K/k *we have the following exact sequences*:

$$0 \to \boldsymbol{H}^2(R, G) \to \prod_{\mathfrak{p} \in S} \boldsymbol{Z}/e_{\mathfrak{p}}\boldsymbol{Z} \to \boldsymbol{Z}/e\boldsymbol{Z} \to 0 \tag{4.7}$$

$$0 \to \boldsymbol{Z}\Big/\frac{n}{e}\boldsymbol{Z} \to \boldsymbol{H}^3(R, G) \to \prod_{\mathfrak{p} \in S, \text{finite}} \boldsymbol{Z}/e_{\mathfrak{p}}\boldsymbol{Z} \to 0 . \tag{4.8}$$

In particular, we have

COROLLARY 4.4. $\boldsymbol{H}^2(R, G) = 0$ *if and only if* $e_{\mathfrak{p}}$ $(\mathfrak{p} \in S)$ *are pairwise relatively prime.*

Obviously this is the case when the number of ramified primes of k is at most one.

4.2. Let K/k be a cyclic extension, and assume that all primes of k are unramified in K/k except possibly one finite prime $\mathfrak{p}$ which decomposes in K as $\mathfrak{p}R = \mathfrak{P}^e$, $\mathfrak{P}$ being a prime of K. Then we have that $\boldsymbol{H}^2(R, G) \simeq \boldsymbol{H}^4(R, G) = 0$ and that $\boldsymbol{H}^3(R, G)$ is of order n by Proposition 4.3. The second exact sequence then gives

$$0 \to H^1(G, P_K) \to H^3(G, E_K) \to (\text{a group of order } n) \to H^2(G, P_K) \to H^4(G, E_K) \to 0 .$$

Since $H^1(G, P_K)$ and $H^2(G, P_K)$ are of the same order by the finiteness of P_K, it follows that

$$|\hat{H}^{2m+1}(G, E_K)| = n\,|\hat{H}^{2m}(G, E_K)| .$$

Applying this to the beginning part of second exact sequence

$$0 \to H^1(G, E_K) \to \boldsymbol{H}^1(R, G) \to P_K^G \to H^2(G, E_K) \to 0$$

we get

$$|\boldsymbol{H}^1(R, G)| = n\,|P_K^G| . \tag{4.9}$$

Let R' (resp. R_0') be the ring of $\mathfrak{P}$-integers of K (resp. ring of $\mathfrak{p}$-integers of k), and consider the first exact sequence concerning the morphism $(K^* \to I(R)) \to (K^* \to I(R'))$:

$$0 \to U(R_0) \to U(R_0') \to Y^G \to \boldsymbol{H}^1(R, G) \to \boldsymbol{H}^1(R', G) \to H^1(G, Y) .$$

In this case, $Y = \ker(I(R) \to I(R'))$ is the free abelian group generated by $\mathfrak{P}$, on which G acts trivially. Hence $Y^G = Y$ and $H^1(G, Y) = 0$. Since R'/R_0', being an unramified extension of Dedeking domains, is G-Galois, we have $\boldsymbol{H}^1(R', G) \simeq \operatorname{Pic}(R_0')$ by Theorem 3.3. We shall examine the image of $U(R_0')$ in Y. This is the subgroup Y_0 consisting of $\mathfrak{P}^r = \alpha R$

with some $\alpha \in R_0'$. Let $\mathfrak{P}^r$ $(r > 0)$ be a generator of Y_0. Then $\alpha \in R_0$, and $\mathfrak{P}^r$ must be a power of $\mathfrak{p}R$: $\mathfrak{P}^r = \mathfrak{p}^s R$, $r = es$. This s is nothing but the order of the ideal class of $\mathfrak{p}$ in $\mathrm{Pic}(R_0)$, and is equal to the order of the kernel of the epimorphism $\mathrm{Pic}(R_0) \to \mathrm{Pic}(R_0')$. Hence, by the above exact sequence, we have

$$|\boldsymbol{H}^1(R, G)| = es|\boldsymbol{H}^1(R', G)| = e(s|\mathrm{Pic}(R_0')|) = e|\mathrm{Pic}(R_0)| .$$

Combining this with (4.9), we obtain

PROPOSITION 4.5. *Undr the assumption at the beginning of this section, we have the following identity*:

$$h_k(=|P_k|) = \frac{n}{e}|P_K^G| . \tag{4.10}$$

Notice that n/e is the degree of the maximal unramified subextension of K/k. Assuming moreover that $e = n$ and that G is of prime power order, we recover the following theorem of Iwasawa [11], which immediately yields a generalization of the classical theorem of Weber on cyclotomic fields.

THEOREM 4.6. *If K/k is a cyclic extension of prime power degree p^a of algebraic number fields, and if a prime $\mathfrak{p}$ is fully ramified in K/k and all the other primes are unramified, then we have $p|h_K$ if and only if $p|h_k$.*

5. On the Hasse norm theorem and $\hat{\boldsymbol{H}}^0(R, G)$. We look at the basic diagram in dimensions -1 and 0:

$$\begin{array}{ccccccccccc}
\hat{H}^{-1}(J_K) & \xrightarrow{j^{-1}} & \hat{H}^{-1}(C_K) & \xrightarrow{\Delta} & \hat{H}^0(K^*) & \xrightarrow{i^0} & \hat{H}^0(J_K) & \xrightarrow{j^0} & \hat{H}^0(C_K) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \omega^{-1}} & & \| & & \downarrow{\scriptstyle w^0} & & \downarrow{\scriptstyle \omega^0} & & \\
0 & \longrightarrow & \hat{\boldsymbol{H}}^0(R, G) & \xrightarrow{-\varphi} & \hat{H}^0(K^*) & \xrightarrow{\chi} & \hat{H}^0(I_K) & \xrightarrow{\psi} & \boldsymbol{H}^1(R, G) & \longrightarrow & 0 .
\end{array} \tag{5.1}$$

(Notice that $\hat{H}^{-1}(G, I_K) = 0$.) From the exactness of the lower sequence, it follows immediately that

$$\hat{\boldsymbol{H}}^0(R, G) \simeq E_{K/k}/N_{K/k}K^* , \tag{5.2}$$

where $E_{K/k}$ means the group of $a \in k^*$ such that (a) is the norm of an ideal of K. We put

$$\mathscr{I}(K/k) = \ker i^0 = \{\text{everywhere local norms}\}/\{\text{global norms}\} ,$$

whose order is usually denoted $i(K/k)$, and which we call the *Hasse norm index* of K/k.

LEMMA 5.1. *$\mathscr{I}(K/k)$ is isomorphic to* $\mathrm{im}\,\omega^{-1}$.

PROOF. $\mathscr{I}(K/k)$ is isomorphic to coker j^{-1}, and Lemma 5.1 is immediate by diagram chasing.

THEOREM 5.2 (Gurak [6], Razar [19]). *Let K' be an intermediate field of K/k, normal over k and corresponding to a (normal) subgroup H of G. If $(G, G)\cap H=(G, H)$, then $\mathscr{I}(K'/k)$ is a factor group of $\mathscr{I}(K/k)$. Hence, under this condition, if the Hasse norm theorem (HNT) holds for K/k, then it holds for K'/k.*

COROLLARY 5.3. (1) ([6], [19], Garbanati [3]) *Let K/k be an abelian extension and K' an intermediate field. Then $\mathscr{I}(K'/k)$ is a factor group of $\mathscr{I}(K/k)$. Hence if HNT holds for K/k, it holds for every subextension.*

(2) ([6], [19]) *If $K\supset K'\supset k$ is a normal tower such that $[K:K']$ and $[K':k]$ are relatively prime, then HNT for K/k implies HNT for K'/k.*

PROOF OF THEOREM 5.2. Clearly $E_{K/k}$ is a subgroup of $E_{K'/k}$, and the inclusion map yields a homomorphism $\hat{\boldsymbol{H}}^0(R, G)\to\hat{\boldsymbol{H}}^0(R', G/H)$, where $R'=R_{K'}$. Now, $Z^{-1}(G, C_K)$ consists of idèle classes $C_{\boldsymbol{a}}$ represented by idèles $\boldsymbol{a}$ such that $N_{K/k}\boldsymbol{a}=a^{-1}\in k^*$, and ω^{-1} takes the cohomology class of $C_{\boldsymbol{a}}$ to $a(\bmod N_{K/k}K^*)\in E_{K/k}/N_{K/k}K^*$. Hence the following diagram is commutative:

$$\begin{array}{ccc}\hat{H}^{-1}(G, C_K) & \xrightarrow{N_{K/K'}} & \hat{H}^{-1}(G/H, C_{K'}) \\ \downarrow{\scriptstyle\omega^{-1}} & & \downarrow{\scriptstyle\omega^{-1}} \\ \hat{\boldsymbol{H}}^0(R, G) & \longrightarrow & \hat{\boldsymbol{H}}^0(R', G/H)\ .\end{array}$$

So, by Lemma 5.1, it suffices to show that the upper map is surjective. As was observed by Nakayama [18], there is an exact sequence

$$\hat{H}^{-1}(G, C_K)\xrightarrow{N_{K/K'}}\hat{H}^{-1}(G/H, C_{K'})\xrightarrow{\tau}\hat{H}^0(H, C_K)_G\xrightarrow{\varphi}\hat{H}^0(G, C_K)\ , \tag{5.3}$$

where X_G of a G-module X designates the maximal factor group of X on which G acts trivially, τ is induced from the identity map $C_{K'}\to C_{K'}$, and φ by the norm map $N_{K'/k}$. But, translated by the Artin map, $N_{K'/k}$: $\hat{H}^0(H, C_K)\to\hat{H}^0(G, C_K)$ is nothing but the natural map $H/(H, H)\to G/(G, G)$. Hence the assumption of Theorem 5.2 means that φ is injective, so that the map denoted $N_{K/K'}$ of the diagram is surjective. This proves our assertion.

Gurak gave a simple direct proof for Corollary 5.3.(2). Razar proved Theorem 5.2 by employing Tate's description of $\mathscr{I}(K/k)$. Gurak dealt with a more general case where K' is not necessarily normal over k by making use of the connection of HNT with the relation of the genus field and the central class field. It will be possible to deal with this general case in a way similar to the above, if we suitably define $\hat{\boldsymbol{H}}^q$ for the relative cohomology.

Now we examine the map w^0 in (5.1). It decomposes into local maps $w^0_{\mathfrak{p}}$, $\mathfrak{p}$ running over all primes of k. For an unramified $\mathfrak{p}$, $w^0_{\mathfrak{p}}$ is an isomorphism. If $\mathfrak{p}$ is a real prime which ramifies in K, then I_K has no $\mathfrak{p}$-component, while $\hat{H}^0(G, J_K)$ has a $\mathfrak{p}$-component isomorphic to $\boldsymbol{R}^*/\boldsymbol{R}^+ \simeq \boldsymbol{Z}/2\boldsymbol{Z} \simeq T_{\mathfrak{p}}$ (the inertia group of any one of the prime divisors of $\mathfrak{p}$ in K). Next, let $\mathfrak{p}$ be a ramified finite prime, $\mathfrak{P}$ any one of the primes of K lying above $\mathfrak{p}$, and $G_{\mathfrak{P}}$, $T_{\mathfrak{P}}$ the decomposition group and the inertia group of $\mathfrak{P}$, respectively. By Shapiro's lemma, $w^0_{\mathfrak{p}}$ becomes the map $\hat{H}^0(G_{\mathfrak{P}}, K^*_{\mathfrak{P}}) \to \hat{H}^0(G_{\mathfrak{P}}, \boldsymbol{Z})$. Since $\hat{H}^{-1}(G_{\mathfrak{P}}, \boldsymbol{Z}) = 0$ and $\hat{H}^1(G_{\mathfrak{P}}, K^*_{\mathfrak{P}}) = 0$, we have the following exact sequence:

$$0 \to \hat{H}^0(G_{\mathfrak{P}}, U_{\mathfrak{P}}) \to \hat{H}^0(G_{\mathfrak{P}}, K^*_{\mathfrak{P}}) \to \hat{H}^0(G_{\mathfrak{P}}, \boldsymbol{Z}) \to \hat{H}^1(G_{\mathfrak{P}}, U_{\mathfrak{P}}) \to 0 .$$

Since the norm residue symbol at $\mathfrak{P}$ maps $U_{\mathfrak{p}}$ precisely onto $T_{\mathfrak{P}}$, this sequence can be written as

$$0 \to T_{\mathfrak{P}}/G'_{\mathfrak{P}} \to G_{\mathfrak{P}}/G'_{\mathfrak{P}} \to \boldsymbol{Z}/n_{\mathfrak{p}}\boldsymbol{Z} \to H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}}) \to 0 ,$$

where $n_{\mathfrak{p}} = |G_{\mathfrak{P}}|$ and $G'_{\mathfrak{P}}$ denotes the commutator subgroup of $G_{\mathfrak{P}}$. It follows that $H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}})$ is cyclic of order $e_{\mathfrak{p}}$ (ramification index). Hence we have

$$\ker w^0 \simeq \prod_{\mathfrak{p} \in S}{}' T_{\mathfrak{P}}/G'_{\mathfrak{P}} , \qquad \operatorname{coker} w^0 \simeq \prod_{\mathfrak{p} \in S, \text{finite}} \boldsymbol{Z}/e_{\mathfrak{p}}\boldsymbol{Z} ,$$

where the notation $\prod'_{\mathfrak{p} \in S} X_{\mathfrak{P}}$ means the product of $X_{\mathfrak{P}}$, one $\mathfrak{P}|\mathfrak{p}$ for each $\mathfrak{p} \in S$. Now the well-known formula

$$(\boldsymbol{a}, K/k) = \prod_{\mathfrak{p}} \left(\frac{a_{\mathfrak{p}}, K/k}{\mathfrak{p}}\right) \qquad (\boldsymbol{a} = (a_{\mathfrak{p}}) \in J_k)$$

means that the map $\hat{H}^0(G, J_K) \to \hat{H}^0(G, C_K)$, when interpreted by the reciprocity map, reduces to the natural homomorphism $\prod G_{\mathfrak{P}}/G'_{\mathfrak{P}} \to G/G'$, induced by inclusion maps $G_{\mathfrak{P}} \to G$. The image of $\ker w^0$ by this map, the subgroup G_u/G' generated by all $T_{\mathfrak{P}}G'/G'$, is the subgroup of G/G' which corresponds to the maximal unramifield subextension K_u. Since $\ker w^0 \to \ker \boldsymbol{\omega}^0$ is surjective, we obtain, by (4.5), Lemma 5.1 and the above, the following description of $\hat{\boldsymbol{H}}^0$ and $\hat{\boldsymbol{H}}^1$.

PROPOSITION 5.4. (1) *We have the following exact sequences*:

$$0 \to \mathscr{I}(K/k) \to \hat{\boldsymbol{H}}^0(R, G) \to \prod_{\mathfrak{p} \in S}{}' T_{\mathfrak{P}}/G'_{\mathfrak{P}} \to G_u/G' \to 0 \tag{5.4}$$

$$(5.5) \qquad 0 \to G/G_u \to \hat{H}^1(R, G) \to \prod_{\mathfrak{p} \in S, \text{finite}} Z/e_{\mathfrak{p}}Z \to 0 .$$

(2) *If K/k has no unramified subextension, ω^0 is the zero map.*

6. Theory of genera and $\hat{H}^0(R, G)$. Let K/k be a finite Galois extension of degree n with Galois group G. Let L be a finite abelian extension of K, corresponding to a closed subgroup N_L of finite index of C_K by the reciprocity map. We assume that L is normal over k. Then $\Gamma = \mathrm{Gal}(L/k)$ is a group extension of G by an abelian kernel $A = \mathrm{Gal}(L/K) \simeq C_K/N_L$. Let L_g be the *genus field* of K/k relative to N_L, i.e., $L_g = K \cdot L_a$, where L_a is the maximal abelian subextension of L/k. We have $\mathrm{Gal}(L/L_g) = A \cap (\Gamma, \Gamma)$. Let L_z be the *central class field* of K/k relative to N_L, i.e., the maximal subextension of L/K such that $\mathrm{Gal}(L_z/K)$ is contained in the center of $\mathrm{Gal}(L_z/k)$. Then $\mathrm{Gal}(L/L_z) = (\Gamma, A) = I_G A$, where I_G is the kernel of the augmentation $ZG \to Z$. It follows that

$$\mathrm{Gal}(L_z/L_g) = (A \cap (\Gamma, \Gamma))/(\Gamma, A) .$$

Now we recall the Nakayama exact sequence (5.3)

$$\hat{H}^{-1}(G, C_K) \xrightarrow{\tau} \hat{H}^0(A, C_L)_\Gamma \xrightarrow{\varphi} \hat{H}^0(\Gamma, C_L) .$$

By the reciprocity map, $\mathrm{Gal}(L_z/L_g)$ given above is isomorphic to the kernel of φ, hence to the image of τ, which can be factored as

$$\begin{array}{ccc} \hat{H}^{-1}(G, C_K) & \xrightarrow{\tau} & \hat{H}^0(A, C_L)_\Gamma (\simeq A/I_G A) \\ & \searrow^{\sigma} & \uparrow \\ & & \hat{H}^{-1}(G, C_K/N_L) (\simeq {}_N A/I_G A) , \end{array}$$

where σ is the homomorphism induced by the natural map $C_K \to C_K/N_L$, and the subscript N means the kernel of the norm map. Hence we have

LEMMA 6.1 ([3], [19]). *$\mathrm{Gal}(L_z/L_g)$ is isomorphic to* $\mathrm{im}\,\sigma$.

Let us consider the particular case $N_L = K^* U_K^+/K^*$, and write out L^+, L_g^+, L_z^+ in this case. Then $\mathrm{Gal}(L^+/K) \simeq P_K^+$ and L^+ is the *narrow absolute class field* of K. $\mathrm{Gal}(L^+/L_g^+)$ corresponds to the subgroup of P_K^+ consisting of narrow ideal classes represented by $\mathfrak{a} \in J_K$ such that $N\mathfrak{a} \in k^* N U_K^+$, namely the classes in the principal genus, and $g^+ = [L_g^+ : K]$ gives the number of genera in the narow sense. We put $z^+ = [L_z^+ : K]$. If $g^+ = z^+$, i.e., if $L_g^+ = L_z^+$, we shall say that the *principal genus theorem* (PGT) holds for K/k. Since the above map σ is factored through

ω^{-1} of the basic diagram (cf. Proposition 4.2. 4°), we obtain, in view of Lemma 5.1,

PROPOSITION 6.2. $\mathrm{Gal}(L_z^+/L_g^+)$ *is a factor group of* $\mathscr{I}(K/k)$. *In particular, if the Hasse norm theorem holds for* K/k, *then the principal genus theorem also holds.*

This is classically well-known.

The following also gives a sufficient condition for PGT.

PROPOSITION 6.3. *If there is a prime fully ramified in* K/k, *then the principal genus theorem holds for* K/k, *and there is a subfield* M *of* L_g^+ *such that* $L_g^+ = K \otimes_k M$ *(linearly disjoint compositum).*

PROOF. By assumption, ω^2: $H^2(G, C_K) \to \boldsymbol{H}^3(R, G)$ of the basic diagram (4.6) is the zero map, hence *a fortiori* so is $H^2(G, C_K) \to H^2(G, P_K^+)$. It follows from the Šafarevič-Weil theorem ([1, Chap. XIV, Theorem 6]) that the extension

$$0 \to \mathrm{Gal}(L^+/K) \to \mathrm{Gal}(L^+/k) \to G \to 0$$

splits. Hence so does the extension

$$0 \to \mathrm{Gal}(L_z^+/K) \to \mathrm{Gal}(L_z^+/k) \to G \to 0$$

and therefore there is a subfield M of L_z^+ such that $K \cap M = k$, $K \cdot M = L_z^+$. But, since $\mathrm{Gal}(L_z^+/K)$ is central in $\mathrm{Gal}(L_z^+/k)$, M is normal over k, and $\mathrm{Gal}(M/k) \simeq \mathrm{Gal}(L_z^+/K)$ which is abelian. The assertion of Proposition 6.3 is now clear.

An expression of the narrow genus number g^+ is given by

$$g^+ = |\mathrm{coker}\,\sigma| \frac{h_k^+}{(P_k^+ \colon N_{K/k}P_K^+)} \tag{6.1}$$

where h_k^+ denotes the narrow class number of k. To see this, compute $[K_z^+ : K]$ in two ways. This is equal to $g^+|\mathrm{im}\,\sigma|$ by Lemma 6.1 on the one hand, and to

$$(P_K^+ : I_G P_K^+) = (P_K^+ : {}_N(P_K^+)) \cdot |\hat{H}^{-1}(G, P_K^+)|$$

on the other. Our identity holds, since we have

$$(P_K^+ : {}_N(P_K^+)) = |N_{K/k}P_K^+| = h_k^+/(P_k^+ : N_{K/k}P_K^+) .$$

Then, how about $\mathrm{coker}\,\sigma$? We consider the second exact sequence augmented by $\hat{H}^{-1}(G, C_K)$:

$$\begin{array}{ccccccc} & & \hat{H}^{-1}(G, C_K) & & & & \\ & & \downarrow{\scriptstyle \omega^{-1}} & \searrow{\scriptstyle \sigma} & & & \\ \hat{H}^0(G, E_K^+) & \longrightarrow & \hat{\boldsymbol{H}}^0(R, G) & \longrightarrow & \hat{H}^{-1}(G, P_K^+) & \xrightarrow{\gamma} & \hat{H}^1(G, E_K^+) \\ & & \downarrow & & \downarrow & & \\ & & \operatorname{coker} \omega^{-1} & \longrightarrow & \operatorname{coker} \sigma\,. & & \end{array}$$

Assume that γ is the zero map, as is satisfied by the extension over $\boldsymbol{Q}$ to be considered just below. Then we easily observe that

$$\hat{H}^0(G, E_K^+) \to \operatorname{coker} \omega^{-1} \to \operatorname{coker} \sigma \to 0 \tag{6.2}$$

is exact. By (5.4), $\operatorname{coker} \omega^{-1}$ can be determined if we have enough information about ramification in K/k, and we know $\operatorname{coker} \sigma$ modulo the image of $\hat{H}^0(G, E_K^+)$. But the latter (units modulo local norms) seems difficult to calculate.

When $k = \boldsymbol{Q}$, the situation is largely simplified.

(1) Since $h_{\boldsymbol{Q}}^+ = 1$, we have $g^+ = |\operatorname{coker} \sigma|$.

(2) γ is the zero map. This is verified by the definition of γ. Hence the exact sequence (6.2) holds.

(3) $\hat{H}^0(G, E_K^+) = 0$ or $\simeq \boldsymbol{Z}/2\boldsymbol{Z}$, according as whether K is real or imaginary. When K is imaginary, the image of this group in $\hat{\boldsymbol{H}}^0(R, G)$ is mapped, in the exact sequence (5.4), precisely to the factor T_∞ ($\simeq \boldsymbol{Z}/2\boldsymbol{Z}$) in $\ker w^0$, where ∞ denotes the unique infinite prime of $\boldsymbol{Q}$.

(4) Since there is no unramified extension of $\boldsymbol{Q}$, G is generated by all $T_{\mathfrak{P}}$ for finite primes $\mathfrak{P}$.

Applying these observations to the exact sequences (5.4) and (6.2), we have the following exact sequence:

$$0 \longrightarrow \underset{\displaystyle \operatorname{coker} \sigma}{\underset{\wr\!\wr}{\operatorname{coker} \omega^{-1}/\hat{H}^0(G, E_K^+)}} \longrightarrow \prod_{p \in S,\,\text{finite}}{}' T_{\mathfrak{P}}/G'_{\mathfrak{P}} \longrightarrow G/G' \longrightarrow 0\,. \tag{6.3}$$

If, in particular, K is an abelian extension, this yields the following well-known formula for the narrow genus number:

$$g^+ = \prod e_p/[K : Q] \tag{6.4}$$

which is due to Gauss in the quadratic case, generalized to cyclic extensions by Iyanaga and Tamagawa [15], and to abelian extensions by Leopoldt [16].

If $K/\boldsymbol{Q}$ is cyclic, ω^{-1} and σ are the zero maps, and we have the equally well-known identity

(6.5) $g^+ = |\hat{H}^{-1}(G, P_K^+)| = |\hat{H}^0(G, P_K^+)|$
= the order of the group of ambiguous ideal classes .

Finally we return to the general Galois extension of $\boldsymbol{Q}$, and observe that $\operatorname{im}\alpha \cap \operatorname{im}\omega^{-1} = 0$ in $\hat{\boldsymbol{H}}^0(R, G)$. This is easily verified by the definition of maps and is also clear by the above statement (3). It follows that β maps $\operatorname{im}\omega^{-1}$ isomorphically to $\operatorname{im}\sigma$, so that we obtain

PROPOSITION 6.4 ([3], [19]). *For a finite Galois extension $K/\boldsymbol{Q}$, we have $\mathscr{I}(K/\boldsymbol{Q}) \simeq \operatorname{Gal}(L_z^+/L_g^+)$. Hence* HNT *holds if and only if* PGT *holds.*

7. Cyclotomic fields. 7.1. Let p be a rational prime and let $K = \boldsymbol{Q}(\zeta)$ where ζ is a primitive p^a-th root of unity $\notin \boldsymbol{Q}$. Let k be a subfield of K of similar type, and let G be the (cyclic) Galois group of K/k. Put $n = |G| = [K:k]$ (a power of p). Since there is only one ramified prime, and this is fully ramified, it follows from Proposition 4.3 (or from Proposition 5.5) that

(7.1) $$\hat{\boldsymbol{H}}^{2m}(R, G) = 0 , \quad \hat{\boldsymbol{H}}^{2m+1}(R, G) \simeq \boldsymbol{Z}/n\boldsymbol{Z} .$$

This is a special case of the situation dealt with in §4.2, where we applied this to deduce a class number relation of k, K. As one more application of this, we prove another theorem of Iwasawa ([13, Theorem 13]).

THEOREM 7.1. *Let K/k be as above. Then we have*

$$\hat{H}^{2m}(G, E_K) \simeq \hat{H}^{2m}(G, P_K) , \qquad \hat{H}^{2m+1}(G, E_K) \simeq \hat{H}^{2m+1}(G, P_K) \times \boldsymbol{Z}/n\boldsymbol{Z} .$$

PROOF. We may, and shall, assume $m = 0$. By the first half of (7.1), the second exact sequence reduces to

$$0 \to \hat{H}^{-1}(P_K) \to \hat{H}^1(E_K) \xrightarrow{\alpha} \hat{\boldsymbol{H}}^1(R, G) \to \hat{H}^0(P_K) \to \hat{H}^2(E_K) \to 0 .$$

So, in view of the second half of (7.1), we have only to prove that α is a split epimorphism. In the present case, $\hat{\boldsymbol{H}}^1(R, G) \simeq \operatorname{coker} w^0$ in the basic diagram (5.1). Since $\hat{H}^0(G, I_K)$ is the direct product of $\operatorname{im} w^0$ and the cyclic group generated by the class $(\operatorname{mod} N_G I_K)$ of the ambiguous ideal $\mathfrak{P} = (1-\zeta)$, $\hat{\boldsymbol{H}}^1(R, G)$ is generated by the class represented by $(1, \mathfrak{P}) \in K^* \times I_K^G$ (the image of the class of $\mathfrak{P}$ by ψ). Let

$$c(\sigma) = \frac{1-\zeta^\sigma}{1-\zeta} \qquad (\sigma \in G)$$

be the *cyclotomic* 1-*cocycle* $\in Z^1(G, E_K)$. The image of the cohomology class of $c(\sigma)$ by α is represented by $(c(\sigma), R)$. But, since $(c(\sigma)^{-1}, \mathfrak{P}) =$

$\delta(1-\zeta, R)^{-1}$, this is identical with the class of $(1, \mathfrak{P})$, the generator of $\hat{\boldsymbol{H}}^1(R, G)$. Finally, since we have $c(\sigma)^n = \eta^{\sigma-1}$ with $\eta = (1-\zeta)^n/N(1-\zeta) \in E_K$, the class of $c(\sigma)$ is precisely of order n, and the map α splits. q.e.d.

Next let R' (resp. R'_0) be the ring of p-integers in K (resp. in k), i.e., the quotient ring of R (resp. R_0) with respect to the powers of p. Since the unique prime of K which divides p is principal, the natural homomorphism $P_K = \mathrm{Pic}\,(R) \to \mathrm{Pic}\,(R')$ is an isomorphism, and similarly for the map $P_k = \mathrm{Pic}\,(R_0) \to \mathrm{Pic}\,(R'_0)$. Since the extension R'/R'_0 is unramified, we have, by Theorem 3.3,

$$\boldsymbol{H}^1(R', G) \simeq \mathrm{Pic}\,(R'_0) \simeq P_k\,. \tag{7.2}$$

Let $E'_K = U(R')$. Then we have an exact sequence

$$0 \to E_K \to E'_K \to \boldsymbol{Z} \to 0 \tag{7.3}$$

in which $1-\zeta \in E'_K$ maps to $1 \in \boldsymbol{Z}$. The cyclotomic 1-cocycle $c(\sigma)$ defines the characteristic class of this extension.

The basic facts in §4 hold for R' as well after minor modification. The only difference in calculating $\boldsymbol{H}^2$ and $\boldsymbol{H}^3$ by Proposition 4.3 is that the p-component of $H^2(G, I(R'))$ reduces to 0, and it follows that

$$\boldsymbol{H}^2(R', G) = \boldsymbol{H}^3(R', G) = 0\,. \tag{7.4}$$

We shall inspect a part of the diagram of Proposition 1.8 concerning the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_K & \longrightarrow & K^* & \longrightarrow & I(R) & \longrightarrow & \mathrm{Pic}\,(R) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \downarrow\wr & & \\
0 & \longrightarrow & E'_K & \longrightarrow & K^* & \longrightarrow & I(R') & \longrightarrow & \mathrm{Pic}\,(R') & \longrightarrow & 0\,.
\end{array}$$

Noticing $H^1(G, \boldsymbol{Z}) = 0$, we have the following (exact and commutative) diagram:

$$\begin{array}{ccccccccccc}
 & & H^0(G, \boldsymbol{Z}) & \longrightarrow & \{\mathfrak{P}^i\} & \longrightarrow & 0 & \longrightarrow & 0 & & \\
 & & \downarrow \Delta & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(G, E_K) & \longrightarrow & \boldsymbol{H}^1(R, G) & \longrightarrow & (\mathrm{Pic}\,(R))^G & \longrightarrow & H^2(G, E_K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow\wr & & \downarrow * & & \\
0 & \longrightarrow & H^1(G, E'_K) & \longrightarrow & \boldsymbol{H}^1(R', G) & \longrightarrow & (\mathrm{Pic}\,(R'))^G & \longrightarrow & H^2(G, E'_K) & \longrightarrow & 0\,. \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & 0 & & & &
\end{array}$$

It follows that the map denoted $*$ is surjective, hence is an isomorphism.

The map denoted Δ takes the generator $1 (\bmod n)$ to the characteristic class $c(\sigma)$ of (7.3), which have order n, as was shown in the proof of Theorem 7.1.

PROPOSITION 7.2. *Assumptions and notations being as above, we have*

(1) $\hat{H}^q(R', G) = 0$ *for every* q.

(2) $\hat{H}^q(G, P_K) \simeq \hat{H}^q(G, E'_K)$ *for every* q.

(3) $H^2(G, E_K) \simeq H^2(G, E'_K)$, *and*

$0 \to Z/nZ \to H^1(G, E_K) \to H^1(G, E'_K) \to 0$ (*exact*).

(4) $0 \to H^1(G, E'_K) \to P_k \to P_K^G \to H^2(G, E_K) \to 0$ (*exact*)

(*cf.* [13, *Theorem* 11] *and* [14, §5.4]).

PROOF. (1) follows from (7.4) since G is cyclic. (2) is obtained by (1) applied to the second exact sequence. (3) was already remarked above, and (4) is the bottom sequence of the above diagram, on which are applied the isomorphisms of (3) and (7.2).

7.2. Finally we consider extensions over Q. Let $K \subset Q(\zeta)$, where, as above, ζ is a primitive p^a-th root of unity, and G is the absolute Galois group of K. Since there is only one $T_{\mathfrak{P}} \neq \{1\}$, namely $T_p = G$, in the exact sequence (6.3), we have $\operatorname{coker} \sigma = 0$. On the other hand, by Proposition 6.3, PGT holds in K/Q, which means that $\operatorname{im} \sigma = 0$. It follows that

$$\hat{H}^{-1}(G, P_K^+) = 0\ . \tag{7.5}$$

We first consider the case $p = 2$, and obtain the theorem of Weber once again (cf. §4.2).

PROPOSITION 7.3. *Let K be a subfield of $Q(\zeta_{2^a})$. Then the narrow class number h_K^+ is odd.*

PROOF. (7.5) implies that the finite abelian group P_K^+ has no non-trivial quotient on which G acts trivially. Since G is a 2-group, this implies that the Sylow 2-subgroup of P_K^+ reduces to the identity.

If p is an odd prime, G is cyclic. In this case, we have

PROPOSITION 7.4. *Let K be a subfield of $Q(\zeta_{p^a})$, where p is an odd prime.*

(1) $$\hat{H}^q(G, P_K^+) = 0 \qquad (q \in Z)$$

and if G is a p-group, then the narrow class number h_K^+ is relatively prime to p.

(2) $$\hat{H}^{2m}(G, E_K^+) = \begin{cases} 0 & (K\ real) \\ Z/2Z & (K\ imaginary) \end{cases}$$

$$\hat{H}^{2m+1}(G, E_K^+) \simeq Z/nZ, \text{ where } n = [K:Q] .$$

PROOF. (1) The vanishing of cohomology groups is an immediate consequence of the facts that (i) G is cyclic, (ii) P_K^+ is finite, and (iii) (7.5) holds. The statement on h_K^+ is similarly proved as in the preceding proposition.

(2) The statement on $\hat{H}^0(G, E_K^+)$ is clear by definition. $\hat{H}^1(G, E_K^+)$ is isomorphic to $\hat{H}^1(R, G)$, since $\hat{H}^q(G, P_K^+) = 0$ by (1). But the latter is isomorphic to Z/nZ by (5.5).

Appendix. We gave in [7] an elementary proof to the following theorem of Hochschild and Serre ([10, III Theorem 3]). As an application of the method of mapping cones, we shall give it yet another proof.

THEOREM. *Let M be a G-module and H be a normal subgroup of G. Let $q \geqq 1$, and if $q > 1$, assume that $H^i(H, M) = 0$ for $i = 2, \cdots, q$. Then we have the following exact sequence:*

$$H^q(G/H, M^H) \xrightarrow{\lambda} H^q(G, M) \to H^{q-1}(G/H, H^1(H, M))$$
$$\to H^{q+1}(G/H, M^H) \xrightarrow{\lambda} H^{q+1}(G, M) ,$$

where λ means the inflation map.

PROOF. Put $\bar{G} = G/H$. Define a G-module N by the exact sequence

$$0 \to M \to \mathrm{Hom}_Z(ZG, M) \to N \to 0 .$$

Since $H^i(H, \mathrm{Hom}_Z(ZG, M)) = 0$ for $i \geqq 1$ as is well-known, we have isomorphisms

(A.1) $$H^i(H, N) \simeq H^{i+1}(H, M) \qquad (i \geqq 1)$$

and an exact sequence of $\bar{G}$-modules

$$0 \to M^H \to \mathrm{Hom}_Z(Z\bar{G}, M) \xrightarrow{h} N^H \to H^1(H, M) \to 0 .$$

We apply the mapping cone construction to this $\bar{G}$-homomorphism h. Since $\mathrm{Hom}_Z(Z\bar{G}, M)$ has trivial $\bar{G}$-cohomology in positive dimensions, the first exact sequence collapses to

$$H^0(\bar{G}, h) \simeq \mathrm{coker}\,(M \to N^G) \simeq H^1(G, M)$$

and

$$H^i(\bar{G}, N^H) \simeq H^i(\bar{G}, h) \qquad (i \geqq 1) .$$

Hence the second exact sequence gives the following *long exact sequence*

$$\text{(A.2)}\quad \begin{array}{l} 0 \to H^1(\bar{G}, M^H) \to H^1(G, M) \to H^0(\bar{G}, H^1(H, M)) \to H^2(\bar{G}, M^H) \to \cdots \\ \cdots \to H^i(\bar{G}, M^H) \xrightarrow{\mu^i} H^{i-1}(\bar{G}, N^H) \to H^{i-1}(\bar{G}, H^1(H, M)) \to H^{i+1}(\bar{G}, M^H) \to \cdots . \end{array}$$

These facts can be applied in particular to $H = \{1\}$, in which case (A.2) collapses to a series of isomorphisms of (A.1):

$$H^{i+1}(G, M) \overset{\mu^{i+1}}{\simeq} H^i(G, N) \qquad (i \geqq 1) .$$

The naturality of (A.2) shows the commutativity of the diagram

$$\begin{array}{ccc} H^{i+1}(\bar{G}, M^H) & \xrightarrow{\mu} & H^i(\bar{G}, N^H) \\ \downarrow{\scriptstyle \lambda^{i+1}} & & \downarrow{\scriptstyle \lambda^i} \\ H^{i+1}(G, M) & \xrightarrow{\mu} & H^i(G, N) , \end{array}$$

where vertical maps are inflations. Since λ^1 is injective, we obtain the case $q = 1$ of Theorem by replacing the fifth term $H^1(\bar{G}, N^H)$ of (A.2) by $H^2(G, M)$. If $H^i(H, M) = 0$ for $i = 2, \cdots, q$, then $H^i(H, N) = 0$ for $i = 1, \cdots, q-1$. Then, for the module N, λ^{q-1} is isomorphic, and λ^q is injective. (This fact which follows from another exact sequence of Hochschild and Serre can be elementarily proved by induction.) Hence we can replace $\xrightarrow{\mu} H^{i-1}(\bar{G}, N^H)$ in (A.2) by $\xrightarrow{\lambda} H^i(G, M)$ for $i = q-1$ and q, thus obtaining the general case of Theorem.

REFERENCES

[1] E. ARTIN AND J. TATE, Class Field Theory, Benjamin, New York, 1967.
[2] S. U. CHASE, D. K. HARRISON AND A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, Memoirs Amer. Math. Soc. 52 (1965), 15–33.
[3] D. A. GARBANATI, The Hasse norm theorem for non-cyclic extensions of the rationals, Proc. London Math. Soc. 37 (1978), 143–164.
[4] F. GERTH III, The Hasse norm principle in cyclotomic number fields, J. reine angew. Math. 303/4 (1978), 249–252.
[5] S. GURAK, On the Hasse norm principle, ibid. 299 (1978), 16–27.
[6] S. GURAK, Hasse norm principle in non-abelian extensions, ibid. 303/4 (1978), 314–317.
[7] A. HATTORI, On exact sequences of Hochschild and Serre, J. Math. Soc. Japan 7 (1955), 312–321.
[8] A. HATTORI, On groups $\boldsymbol{H}^n(S, G)$ and the Brauer group of commutative rings, Sci. Pap. Coll. Gen. Educ. Univ. Tokyo 28 (1978), 1–20.
[9] A. HATTORI, On groups $\boldsymbol{H}^n(S/R)$ related to the Amitsur cohomology and the Brauer group of commutative rings, Osaka J. Math. 16 (1979), 357–382.
[9a] A. HATTORI, On Amitsur cohomology of rings of algebraic integers, to appear.
[10] G. HOCHSCHILD AND J.-P. SERRE, Cohomology of group extensions, Trans. Amer. Math. Soc. 74 (1953), 110–134.

[11] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257-258.

[12] K. IWASAWA, A note on the group of units of an algebraic number field, J. Math. pures et appl. 35 (1956), 189-192.

[13] K. IWASAWA, On the theory of cyclotomic fields, Ann. Math. 70 (1959), 530-561.

[14] K. IWASAWA, On $\boldsymbol{Z}_l$-extensions of algebraic number fields, ibid. 98 (1973), 246-326.

[15] S. IYANAGA AND T. TAMAGAWA, Sur la théorie du corps de classes sur le corps de nombres rationnels, J. Math. Soc. Japan 3 (1951), 220-227.

[16] H. W. LEOPOLDT, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr. 9 (1953), 351-362.

[17] S. MACLANE, Group extensions by primary abelian groups, Trans. Amer. Math. Soc. 95 (1960), 1-16.

[18] T. NAKAYAMA, A remark on fundamental exact sequences in cohomology of finite groups, Proc. Japan Acad. 32 (1956), 731-735.

[19] M. J. RAZAR, Central and genus class fields and the Hasse norm theorem, Compositio Math. 35 (1977), 281-298.

[20] K.-H. ULBRICH, An abstract version of the Hattori-Villamayor-Zelinsky sequences, Sci. Pap. Coll. Gen. Educ. Univ. Tokyo 29 (1979), 125-137.

[21] O. E. VILLAMAYOR AND D. ZELINSKY, Brauer groups and Amitsur cohomology for general commutative ring extensions, J. pure appl. Algebra 10 (1977), 19-55.

DEPARTMENT OF MATHEMATICS
COLLEGE OF GENERAL EDUCATION
UNIVERSITY OF TOKYO
TOKYO, 153 JAPAN