Preliminaries

1. Idèles and Idèle Classes

A *global field* is either a number field of finite degree over the rational field $\mathbb{Q}$, or a function field in one variable over a finite constant field. Such fields have primes $\mathfrak{p}$, and corresponding canonical absolute values $|\ |_{\mathfrak{p}}$, for which the product formula holds. A *local field* is the completion $k_{\mathfrak{p}}$ of a global field k at a prime $\mathfrak{p}$. Thus a local field is either the real field $\mathbb{R}$, the complex field $\mathbb{C}$, a finite extension of the rational p-adic field $\mathbb{Q}_p$, for some prime number p, or a field of formal power series in one variable over a finite constant field. In other words, a local field is a locally compact non discrete topological field.

The *idèle group* and the *idèle class group* of a global field k are denoted by $J = J_k$ and $C = C_k$ respectively. The *absolute value* (or volume) of an idèle $\mathfrak{a}$ is the product of the absolute values of its components: $|\mathfrak{a}| = \prod_{\mathfrak{p}} |\mathfrak{a}_{\mathfrak{p}}|_{\mathfrak{p}}$. In view of the product formula, the absolute value of an idèle depends only on its class. We denote by J^0 (resp. C^0) the group of idèles (resp. idèle classes) of absolute value 1.

By a *finite set of primes* S of k we always mean a non-empty set, containing the archimedean primes in case k is a number field. The group of S-idèles,

$$J_{k,S} = J_S = \prod_{\mathfrak{p}\in S} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$$

consists of the idèles whose components are units for $\mathfrak{p} \notin S$. The group of S-idèle classes,

$$C_{k,S} = C_S = k^* J_S/k^* \approx J_S/k^* \cap J_S \approx J_S/k_S^*$$

consists of the idèle classes which are represented by S-idèles. Notice that $k_S^* = k^* \cap J_S$ is the group of *S-units* of k, i.e. elements of k which are units for all $\mathfrak{p} \notin S$, and that $C/C_S \approx J/k^* J_S$ is isomorphic to the group of divisor classes in the Dedekind ring formed by the elements of k which are integral for $\mathfrak{p} \notin S$.

We give J the unique topology such that, for each S, J_S is open in J and the topology induced on J_S is the product topology. Uniqueness because $J = \bigcup_S J_S$. Existence because the group of units $U_{\mathfrak{p}}$ is open in $k_{\mathfrak{p}}$ for each non-archimedean $\mathfrak{p}$. Note that J is locally compact because each $U_{\mathfrak{p}}$ is compact, and each $k_{\mathfrak{p}}^*$ is locally compact.

Applying the product formula to $a - 1$ for $a \in k$, $a \neq 1$, one proves that k is a discrete subgroup of J. The theorems on finiteness of class number and the existence of units can be used to show that $C^0 = J^0/k^*$ is compact. Of course, $C/C^0 \approx J/J^0$ is isomorphic to $\mathbb{R}^+$ or to $\mathbb{Z}$ in the number field and function field cases respectively.

If K is a finite extension of k, then there are injections $J_k \to J_K$ and $C_k \to C_K$, and in each case the smaller group maps homeomorphically onto a closed

subgroup of the larger one. If K/k is Galois, the Galois group G operates on K, J_K, and C_K, and we have $k \approx K^G$, $J_k \approx J_K^G$, and $C_k \approx C_K^G$. The first of these isomorphisms follows from Galois theory, the second from definitions of idèles and of the imbedding $J_k \subset J_K$, and the last follows from the first two in view of "Hilbert's Theory 90": $H^1(G, K^*) = 0$.

If S is a finite set of primes $\mathfrak{p}$ of k, we let the same symbol S stand also for the set of primes $\mathfrak{P}$ of K which divide some prime $\mathfrak{p} \in S$. With this understanding we have

$$J_{K,S} = \prod_{\mathfrak{P} \in S} K_{\mathfrak{P}}^* \times \prod_{\mathfrak{P} \notin S} U_{\mathfrak{P}} = \prod_{\mathfrak{p} \in S} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^* \Big) \times \prod_{\mathfrak{P} \notin S} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}} \Big)$$

and consequently

$$H^r(G, J_{K,S}) \approx \prod_{\mathfrak{p} \in S} H^r\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big) \times \prod_{\mathfrak{p} \notin S} H^r\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big).$$

Now the operation of G on $\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*$ permutes the factors, and the subgroup of G consisting of the elements which carry a given factor $K_{\mathfrak{P}}^*$, into itself is the decomposition group $G_{\mathfrak{P}}$ of $\mathfrak{P}$. It follows that $\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*$ is the G-module "induced" by the $G_{\mathfrak{P}}$-module $K_{\mathfrak{P}}^*$ and the cohomological theory of induced modules (some time referred to as Shapiro's Lemma, referred to in these notes by the catchword *semilocal theory*) shows that we have isomorphisms

$$H^r\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big) \approx H^r(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*)$$

for any fixed prime $\mathfrak{P}$ dividing $\mathfrak{p}$, and similarly

$$H^r\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big) \approx H^r(G_{\mathfrak{P}}, U_{\mathfrak{P}}).$$

These isomorphisms are canonical, coming from the restriction from G to $G_{\mathfrak{P}}$ and the projection of the $\mathfrak{P}$-factor. By the theory of local fields, we have $H^r(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 0$ for $r > 0$ if $K_{\mathfrak{P}}$ is unramified over $k_{\mathfrak{p}}$, and therefore if our set S contains all primes $\mathfrak{p}$ of k which ramify in K we have

$$H^r\big(G, J_{K,S}\big) \approx \prod_{\mathfrak{p} \in S} H^r\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big) \approx \prod_{\mathfrak{p} \in S} H^r(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*).$$

Passing to the direct limit over larger and larger S, we find for $r > 0$:

$$H^r(G, J_K) \approx \varinjlim_S H^r(G, J_{K,S}) \approx \coprod_{\mathfrak{p}} H^r(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*)$$

where $\coprod$ denotes direct sum, and for each $\mathfrak{p}$ of k, $\mathfrak{P}$ denotes a selected prime of K above $\mathfrak{p}$. In this way, the Galois cohomology of the idèles is reduced to the cohomology of the local fields. The isomorphism is of course functorial and commutes with restriction, transfer, and inflation in the $k \subset L \subset K$ situation in the obvious way: A global restriction from $G_{K/k}$ to $G_{K/L}$ is reflected in the local restrictions from $G_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$ to $G_{K_{\mathfrak{P}}/L_{\mathfrak{q}}}$. The global transfer in the other direction is reflected, for each $\mathfrak{p}$, in the sum over the primes $\mathfrak{q}$ of L dividing $\mathfrak{p}$, of the local transfers. The global inflation corresponds to the totality of all local inflations.

Let Ω be an infinite extension of k. The idèle group J_Ω is by definition the union of the idèle groups J_K of the finite subextensions K/k of Ω/k, and the same goes for the idèle class group C_Ω. If Ω is a Galois extension then its Galois group $G = G_{\Omega/k}$

operates on J_Ω, C_Ω, and Ω^*. For each K, we have $J_K = J_\Omega^{G_K}$, where $G_K = G_{\Omega/K}$ is the subgroup of G_Ω corresponding to the field K, and the same is true for the idèle class groups and for the multiplicative groups of the fields. Thus for $A = J_\Omega$, C_Ω, or Ω^*, the mathematical system $(G, \{G_K\}, A)$ represents a "formation" in the sense of the beginning paragraphs of Chapter XIV. The reader might well begin his study of these notes by reading the first three sections of Chapter XIV, where the notion of class formation is defined in abstracto, because the first three chapters (Chapters V–VII) of these notes are devoted to the proof that the idèle classes of global fields do constitute a class formation.

Our notation and terminology for formations is rather naive. For all intents and purposes, the notion of a formation is equivalent to a pair (G, A) consisting of a compact totally disconnected topological group G and a G-module A on which G acts continuously in the sense that the stabilizer of every element $a \in A$ is an open subgroup of G. Given such a pair one defines cohomology groups $H^r(G, A)$ for $r \geq 0$ either by using *continuous* standard cochains, or equivalently, as the direct limits under the inflation maps of the cohomology groups $H^r(G/U, A^U)$ of the finite quotients of G by its open normal subgroups U. As functors of (G, A) these cohomology groups have all the properties of ordinary cohomology groups of groups, and the freedom to vary the "formation" module A and "Galois group" G is a considerable technical advantage. For more details the reader can consult [**21**, Ch. X] or for still more details, [**22**].

2. Cohomology

In the proof of the main theorem, p. 154, we refer to the following result in the cohomology of finite groups.

THEOREM A. *Let G be a finite group, and let $A \times B \to C$ be a G-pairing of two G-modules into a third. Let $a \in H^p(G, A)$. Then for each $q \in \mathbb{Z}$ and each subgroup $S \subset G$ the cup product with the restriction of α to S yields a homomorphism*

$$\alpha_{q,S} \colon H^q(S, B) \to H^{p+q}(S, C).$$

Suppose for some q_0 that the maps $\alpha_{q_0-1,S}$ are surjective, the maps $\alpha_{q_0,S}$ are bijective, and the maps $\alpha_{q_0+1,S}$ are injective for all subgroups S. Then the maps $\alpha_{q,S}$ are bijective for all q and all S.

The proof is not difficult. By dimension shifting, one reduces to the case $p = 0$, in which case $\alpha_{q,S}$ is just the map induced by some G-homomorphism $f \colon B \to C$. Adding to C a cohomologically trivial module into which B injects, we see that it is no loss of generality to assume that f is an injection. We then consider the cohomology sequence associated with the exact sequence

$$0 \to B \xrightarrow{f} C \to D \to 0$$

and see from our hypotheses that

$$H^{q_0-1}(S, D) = H^{q_0}(S, D) = 0$$

for all subgroups S of G. It follows now from the theory of cohomological triviality that $H^q(S, D) = 0$ for all q and all S, whence the result.

In discussing cohomological triviality one first reduces to the Sylow groups and then, by induction in cyclic towers, to cyclic groups, where the matter is trivial. These methods have been refined in recent works of Nakayama and Rim. The main

theorem itself is proved directly in Serre's Bourbaki seminar report of February 1953 ([**23**], see also [**21**, Chap. IX]).

At the time when Chapters V–XII of these notes were written, the isomorphism of the main theorem were not known except for $q = -2, -1, 0, 1, 2$, nor was it seen that these constituted part of a general pattern. Indeed, the possibility of extending the cohomology of finite groups to negative dimensions was not known at that time. Therefore the all-important norm-residue isomorphisms

$$(*) \qquad G_{K/F}/G^c_{K/F} \approx H^{-2}(G_{K/F}, \mathbb{Z}) \xrightarrow[\approx]{\alpha_{-2}} H^0(G_{K/F}, A_K) \approx A_F/N_{K/F}A_K,$$

(here G^c denotes the commutator subgroup of a group G) for a normal layer K/F in a class formation was treated separately by itself in the missing Chapters I–IV. Two descriptions of it were given.

The first method was to map $\sigma \in G_{K/F}$ onto the element $\prod_\tau a_{\tau,\sigma} \in A_F$ (mod $N_{K/F}A_K$), where $\{a_{\tau,\sigma}\}$ is a fundamental 2-cocycle for the layer K/F. Indeed, this Nakayama map[1] is just an explicit formula for the cup product of the fundamental class with the class $\zeta_\sigma \in H^{-2}(G, \mathbb{Z})$ corresponding to σ, so that this method amounts to giving an explicit description of the map α_{-2} of the main theorem without recognizing it as a cup product.

However in Chapters V–XII, the emphasis is placed on a dual description of the isomorphism $(*)$, namely that of Propositions 6 and 6′ of Chapter XIV, which involves no negative dimensional cohomology, even implicitly. Before explaining this method, we must introduce a formalism with characters which is also useful in other connections. Let G be a finite group. Since $\mathbb{Q}$ is infinitely and uniquely divisible it has trivial cohomology, and the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

gives an isomorphism

$$\delta\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

We can identify $H^1(G, \mathbb{Q}/\mathbb{Z})$ with the character group $\widehat{G} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ and we then denote the image of a character χ under the isomorphism δ by $\delta\chi \in H^2(G, \mathbb{Z})$. Thus if for each $\sigma \in G$ we let $\bar{\chi}(\sigma)$ be a rational number such that $\chi(\sigma) \equiv \bar{\chi}(\sigma)$ (mod 1), then

$$\delta\bar{\chi}(\tau, \sigma) = \bar{\chi}(\tau) + \bar{\chi}(\sigma) - \bar{\chi}(\tau\sigma)$$

is a 2-cocycle with values in $\mathbb{Z}$ representing the class $\delta\chi$. Summing over τ we obtain

$$\sum_{\tau \in G} \delta\bar{\chi}(\tau, \sigma) = n\bar{\chi}(\sigma)$$

where $n = (G : 1)$ is the order of G. Thus passing to cohomology, it follows that the pairing

$$H^{-2}(G, \mathbb{Z}) \times H^2(G, \mathbb{Z}) \to H^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

[1] The map $\sigma \mapsto \prod_{\tau \in G} a_{\tau,\sigma}$ was introduced by Tadasi Nakayama in 1935 in his paper [**19**]. He showed that if K/k is a Galois extension with group G, and $a_{\sigma,\tau}$ is a 2-cocycle of G in K^*, then: (1) The map $\sigma \mapsto \prod_{\tau \in G} a_{\tau,\sigma}$ induces a homomorphism $G \to k^*/NK^*$; (2) If the cohomology class of $a_{\tau,\sigma}$ has the maximum possible order $n = |G|$, and G is abelian, that homomorphism is injective; and (3) If k is a $\mathfrak{p}$-adic field, and $a_{\sigma,\tau}$ corresponds to a division algebra with Hasse invariant $1/n$, then the homomorphism is the inverse of the norm residue homomorphism of local class field theory. A few months later, Yasuo Akizuki showed that for $a_{\sigma,\tau}$ as in (2), then for arbitrary G the kernel of the homomorphism is G', by reducing the general case to the abelian one (see footnote after (XIII, Sect. 3, Theorem 5)).

is given by

$$\boxed{\zeta_\sigma \cup \delta\chi = n\bar{\chi}(\sigma) \pmod{n\mathbb{Z}}}.$$

From this formula we obtain a conceptual proof for the periodicity of the cohomology of cyclic groups:

THEOREM B. *Let G be a finite cyclic group of order n, and A a G-module, and φ a generator of G. Let χ be the character of G such that $\chi(\varphi) = 1/n \pmod 1$. Then the cup products with $\delta\chi$ and with ζ_φ give mutually inverse isomorphisms*

$$H^p(G, A) \underset{\cup\zeta_\varphi}{\overset{\cup\delta\chi}{\rightleftarrows}} H^{p+2}(G, A).$$

Indeed, we have $\zeta_\varphi \cup \delta\chi = \delta\chi \cup \zeta_\varphi = n\bar{\chi}(\varphi) \equiv 1 \pmod n$ in this case.

Now let K/F be a normal layer in a class formation. For each $a \in A_F$, we let $(a, K/F)$ denote the element of $G_{K/F}/G^c_{K/F}$ corresponding to the residue class of $a \mod N_{K/F}A_K$ under the norm residue isomorphism $(*)$. Then $(a, K/F)$ is characterized by the fact that

$$\chi((a, K/F)) = \mathrm{inv}_F(\varkappa a \cup \delta\chi) \qquad \text{for all } \chi \in \hat{G}_{K/F}$$

where $\varkappa a$ denotes the 0-dimensional cohomology class corresponding to a. Indeed, if $(a, K/F) = \sigma \mod G^c$ then by definition, $\varkappa a = \alpha \cup \zeta_\sigma$ where α is the fundamental class of the layer, hence

$$\varkappa a \cup \delta\chi = \alpha \cup \zeta_\sigma \cup \delta\chi = n\bar{\chi}(\sigma)\alpha$$

and this 2-dimensional class does have invariant $\chi(\sigma)$ because α has invariant $1/n$.[2]

3. The Herbrand Quotient

The Herbrand quotient is used so frequently in class field theory that we recall here its definition and properties. If f is an endomorphism of an abelian group A, we shall denote its kernel and image by A_f and A^f respectively.

Let f and g be endomorphisms of an abelian group A such that $fg = 0 = gf$. Then the *Herbrand quotient* is defined by the expression

$$q(A) = q_{f,g}(A) = \frac{(A_f : A^g)}{(A_g : A^f)}$$

provided both indices are finite.

Special Case: G is a finite cyclic group of order n. A is a G-module, $f = 1 - \varphi$ and $g = 1 + \varphi + \cdots + \varphi^{n-1}$ where φ is a generator of G. We have

$$A_f/A^g \approx H^0(G, A) \approx H^2(G, A)$$
$$A_g/A^f \approx H^{-1}(G, A) \approx H^1(G, A)$$

and thus the Herbrand quotient is denoted in this case by $h_{2/1}(G, A)$ or by $h_{2/1}(A)$, because it is the ratio of the orders of the 2- and 1-dimensional cohomology groups, and so appears in many applications.

[2]The interpretation of the Nakayama map as the cup product with ζ_σ gives a quick proof of the theorem of Akizuki–Nakayama mentioned in the previous footnote. Indeed, denoting the class of $a_{\sigma.\tau}$ by α and the class of $\delta\bar{\chi}$ by $\delta\chi$ we have

$$(\zeta_\sigma \cdot \alpha) \cdot \delta\chi = (\alpha \cdot \zeta_\sigma) \cdot \delta\chi = \alpha \cdot (\zeta_\sigma \cdot \delta\chi) = n\bar{\chi}(\sigma)\alpha.$$

Hence, if α is of order $n = |G|$ and $\zeta_\sigma \cdot \alpha = 0$, then $\bar{\chi}(\sigma)$ is an integer, i.e., $\chi(\sigma) = 0$, for all χ, so $\sigma \in G'$. (More generally, if α is of order m, then $\sigma^{n/m} \in G'$.)

The basic properties of the Herbrand quotient result from the fact that it is the "multiplicative" Euler–Poincaré characteristic of the circular complex

$$A \underset{g}{\overset{f}{\rightleftarrows}} A$$

i.e. is the ratio of the orders of the two cohomology groups of the complex. Thus, by usual arguments, we find:

THEOREM q.1. *Suppose in the following diagram the horizontal rows are exact and the horizontal arrows commute with the vertical arrows*:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow f' \uparrow g' & & \downarrow f \uparrow g & & \downarrow f'' \uparrow g'' & & \\ 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0. \end{array}$$

Then $q(A) = q(A')q(A'')$ in the sense that if any two of the three quotients are defined then the third is also and the above equality holds.

THEOREM q.2. *If A is finite, then $q(A) = 1$.*

It is an elementary exercise to prove:

THEOREM q.3. *If g and h are commuting endomorphisms of an abelian group A, then*

$$q_{0,gh}(A) = q_{0,g}(A)q_{0,h}(A)$$

in the sense that if either side is defined then the other is also, and equality holds.

We sketch a proof of the following theorem which generalizes a theorem of Chevalley (Class Field Theory, Nagoya, 1953–54, Theorem 10.3).

THEOREM q.4. *Let G be a cyclic group of prime order p, and let A be a G-module such that $q_{0,p}(A)$ is defined. Then $q_{0,p}(A^G)$ and $h_{2/1}(A)$ are defined and we have*:

$$(h_{2/1}(G, A))^{p-1} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}.$$

Let φ be a generator of G and consider the exact sequence

$$0 \to A^G = A_{1-\varphi} \to A \xrightarrow{1-\varphi} A^{1-\varphi} \to 0.$$

Since $A^{1-\varphi}$ is at the same time a quotient group and subgroup of A, we see that $q_{0,p}(A^{1-\varphi})$ is defined, because $q_{0,p}(A)$ is so by hypothesis. Since both of these are defined, so also is $q_{0,p}(A^G)$ by Theorem q.1. But $h_{2/1}(A^G) = q_{0,p}(A^G)$ because G operates trivially on A^G. Hence

$$h_{2/1}(A) = q_{0,p}(A^G)h_{2/1}(A^{1-\varphi})$$
$$q_{0,p}(A) = q_{0,p}(A^G)q_{0,p}(A^{1-\varphi}).$$

Substituting these equations in the statement of the theorem, we see that we are reduced to proving that $h_{2/1}(A^{1-\varphi})$ is defined, and satisfies

$$h_{2/1}(A^{1-\varphi})^{p-1} = \frac{1}{q_{0,p}(A^{1-\varphi})}.$$

But the endomorphism $1 + \varphi + \cdots + \varphi^{p-1}$ annihilates $A^{1-\varphi}$ so that we can view $A^{1-\varphi}$ as a module over the ring $\mathbb{Z}[X]/(1 + X + \cdots + X^{p-1})$, i.e. we can treat φ as a primitive p-th root of unity, and we are to prove

$$q_{0,p}(A^{1-\varphi}) = \big(q_{0,1-\varphi}(A^{1-\varphi})\big)^{p-1}.$$

But this follows from Theorem q.3 because in the ring of integers in the field of p-th roots of unity, the factorization of p is given by $p = (1-\varphi)^{p-1}\varepsilon$ where ε is a unit.

Another proof can be found in notes of Serre's course "Homologie des groupes, applications arithmetiques", Collège de France, 1958–59.

Theorem q.4 gives the fastest known proof of the basic lemma (Chapter V, § 3) in the proof of the global first inequality in case of cyclic extension of prime degree p, which is the only case necessary. To compute the Herbrand quotient $h_{2/1}(K_S)$ of the S-units one needs only know the ranks of the finitely generated groups K_S and $k_S = K_S^G$, because $q_{0,p}$ depends obviously on the rank. The details can be found in Chevalley's Nagoya book.

Another application of Herbrand's quotient is in the computation of the power index

$$(k^* : k^{*n})$$

in a local field k. Since this index is used at the end of the proof of Lemma 2, Chapter VI, § 3 we outline the computation here. Let k be a non-archimedean local field, let U be the group of units in k, and for each integer $i \geq 1$, let $U_i = 1 + \mathfrak{p}^i$ be the group of units congruent to 1 mod $\mathfrak{p}^i$. We let f be the map $f(x) = 1$ for all $x \in k^*$, and $g(x) = x^n$. Then

$$q_{0,n}(k^*) = \frac{(k^* : k^{*n})}{(k_n^* : 1)}.$$

We observe that the denominator is the order of the group of n-th roots of unity in k. Now for any i,

$$\begin{aligned} q_{0,n}(k^*) &= q_{0,n}(k^*/U)q_{0,n}(U/U_i)q_{0,n}(U_i) \\ &= q_{0,n}(\mathbb{Z})q_{0,n}(\text{finite group})q_{0,n}(U_i) \\ &= n\, q_{0,n}(U_i). \end{aligned}$$

If i is large and n prime to the characteristic of k, then the map $x \to x^n$ maps U_i isomorphically onto U_{i+m} where $m = \operatorname{ord}_k(n)$, as one sees for example by the binomial series for $(1+t)^n$ and $(1+t)^{1/n}$. Hence

$$q_{0,n}(U_i) = (U_i : U_{i+m}) = (\mathfrak{o} : \mathfrak{p})^m = (\mathfrak{o} : n\mathfrak{o}) = 1/|n|_k$$

where $|n|_k$ denotes the normed absolute value of n in k. Thus finally:

$$(k^* : k^{*n}) = \frac{n}{|n|_k}(k_n^* : 1)$$

and in particular, if the n-th roots of unity are contained in k, then

$$(k^* : k^{*n}) = \frac{n^2}{|n|_k}.$$

These formulaa can be checked directly in the archimedean cases, $k = \mathbb{R}$ and $k = \mathbb{C}$ (recall that in the latter case, the normed absolute value is the square of the ordinary absolute value). They hold formally if the characteristic of k divides n, because then $|n|_k = 0$ and $(k^* : k^{*n}) = \infty$.

4. Local Class Field Theory

We now turn to local class field theory. Let k be a local field, and Ω its algebraic closure. We are to show that the formation $(G_{\Omega/k}, \Omega^*)$ is a class formation. If k is archimedean this is completely trivial, so we assume k non-archimedean. For any normal layer K/F we have $H^1(G_{K/F}, K^*) = 0$ by Hilbert's Theorem 90, i.e. our formation is trivially a field formation in the terminology of Chapter XIV, because it is a formation of (multiplicative groups of) fields.

Probably the best way to prove the Second Inequality

$$(F^* : N_{K/F}K^*) \leqslant [K : F]$$

is the method of Chapter XI, because the detailed study of the norm mapping carried out there is necessary for the ramification theory, and must be done sometime anyhow. On the other hand, there are short cuts if one wants only the inequality. As explained in Chapter XIV, § 3, one needs only establish our inequality for cyclic layers of prime degree.

Let K/F be cyclic of degree n. Then for any submodule V of finite index in the group of units U of K, we have

$$\begin{aligned} h_{2/1}(G_{K/F}, K^*) &= h_{2/1}(G_{K/F}, \mathbb{Z}) h_{2/1}(G_{K/F}, U/V) h_{2/1}(G_{K/F}, V) \\ &= n\, h_{2/1}(G_{K/F}, V) \end{aligned}$$

and we shall prove this is equal to n by constructing in any normal layer K/F, cyclic or not, a subgroup V such that $H^r(G, V) = 0$ for all r. Indeed, let $\{\theta^\sigma\}$ be a normal basis for K/F. Replace θ by $\pi^i\theta$ where π is a prime element in F, and where i is sufficiently large so that if we put

$$M = \sum_{\sigma \in G} \mathfrak{o}_F \theta^\sigma$$

we have $M^2 \subset \pi M$ and $M \subset \pi \mathfrak{o}_K$. Finally, put $V = 1 + M$. Then it is easy to see that V is an open G-submodule of U, and moreover V is filtered by subgroups $V_i = 1 + \pi^i M$ such that for each i, the module

$$V_i / V_{i+1} \approx M/\pi M$$

is G-regular, and hence has vanishing cohomology. Now we can apply the following elementary lemma whose proof we leave to the reader.

Lemma. *Let A be a complete topological group and G a finite group operating continuously on A. Let*

$$A = A_0 \supset A_1 \supset A_2 \supset \dots$$

be a decreasing sequence of subgroups invariant under G, and which shrink to the identity in the sense that for each neighborhood U of 1 in A, there is an index i such that $A_i \subset U$. If $H^r(G, A_i/A_{i+1}) = 0$ for all i and some r, then $H^r(G, A) = 0$.

(In characteristic 0, one could avoid the preceding construction by taking a sufficiently small neighborhood of 0 in the additive group of K, and mapping it onto a neighborhood of 1 in K^* by means of the exponential function.)

For cyclic layers K/F of prime degree p different from the characteristic, one can also deduce $h_{2/1}(G_{K/F}, K^*) = p$ from Theorem q.4 above, using the equations

$$q_{0,p}(K^*) = \frac{p}{|p|_k} \qquad \text{and} \qquad q_{0,p}(F^*) = \frac{p}{|p|_k}$$

obtained in our computation of the power index $(K^* : K^{*p})$ above.

Finally, one could ignore the second inequality completely by proving directly that every 2-dimensional class has an unramified splitting field, or what is the same, that the Brauer group of the maximal unramified extension of k is trivial (cf. for example [**15**]).

To complete the proof that our formation of multiplicative groups of local fields is a class formation, we must establish Axiom II′ of Chapter XIV. For this, we consider the *unramified* extension K/F of degree n. Since the residue class field is finite, the Galois group $G_{K/F}$ is cyclic, with a canonical generator, the Frobenius automorphism $\varphi = \varphi_{K/F}$.

For any normal layer K/F, unramified or not, the exact sequence

$$0 \to U_K \to K^* \to \mathbb{Z} \to 0$$

yields, on passage to cohomology,

$$F^* = K^{*G} \to \mathbb{Z} \to H^1(G_{K/F}, U_K) \to H^1(G_{K/F}, K^*) = 0,$$

from which we see that $H^1(G_{K/F}, U_K)$ is isomorphic to the cokernel of $F^* \to \mathbb{Z}$, i.e. is cyclic of order equal to the ramification index $e_{K/F}$, because $\mathbb{Z}$ here represents the value group of K. Thus, for our unramified K/F, we have $H^1(G_{K/F}, U_K) = 0$.

On the other hand, we have $H^0(G_{K/F}, U_K) = U_F/N_{K/F}U_K = 0$ also. This follows in various ways: either a direct refinement process showing that every unit in F is a norm of a unit in K, or from the fact that $h_{2/1}(U_K) = 1$, as was shown in course of proving $h_{2/1}(K^*) = n$ above. Thus for unramified K/F we have $H^r(G_{K/F}, U_K) = 0$ for all r, a fact of importance for the idèle cohomology, as mentioned in the first paragraphs of this introduction.

From our exact sequence we obtain canonical isomorphisms

$$H^2(G_{K/F}, K^*) \approx H^2(G_{K/F}, \mathbb{Z}) \approx \widehat{G}_{K/F}.$$

On the other hand, $\chi \to \chi(\varphi_{K/F})$ gives an isomorphism

$$\widehat{G}_{K/F} \approx \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Composing these two we obtain an injection

$$\mathrm{inv}_{K/F} \colon H^2(G_{K/F}, K^*) \to \mathbb{Q}/\mathbb{Z}.$$

For any $a \in F^*$, and $\chi \in \widehat{G}$, the class $\varkappa a \cup \delta\chi \in H^2(G_{K/F}, K^*)$ is represented by the 2-cocycle $a^{\delta\bar{\chi}(\sigma,\tau)}$. Taking ordinals, i.e. applying the map $K^* \to \mathbb{Z}$, we get the 2-cocycle

$$(\mathrm{ord}_K\, a)\delta\bar{\chi}(\sigma, \tau)$$

which represents the class $\mathrm{ord}_K\, a \cup \delta\chi = \delta(\chi^{\mathrm{ord}_K\, a})$ in $H^2(G_{K/F}, \mathbb{Z})$. Thus we have

$$(**) \qquad \mathrm{inv}_{K/F}(\varkappa a \cup \delta\chi) = \chi^{\mathrm{ord}_K\, a}(\varphi) = \chi(\varphi^{\mathrm{ord}_F\, a})$$

since $\mathrm{ord}_F\, a = \mathrm{ord}_K\, a$, our extension being unramified. This shows that for an unramified extension K/F, we will have

$$(a, K/F) = \varphi_{K/F}^{\mathrm{ord}_F\, a}$$

(In some classical texts, the opposite sign is chosen.) Furthermore, since $G_{K/F}$ is cyclic, every 2-dimensional class is of the form $\varkappa a \cup \delta\chi$ and we can use the rule $(**)$ to establish the required properties of $\mathrm{inv}_{K/F}$. First of all, the invariant does not change under inflation to a bigger unramified extension L/F with $L \supset K \supset F$,

because $\varphi_{K/F}$ is the image of $\varphi_{L/F}$ under the canonical map $G_{L/F} \to G_{K/F}$, and inflation of $\varkappa a \cup \delta\chi$ amounts to viewing a character χ of $G_{K/F}$, as a character of $G_{L/F}$ by this same canonical map. Hence

$$\bar{H}^2(*/F) = \bigcup_{K/F \text{ unramified}} H^2(G_{K/F}, K^*)$$

the subgroup of the Brauer group $H^2(*/F)$ consisting of the elements coming from unramified layers. We obtain an isomorphism

$$\mathrm{inv}_F \colon \bar{H}^2(*/F) \to \mathbb{Q}/\mathbb{Z}$$

(surjectivity because there exist unramified extension of arbitrary degree).

To complete the proof of Axiom II′, we must show that the invariant multiplies by the degree $[E : F]$ under restriction from F to E. This follows from $(**)$ when one takes into account that $\mathrm{ord}_E = e\,\mathrm{ord}_F$, where e is the ramification index, and that, under the canonical map $G_{KE/E} \to G_{K/F}$ the image of $\varphi_{KE/E}$ is $\varphi^f_{K/F}$ where f is the residue class degree. Hence the invariant multiplies by $ef = [E : F]$.

This just about completes our introductory comments. Concerning the existence theorem, we have given in Chapter XIV, §6 an abstract discussion which shows that the existence theorem follows in abstracto from Axioms IIIa–IIIe. In both global and local class field theory, these axioms are all trivial to verify except for IIId. The proof of this axiom in the global case is carried out in Chapter VI, § 5. In the local case, it is not covered in these notes, but would follow readily from the theory of the norm residue symbol in Kummer fields.

Chapter XIII and Chapter XV are not needed for the remaining parts, but note that there is a proof of the principal ideal theorem in Chapter XIII.

We hope that the preceding remarks will to some extent reduce the inconvenience which the reader will suffer from the missing portions of the notes, and other imperfections occurring in them.

CHAPTER V

The First Fundamental Inequality

1. Statement of the First Inequality

In this entire chapter, k is a global field and K/k a *cyclic* extension of degree n with Galois Group G. We let $J = J_K$ be the idèles of K, and $C = C_K$ be the idèle classes of K. Then G acts on J and C, and the fixed groups are $J^G = J_k$, $C^G = C_k$.

We let h_1 and h_2 denote the orders of the first and second cohomology groups. $h_{2/1}$ abbreviates h_2/h_1. We wish to determine the order $h_2(G, C)$ of $\mathcal{H}^2(G, C)$, and it will be shown in this chapter that $h_2(G, C) \geqslant n$. In fact, we prove

THEOREM 1. *Let k be a global field and let K/k be a cyclic extension of degree n with group G. Then*

$$h_2(G, C_K) = n \cdot h_1(G, C_K)$$

or in other words,

$$h_{2/1}(G, C_K) = n.$$

To simplify the notation we omit G and write $h_i(C)$ instead of $h_i(G, C)$ whenever G is the group of operators.

We shall prove this inequality first in function fields, because considerable simplifications occur in this special case. Afterwards, we shall give a unified proof for all global fields.

We shall make constant use of the properties of the index $h_{2/1}$ developed on pages 5–7 (Section 3 of "Preliminaries"), and recall here the three most important properties for the convenience of the reader.

PROPERTY 1. The index $h_{2/1}$ is multiplicative. In other words, if A is an abelian group on which G acts, and A_0 is a subgroup invariant under G we have

$$h_{2/1}(A) = h_{2/1}(A/A_0)h_{2/1}(A_0),$$

in the sense that if two of these quotients are finite, then so is the third, and the relation holds.

PROPERTY 2. If A_0 is a finite group, then $h_{2/1}(A_0) = 1$, and hence $h_{2/1}(A) = h_{2/1}(A/A_0)$.

PROPERTY 3. If $A \approx \mathbb{Z}$ is infinite cyclic and G operates trivially, then $h_{2/1}(\mathbb{Z}) = n$ is the order of G.

2. First Inequality in Function Fields

We suppose here that k is a function field. We let $U = \prod_{\mathfrak{P}} U_{\mathfrak{P}}$ be the unit idèles of K, and $J_0 = J_K^0$ the idèles of volume 1 of K, i.e. those idèles $\mathfrak{a}$ such that

$\prod_{\mathfrak{P}} |\mathfrak{a}|_{\mathfrak{P}} = 1$. Then $J_0 \supset U$ obviously, and $J_0 \supset K^*$ by the product formula. Hence $J_0 \supset UK^*$.

The multiplicativity of $h_{2/1}$ gives

$$h_{2/1}(J/K^*) = h_{2/1}(J/J_0)h_{2/1}(J_0/UK^*)h_{2/1}(UK^*/K^*),$$

and it will come out that all three quotients on the right are finite.

To begin with, J/J_0 is G-isomorphic to the additive group of integers $\mathbb{Z}$ with trivial action under G, via the degree map. Hence

$$h_{2/1}(J/J_0) = n.$$

Since the number of divisor classes of degree zero is finite, J_0/UK^* is a finite group. Hence

$$h_{2/1}(J_0/UK^*) = 1.$$

The factor group UK^*/K^* is G-isomorphic to $U/(U \cap K^*)$ and hence

$$h_{2/1}(UK^*/K^*) = h_{2/1}(U/(U \cap K^*)) = h_{2/1}(U)\big(h_{2/1}(U \cap K^*)\big)^{-1}.$$

Here we use the multiplicativity in reverse, and it will be shown that both $h_{2/1}(U)$ and $h_{2/1}(U \cap K^*)$ are 1.

We know that $U \cap K^* = K_0^*$ is the multiplicative group of the constant field of K, and is finite. Hence $h_{2/1}(U \cap K^*) = 1$. We contend finally that $h_{2/1}(U) = 1$. Indeed, we can express U as a direct product,

$$U = \prod_{\mathfrak{p}} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}} \Big)$$

where each component $\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}$ is semilocal, and invariant under G. For each $\mathfrak{p}$ let $U_{\mathfrak{p}}$ be one of the groups $U_{\mathfrak{P}}$, and let $G_{\mathfrak{p}}$ be the local group, leaving $U_{\mathfrak{p}}$ invariant. The semilocal theory states that

$$\mathcal{H}^r\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big) \approx \mathcal{H}^r(G_{\mathfrak{p}}, U_{\mathfrak{p}})$$

and we have

$$\mathcal{H}^r(U) \approx \prod_{\mathfrak{p}} \mathcal{H}^r(G_{\mathfrak{p}}, U_{\mathfrak{p}}).$$

We know from the local class field theory that

$$h_1(G_{\mathfrak{p}}, U_{\mathfrak{p}}) = h_2(G_{\mathfrak{p}}, U_{\mathfrak{p}}) = e_{\mathfrak{p}}$$

where $e_{\mathfrak{p}}$ is the ramification index. But $e_{\mathfrak{p}} = 1$ at almost all $\mathfrak{p}$. This shows that $h_2(U)$ and $h_1(U)$ are both equal to $\prod_{\mathfrak{p}} e_{\mathfrak{p}}$ and therefore that $h_{2/1}(U) = 1$, as was to be shown.

If we piece together the information just derived, we get the desired result:

$$h_{2/1}(C) = h_{2/1}(J/K^*) = n.$$

3. First Inequality in Global Fields

We treat now the two cases simultaneously. The existence of archimedean primes prevents us from giving the same proof for number fields that was given for function fields in the preceding section. Using Haar measure, and a generalized Herbrand quotient for Haar measure, one could indeed give an argument in number fields which parallels completely that of function fields. Since we wish to avoid the use of Haar measure, we give below a modified version of our preceding proof.

We let k be a global field and S a finite non-empty set of primes of k including all archimedean primes. The subgroups K^*, J_S, K^*J_S of J are invariant under G. (Recall that S also stands for the set of all the primes of K dividing those of k which are in S.) We have therefore

$$h_{2/1}(J/K^*) = h_{2/1}(J/J_SK^*)h_{2/1}(J_SK^*/K^*),$$

and it will be shown that both indices on the right are finite.

From the finiteness of class number theorem we know that J/J_SK^* is a finite group, and consequently $h_{2/1}(J/J_SK^*) = 1$.

J_SK^*/K^* is G-isomorphic to $J_S/J_S \cap K^* = J_S/K_S^*$. Consequently

$$h_{2/1}(J/K^*) = h_{2/1}(J_S)(h_{2/1}(K_S^*))^{-1},$$

and it will be shown that both quotients on the right are finite. We can write

$$J_S = \Big(\prod_{\mathfrak{P}\notin S} U_{\mathfrak{P}}\Big) \times \Big(\prod_{\mathfrak{P}\in S} K_{\mathfrak{P}}^*\Big)$$

where each factor is invariant under G. By an argument similar to that used in function fields, we have $h_{2/1}\Big(\prod_{\mathfrak{P}\notin S} U_{\mathfrak{P}}\Big) = 1$. We can decompose the finite product

$$\prod_{\mathfrak{P}\in S} K_{\mathfrak{P}}^* = \prod_{\mathfrak{p}\in S}\Big(\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big).$$

Let $K_{\mathfrak{p}}^*$ be any one of the fields $K_{\mathfrak{P}}^*$, and let $G_{\mathfrak{p}}$ be its local group. The semilocal theory shows that

$$h_{2/1}\Big(G, \prod_{\mathfrak{P}\in S} K_{\mathfrak{P}}^*\Big) = \prod_{\mathfrak{p}\in S} h_{2/1}\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big) = \prod_{\mathfrak{p}\in S} h_{2/1}\left(G_{\mathfrak{p}}, K_{\mathfrak{p}}^*\right).$$

From the local theory we know that $h_2(G_{\mathfrak{p}}, K_{\mathfrak{p}}^*) = n_{\mathfrak{p}}$ is the local degree, and $h_1(G_{\mathfrak{p}}, K_{\mathfrak{p}}^*) = 1$ is trivial. Hence

$$h_{2/1}(J_S) = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}.$$

We shall therefore have completed the proof of the first inequality if we succeed in proving the following

LEMMA. *Let S be a finite set of primes of k including all archimedean primes and let K/k be a cyclic extension of degree n with group G. Then*

$$h_{2/1}(K_S^*) = \Big(\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}\Big)/n$$

where $n_{\mathfrak{p}}$ is the local degree $[K_{\mathfrak{P}} : k_{\mathfrak{p}}]$.

PROOF. [1] Let s be the number of primes $\mathfrak{P}$ of the set S in K, and let $\mathbb{R}^s$ be the additive group of Euclidean s-space. Let $\{X_{\mathfrak{P}}\}_{\mathfrak{P}\in S}$ be a basis of $\mathbb{R}^s$ and map the S-idèles of K into $\mathbb{R}^s$ as follows:

$$\mathfrak{a} \to L(\mathfrak{a}) = \sum_{\mathfrak{P}\in S} \log |\mathfrak{a}|_{\mathfrak{P}} X_{\mathfrak{P}}.$$

This map is an algebraic homomorphism of J_S into $\mathbb{R}^s$. We shall make it a G-homomorphism by defining a suitable action of G on $\mathbb{R}^s$. Namely we let

$$X_{\mathfrak{P}}^{\sigma} = X_{\mathfrak{P}^{\sigma}}, \qquad \sigma \in G,$$

and extend σ to $\mathbb{R}^s$ by linearity. Then G acts on $\mathbb{R}^s$, permutes the vectors $X_{\mathfrak{P}}$ but not necessarily transitively. We recall that $|\mathfrak{a}^{\sigma}|_{\mathfrak{P}^{\sigma}} = |\mathfrak{a}|_{\mathfrak{P}}$ and using these facts we have

$$\begin{aligned} L(\mathfrak{a}^{\sigma}) &= \sum_{\mathfrak{P}\in S} \log |\mathfrak{a}^{\sigma}|_{\mathfrak{P}} X_{\mathfrak{P}} \\ &= \sum_{\mathfrak{P}\in S} \log |\mathfrak{a}^{\sigma}|_{\mathfrak{P}^{\sigma}} X_{\mathfrak{P}^{\sigma}} \\ &= \sum_{\mathfrak{P}\in S} \log |\mathfrak{a}|_{\mathfrak{P}} X_{\mathfrak{P}^{\sigma}} \\ &= L(\mathfrak{a})^{\sigma}. \end{aligned}$$

This proves that L is a G-homomorphism of J_S into $\mathbb{R}^s$.

The image $L(K_S)$ is a lattice of dimension $s-1$ in $\mathbb{R}^s$, according to the Unit Theorem (see [**16**, p. 104] or [**5**, proof of theorem, p. 72]). This lattice is contained in the hyperplane $\mathbb{R}^{s-1}$ of all elements $\sum x_{\mathfrak{P}} X_{\mathfrak{P}}$ such that $\sum x_{\mathfrak{P}} = 0$ because of the product formula, and consequently the lattice $L(K_S)$ spans this hyperplane.

The kernel of L in K_S consists of all roots of unity and is a finite group. The map

$$K_S \to L(K_S)$$

is a G-homomorphism and $L(K_S)$ is G-isomorphic to $K_S/$(roots of unity). Hence

$$h_{2/1}(L(K_S)) = h_{2/1}(K_S)$$

because $h_{2/1}$ of a finite group is 1.

We now face the task of determining $h_{2/1}(L(K_S))$. We first extend the $s-1$ dimensional lattice $L(K_S)$ to an s-dimensional lattice M as follows. We let $X = \sum_{\mathfrak{P}} X_{\mathfrak{P}}$. Then the vector X does not lie in the hyperplane $\mathbb{R}^{s-1}$ spanned by $L(K_S)$. We let M be the lattice generated by $L(K_S)$ and by X, i.e.

$$M = L(K_S) + \mathbb{Z}X \qquad (\mathbb{Z} \text{ are the integers}).$$

Then M is s-dimensional, and spans $\mathbb{R}^s$. Since $X^{\sigma} = X$ for all $\sigma \in G$, M is invariant under G and both $L(K_S)$ and $\mathbb{Z}X$ are G-modules. The module $\mathbb{Z}X$ is

[1] The key idea in this proof is that for a finite cyclic group G and a finitely generated G-module M, the Herbrand quotient $h_{2/1}(G, M)$ is defined and depends only on the $\mathbb{R}(G)$-module $M \otimes_{\mathbb{Z}} \mathbb{R}$ (see, for example, [**5**, Ch. IV, Sect. 8, Prop. 12]). In fact, if G is of order n, generated by σ, and the characteristic polynomial of σ acting on the vector space $M \otimes \mathbb{R}$ is $\Phi(x) = (x-1)^n \Psi(x)$ with $\Psi(1) \neq 0$, then

$$h_{2/1}(G, M) = \frac{n^r}{\Psi(1)}.$$

For example, if $\Phi(x) = x^n - 1$, then $h_{2/1} = n/r$.

G-isomorphic to $\mathbb{Z}$ with trivial action. Hence $h_{2/1}(\mathbb{Z}X) = n$. Furthermore, the above sum is clearly direct, and therefore

$$h_{2/1}(M) = h_{2/1}(L(K_S)) \cdot n.$$

The proof of our lemma will therefore be complete if we prove that

$$h_{2/1}(M) = \prod_{\mathfrak{p} \in S} n_{\mathfrak{p}}.$$

For this purpose, we prove the following proposition.

PROPOSITION. *Given any s-dimensional lattice M in our $\mathbb{R}^s$ that is invariant under G, there exists a sublattice of finite index $\widetilde{M}$ which is invariant under G, and generated by basis elements $Y_{\mathfrak{P}}$ ($\mathfrak{P} \in S$) on which the action of G is given by*

$$Y_{\mathfrak{P}}^{\sigma} = Y_{\mathfrak{P}^{\sigma}} \qquad \sigma \in G.$$

Before proving the proposition, we show how our lemma follows from it. Suppose we have found a sublattice $\widetilde{M}$ of M with the action described in the proposition. For each prime $\mathfrak{p}$, let $\widetilde{M}_{\mathfrak{p}}$ be the sublattice of $\widetilde{M}$ generated by all elements $Y_{\mathfrak{P}}$, $\mathfrak{P} \mid \mathfrak{p}$. (In other words, break up $\widetilde{M}$ into transitivity domains under G.) Then each $\widetilde{M}_{\mathfrak{p}}$ is invariant under G and

$$\widetilde{M} = \sum \widetilde{M}_{\mathfrak{p}}$$

is a direct sum. Furthermore, each pair $(G, \widetilde{M}_{\mathfrak{p}})$ is semilocal. By the semilocal theory, we have for each

$$h_{2/1}(G, \widetilde{M}_{\mathfrak{p}}) = h_{2/1}(G_{\mathfrak{P}}, \mathbb{Z}Y_{\mathfrak{P}})$$

and $G_{\mathfrak{P}}$ acts trivially on the infinite cyclic group generated by $Y_{\mathfrak{P}}$. Consequently $h_{2/1}(\widetilde{M}_{\mathfrak{p}}) = n_{\mathfrak{p}}$ and $h_{2/1}(\widetilde{M}) = \prod n_{\mathfrak{p}}$. Since $\widetilde{M}$ is of finite index in M, it follows that

$$h_{2/1}(M) = h_{2/1}(\widetilde{M}) = \prod n_{\mathfrak{p}}.$$

This proves our lemma. □

PROOF OF PROPOSITION. For convenience we define a norm on $\mathbb{R}^s$ by putting

$$\left| \sum_{\mathfrak{P}} x_{\mathfrak{P}} X_{\mathfrak{P}} \right| = \max_{\mathfrak{P}} |x_{\mathfrak{P}}| \qquad x_{\mathfrak{P}} \in \mathbb{R}.$$

This norm is clearly invariant under the effect of $\sigma \in G$.

Let b be a constant such that for any vector $A \in \mathbb{R}^s$ there exists $Y \in M$ such that $|A - Y| < b$. Such a b exists since M is s-dimensional.

For each prime $\mathfrak{p} \in S$ let $\bar{\mathfrak{p}}$ be one of the primes $\mathfrak{P} \mid \mathfrak{p}$. Let $Y_{\bar{\mathfrak{p}}} \in M$ be such that

$$|Y_{\bar{\mathfrak{p}}} - bX_{\bar{\mathfrak{p}}}| < b. \tag{1}$$

Let $Y_{\mathfrak{P}} = \sum_{\substack{\sigma \in G \\ \bar{\mathfrak{p}}^{\sigma} = \mathfrak{P}}} Y_{\bar{\mathfrak{p}}}^{\sigma}$. We contend that the vectors $Y_{\mathfrak{P}}$ generate a sublattice of the desired kind.

We first verify that G has the proper effect, i.e. $Y_{\mathfrak{P}}^{\tau} = Y_{\mathfrak{P}^{\tau}}$. Indeed

$$Y_{\mathfrak{P}}^{\tau} = \sum_{\bar{\mathfrak{p}}^{\sigma} = \mathfrak{P}} Y_{\bar{\mathfrak{p}}}^{\tau\sigma} = \sum_{\substack{\sigma \in G \\ \bar{\mathfrak{p}}^{\tau^{-1}\sigma} = \mathfrak{P}}} Y_{\bar{\mathfrak{p}}}^{\sigma} = \sum_{\substack{\sigma \in G \\ \bar{\mathfrak{p}}^{\sigma} = \mathfrak{P}^{\tau}}} Y_{\bar{\mathfrak{p}}}^{\sigma} = Y_{\mathfrak{P}^{\tau}}$$

as was to be shown.

All that remains to be done is to show that the vectors $Y_{\mathfrak{P}}$ are linearly independent. Given a relation

$$\sum x_{\mathfrak{P}} Y_{\mathfrak{P}} = 0$$

we shall prove that all $x_{\mathfrak{P}} = 0$.

We note that the number of $\sigma \in G$ such that $\bar{\mathfrak{p}}^{\sigma} = \mathfrak{P}$ is exactly the local degree $n_{\mathfrak{p}}$. Because of (1) there exist vectors $B_{\bar{\mathfrak{p}}}$ such that

$$Y_{\bar{\mathfrak{p}}} = bX_{\bar{\mathfrak{p}}} + B_{\bar{\mathfrak{p}}}$$

where $|B_{\bar{\mathfrak{p}}}| < b$.

From the definition of $Y_{\mathfrak{P}}$ we get

$$\begin{aligned} Y_{\mathfrak{P}} &= \sum_{\bar{\mathfrak{p}}^{\sigma}=\mathfrak{P}} bX_{\bar{\mathfrak{p}}}^{\sigma} + \sum_{\bar{\mathfrak{p}}^{\sigma}=\mathfrak{P}} B_{\bar{\mathfrak{p}}}^{\sigma} \\ &= \sum_{\bar{\mathfrak{p}}^{\sigma}=\mathfrak{P}} bX_{\mathfrak{P}} + C_{\mathfrak{P}} \\ &= n_{\mathfrak{p}} bX_{\mathfrak{P}} + C_{\mathfrak{P}} \end{aligned}$$

where $C_{\mathfrak{P}}$ is a vector such that $|C_{\mathfrak{P}}| < n_{\mathfrak{p}} b$. Substituting in the relation yields

$$0 = \sum_{\mathfrak{P}} x_{\mathfrak{P}} n_{\mathfrak{p}} bX_{\mathfrak{P}} + \sum_{\mathfrak{P}} x_{\mathfrak{P}} C_{\mathfrak{P}}. \tag{2}$$

Let $(C_{\mathfrak{P}}, X_{\mathfrak{P}})$ be the component of $C_{\mathfrak{P}}$ along $X_{\mathfrak{P}}$. Since the vectors $X_{\mathfrak{P}}$ are independent, the component of each $X_{\mathfrak{P}}$ in (2) must be 0. It is

$$x_{\mathfrak{P}}\big[n_{\mathfrak{p}} b + (C_{\mathfrak{P}}, X_{\mathfrak{P}})\big]$$

and the inequality $|C_{\mathfrak{P}}| < n_{\mathfrak{p}} b$ shows that $n_{\mathfrak{p}} b + (C_{\mathfrak{P}}, X_{\mathfrak{P}})$ cannot be 0. Hence $x_{\mathfrak{P}} = 0$, and the $Y_{\mathfrak{P}}$ are linearly independent.

This concludes the proof of the first inequality. □

4. Consequences of the First Inequality

We note that in Theorem 1, we have proved more than an inequality. Namely, we have actually proved that $h_2(G, C)$ is equal to $n \cdot h_1(G, C)$. This will be used at a later stage of the theory. However, at this point we shall only give applications of the inequality itself.

Since G is cyclic, we have

$$h_2(G, C) = (C^G : NC) = (C_k : N_{K/k} C_K)$$

or in terms of idèles,

$$h_2(G, C) = (J_k : k^* N_{K/k} J_K).$$

To simplify the notation, we abbreviate $N_{K/k}$ by N, and locally write $N_{\mathfrak{P}}$ for $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$.

The first inequality implies therefore that the norm index $(J_k : kNJ_K)$ of a cyclic extension is greater or equal to its degree. In particular, if this index is 1, then the cyclic extension is trivial, and $[K : k] = 1$ also. This remark is used to prove an important consequence of the first inequality.

THEOREM 2. *Let K be a normal extension of a global field k. If $K \neq k$ then there exists infinitely many primes $\mathfrak{p}$ of k which do not split completely in K. Phrased another way: If $K_{\mathfrak{P}} = k_{\mathfrak{p}}$ for all but a finite number of primes $\mathfrak{p}$, then $K = k$.*

PROOF. First let K/k be cyclic. Suppose $K_{\mathfrak{P}} = k_{\mathfrak{p}}$ at almost all primes. We shall prove that any idèle $\mathfrak{a} \in J_k$ can be written

$$\mathfrak{a} = \alpha N \mathfrak{a}_K \qquad \mathfrak{a}_K \in J_K.$$

Let S be the set of primes where $K_{\mathfrak{P}} \neq k_{\mathfrak{p}}$. We can find $\alpha \in k$ such that $\alpha^{-1}\mathfrak{a}$ is so close to 1 at all $\mathfrak{p} \in S$ that $\alpha^{-1}\mathfrak{a}_{\mathfrak{p}}$ is a local norm: $\alpha^{-1}\mathfrak{a}_{\mathfrak{p}} = N_{\mathfrak{P}}\alpha_{\mathfrak{P}}$. At all other primes, $\alpha^{-1}\mathfrak{a}$ is a fortiori a local norm of an $\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{p}}$ because $K_{\mathfrak{P}} = k_{\mathfrak{p}}$. We make up an idèle $\mathfrak{a}_K \in J_K$ by giving it the component $\alpha_{\mathfrak{P}}$ at one $\mathfrak{P} \mid \mathfrak{p}$, and 1 at the other $\mathfrak{P} \mid \mathfrak{p}$. Then

$$\mathfrak{a} = \alpha \cdot N\,\mathfrak{a}_K$$

as was to be shown. Therefore $(J_k : kNJ_K) = 1$, $K = k$

If K/k is normal, and $K \neq k$, then there is a *non trivial* cyclic subgroup of G which leaves fixed a subfield F of K over which K is cyclic. The theorem is now obvious since there are infinitely many primes in F that do not split completely in K. □

In the following special cases, one can use the Hilbert Theory to sharpen Theorem 2.

THEOREM 3. *Let K/k be a cyclic extension of prime power degree p^r. Then there exist infinitely many primes of k which do not split at all in K, i.e. which remain prime in K.*

PROOF. K contains exactly one subfield F of degree p over k. Suppose that almost all primes split in some way. Then for such primes $\mathfrak{p}$,

$$[K_{\mathfrak{p}} : k_{\mathfrak{p}}] = [Kk_{\mathfrak{p}} : k_{\mathfrak{p}}] = [K : (K \cap k_{\mathfrak{p}})] = \frac{[K : k]}{[(K \cap k_{\mathfrak{p}}) : k]}$$

is the local degree and is strictly less than p^r. Hence $[(K \cap k_{\mathfrak{p}}) : k] > 1$ and therefore $F \subset k_{\mathfrak{p}}$. This would mean that all but a finite number of primes split completely in F, and this is impossible. □

The next theorem will be used in the proof of the second inequality.

THEOREM 4. *Let $K_1, \ldots, K_r/k$ be r cyclic extensions of prime degree p which are mutually disjoint over k, i.e. $K_\nu \cap (K_1 \ldots \widehat{K}_\nu \ldots K_r) = k$. Then there exist infinitely many primes $\mathfrak{p}$ that split completely in K_i $(i > 1)$ and remain prime in K_1.*

PROOF. Let $K = K_1 \ldots K_r$ be the compositum of all K_ν. Then $K/(K_2 \ldots K_r)$ is cyclic. Let $\mathfrak{q}$ be a prime in $(K_2 \ldots K_r)$ which remains prime in K and which divides a prime $\mathfrak{p}$ of k which is unramified in K. (There exist infinitely many such primes.) Then $K_{\mathfrak{q}}/(K_2 \ldots K_r)_{\mathfrak{q}}$ is cyclic of degree p. But $K_{\mathfrak{q}}/k_{\mathfrak{p}}$ is also cyclic because $\mathfrak{p}$ is unramified in K. The Galois group of K/k is of type $(p, p, \ldots, p)$ and that of $K_{\mathfrak{q}}/k_{\mathfrak{p}}$ a cyclic subgroup. This means that $[K_{\mathfrak{q}} : k_{\mathfrak{p}}] \leqslant p$. Together with $[K_{\mathfrak{q}} : (K_2 \ldots K_r)_{\mathfrak{q}}] = p$ this shows $(K_2 \ldots K_r)_{\mathfrak{q}} = k_{\mathfrak{p}}$. It follows that $\mathfrak{p}$ splits completely in $(K_2 \ldots K_r)$. It remains prime in K_1, or else $K_{\mathfrak{q}} = k_{\mathfrak{p}}$ which is not the case. □

The previous theorems concerning the existence of primes splitting in a certain way are weak instances of more general results concerning the statistical behavior of primes in normal extension, which can be proved using analysis. What we have proved in Theorems 2, 3, and 4 will suffice for our development of class field theory.

We shall obtain one more consequence of the first inequality in function fields.

THEOREM 5. *Let k be a function field in one variable over a finite constant field k_0. Then there exists a divisor of degree 1 in k.*

PROOF. We have already observed (Section 3, Theorem 8) that the degrees of the divisors of k form an ideal of the ordinary integers. This ideal is principal, generated by the positive integer δ, which is the greatest common divisor of all degrees of the divisors. It is also the g.c.d. of the degrees of the primes, and we shall now prove that $\delta = 1$.

Let k_1/k_0 be the extension of degrees δ and let $K = kk_1$ be the corresponding constant field extension of K. For each prime $\mathfrak{p}$ of k, the residue class field $\bar{k}_\mathfrak{p}$ contains k_1, and therefore for any $\mathfrak{P} \mid \mathfrak{p}$, $K_\mathfrak{P} = k_\mathfrak{p}$. By the first inequality (Theorem 2) it follows that $K = k$, i.e. $\delta = 1$. □

It may be convenient for the reader to recapitulate the essential ingredients of the preceding proof:

The first inequality in function fields is actually an immediate consequence of the Riemann–Roch Theorem and of the fact that the constant field is finite. The only other facts used in its proof are the elementary properties of the index $h_{2/1}$, and some elementary local properties.

We see therefore that the existence of a divisor of degree 1 is fairly shallow. The existence of a prime of degree 1 is a much more serious question. Such primes do not always exist, and conditions under which they exist are obtained from the Riemann Hypothesis in function fields.

We see that in function fields, the value group of the idèle classes is the integers, and is generated by an idèle class having volume exactly q. Denoting such an idèle class by a_1, so that $|a_1| = q$, we see that we can write any idèle class a uniquely in the form $a = a_1^\nu \cdot a_0$ where a_0 is an idèle class of absolute value 1. We may therefore assign ordinals to idèle classes, just as we did in the local theory, and we shall see later that from the point of view of class field theory, the group of idèle classes behaves in exactly the same fashion as does the local group.