Chapter VI

Local Class Field Theory

J-P. Serre

Introduction

We call a field K a *local field* if it is complete with respect to the topology defined by a discrete valuation v and if its residue field k is finite. We write $q = p^f = \text{Card}\,(k)$ and we always assume that the valuation v is normalized; that is, that the homomorphism $v: K^* \to \mathbf{Z}$ is surjective. The structure of such fields is known:

1. If K has characteristic 0, then K is a finite extension of the p-adic field $\mathbf{Q}_p$, the completion of $\mathbf{Q}$ with respect to the topology defined by the p-adic valuation. If $[K:\mathbf{Q}_p] = n$ then $n = ef$ where f is the residue degree (that is, $f = [k:\mathbf{F}_p]$ and e is the ramification index $v(p)$.

2. If K has characteristic p ("the equal characteristic case"), then K is isomorphic to a field $k((T))$ of formal power series, where T is a uniformizing parameter.

The first case is the one which arises in completions of a number field relative to a prime number p.

We shall study the Galois groups of extensions of K and would of course like to know the structure of the Galois group $G(K_s/K)$ of the separable closure K_s of K, since this contains the information about all such extensions. (In the case of characteristic 0, $K_s = \bar{K}$). We shall content ourselves with the following:

1. The cohomological properties of all galois extensions, whether abelian or not.

2. The determination of the abelian extensions of K, that is, the determination of G modulo its derived group G'.

Throughout this Chapter, we shall adhere to the notation already introduced above, together with the following. We denote the ring of integers of K by O_K, the multiplicative group of K by K^* and the group of units by U_K. A similar notation will be used for extensions L of K, and if L is a galois extension, then we denote the Galois group by $G(L/K)$ or $G_{L/K}$ or even by G. If $s \in G$ and $\alpha \in L$, then we denote the action of s on α by ${}^s\alpha$ or by $s(\alpha)$.

In addition to the preceding Chapters, the reader is referred to "Corps Locaux" (Actualités scientifiques et industrielles, 1296; Hermann, Paris, 1962) for some elided details. In what follows theorems etc. in the four sections are numbered independently.

1. The Brauer Group of a Local Field

1.1. *Statements of Theorems*

In this first section, we shall state the main results; the proofs of the theorems will extend over §§ 1.2–1.6.

We begin by recalling the definition of the Brauer group, Br (K), of K.

(See Chapter V, § 2.7.) Let L be a finite galois extension of K with Galois group $G(L/K)$. We write $H^2(L/K)$ instead of $H^2(G_{L/K}, L^*)$ and we consider the family $(L_i)_{i\in I}$ of all such finite galois extensions of K. The inductive (direct) limit $\varinjlim H^2(L_i/K)$ is by definition the Brauer group, $\mathrm{Br}(K)$, of K.

It follows from the definition that $\mathrm{Br}(K) = H^2(K_s/K)$. In order to compute $\mathrm{Br}(K)$ we look first at the intermediate field K_{nr}, $K \subset K_{nr} \subset K_s$, where K_{nr} denotes the maximal unramified extension of K. The reader is referred to Chapter I, § 7 for the properties of K_{nr}. We recall in particular, that the residue field of K_{nr} is $\bar{k}$, the algebraic closure of k, and that $G(K_{nr}/K) = G(\bar{k}/k)$. We denote by F the Frobenius element in $G(K_{nr}/K)$; the effect of F on the residue field $\bar{k}$ is given by $\lambda \mapsto \lambda^q$. The map $v \mapsto F^v$ is an isomorphism $\hat{\mathbf{Z}} \to G(K_{nr}/K)$ of topological groups. From Chapter V § 2.5, we recall that $\hat{\mathbf{Z}}$ is the projective (inverse) limit, $\varprojlim \mathbf{Z}/n\mathbf{Z}$, of the cyclic groups $\mathbf{Z}/n\mathbf{Z}$.

Since K_{nr} is a subfield of K_s, $H^2(K_{nr}/K)$ is a subgroup of $\mathrm{Br}(K) = H^2(K_s/K)$. In fact:

THEOREM 1. $H^2(K_{nr}/K) = \mathrm{Br}(K)$.

We have already noted above that $H^2(K_{nr}/K) = H^2(\hat{\mathbf{Z}}, K_{nr}^{\bullet})$.

THEOREM 2. *The valuation map* $v: K_{nr}^{\bullet} \to \mathbf{Z}$ *defines an isomorphism* $H^2(K_{nr}/K) \to H^2(\hat{\mathbf{Z}}, \mathbf{Z})$.

We have to compute $H^2(\hat{\mathbf{Z}}, \mathbf{Z})$. More generally let G be a profinite group and consider the exact sequence

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

of G-modules with trivial action. The module $\mathbf{Q}$ has trivial cohomology, since it is uniquely divisible (that is, $\mathbf{Z}$-injective) and so the coboundary $\delta: H^1(\mathbf{Q}/\mathbf{Z}) \to H^2(\mathbf{Z})$ yields an isomorphism $H^1(\mathbf{Q}/\mathbf{Z}) \to H^2(G, \mathbf{Z})$. Now $H^1(\mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ and so $\mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \cong H^2(G, \mathbf{Z})$.

We turn now to $\mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z})$. Let $\phi \in \mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z})$ and define a map $\gamma: \mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) \to \mathbf{Q}/\mathbf{Z}$ by $\phi \mapsto \phi(1) \in \mathbf{Q}/\mathbf{Z}$. It follows from Theorem 2 that we have isomorphisms

$$H^2(K_{nr}/K) \xrightarrow{v} H^2(\hat{\mathbf{Z}}, \mathbf{Z}) \xrightarrow{\delta^{-1}} \mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z}.$$

The map $\mathrm{inv}_K: H^2(K_{nr}/K) \to \mathbf{Q}/\mathbf{Z}$ is now defined by

$$\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ v.$$

For future reference, we state our conclusions in:

COROLLARY. *The map* $\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ v$ *defines an isomorphism between the groups* $H^2(K_{nr}/K)$ *and* $\mathbf{Q}/\mathbf{Z}$.

Since, by Theorem 1, $H^2(K_{nr}/K) = \mathrm{Br}(K)$, we see that *we have defined an isomorphism* $\mathrm{inv}_K: \mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}$.

If L is a finite extension of K, the corresponding map will be denoted by inv_L.

THEOREM 3. *Let L/K be a finite extension of degree n. Then*

$$\mathrm{inv}_L \circ \mathrm{Res}_{K/L} = n \,.\, \mathrm{inv}_K.$$

In other words, the following diagram is commutative

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{Res}_{K/L}"] \arrow[d, "\mathrm{inv}_K"'] & \mathrm{Br}(L) \arrow[d, "\mathrm{inv}_L"] \\
\mathbf{Q}/\mathbf{Z} \arrow[r, "n"] & \mathbf{Q}/\mathbf{Z}
\end{tikzcd}$$

(For the definition of $\mathrm{Res}_{K/L}$, the reader is referred to Chapter IV § 4 and to Chapter V § 2.7.)

COROLLARY 1. *An element* $\alpha \in \mathrm{Br}(K)$ *gives* 0 *in* $\mathrm{Br}(L)$ *if and only if* $n\alpha = 0$.

COROLLARY 2. *Let L/K be an extension of degree n. Then $H^2(L/K)$ is cyclic of order n. More precisely, $H^2(L/K)$ is generated by the element* $u_{L/K} \in \mathrm{Br}(K)$, *the invariant of which is* $1/n \in \mathbf{Q}/\mathbf{Z}$.

Proof. This follows from the fact that $H^2(L/K)$ is the kernel of Res.

1.2 *Computation of* $H^2(K_{nr}/K)$

In this section we prove Theorem 2. We have to prove that the homomorphism $H^2(K_{nr}/K) \to H^2(\hat{\mathbf{Z}}, \mathbf{Z})$ is an isomorphism.

PROPOSITION 1. *Let K_n be an unramified extension of K of degree n and let $G = G(K_n/K)$. Then for all $q \in \mathbf{Z}$ we have:*

(1). $H^q(G, U_n) = 0$, where $U_n = U_{K_n}$;

(2). the map $v: H^q(G, K_n^*) \to H^q(G, \mathbf{Z})$ is an isomorphism.

(Theorem 2 is evidently a consequence of (2) of Proposition 1, since $H^2(K_{nr}/K) = H^2(\hat{\mathbf{Z}}, K_{nr}^*)$.)

Proof. The fact that (1) implies (2) follows from the cohomology sequence

$$H^q(G, U_n) \to H^q(G, K_n^*) \to H^q(G, \mathbf{Z}) \to H^{q+1}(G, U_n)$$

It remains to prove (1). Consider the decreasing sequence of open subgroups $U_n \supset U_n^1 \supset U_n^2 \supset \ldots$ defined as follows: $x \in U_n^i$ if and only if $v(x-1) \geqslant i$. Now let $\pi \in K$ be a uniformizing element; so that $U_n^i = 1+\pi^i O_n$, where $O_n = O_{K_n}$. Then $U_n = \varprojlim U_n/U_n^i$. The proof will now be built up from the three following lemmas.

LEMMA 1. *Let k_n be the residue field of K_n. Then there are galois isomorphisms $U_n/U_n^1 \cong k_n^*$ and, for $i \geqslant 1$, $U_n^i/U_n^{i+1} \cong k_n^+$.*

(By a galois isomorphism we mean an isomorphism which is compatible with the action of the Galois group on either side.)

Proof. Take $\alpha \in U_n$ and map $\alpha \mapsto \bar{\alpha}$ where $\bar{\alpha}$ is the reduction of α into k_n. By definition, $U_n^1 = 1+\pi O_n$; so if $\alpha \in U_n^1$ then $\bar{\alpha} = 1$, and the first part of the lemma is proved.

To prove the second part, take $\alpha \in U_n^i$ and write $\alpha = 1+\pi^i\beta$ where $\beta \in O_n$. Now map $\alpha \mapsto \bar{\beta}$. We have to show that in this map a product $\alpha\alpha'$ corresponds to the sum $\bar{\beta}+\bar{\beta}'$. By definition, $\alpha\alpha' = 1+\pi^i(\beta+\beta')+\dots$, whence $\alpha\alpha' \mapsto \bar{\beta}+\bar{\beta}'$.

Finally, the isomorphisms are galois since ${}^s\alpha = 1+\pi^i.{}^s\beta$.

LEMMA 2. *For all integers q and for all integers $i \geqslant 0$, $H^q(G, U_n^i/U_n^{i+1}) = 0$.*

Proof. For $i = 0$, $U_n^0 = U_n$, and the first part of Lemma 1 gives

$$H^q(G, U_n/U_n^1) = H^q(G, k_n^*) = H^q(G_{k_n/k}, k_n^*).$$

Now for $q = 1$, $H^1(G_{k_n/k}, k_n^*) = 0$ ("Hilbert Theorem 90", cf. Chapter V, § 2.6). For $q = 2$, observe that G is cyclic. Since k_n^* is finite, the Herbrand quotient $h(k_n^*) = 1$ (cf. Chapter IV, § 8, Prop. 11); hence the result for $q = 2$. For other values of q the result follows by periodicity.

For $i \geqslant 1$, the lemma follows from Lemma 1 and the fact that k_n^+ has trivial cohomology.

The proof of Theorem 2 will be complete if we can go from the groups U_n^i/U_n^{i+1} to the group U_n itself and the following lemma enables us to do this.

LEMMA 3. *Let G be a finite group and let M be a G-module. Let M^i, $i \geqslant 0$ and $M^0 = M$, be a decreasing sequence of G-submodules and assume that $M = \varprojlim M/M^i$; (more precisely, the map from M to the limit is a bijection). Then, if, for some $q \in \mathbf{Z}$, $H^q(G, M^i/M^{i+1}) = 0$ for all i, we have $H^q(G, M) = 0$.*

Proof. Let f be a q-cocycle with values in M. Since $H^q(G, M/M^1) = 0$, there exists a $(q-1)$-cochain ψ_1 of G with values in M such that $f = \delta\psi_1+f_1$, where f_1 is a q-cocycle in M^1. Similarly, there exists ψ_2 such that $f_1 = \delta\psi_2+f_2$, $f_2 \in M^2$, and so on. We construct in this way a sequence (ψ_n, f_n) where ψ_n is a $(q-1)$-cochain with values in M^{n-1} and f_n is a q-cocycle with values in M^n, and $f_n = \delta.\psi_{n+1}+f_{n+1}$. Set $\psi = \psi_1+\psi_2+\dots$. In view of the hypotheses on M, this series converges and defines a $(q-1)$-cochain of G with values in M. On summing the equations $f_n = \delta\psi_{n+1}+f_{n+1}$, we obtain $f = \delta\psi$, and this proves the lemma.

We return now to the proof of Proposition 1. Take M in Lemma 3 to be U_n. It follows from Lemma 3 and from Lemma 2 that the cohomology of U_n is trivial and this completes the proof of Proposition 1 and so also of Theorem 2.

1.3 *Some Diagrams*

PROPOSITION 2. *Let L/K be a finite extension of degree n and let L_{nr} (resp. K_{nr}) be the maximal unramified extension of L (resp. K); so that $K_{nr} \subset L_{nr}$. Then the following diagram is commutative.*

$$\begin{tikzcd}
H^2(K_{nr}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"'] & H^2(L_{nr}/L) \arrow[d, "\mathrm{inv}_L"'] \\
\mathbf{Q}/\mathbf{Z} \arrow[r, "n"] & \mathbf{Q}/\mathbf{Z}
\end{tikzcd}$$

Proof. Let $\Gamma_K = G(K_{nr}/K)$ and let F_K be the Frobenius element of Γ_K; let Γ_L and F_L be defined similarly. We have $F_L = (F_K)^f$ where $f = [l:k]$ is the residue field degree of L/K.

Let e be the ramification index of L/K, and consider the diagram:

$$\begin{tikzcd}
H^2(\Gamma_K, K_{nr}^*) \arrow[r, "v_K"] \arrow[d, "\mathrm{Res}"'] \arrow[dr, phantom, "(1)"] & H^2(\Gamma_K, \mathbf{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "e.\mathrm{Res}"'] \arrow[dr, phantom, "(2)"] & \mathrm{Hom}(\Gamma_K, \mathbf{Q}/\mathbf{Z}) \arrow[r, "\gamma_K"] \arrow[d, "e.\mathrm{Res}"'] \arrow[dr, phantom, "(3)"] & \mathbf{Q}/\mathbf{Z} \arrow[d, "n"'] \\
H^2(\Gamma_L, L_{nr}^*) \arrow[r, "v_L"] & H^2(\Gamma_L, \mathbf{Z}) \arrow[r, "\delta^{-1}"] & \mathrm{Hom}(\Gamma_L, \mathbf{Q}/\mathbf{Z}) \arrow[r, "\gamma_L"] & \mathbf{Q}/\mathbf{Z},
\end{tikzcd}$$

where Res is induced by the inclusion $\Gamma_L \to \Gamma_K$, and γ_K (resp. γ_L) is given by $\varphi \mapsto \varphi(F_K)$ (resp. $\varphi \mapsto \varphi(F_L)$). The three squares (1), (2), (3) extracted from that diagram are *commutative*; for (1), this follows from the fact that v_L is equal to $e.v_K$ on K_{nr}^*; for (3), it follows from $F_L = F_K^f$, and $n = ef$; for (2), it is obvious.

On the other hand, the definition of $\mathrm{inv}_K : H^2(\Gamma_K, K_{nr}^*) \to \mathbf{Q}/\mathbf{Z}$ is equivalent to:

$$\mathrm{inv}_K = \gamma_K \circ \delta^{-1} \circ v_K,$$

and similarly:

$$\mathrm{inv}_L = \gamma_L \circ \delta^{-1} \circ v_L.$$

Proposition 2 is now clear.

COROLLARY 1. *Let $H^2(L/K)_{nr}$ be the subgroup of $H^2(K_{nr}/K)$ consisting of those $\alpha \in H^2(K_{nr}/K)$ which are "killed by L" (that is, which give 0 in $Br(L)$). Then $H^2(L/K)_{nr}$ is cyclic of order n and is generated by the element $u_{L/K}$ in $H^2(K_{nr}/K)$ such that $\mathrm{inv}_K(u_{L/K}) = 1/n$.*

Proof. Note that a less violent definition of $H^2(L/K)_{nr}$ is provided by $H^2(L/K)_{nr} = H^2(L/K) \cap H^2(K_{nr}/K)$.

Consider the exact sequence

$$0 \to H^2(L/K)_{nr} \to H^2(K_{nr}/K) \xrightarrow{\mathrm{Res}} H^2(L_{nr}/L).$$

The kernel of the map $H^2(K_{nr}/K) \to H^2(L_{nr}/L)$ is $H^2(L/K)_{nr}$ and this goes to 0 under $\mathrm{inv}_L : H^2(L_{nr}/L) \to \mathbf{Q}/\mathbf{Z}$. On the other hand, it follows from Proposition 2 that $\mathrm{inv}_L \circ \mathrm{Res} = n.\mathrm{inv}_K$. The kernel of the latter is $(1/n)\mathbf{Z}/\mathbf{Z}$ and so $H^2(L/K)_{nr}$ is cyclic of order n, and is generated by $u_{L/K} \in H^2(K_{nr}/K)$ with $\mathrm{inv}_K(u_{L/K}) = 1/n$.

Corollary 2. *The order of $H^2(L/K)$ is a multiple of n.*

Proof. $H^2(L/K)$ contains a cyclic subgroup of order n by Corollary 1.

1.4 *Construction of a Subgroup with Trivial Cohomology*

Let L/K be a finite galois extension with Galois group G, where L and K are local fields. According to the discussion in Proposition 1, the G-module U_L has trivial cohomology when L is unramified.

Proposition 3. *There exists an open subgroup, V, of U_L with trivial cohomology. That is, $H^q(G, V) = 0$ for all q.*

Proof. We shall give two proofs; the first one works only in characteristic 0, the second works generally.

Method 1. The idea is to compare the multiplicative and the additive groups of L. We know that L^+ is a free module over the algebra $K[G]$. That is, there exists $\alpha \in L$ such that $[{}^s\alpha]_{s \in G}$ is a basis for L considered as a vector space over K.

Now take the ring O_K of integers of K and define $A = \sum_{s \in G} O_K . {}^s\alpha$. This is free over G and so has trivial cohomology. Moreover, by multiplying α by a sufficiently high power of the local uniformizer π_K, we may take such an A to be contained in any given neighbourhood of 0.

It is a consequence of Lie theory that the additive group of L is locally isomorphic to the multiplicative group. More precisely, the power series $e^x = 1+x+\ldots+x^n/n!+\ldots$, converges for $v(x) > v(p)/(p-1)$. Thus in the neighbourhood $v(x) > v(p)/(p-1)$ of 0, L^* is locally isomorphic to L^+ under the map $x \mapsto e^x$. (Note that, in the same neighbourhood, the inverse mapping is given by $\log(1+x) = x - x^2/2 + x^3/3 - \ldots$.)

Now define $V = e^A$; it is clear that V has trivial cohomology.

The foregoing argument breaks down in characteristic p; namely at the local isomorphism of L^+ and L^*.

Method 2. We start from an A constructed as above: $A = \sum_{s \in G} O_K . {}^s\alpha$. We may assume that $A \subset O_L$. Since A is open in O_L, $\pi_K^N O_L \subset A$ for a suitable N. Set $M = \pi_K^i A$. Then $M . M \subset \pi_K M$ if $i \geqslant N+1$. For $M . M = \pi_K^{2i} A . A \subset \pi_K^{2i} O_L$ and if $i \geqslant N+1$ then

$$\pi_K^{2i} O_L \subset \pi_K . \pi_K^i A \subset \pi_K M.$$

Now let $V = 1+M$. Then V is an open subgroup of U_L. It remains to be proved that V has trivial cohomology. We define a filtration of V by means of subgroups $V^i = 1+\pi_K^i M$, $i \geqslant 0$. (Note that V^i is a subgroup since $(1+\pi_K^i x)(1+\pi_K^i y) = 1+\pi_K^i(x+y+\pi_K^i xy)$, etc.) This yields a decreasing filtration $V = V^0 \supset V^1 \supset V^2 \supset \ldots$. As in § 1.2, Lemma 2, we are reduced to proving that $H^q(G, V^i/V^{i+1}) = 0$ for all q. Take $x = 1+\pi_K^i\beta$, $\beta \in M$ and associate with this its image $\bar{\beta} \in M/\pi_K M$. This is a group isomorphism of V^i/V^{i+1} and $M/\pi_K M$ and we know that the latter has trivial cohomology, since it is free over G.

This completes our proofs of Proposition 3.

We recall the definition of the Herbrand quotient $h(M)$. Namely, $h(M) = \text{Card}\,(\hat{H}^0(M))/\text{Card}\,(H^1(M))$, when both sides are finite. (See Chapter IV, § 8.)

Corollary 1. *Let L/K be a cyclic extension of degree n. Then we have $h(U_L) = 1$ and $h(L^*) = n$.*

Proof. Let V be an open subgroup of U_L with trivial cohomology (cf. Prop. 3). Since h is multiplicative, $h(U_L) = h(V) . h(U_L/V) = 1$.

Again, $L^*/U_L \cong \mathbf{Z}$. So $h(L^*) = h(\mathbf{Z}) . h(U_L)$. Now $h(U_L) = 1$ and $h(\mathbf{Z}) = n$, since $\hat{H}^0(G, \mathbf{Z}) = n$ and $H^1(G, \mathbf{Z})$ is trivial. Hence $h(L^*) = n$.

Corollary 2. *Let L/K be a cyclic extension of degree n. Then $H^2(L/K)$ is of order $n = [L : K]$.*

Proof. We have

$$h(L^*) = \frac{\text{Card}\,(H^2(G, L^*))}{\text{Card}\,(H^1(G, L^*))}.$$

Now Corollary 1 gives $h(L^*) = n$. Moreover, $H^1(G, L^*) = 0$ (Hilbert Theorem 90). Hence $\text{Card}\,(H^2(G, L^*)) = n$. But $H^2(G, L^*)$ is $H^2(L/K)$, whence the result.

1.5 *An Ugly Lemma*

Lemma 4. *Let G be a finite group and let M be a G-module and suppose that ρ, q are integers with $\rho \geqslant 0, q \geqslant 0$. Assume that:*

(a) *$H^i(H, M) = 0$ for all $0 < i < q$ and all subgroups H of G;*

(b) *if $H \subset K \subset G$, with H invariant in K and K/H cyclic of prime order, then the order of $H^q(H, M)$ (resp. $\hat{H}^0(H, M)$ if $q = 0$) divides $(K : H)^\rho$.*

Then the same is true of G. That is, $H^q(G, M)$ (resp. $\hat{H}^0(G, M)$ is of order dividing $(G : 1)^\rho$.

Proof. Since the restriction map $\text{Res} : \hat{H}^q(G, M) \to \hat{H}^q(G_p, M)$ is injective on the p-primary components of $\hat{H}^q(G, M)$, where G_p denotes a Sylow p-subgroup of G, we may confine our attention to the case in which G is a p-group. We now argue by induction on the order of G.

Assume that G has order greater than 1. Choose a subgroup H of G which is invariant and of index p. We apply the induction hypothesis to G/H. We know from (b) that, for $q > 0$, the order of $H^q(G/H, M^H)$ divides $(G : H)^\rho = p^\rho$ and by the induction hypothesis $H^q(H, M)$ divides $(H : 1)^\rho$. Now it follows from (a) that we have an exact sequence (Chapter IV, § 5).

$$0 \longrightarrow H^q(G/H, M^H) \xrightarrow{\text{Inf}} H^q(G, M) \xrightarrow{\text{Res}} H^q(H, M).$$

Thus $H^q(G, M)$ has order dividing $p^\rho . (H : 1)^\rho = (G : 1)^\rho$.

For $q = 0$, we recall (see Chapter IV, § 6) that

$$\hat{H}^0(G, M) = M^G/N_G M.$$

Then we have the exact sequence

$$M^H/N_H M \xrightarrow{N_{G/H}} M^G/N_G M \longrightarrow (M^H)^{G/H}/N_{G/H} M^H$$

where $N_{G/H}$ denotes the norm map and the second map is induced by the identity. The remainder of the argument now runs as before.

1.6 *End of Proofs*

Proposition 4. *Let L/K be a finite galois extension with Galois group G of order $n = [L:K]$. Then $H^2(L/K)$ is cyclic of order n and has a generator $u_{L/K} \in H^2(K_{nr}/K)$ such that* $\mathrm{inv}_K(u_{L/K}) = 1/n$.

Proof. In Lemma 4, take $M = L^*$, $\rho = 1$ and $q = 2$. Condition (a) is satisfied by "Theorem 90" and (b) is true by Prop. 3, Cor. 2. Hence $H^2(G, L^*)$ has order dividing $(G:1) = n$. But by Prop. 2, Cor. 1, $H^2(L/K)$ contains a cyclic subgroup of order n, generated by $u_{L/K} \in H^2(K_{nr}/K)$ and such that $\mathrm{inv}_K(u_{L/K}) = 1/n$. Whence Proposition 4.

It follows from this proposition that $H^2(L/K)$ is contained in $H^2(K_{nr}/K)$. We turn now to the proof of Theorem 1. The theorem asserts that the inclusion $\mathrm{Br}(K) \supset H^2(K_{nr}/K)$ is actually equality. Now by definition, $\mathrm{Br}(K) = \cup H^2(L/K)$, where L runs through the set of finite galois extensions of K. But as remarked above, $H^2(L/K) \subset H^2(K_{nr}/K)$. Hence $\mathrm{Br}(K) \subset H^2(K_{nr}/K)$, as was to be proved.

Evidently, Theorem 3 follows from Theorem 1 and Proposition 2.

1.7 *An Auxiliary Result*

We have now proved all the statements in § 1.1 and we conclude the present chapter with a result which has applications to global fields.

Let A be an abelian group and let n be an integer $\geqslant 1$. Consider the cyclic group $\mathbf{Z}/n\mathbf{Z}$ with trivial action on A. We shall denote the corresponding Herbrand quotient by $h_n(A)$, whenever it is defined. We have

$$h_n(A) = \frac{\mathrm{Order}\,(A/nA)}{\mathrm{Order}\,{}_nA}$$

where ${}_nA$ is the set of $\alpha \in A$ such that $n\alpha = 0$. (Alternatively, we could begin with the map $A \xrightarrow{n} A$ and take $h_n(A)$ to be:

$$\text{order (Coker }(n))/\text{order (Ker }(n)).)$$

Now let K be a local field. Then for $\alpha \in K$ there is a normalized absolute value, denoted by $|\alpha|_K$ (see Chapter II, § 11). If $\alpha \in O_K$, then $|\alpha|_K = 1/\mathrm{Card}\,(O_K/\alpha O_K)$.

Proposition 5. *Let K be a local field and let $n \geqslant 1$ be an integer prime to the characteristic of K. Then $h_n(K^*) = n/|n|_K$.*

Proof. Suppose that K has characteristic 0. We have $h_n(K^*) = h_n(\mathbf{Z}).h_n(U_K)$. Now $h_n(\mathbf{Z}) = n$; so we must compute $h_n(U_K)$. As in Proposition 3, we consider a subgroup V of U which is open and isomorphic to the additive group of O_K. We have $h_n(U_K) = h_n(V).h_n(U_K/V)$ and since U_K/V is finite, $h_n(U_K/V) = 1$. We have

$$h_n(V) = h_n(O_K)$$

and

$$h_n(O_K) = \mathrm{Card}\,(O_K/nO_K) = 1/|n|_K.$$

Whence

$$h_n(K^*) = n.(1/|n|_K) = n/|n|_K.$$

Suppose now that K has characteristic p. We take the same steps as before. First, $h_n(K^*) = n.h_n(U_K)$. Now consider the exact sequence

$$0 \to U_K^1 \to U_K \to k^* \to 0$$

where U_K^1 is a pro-p-group (cf. Lemma 1). Since n is prime to p it follows that $h_n(U_K^1) = 1$ and that $h_n(k^*) = 1$. So $n.h_n(U_K) = n$. Whence the result.

We note that the statement of the proposition is also correct for $\mathbf{R}$ *or* $\mathbf{C}$. In these cases we have $|n|_{\mathbf{R}} = |n|$, $|n|_{\mathbf{C}} = |n|^2$ and one can check directly that, for $\mathbf{R}$, $h_n(\mathbf{R}^*) = n/|n| = 1$ and, for $\mathbf{C}$, $h_n(\mathbf{C}^*) = n/|n|_{\mathbf{C}} = 1/n$.

Appendix

Division Algebras Over a Local Field

It is known that elements of Brauer groups correspond to skew fields (cf., for instance, "Séminaire Cartan", 1950/51, Exposés 6/7), and we are going to use this correspondence to give a description of skew fields and the corresponding invariants. Most results will be stated without proof.

Let K be a local field and let D be a division algebra over K, with centre K and $[D:K] = n^2$. The valuation v of K extends in a unique way from K to D (for example, by extending first to $K(\alpha)$, $\alpha \in D$, and then fitting the resulting extensions together). The field D is complete with respect to this valuation and, in an obvious notation, O_D is of degree n^2 over O_K. Let d be the residue field of D; we have $n^2 = ef$ where e is the ramification index and $f = [d:k]$.

Now $e \leqslant n$; for there exists $\alpha \in D$ such that $v_D(\alpha) = e^{-1}$ and α belongs to a commutative subfield of degree at most n over K. The residue field d is commutative, since k is a finite field, and $d = k(\bar{\alpha})$ for some $\alpha \in D$. Hence $f \leqslant n$. Together with $n^2 = ef$, the inequalities $e \leqslant n$ and $f \leqslant n$ yield $e = n$ and $f = n$.

Since $[d:k] = n$, we can find $\bar{\alpha} \in d$ such that $k(\bar{\alpha}) = d$. Now choose a corresponding $\alpha \in O_D$ and let $L = K(\alpha)$. Evidently $[L:K] \leqslant n$, since L is a commutative subfield of D. On the other hand, $\bar{\alpha}$ is an element of l (the residue field of L) and $l = d$; hence $[l:k] = n$. It follows that $[L:K] = n$ and L is unramified. We state this last conclusion as: *D contains a maximal commutative subfield L which is unramified over K.*

The element $\delta \in \mathrm{Br}(K)$ corresponding to D splits in L, that is $\delta \in H^2(L/K)$. So any element in $\mathrm{Br}(K)$ is split by an unramified extension and we have obtained a new proof of Theorem 1.

Description of the Invariant

The extension L of K constructed above is not unique, but the Skolem-Noether theorem (Bourbaki, "Algèbre", Chap. 8, § 10) shows that all such extensions are conjugate. The same theorem shows that any automorphism of L is induced by an inner automorphism of D. Hence there exists $\gamma \in D$ such that $\gamma L \gamma^{-1} = L$ and the inner automorphism $x \mapsto \gamma x \gamma^{-1}$ on L is the Frobenius F. Moreover γ is determined, up to multiplication by an element of L^*.

Let v_L be the valuation $v_L : L^* \to \mathbf{Z}$ of L; so that $v_D : D^* \to (1/n)\mathbf{Z}$ extends v_L on D. The image $i(D)$ of $v_D(\gamma)$ in $(1/n)\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$ is independent of the choice of γ. One can prove that $i(D) = \mathrm{inv}_K(\delta)$, where $\delta \in \mathrm{Br}(K)$ is associated with D.

We can express the definition of $i(D)$ in a slightly different way. The map $x \mapsto \gamma^n x \gamma^{-n}$ is equal to F^n on L and so is the identity. It follows that γ^n commutes with L and $\gamma^n = c \in L^*$. Now

$$v_D(\gamma) = \frac{1}{n}\, v_D(\gamma^n) = \frac{1}{n}\, v_D(c) = \frac{1}{n}\, v_L(c).$$

Hence we have $v_D(\gamma) = (1/n)v_L(c) = i/n$ where $c = \pi_L^i u$.

Application

Suppose that K'/K is an extension of degree n. By Theorem 3, Cor. 2, an element $\delta \in \mathrm{Br}(K)$ is killed by K'. Hence: *any extension K'/K of degree n can be embedded in D as a maximal commutative subfield.* This may be stated more spectacularly as: any irreducible equation of degree n over K can be solved in D.

Exercise

Consider the 2-adic field $\mathbf{Q}_2$ and let H be the quaternion skew field over $\mathbf{Q}_2$. Prove that the ring of integers in H consists of the elements $a+bi+cj+dk$ where $a, b, c, d \in \mathbf{Z}_2$ or $a, b, c, d \equiv \frac{1}{2} \pmod{\mathbf{Z}_2}$. Make a list of the seven (up to conjugacy) quadratic subfields of H.

2. Abelian Extensions of Local Fields

2.1 *Cohomological Properties*

Let L/K be a finite galois extension of local fields with Galois group $G = G(L/K)$ of order n. We have seen (§ 1.1, Theorem 3, Cor. 2.) that the group $H^2(L/K) = H^2(G, L^*)$ is cyclic of order n and contains a generator $u_{L/K}$ such that $\mathrm{inv}_K(u_{L/K}) = 1/n \in \mathbf{Q}/\mathbf{Z}$. On the other hand, we know that $H^1(G, L^*) = 0$.

Now let H be a subgroup of G of order m. Since H is the Galois group of L/K' for some $K' \supset K$, we also have $H^1(H, L^*) = 0$ and $H^2(H, L^*)$ is cyclic of order m and generated by $u_{L/K'}$.

To go further, we need to know more about $u_{L/K'}$. Now we have the restriction map $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(K')$ and this suggests that $u_{L/K'} = \mathrm{Res}\,(u_{L/K})$. To see that this is the case, we simply check on invariants. We have

$$\mathrm{inv}_{K'}(\mathrm{Res}\, u_{L/K}) = [K':K]\,\mathrm{inv}_K(u_{L/K}) = [K':K]\,.\,\frac{1}{n} = \frac{1}{m} = \mathrm{inv}_{K'}(u_{L/K'}).$$

We can now apply Tate's theorem (Chapter IV, § 10) to obtain:

THEOREM 1. *For all $q \in \mathbf{Z}$, the map $\alpha \mapsto \alpha . u_{L/K}$ given by the cup-product is an isomorphism of $\hat{H}^q(G, \mathbf{Z})$ onto $\hat{H}^{q+2}(G, L^*)$.*

A similar statement holds if H is a subgroup of G corresponding to an extension L/K'. The mappings Res and Cor connect the two isomorphisms and we have a more explicit statement in terms of diagrams.

STATEMENT. *The diagrams*

$$\begin{tikzcd} \hat{H}^q(G, \mathbf{Z}) \arrow[r, "u_{L/K}"] \arrow[d, "\mathrm{Res}"'] & \hat{H}^{q+2}(G, L^*) \arrow[d, "\mathrm{Res}"'] \\ \hat{H}^q(H, \mathbf{Z}) \arrow[r, "u_{L/K'}"] & \hat{H}^{q+2}(H, L^*) \end{tikzcd} \qquad \begin{tikzcd} \hat{H}^q(G, \mathbf{Z}) \arrow[r, "u_{L/K}"] & \hat{H}^{q+2}(G, L^*) \\ \hat{H}^q(H, \mathbf{Z}) \arrow[r, "u_{L/K'}"] \arrow[u, "\mathrm{Cor}"] & \hat{H}^{q+2}(H, L^*) \arrow[u, "\mathrm{Cor}"] \end{tikzcd}$$

are commutative.

Proof. As above, $u_{L/K'} = \mathrm{Res}\,(u_{L/K})$. We must show that

$$\mathrm{Res}_{K/K'}\,(u_{L/K} . \alpha) = u_{L/K'} . \mathrm{Res}_{K/K'}\,(\alpha).$$

The left-hand side is $\mathrm{Res}_{K/K'}\,(u_{L/K}) . \mathrm{Res}_{K/K'}\,(\alpha)$ (see Cartan-Eilenberg, "Homological Algebra", Chap. XII, p. 256) and so commutativity with Res is proved.

For the second diagram we have to show that $\mathrm{Cor}\,(u_{L/K'} . \beta) = u_{L/K} . \mathrm{Cor}(\beta)$. Now $\mathrm{Cor}\,(u_{L/K'} . \beta) = \mathrm{Cor}\,(\mathrm{Res}\,(u_{L/K}) . \beta) = u_{L/K} . \mathrm{Cor}\,(\beta)$ (Cartan-Eilenberg, *loc. cit.*) and this proves the commutativity of the second diagram.

2.2 *The Reciprocity Map*

We shall be particularly concerned with the case $q = -2$ of the foregoing discussion. By definition $\hat{H}^{-2}(G, \mathbf{Z})$ is $H_1(G, \mathbf{Z})$ and we know that

$H_1(G, \mathbf{Z}) = G/G' = G^{ab}$. On the other hand, $\hat{H}^0(L/K) = K^*/N_{L/K}L^*$, where $N_{L/K}$ denotes the norm. In this case, Theorem 1 reads as follows.

THEOREM 2. *The cup-product by $u_{L/K}$ defines an isomorphism of $G^{ab}(L/K)$ onto $K^*/N_{L/K}L^*$.*

We give a name to the isomorphism just constructed, or rather to its inverse. Define $\theta = \theta_{L/K}$ to be the isomorphism of $K^*/N_{L/K}L^*$ on to G^{ab}, which is inverse to the cup-product by $u_{L/K}$. The map θ is called the *local reciprocity map* or the *norm residue symbol.*

If $\alpha \in K^*$ corresponds to $\bar{\alpha} \in K^*/N_{L/K}L^*$, then we write $\theta_{L/K}(\bar{\alpha}) = (\alpha, L/K)$. The norm residue symbol is so named since it tells whether or not $\alpha \in K^*$ is a norm from L^*. Namely, $(\alpha, L/K) = 0$ (remember that 0 means 1!) if and only if α is a norm from L^*.

Observe that if L/K is abelian, then $G^{ab} = G$ and we have an isomorphism $\theta: K^*/N_{L/K}L^* \to G$.

2.3 *Characterization of $(\alpha, L/K)$ by Characters*

Let L/K be a galois extension with group G. We start from an $\alpha \in K^*$ and we seek a characterization of $(\alpha, L/K) \in G^{ab}$. For ease of writing we set $s_\alpha = (\alpha, L/K)$. Let $\chi \in \mathrm{Hom}\,(G, \mathbf{Q}/\mathbf{Z}) = H^2(G, \mathbf{Z})$ be a character of degree 1 of G and let $\delta\chi \in H^2(G, \mathbf{Z})$ be the image of χ by the coboundary map $\delta: H^1(G, \mathbf{Q}/\mathbf{Z}) \to H^2(G, \mathbf{Z})$ (cf. § 1.1) Let

$$\bar{\alpha} \in K^*/N_{L/K}(L^*) = \hat{H}^0(G, L^*)$$

be the image of α. The cup-product $\bar{\alpha}.\delta\chi$ is an element of $H^2(G, L^*) \subset \mathrm{Br}(K)$.

PROPOSITION 1. *With the foregoing notation, we have the formula*

$$\chi(s_\alpha) = \mathrm{inv}_K(\bar{\alpha}.\delta\chi).$$

Proof. By definition $s_\alpha.u_{L/K} = \bar{\alpha} \in \hat{H}^0(G, L^*)$, s_α being identified with an element of $H^{-2}(G, \mathbf{Z})$. Using the associativity of the cup-product, this gives $\bar{\alpha}.\delta\chi = u_{L/K}.s_\alpha.\delta\chi = u_{L/K}.(s_\alpha.\delta\chi) = u_{L/K}.\delta(s_\alpha.\chi)$ with $s_\alpha.\chi \in \hat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z})$. Now $\hat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\delta} \hat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}$ and we identify $\hat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z})$ with $\mathbf{Z}/n\mathbf{Z}$. Moreover, the identification between $H^{-2}(G, \mathbf{Z})$ and G^{ab} has been so made in order to ensure that $s_\alpha.\chi = \chi(s_\alpha)$ (see "Corps Locaux", Chap. XI, Annexe pp. 184–186). Write $s_\alpha.\chi = r/n$, $r \in \mathbf{Z}$. Then $\delta(r/n) \in \hat{H}^0(G, \mathbf{Z})$ and $\delta(r/n) = r$. Hence $u_{L/K}.(s.\delta\chi) = r.u_{L/K}$ and the invariant of this cohomology class is just $r/n = \chi(s_\alpha)$. So Proposition 1 is proved.

As an application we consider the following situation. Consider a tower of galois extensions $K \subset L' \subset L$ with $G = G(L/K)$ and $H = G(L/L')$. Then, if χ' is a character of $(G/H)^{ab}$ and χ is the corresponding character of G^{ab}, and if $\alpha \in K^*$ induces $s_\alpha \in G^{ab}$ and $s'_\alpha \in (G/H)^{ab}$ under the natural map $s_\alpha \mapsto s'_\alpha$, we have $\chi(s_\alpha) = \chi'(s'_\alpha)$. This follows from Prop. 2 1 and the fact that the inflation map transforms χ' (resp. $\delta\chi'$) into χ (resp. $\delta\chi$).

This compatibility allows us to define s_α for any abelian extension; in particular, taking $L = K^{ab}$, the maximal abelian extension of K, we get a homomorphism $\theta_K: K^* \to G(K^{ab}/K)$ defined by $\alpha \mapsto (\alpha, K^{ab}/K)$.

2.4 *Variations with the Fields Involved*

Having considered the effect on $(\alpha, L/K)$ of extensions of L we turn now to consider extensions of K. Let K'/K be a separable extension and let K^{ab}, K'^{ab} be the maximal abelian extensions of K, K' respectively.

We look at the first of the diagrams in the Statement of § 2.1 and the case $q = -2$. Taking the projective limit of the groups involved, we obtain a commutative diagram:

$$\begin{tikzcd}
K^* \arrow[r, "\theta_K"] \arrow[d, "\mathrm{incl}"'] & G_K^{ab} \arrow[d, "V"] \\
K'^* \arrow[r, "\theta_{K'}"] & G_{K'}^{ab}
\end{tikzcd}$$

Here V denotes the transfer (Chapter IV, § 6), $G_{K'}^{ab}$ denotes $G(K'^{ab}/K')$ and G_K^{ab} denotes $G(K^{ab}/K) = G^{ab}(K'^{ab}/K)$.

Similarly, using the second of the diagrams in the Statement, we obtain a commutative diagram:

$$\begin{tikzcd}
K'^* \arrow[r, "\theta'_K"] \arrow[d, "N_{K'/K}"'] & G_{K'}^{ab} \arrow[d, "i"] \\
K^* \arrow[r, "\theta_K"] & G_K^{ab}
\end{tikzcd}$$

where i is induced by the inclusion of $G_{K'}$ into G_K.

[Note that if K'/K is an inseparable extension, then in the first of these diagrams the transfer, V, should be replaced by qV where q is the inseparable factor of the degree of the extension K'/K. The second diagram holds even in the inseparable case.]

2.5 *Unramified Extensions*

In this case it is possible to compute the norm residue symbol explicitly in terms of the Frobenius element:

PROPOSITION 2. *Let L/K be an unramified extension of degree n and let $F \in G_{L/K}$ be the Frobenius element. Let $\alpha \in K^*$ and let $v(\alpha) \in Z$ be its normalized valuation. Then $(\alpha, L/K) = F^{v(\alpha)}$.*

Proof. Let χ be an element of $\mathrm{Hom}\,(G_{L/K}, \mathbf{Q}/\mathbf{Z})$. By Prop. 1, we have:

$$\chi((\alpha, L/K)) = \mathrm{inv}_K(\bar{\alpha}.\delta\chi).$$

The map $\mathrm{inv}_K: H^2(G_{L/K}, L^*) \to \mathbf{Q}/\mathbf{Z}$ has been defined as a composition:

$$H^2(G_{L/K}, L^*) \xrightarrow{v} H^2(G_{L/K}, \mathbf{Z}) \xrightarrow{\delta^{-1}} H^1(G_{L/K}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z}.$$

We have $v(\bar{\alpha}.\delta\chi) = v(\alpha).\delta\chi$, hence:

$$\mathrm{inv}_K(\bar{\alpha}.\delta\chi) = \gamma\circ\delta^{-1}\circ v(\bar{\alpha}.\delta\chi) = v(\alpha).\gamma(\chi) = v(\alpha)\chi(F) = \chi(F^{v(\alpha)}).$$

This shows that

$$\chi((\alpha, L/K)) = \chi(F^{v(\alpha)})$$

for any character χ of $G_{L/K}$; hence $(\alpha, L/K) = F^{v(\alpha)}$.

COROLLARY. *Let E/K be a finite abelian extension. The norm residue symbol $K^* \to G_{E/K}$ maps U_K onto the inertia subgroup T of $G_{E/K}$.*

Proof. Let L be the sub-extension of E corresponding to T. By Prop. 2, the image of U_K in $G_{L/K}$ is trivial; this means that the image of U_K in $G_{E/K}$ is contained in T. Conversely, let $t \in T$, and let $f = [L:K]$; there exists $a \in K^*$ such that $t = (a, E/K)$. Since $t \in T$, Prop. 2 shows that f divides $v_K(a)$; hence, there exists $b \in E^*$ such that $v_K(a) = v_K(Nb)$. If we put $u = a.Nb^{-1}$, we have $u \in U_K$ and $(u, E/K) = (a, E/K) = t$.

2.6 *Norm Subgroups*

DEFINITION. *A subgroup M of K^* is called a norm subgroup if there exists a finite abelian extension L/K with $M = N_{L/K}L^*$.*

Example: Let $m \geqslant 1$ be an integer, and let M_m be the set of elements $a \in K^*$ with $v_K(a) \equiv 0 \bmod m$; it follows from Prop. 2 (or from a direct computation of norms) that M_m is the norm group of the unramified extension of K of degree m.

Norm subgroups are closely related to the reciprocity map

$$\theta_K : K^* \to G_K^{ab} = G(K^{ab}/K)$$

defined in § 2.3. By construction, θ_K is obtained by projective limit from the isomorphisms $K^*/NL^* \to G_{L/K}$, where L runs through all finite abelian extensions of K. If we put:

$$\tilde{K} = \varprojlim . K^*/NL^*,$$

we see that θ_K can be factored into

$$K^* \xrightarrow{i} \tilde{K} \xrightarrow{\tilde{\theta}} G_K^{ab}.$$

where i is the natural map, and $\tilde{\theta}$ is an *isomorphism*. Note that $\tilde{K}$ is just the *completion* of K^* with respect to the topology defined by the norm subgroups.

This shows that norm subgroups of K^* and open subgroups of G_K^{ab} correspond to each other in a one–one way: if U is an open subgroup of G_K^{ab}, with fixed field L, we attach to U the norm subgroup $\theta_K^{-1}(U) = N_{L/K}L^*$; if M is a norm subgroup of K^*, we attach to it the adherence of $\theta_K(M)$; the corresponding field L_M is then the set of elements in K^{ab} which are invariant by the $\theta_K(a)$, for $a \in M$. We thus get a "Galois correspondence" between norm subgroups and finite abelian extensions; we state it as a proposition:

PROPOSITION 3. (a) *The map $L \mapsto NL^*$ is a bijection of the set of finite abelian extensions of K onto the set of norm subgroups of K^*.*

(b) *This bijection reverses the inclusion.*

(c) *$N(L.L') = NL \cap NL'$ and $N(L \cap L') = NL.NL'$.*

(d) *Any subgroup of K^* which contains a norm subgroup is a norm subgroup.*

(For a direct proof, see "Corps Locaux", Chap. XI, § 4.)

Non-abelian extensions give the same norm subgroups as the abelian ones:

PROPOSITION 4. *Let E/K be a finite extension, and let L/K be the largest abelian extension contained in E. Then we have:*

$$N_{E/K}E^* = N_{L/K}L^*.$$

Proof. This follows easily from the properties of the norm residue symbol proved in § 2.4; for more details, see Artin-Tate, "Class Field Theory", pp. 228–229, or "Corps Locaux", p. 180. (These two books give only the case where E/K is separable; the general case reduces to this one by observing that $NL = K$ when L is a purely inseparable extension of K.)

COROLLARY ("Limitation theorem"). *The index $(K^* : NE^*)$ divides $[E:K]$. It is equal to $[E:K]$ if and only if E/K is abelian.*

Proof. This follows from the fact that the index of NL^* in K^* is equal to $[L:K]$.

2.7 *Statement of the Existence Theorem*

It gives a characterization of the norm subgroups of K^*:

THEOREM 3. *A subgroup M of K^* is a norm subgroup if and only if it satisfies the following two conditions:*

(1) *Its index $(K^* : M)$ is finite.*

(2) *M is open in K^*.*

(Note that, if (1) is satisfied, (2) is equivalent to " M is closed".)

Proof of necessity. If $M = NL^*$, where L is a finite abelian extension of K, we know that K^*/M is isomorphic to $G_{L/K}$; hence $(K^* : M)$ is finite. Moreover, one checks immediately that $N : L^* \to K^*$ is continuous and *proper* (the inverse image of a compact set is compact); hence $M = NL^*$ is closed, cf. Bourbaki, "Top. Gén.", Chap. I, § 10. As remarked above, this shows that M is open. [This last property of the norm subgroups may also be expressed by saying that the reciprocity map

$$\theta_K : K^* \to G_K^{ab}$$

is *continuous*.]

Proof of sufficiency. See § 3.8, where we shall deduce it from Lubin-Tate's theory. The usual proof, reproduced for instance in "Corps Locaux", uses Kummer and Artin-Schreier equations.

We give now some equivalent formulations.

Consider the reciprocity map $\theta_K : K^* \to G_K^{ab}$. By Prop. 2, the composition

$$K^* \xrightarrow{\theta_K} G_K^{ab} \to G(K_{nr}/K) = \hat{\mathbf{Z}}$$

is just the valuation map $v : K^* \to Z$. Hence we have a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & U_K \arrow[r] \arrow[d, "\theta"] & K^* \arrow[r] \arrow[d, "\theta"] & \mathbf{Z} \arrow[r] \arrow[d, "\mathrm{id.}"] & 0 \\
0 \arrow[r] & I_K \arrow[r] & G_K^{ab} \arrow[r] & \hat{\mathbf{Z}} \arrow[r] & 0,
\end{tikzcd}$$

where $I_K = G(K^{ab}/K_{nr})$ is the *inertia subgroup* of G_K^{ab}, and $G(K_{nr}/K)$ is identified with $\hat{\mathbf{Z}}$.

The map $\theta : U_K \to I_K$ is continuous, and its image is dense (cf. Cor. to Prop. 2); since U_K is compact, it follows that it is *surjective*.

We can now state two equivalent formulations of the existence theorem.

THEOREM 3a. *The map $\theta : U_K \to I_K$ is an isomorphism.*

THEOREM 3b. *The topology induced on U_K by the norm subgroups is the natural topology of U_K.*

The group I_K is just $\varprojlim . U_K/(M \cap U_K)$, where M runs through all norm subgroups of K^*; the equivalence of Theorem 3a and Theorem 3b follows from this and a compacity argument. The fact that Theorem 3 $\Rightarrow$ Theorem 3b is clear; the converse is easy, using Prop. 2.

COROLLARY. *The exact sequence $0 \to U_K \to K^* \to \mathbf{Z} \to 0$ gives by completion the exact sequence:*

$$0 \to U_K \to \tilde{K} \to \hat{\mathbf{Z}} \to 0.$$

Loosely speaking, this means that $\tilde{K}$ is obtained from K^* by "replacing $\mathbf{Z}$ by $\hat{\mathbf{Z}}$".

2.8 *Some Characterizations of* $(\alpha, L/K)$

Let L be an abelian extension of K containing K_{nr}, the maximal unramified extension. We want to give characterizations of the reciprocity map $\theta : K^* \to G_{L/K}$.

Since $K_{nr} \subset L$, we have an exact sequence $0 \to H \to G_{L/K} \to \hat{\mathbf{Z}} \to 0$ where $H = G(L/K_{nr})$ and $\hat{\mathbf{Z}}$ is identified with $G(K_{nr}/K)$. Choose a local uniformizer π in K and write $\sigma_\pi = \theta(\pi) = (\pi, L/K) \in G_{L/K}$. We know that σ_π maps onto the Frobenius element $F \in G_{K_{nr}/K}$. Moreover, we can write $G_{L/K}$ as a direct product of subgroups $G_{L/K} = H . I_\pi$ where I_π is generated by σ_π. Corresponding to this we have $L = K_{nr} \otimes K_\pi$, where K_π is the fixed field of $\sigma_\pi = \theta(\pi)$. In terms of a diagram, the interrelationship between the fields is expressed by

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
K_{nr} \arrow[dr, dash] & & K_\pi \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

where K_{nr} and K_π are linearly disjoint.

PROPOSITION 5. *Let $f : K^* \to G$ be a homomorphism and assume that:*

(1) *the composition $K^* \xrightarrow{f} G \to G(K_{nr}/K)$, where $G \to G(K_{nr}/K)$ is the natural map, is the valuation map $v : K^* \to \mathbf{Z}$;*

(2) *for any uniformizing element $\pi \in K$, $f(\pi)$ is the identity on the corresponding extension K_π.*

Then f is equal to the reciprocity map θ.

Proof. Note that condition (1) can be restated as: for $\alpha \in K^*$, $f(\alpha)$ induces on K_{nr} the power of the Frobenius element, $F^{v(\alpha)}$.

We know that $f(\pi)$ is F on K_{nr} and that $\theta(\pi)$ is F on K_{nr}. On the other hand, $f(\pi)$ is 1 on K_π and $\theta(\pi)$ is 1 on K_π. Hence $f(\pi) = \theta(\pi)$ on L.

Now K^* is generated by its uniformizing elements πu (write $\pi^n u$ as $(\pi u) . \pi^{n-1}$). Hence $f = \theta$.

PROPOSITION 6. *Let $f : K^* \to G$ be a homomorphism and assume that (1) of Proposition $\underset{5}{\textcircled{3}}$ holds, whilst (2) is replaced by:*

(2′) *if $\alpha \in K^*$, if K'/K is a finite sub-extension of L and if α is a norm from K'^*, then $f(\alpha)$ is trivial on K'.*

Then f is equal to the reciprocity map θ.

Proof. It suffices to prove that (2′) implies (2). That is, we have to prove that if π is a uniformizing element, then $f(\pi)$ is trivial on K_π. Let K'/K be a finite sub-extension of K_π. We want to prove that $\pi \in NK'^*$. But $\theta(\pi)$ is trivial on K_π and so on K'. This implies $\pi \in NK'^*$.

2.9 *The Archimedean Case*

For global class-field theory it is necessary to extend these results to the (trivial) cases in which K is either R or C. Let $G = G(\mathrm{C}/\mathrm{R})$. In the case $K = \mathbf{C}$, the Brauer group is trivial, $\mathrm{Br}(\mathrm{C}) = 0$. On the other hand, $\mathrm{Br}(\mathbf{R}) = H^2(G, \mathbf{C}^*) = \mathbf{R}^*/\mathbf{R}^*_+$ and so $\mathrm{Br}(\mathbf{R})$ is of order 2.

The invariant $\mathrm{inv}_{\mathbf{R}} : \mathrm{Br}(\mathbf{R}) \to \mathbf{Q}/\mathbf{Z}$ has image $\{0, 1/2\}$ in $\mathbf{Q}/\mathbf{Z}$ and $\mathrm{inv}_{\mathbf{C}} : \mathrm{Br}(\mathbf{C}) \to \mathbf{Q}/\mathbf{Z}$ has image $\{0\}$. The group $H^2(G, \mathbf{C}^*) = H^2(\mathbf{C}/\mathbf{R})$ is cyclic of order 2 and is generated by $u \in \mathrm{Br}(\mathbf{R})$ such that $\mathrm{inv}_{\mathbf{R}}(u) = 1/2$.

Under the reciprocity map (or rather its inverse) we have an isomorphism $G = H^{-2}(G, \mathbf{Z}) \to H^0(G, \mathbf{C}^*) = \mathbf{R}^*/\mathbf{R}^*_+$.

3. Formal Multiplication in Local Fields

The results given in this chapter are due to Lubin-Tate, *Annals of Mathematics*, **81** (1965), 380–387.

For our purposes, the main consequences will be: (1) the construction of a cofinal system of abelian extensions of a given local field K; (2) a formula giving $(\alpha, L/K)$ explicitly in such extensions; (3) the Existence Theorem of § 2.7.

In order to illustrate the ideas involved, we begin with the case $K = \mathbf{Q}_p$. The results to be proved were already known in this case (but were not easily obtained) and they will be shown to be trivial consequences of Lubin-Tate theory.

3.1 *The Case* $K = \mathbf{Q}_p$

THEOREM 1. *Let $\mathbf{Q}_p^{cycl}$ be the field generated over $\mathbf{Q}_p$ by all roots of unity. Then $\mathbf{Q}_p^{cycl}$ is the maximal abelian extension of $\mathbf{Q}_p$.*

In order to determine $(\alpha, L/K)$ it is convenient to split $\mathbf{Q}_p^{cycl}$ into parts. Define $\mathbf{Q}_{nr}$ to be the field generated over $\mathbf{Q}_p$ by roots of unity of order prime to p (so $\mathbf{Q}_{nr}$ is the maximal unramified extension of $\mathbf{Q}_p$) and define $\mathbf{Q}_{p^\infty}$ to be the field generated over $\mathbf{Q}_p$ by p^vth roots of unity, $v = 1, 2, \ldots$ (so $\mathbf{Q}_{p^\infty}$ is totally ramified). Then $\mathbf{Q}_{nr}$ and $\mathbf{Q}_{p^\infty}$ are linearly disjoint and

$$\mathbf{Q}_p^{cycl} = \mathbf{Q}_{nr} . \mathbf{Q}_{p^\infty} = \mathbf{Q}_{nr} \otimes \mathbf{Q}_{p^\infty}.$$

We have a diagram:

$$\begin{tikzcd}
 & \mathbf{Q}_p^{cycl} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbf{Q}_{nr} \arrow[dr, dash] & & \mathbf{Q}_{p^\infty} \arrow[dl, dash] \\
 & \mathbf{Q}_p &
\end{tikzcd}$$

Now $G(\mathbf{Q}_{nr}/\mathbf{Q}_p) = \hat{\mathbf{Z}}$ and if $\sigma \in G(\mathbf{Q}_{p^\infty}/\mathbf{Q}_p)$ then σ is known by its action on the roots of unity. Let E be the group of p^vth roots of unity, $v = 1, 2, \ldots$. As an abelian group, E is isomorphic to $\varinjlim \mathbf{Z}/p^v\mathbf{Z} = \mathbf{Q}_p/\mathbf{Z}_p$. We shall view E as a $\mathbf{Z}_p$-module. There is a canonical map $\mathbf{Z}_p \to \mathrm{End}\,(E)$, defined in an obvious way and this map is an isomorphism. The action of the Galois group on E defines a homomorphism $G(\mathbf{Q}_{p^\infty}/\mathbf{Q}_p) \to \mathrm{Aut}\,(E) = U_p$ and it is known that this is an isomorphism. (See Chapter III, and "Corps Locaux", Chap. IX, § 4, and Chap. XIV, § 7.) If $u \in U_p$, we shall denote by $[u]$ the corresponding automorphism of $\mathbf{Q}_{p^\infty}/\mathbf{Q}_p$.

THEOREM 2. *If $\alpha = p^n.u$ where $u \in U_p$, then $(\alpha, \mathbf{Q}_p^{cycl}/\mathbf{Q}_p) = \sigma_\alpha$ is described by:*

(1) *on $\mathbf{Q}_{nr}$, σ_α induces the nth power of the Frobenius automorphism;*
(2) *on $\mathbf{Q}_{p^\infty}$, σ_α induces the automorphism $[u^{-1}]$.*

Of these (1) is trivial and has already been proved in § 2.5, Prop. 2. The assertion (2) can be proved by (a) global methods, or (b) hard local methods (Dwork), or (c) Lubin-Tate theory (see § 3.4, Theorem 3).

Remark. Assertion (2) of Theorem 2 is equivalent to the following: if w is a primitive p^vth root of unity and if $u \in U_p$ then

$$\sigma_u(w) = w^{u^{-1}} = 1 + \sum_{n=1}^{\infty} \binom{u^{-1}}{n} x^n,$$

where $w = 1+x$.

3.2 *Formal Groups*

The main game will be played with something which replaces the multiplicative group law $F(X, Y) = X+Y+XY$ and something instead of the binomial expansion. The group law will be a formal power series in two variables and we begin by studying such group laws.

DEFINITION. *Let A be a commutative ring with 1 and let $F \in A[[X, Y]]$. We say that F is a commutative formal group law if:*

(a) *$F(X, F(Y, Z)) = F(F(X, Y), Z)$;*
(b) *$F(0, Y) = Y$ and $F(X, 0) = X$;*
(c) *there is a unique $G(X)$ such that $F(X, G(X)) = 0$;*
(d) *$F(X, Y) = F(Y, X)$;*
(e) *$F(X, Y) \equiv X+Y$ (mod deg 2).*

(In fact one can show that (c) and (e) are consequences of (a), (b) and (d). Here, two formal power series are said to be congruent (mod deg n) if and only if they coincide in terms of degree strictly less than n.

Take $A = O_K$. Let $F(X, Y)$ be a commutative formal group law defined over O_K and let $\mathfrak{m}_K$ be the maximal ideal of O_K. If $x, y \in \mathfrak{m}_K$ then $F(x, y)$ converges and its sum $x{*}y$ belongs to O_K. Under this composition law, $\mathfrak{m}_K$ is a *group* which we denote by $F(\mathfrak{m}_K)$.

The same argument applies to an extension L/K and the maximal ideal $\mathfrak{m}_L$ in O_L. We then obtain a group $F(\mathfrak{m}_L)$ defined for any algebraic extension of K by passage to the inductive limit from the finite case.

If $F(X, Y) = X+Y+XY$ then we recover the multiplicative group law of $1+\mathfrak{m}_K$.

The elements of finite order of $F(\mathfrak{m}_{K_s})$ form a torsion group and $G(K_s/K)$ operates on this group. The structure of this Galois module presents an interesting problem which up to now has been solved only in special cases.

3.3 *Lubin-Tate Formal Group Laws*

Let K be a local field, $q = \mathrm{Card}\,(k)$ and choose a uniformizing element $\pi \in O_K$. Let $\mathfrak{F}_\pi$ be the set of formal power series f with:

(1) $f(X) \equiv \pi X$ (mod. deg. 2);
(2) $f(X) \equiv X^q$ (mod. π).

(Two power series are said to be congruent (mod. π) if and only if each coefficient of their difference is divisible by π. So the second condition means that if we go to the residue field and denote by $\bar{f}(X)$ the corresponding element of $k[[X]]$ then $\bar{f}(X) = X^q$.)

Examples.

(*a*) $f(X) = \pi X + X^q$;

(*b*) $K = \mathbf{Q}_p$, $\pi = p$, $f(X) = pX + \binom{p}{2}X^2 + \ldots + pX^{p-1} + X^p$

The following four propositions will be proved in § 5 as consequences of Prop. 5.

PROPOSITION 1. *Let $f \in \mathfrak{F}_\pi$. Then there exists a unique formal group law F_f with coefficients in A for which f is an endomorphism.*

(This means $f(F_f(X, Y)) = F_f(f(X), f(Y))$, that is $f \circ F_f = F_f \circ (f \times f)$.)

PROPOSITION 2. *Let $f \in \mathfrak{F}_\pi$ and F_f the corresponding group law of Prop. 1. Then for any $a \in A = O_K$ there exists a unique $[a]_f \in A[[X]]$ such that:*

(1) $[a]_f$ commutes with f;

(2) $[a]_f \equiv aX$ (mod. deg. 2).

Moreover, $[a]_f$ is then an endomorphism of the group law F_f.

From Prop. 2 we obtain a mapping $A \to \mathrm{End}\,(F_f)$ defined by $a \mapsto [a]_f$. For example, consider the case

$$K = \mathbf{Q}_p, \quad f = pX + \binom{p}{2}X^2 + \ldots + X^p;$$

then F is the multiplicative law $X + Y + XY$, and

$$[a]_f = (1+X)^a - 1 = \sum_{i=1}^{\infty}\binom{a}{i}X^i.$$

PROPOSITION 3. *The map $a \mapsto [a]_f$ is an injective homomorphism of the ring A into the ring* End (F_f).

PROPOSITION 4. *Let f and g be members of $\mathfrak{F}_\pi$. Then the corresponding group laws are isomorphic.*

3.4 *Statements*

Let K be a local field and let π be a uniformizing element. Let $f \in \mathfrak{F}_\pi$ and let F_f be the corresponding group law (of Prop. 1). We denote by $M_f = F_f(\mathfrak{m}_{K_s})$ the group of points in the separable closure equipped with the group law deduced from F. Let $a \in A$, $x \in M_f$ and put $ax = [a]_f(x)$. By Prop. 3, this defines a structure of an A-module on M_f. Let E_f be the torsion sub-module of M_f; that is the set of elements of M_f killed by a power of π.

THEOREM 3. *The following statements hold.*

(a) *The torsion sub-module E_f is isomorphic (as an A-module) with K/A.*

(b) *Let $K_\pi = K(E_f)$ be the field generated by E_f over K. Then K_π is an abelian extension of K.*

(c) *Let u be a unit in K^*. Then the element $\sigma_u = (u, K_\pi/K)$ of $G(K_\pi/K)$ acts on E_f via $[u^{-1}]_f$.*

(d) *The operation described in* (c) *defines an isomorphism $U_K \to G(K_\pi/K)$.*

(e) *The norm residue symbol $(\pi, K_\pi/K)$ is* 1.

(f) *The fields K_{nr} and K_π are linearly disjoint and $K^{ab} = K_{nr}.K_\pi$.*

We may express the results of Theorem 3 as follows. We have a diagram:

$$\begin{tikzcd}
 & K^{ab} \arrow[dl, dash] \arrow[dr, dash] & \\
K_{nr} \arrow[dr, dash] & & K_\pi \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Here $G(K_{nr}/K) = \hat{\mathbf{Z}}$ and $G(K_\pi/K) = U_K$. Moreover every $\alpha \in K^*$ can be written in the form $\alpha = \pi^n.u$ and σ_π gives σ (the Frobenius) on K_{nr}/K whilst σ_u gives $[u^{-1}]$ on K_π/K.

Example. Take $K = \mathbf{Q}_p$, $\pi = p$ and $f = pX + \binom{p}{2}X^2 + \ldots + X^p$. The formal group law is the multiplicative group law; E_f is the set of p^vth roots of unity; K_π is the field denoted by $\mathbf{Q}_{p^\infty}$ in § 3.1—and we recover Theorems 1 and 2.

3.5 *Construction of F_f, $[a]_f$*

In this section we shall construct the formal group law F_f and the map $a \mapsto [a]_f$.

PROPOSITION 5. *Let $f, g \in \mathfrak{F}_\pi$, let n be an integer and let $\phi_1(X_1, \ldots, X_n)$ be a linear form in $X_1, \ldots, X_n$ with coefficients in A. Then there exists a unique $\phi \in A[[X_1, \ldots, X_n]]$ such that:*

(a) $\phi \equiv \phi_1$ (mod deg 2);

(b) $f \circ \phi = \phi \circ (g \times \ldots \times g)$.

Remarks. (1) The property (b) may be written

$$f(\phi(X_1, \ldots, X_n)) = \phi(g(X_1), \ldots, g(X_n)).$$

(2) The completeness of A will not be used in the proof. Moreover, the proof shows that ϕ is the only power series with coefficients in an extension of A, which is torsion free as an A-module, satisfying (a) and (b).

Proof. We shall construct ϕ by successive approximations. More precisely, we construct a sequence $(\phi^{(p)})$ such that $\phi^{(p)} \in A[[X_1, \ldots, X_n]]$, $\phi^{(p)}$ satisfies (a) and (b) (mod deg $p+1$), and $\phi^{(p)}$ is unique (mod deg $p+1$).

We shall then define $\phi = \lim \phi^{(p)}$ and this will be the ϕ whose existence is asserted.

We take $\phi^{(1)} = \phi_1$.

Suppose that the approximation $\phi_1 + \ldots + \phi_p = \phi^{(p)}$ has been constructed. That is, $f \circ \phi^{(p)} \equiv \phi^{(p)} \circ (g \times \ldots \times g)$ (mod deg $p+1$). For convenience of writing, we shall replace $g \times \ldots \times g$ by the single variable g. Now write $\phi^{(p+1)} = \phi^{(p)} + \phi_{p+1}$. Then we may write

$$f \circ \phi^{(p)} \equiv \phi^{(p)} \circ g + E_{p+1} \qquad (\text{mod deg } p+2),$$

where E_{p+1} ("the error") satisfies $E_{p+1} \equiv 0$ (mod deg $p+1$). Consider $\phi^{(p+1)}$; we have

$$f \circ \phi^{(p+1)} = f \circ (\phi^{(p)} + \phi_{p+1}) \equiv f \circ \phi^{(p)} + \pi \phi_{p+1} \qquad (\text{mod deg } p+2)$$

(the derivative of f at the origin is π) and

$$\phi^{(p)} \circ g + \phi_{p+1} \circ g \equiv \phi^{(p)} \circ g + \pi^{p+1} \phi_{p+1} \qquad (\text{mod deg } p+2).$$

Thus

$$f \circ \phi^{(p+1)} - \phi^{(p+1)} \circ g \equiv E_{p+1} + (\pi - \pi^{p+1}) \phi_{p+1} \qquad (\text{mod deg } p+2).$$

These equations show that we must take

$$\phi_{p+1} = -E_{p+1}/\pi(1-\pi^p).$$

The unicity is now clear and it remains to show that ϕ_{p+1} has coefficients in A. That is, $E_{p+1} \equiv 0 \,(\text{mod}\, \pi)$. Now for $\phi \in \mathbf{F}_q[[X]]$, we have $\phi(X^q) = (\phi(X))^q$ and together with $f(X) \equiv X^q \,(\text{mod}\, \pi)$ this gives

$$f \circ \phi^{(p)} - \phi^{(p)} \circ f \equiv (\phi^{(p)}(X))^q - \phi^{(p)}(X^q) \equiv 0 \qquad (\text{mod } \pi).$$

So, given $\phi^{(p)}$ we can construct a unique $\phi^{(p+1)}$ and the proof is completed by induction and passage to the limit.

Proof of Proposition 1. For each $f \in \mathfrak{F}_\pi$, let $F_f(X, Y)$ be the unique solution of $F_f(X, Y) \equiv X + Y$ (mod deg 2) and $f \circ F_f = F_f \circ (f \times f)$ whose existence is assured by Prop. 5. That F_f is a formal group law now requires the verification of the rules (a) to (e) above. But this is an exercise in the application of Prop. 5: in each case we check that the left-and the right-hand sides are solutions to a problem of the type discussed there and we use the unicity statement of Prop. 5. For example, to prove associativity note that both $F_f(F_f(X, Y), Z)$ and $F_f(X, F_f(Y, Z))$ are solutions of

$$H(X, Y, Z) \equiv X + Y + Z \qquad (\text{mod deg } 2)$$

and

$$H(f(X), f(Y), f(Z)) = f(H(X, Y, Z)).$$

Proof of Proposition 2. For each $a \in A$ and $f, g \in \mathfrak{F}_\pi$ let $[a]_{f,g}(T)$ be the unique solution of

$$[a]_{f,g}(T) \equiv aT \qquad (\text{mod deg } 2)$$

and

$$f([a]_{f,g}(T)) = [a]_{f,g}(g(T)),$$

(that is $f \circ [a]_{f,g} = [a]_{f,g} \circ g$). Write $[a]_f = [a]_{f,f}$.

Now we have

$$F_f([a]_{f,g}(X), [a]_{f,g}(Y)) = [a]_{f,g}(F_g(X, Y)).$$

For each side is congruent to $aX + aY$ (mod deg 2) and if we replace X by $g(X)$ and Y by $g(Y)$ in either side, then the result is the same as if we substitute the sides in question in f. Thus $[a]_{f,g}$ is a formal homomorphism of F_g into F_f. If we take $g = f$, this shows that the $[a]_f$'s are endomorphisms of F_f.

Proof of Proposition 3. In the same way as outlined above, one proves that

$$[a+b]_{f,g} = F_f \circ ([a]_{f,g} \times [a]_{f,g})$$

and

$$[ab]_{f,h} = [a]_{f,g} \circ [b]_{g,h}.$$

It follows from this that the composition of two homomorphisms of the type just established is reflected in the product of corresponding elements of A. Taking $f = g$, we see that the map $a \mapsto [a]_f$ is a ring homomorphism of A into End (E_f). It is injective because the term of degree 1 of $[a]_f$ is aX.

Proof of Proposition 4. If a is a unit in A, then $[a]_{f,g}$ is invertible (cf. the proof of Prop. 2) and so $F_g \cong F_f$ by means of the isomorphism $[a]_{f,g}$.

Note that $[\pi]_f = f$ and $[1]_f$ is the identity (proved as before).

This completes the proofs of the propositions 1, 2, 3, 4.

3.6 *First Properties of the Extension K_π of K*

From now on, we confine our attention to subfields of a fixed separable closure K_s of K. Given $f \in \mathfrak{F}_\pi$, let F_f be the corresponding formal group law and let E_f be the torsion submodule of the A-module $F_f(\mathfrak{m}_{K_s})$. Let E_f^n be the kernel of $[\pi^n]_f$; so that $E_f = \cup E_f^n$. Let $K_\pi^n = K(E_f^n)$ and $K_\pi = \cup K_\pi^n$. If $G_{\pi,n}$ denotes the Galois group of $K(E_f^n)$ over K, then $G(K_\pi/K) = \varprojlim G_{\pi,n}$.

PROPOSITION 6. (a) *The A-module E_f is isomorphic to K/A;*

(b) *the natural homomorphism $G(K_\pi/K) \to \text{Aut}\,(E_f)$ is an isomorphism.*

Proof. We are free to choose f as we please, since, by Prop. 4, different choices give isomorphic group laws. We take $f = \pi X + X^q$. Then $\alpha \in E_f^n$ if and only if $f^{(n)}(\alpha) = 0$, where $f^{(n)}$ denotes the composition $f \circ \ldots \circ f$ n times; that is $f^{(n)} = [\pi^n]_f$.

If $\alpha \in \mathfrak{m}_{K_s}$ then the equation $\pi X + X^q = \alpha$ is separable and so solvable in K_s, its solution belonging indeed to $\mathfrak{m}_{K_s}$. This shows that M_f is divisible.

Hence E_f is divisible also. This already implies that E_f is a direct sum of modules isomorphic to K/A.

Let us consider the submodule E_f^1 of E_f consisting (see above) of those $\alpha \in M_f$ such that $[\pi]_f \alpha = 0$. The submodule E_f^1 is isomorphic with A/m_K since it is an A-module with q elements. This is enough to show that E_f is isomorphic to K/A.

An automorphism $\sigma \in G(K_\pi/K)$ induces an automorphism of the A-module E_f. But since $E_f \cong K/A$ and $\mathrm{End}_A\,(K/A) = A$ this gives a map $G(K_\pi/K) \to \mathrm{Aut}\,(E_f) = U_K$. This map is injective by the definition of K_π and it remains to be proved that it is surjective.

Take $n \geqslant 1$ and define E_f^n and K_π^n as above. We have an injection $G(K_\pi^n/K) \to U_K/U_K^n$, where $U_K^n = 1+\pi^n A$. Let $\alpha \in E_f^n$ be a primitive element, that is an element of E_f^n such that $[\pi^n]_f \alpha = 0$, but $[\pi^{n-1}]_f \alpha \neq 0$. Finally we define ϕ as follows:

$$\phi = f^{(n)}/f^{(n-1)} = f(f^{(n-1)})/f^{(n-1)}.$$

Now $f = X^q + \pi X$; so $f/X = X^{q-1}+\pi$. Hence

$$\frac{f(f^{(n-1)})}{f^{(n-1)}} = (f^{(n-1)}(X))^{q-1}+\pi,$$

which is of degree $q^n - q^{n-1}$ and which is irreducible, since it is an Eisenstein polynomial. All primitive elements α are roots of ϕ. Thus the order of $G(K_\pi^n/K)$ is at least $(q-1)q^{n-1}$. On the other hand, this is actually the order of the group U_K/U_K^n. Hence $G(K_\pi^n/K) = U_K/U_K^n$. It follows that

$$G(K_\pi/K) = \varprojlim G(K_\pi^n/K) = \varprojlim U_K/U_K^n = U_K,$$

and this completes the proof of Prop. 6.

The same proof also yields:

COROLLARY. *The element π is a norm from $K(\alpha) = K_\pi^n$.*

Proof. The polynomial ϕ constructed above is monic and ends with π. Hence $N(-\alpha) = \pi$.

3.7 *The Reciprocity Map*

We shall study the compositum $L = K_{nr}K_\pi$ of K_{nr} and K_π, and the symbol $(\alpha, L/K)$, $\alpha \in K^*$. We need to compare two uniformizing elements π and $\omega = \pi u$, $u \in U_K$.

Let $\hat{K}_{nr}$ be the completion of K_{nr} (remember: K_{nr} is an increasing union of complete fields but is not itself complete) and denote by $\hat{A}_{nr}$ the ring of integers of $\hat{K}_{nr}$. By definition $\hat{K}_{nr}$ is complete; it has an algebraically closed residue field and π is a uniformizing parameter in $\hat{K}_{nr}$. We take $f \in \mathfrak{F}_\pi$ and $g \in \mathfrak{F}_\omega$.

LEMMA 1. *Let $\sigma \in G(K_{nr}/K)$ be the Frobenius automorphism and extend it to $\hat{K}_{nr}$ by continuity. Then there exists a power series $\phi \in \hat{A}_{nr}[[X]]$ with $\phi(X) \equiv \varepsilon X$ (mod deg 2) and ε a unit, such that*

(a) ${}^\sigma\phi = \phi \circ [u]_f$;
(b) $\phi \circ F_f = F_g \circ (\phi \times \phi)$;
(c) $\phi \circ [a]_f = [a]_g \circ \phi$ *for all* $a \in A$.

Proof. Since $\sigma - 1$ is surjective on $\hat{A}_{nr}$ and on $\hat{U}_{nr}$ (cf. "Corps Locaux", p. 209), there exists a $\phi \in \hat{A}_{nr}[[X]]$ such that $\phi(X) \equiv \varepsilon X$ (mod deg 2) where ε is a unit and ${}^\sigma\phi = \phi \circ [u]_f$. This is proved by successive approximation and we refer the reader to Lubin-Tate for the details. This particular ϕ does not necessarily give (b) and (c) but can be adjusted to do so; the computations are given in Lubin-Tate (where they appear as (17) and (18) in Lemma 2 on p. 385). Note that together the above conditions express the fact that ϕ is an A-module isomorphism of F_f into F_g.

Computation of the norm reciprocity map in L/K.

Let $L_\pi = K_{nr}.K_\pi$. Since K_{nr} and K_π are linearly disjoint over K, the Galois group $G(L_\pi/K)$ is the product of the Galois groups $G(K_\pi/K)$ and $G(K_{nr}/K)$. For each uniformizing element $\pi \in A$ we define a homomorphism $r_\pi : K^* \to G(L_\pi/K)$ such that:

(a) $r_\pi(\pi)$ is 1 on K_π and is the Frobenius automorphism σ on K_{nr};
(b) for $u \in U_K$, $r_\pi(u)$ is equal to $[u^{-1}]_f$ on K_π and is 1 on K_{nr}.

We want to prove that *the field L_π and the homomorphism r_π are independent of π.* Let $\omega = \pi u$ be a second uniformizing element.

First, $L_\pi = L_\omega$. For by Lemma 1, F_f and F_g are isomorphic over $\hat{K}_{nr}$. Hence, the fields generated by their division points are the same. So $\hat{K}_{nr}.K_\pi = \hat{K}_{nr}.K_\omega$. On taking completions we find that $\widehat{K_{nr}.K_\pi} = \widehat{K_{nr}.K_\omega}$. In order to deduce that $K_{nr}.K_\pi = K_{nr}.K_\omega$ from this, we require the following:

LEMMA 2. *Let E be any algebraic extension (finite or infinite) of a local field and let $\alpha \in \hat{E}$. Then, if α is separable algebraic over E, α belongs to E.*

Proof. Let E_s be the separable closure of E and let E' be the adherence of E in E_s. We can view α as an element of E'. Hence it is enough to show that $E' = E$.

Let $s \in G(E_s/E)$. Since s is continuous and is the identity on E, it is also the identity on E'. Hence $G(E_s/E) = G(E_s/E')$ and by Galois theory we have $E' = E$.

It follows from Lemma 2 that $L_\pi = L_\omega$ and so $L_\pi = L$ is independent of π.

We turn now to the homomorphism $r_\pi : K^* \to G(L/K)$. *We shall show* that $r_\pi(\omega) = r_\omega(\omega)$. This will imply that $r_\pi(\omega)$ is independent of π and so the r_π's coincide on the local uniformizers. Since these generate K^*, the result will follow.

We look first at $r_\omega(\omega)$. On K_{nr}, $r_\omega(\omega)$ is the Frobenius automorphism σ. On K_ω it is 1. On the other hand, $r_\pi(\omega)$ is σ on K_{nr}; so we must look at $r_\pi(\omega)$ on K_ω.

Now $K_\omega = K(E_g)$, where $g \in \mathfrak{F}_\omega$. Let $\phi \in \hat{A}[[X]]$ be as in Lemma 1; ϕ determines an isomorphism of E_f onto E_g. So if $\lambda \in E_g$, then we can write $\lambda = \phi(\mu)$ with $\mu \in E_f$. We look at $r_\pi(\omega)\lambda$ and we want to show that this is λ. As already remarked, $r_\pi(\omega)(\lambda) = r_\pi(\omega)\phi(\mu)$. Write $s = r_\pi(\omega)$. We want to show that ${}^s\lambda = \lambda$; that is ${}^s\phi(\mu) = \phi(\mu)$. Now, $r_\pi(\omega) = r_\pi(\pi)\,r_\pi(u)$ and the effects of $r_\pi(\pi)$ and $r_\pi(u)$ are described in (a) and (b) above. Since ϕ has coefficients in $\hat{K}_{nr}$, ${}^s\phi = {}^\sigma\phi = \phi \circ [u]_f$ by (a) of Lemma 1. But

$${}^s(\phi(\mu)) = {}^s\phi({}^s\mu) = {}^s\phi([u^{-1}]_f(\mu)).$$

Hence

$${}^s\phi(\mu) = \phi \circ [u]_f \circ [u^{-1}]_f(\mu) = \phi(\mu).$$

So r_π is the identity on K_ω and it follows that r_π is independent of π. Thus $r : K^* \to G(L/K)$ is the reciprocity map θ (§ 2.8, Prop. 5).

All assertions of Theorem 3 have now been proved except the equality $L = K^{ab}$, which we are now going to prove.

3.8 *The Existence Theorem*

Let K^{ab} be the maximal abelian extension of K; it contains K_{nr}. The Existence Theorem is equivalent to the following assertion (§ 2.3, Theorem 3a). If $I_K = G(K^{ab}/K_{nr})$ is the inertia subgroup of $G(K^{ab}/K)$, then *the reciprocity map $\theta : U_K \to I_K$ is an isomorphism.*

Let L be the compositum $K_\pi . K_{nr}$ and let $I'_K = G(L/K_{nr})$ be the inertia subgroup of $G(L/K)$. Consider the maps

$$U_K \xrightarrow{\theta} I_K \xrightarrow{e} I'_K$$

where θ is the reciprocity map and e is the canonical map $I_K \to I'_K$. Both θ and e are surjections.

On the other hand, the composition $e \circ \theta : U_K \to I'_K$ has just been computed. If we identify I'_K with U_K it is $u \mapsto u^{-1}$. Hence the composed map $e \circ \theta$ is an isomorphism. It follows that both θ and e are isomorphisms.

As we have already noted, the first isomorphism is equivalent to the Existence Theorem. The second means that $L = K^{ab}$, since both L and K^{ab} contain K_{nr}.

[*Alternative Proof.* Let us prove directly that every open subgroup M of K^*, which is of finite index, is a norm subgroup corresponding to a finite subextension of L. This will prove both the existence theorem (§ 2.7, Theorem 3) and the fact that $L = K^{ab}$.

Since M is open, there exists $n \geqslant 1$ such that $U_K^n \subset M$; since M is of finite index, there exists $m \geqslant 1$ such that $\pi^m \in M$; hence M contains the subgroup $V_{n,m}$ generated by U_K^n and π^m. Now let K_m be the unramified extension of K of degree m, and consider the subfield $L_{n,m} = K_\pi^n . K_m$ of L. If $u \in U_K$, and $a \in \mathbf{Z}$, we know that $(u\pi^a, L_{n,m}/K)$ is equal to $[u^{-1}]$ on K_π^n and to the a-th power of the Frobenius element on K_m; hence $(u\pi^a, L_{n,m}/K)$ is trivial if and only if $u \in U_K^n$ and $a \equiv 0 \bmod m$, i.e. if and only if $u\pi^a \in V_{n,m}$. This shows that $V_{n,m} = NL_{n,m}$, and, since M contains $V_{n,m}$, M is the norm group of a subextension of $L_{n,m}$. Q.E.D.]

4. Ramification Subgroups and Conductors

4.1 *Ramification Groups*

Let L/K be a galois extension of local fields with Galois group $G(L/K)$. We recall briefly the definition of the upper numbering of the ramification groups. (For details, the reader should consult Chapter I, § 9, or "Corps Locaux", Chap. IV.)

Let the function $i_G : G(L/K) \to \{\mathbf{Z} \cup \infty\}$ be defined as follows. For $s \in G(L/K)$, let x be a generator of O_L as an O_K algebra and put $i_G(s) = v_L(s(x) - x)$. Now define G_u for all positive real numbers u by: $s \in G_u$ if and only if $i_G(s) \geqslant u+1$. The groups G_u are called the ramification groups of $G(L/K)$ (or of L/K). In order to deal with the quotient groups, it is necessary to introduce a second enumeration of the ramification groups called the "upper numbering". This new numbering is given by $G^v = G_u$, where $v = \phi(u)$ and where the function ϕ is characterized by the properties:

(a) $\phi(0) = 0$;
(b) ϕ is continuous;
(c) ϕ is piecewise linear;
(d) $\phi'(u) = 1/(G_0 : G_u)$ when u is not an integer.

The G^v's so defined are compatible with passage to the quotient: $(G/H)^v$ is the image of G^v in G/H ("Herbrand's theorem"). This allows one to define the G^v's even for infinite extensions.

On the other hand, we have a filtration on U_K defined by $U_K^n = 1 + \mathfrak{m}_K^n$. We extend this filtration to real exponents by $U_K^v = U_K^n$ if $n-1 < v \leqslant n$. (It should be noted that v in this context is a real number and is not to be confused with the valuation map!)

THEOREM 1. *Let L/K be an abelian extension with Galois group G. Then the local reciprocity map $\theta : K^* \to G$ maps U_K^v onto G^v for all $v \geqslant 0$.*

Proof. (1) *Verification for the extensions K_π^n of* § 3.6.

Let $u \in U_K^i$ with $i < n$ and $u \notin U_K^{i+1}$. Let $s = \theta(u) \in G(K_\pi^n/K)$. We have

$i(s) = v_{K_\pi^n}(s\lambda - \lambda)$, where λ is a uniformizing element. We choose a primitive root α for λ; that is, an α satisfying $[\pi^n]_f\alpha = 0$ but $[\pi^{n-1}]_f\alpha \neq 0$. Observe that $s_u(\alpha) = [u^{-1}]_f\alpha$ and $u^{-1} = 1+\pi^i v$ (see § $\underset{3.4}{\boxed{3.3}}$, Theorem 3), where v is a unit. These imply that

$$s_u\alpha = [1+\pi^i v]_f\alpha = F_f(\alpha, [\pi^i v]_f\alpha).$$

If we write $\beta = [\pi^i v]_f\alpha$, then β is a primitive $(n-i)$th root (that is, $[\pi^{n-i}]_f\beta = 0$, $[\pi^{n-1-i}]_f\beta \neq 0$), and we have

$$F_f(\alpha, [\pi^i v]_f\alpha) = \alpha+\beta+\sum_{i>1,\, j>1}\gamma_{ij}\alpha^i\beta^j$$

for some $\gamma_{ij} \in O_K$. Accordingly,

$$s_u(\alpha)-\alpha = \beta+\sum\gamma_{ij}\alpha^i\beta^{j}_{\boxed{j}}$$

and

$$v_{K_\pi^n}(s_u(\alpha)-\alpha) = v_{K_\pi^n}(\beta).$$

Now α is a uniformizing element in K_π^n whilst β is a uniformizing element

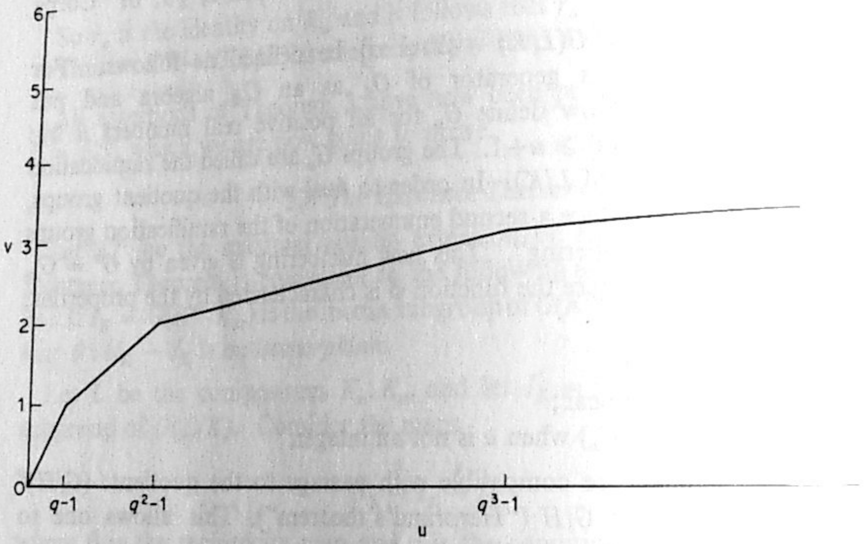

Figure 1.

in K_π^{n-i} and K_π^n/K_π^{n-i} is totally ramified. Its degree is q^i. So we have determined the i function of $\theta(u)$; namely, if $u \in U^i$ but $u \notin U^{i+1}$, then $i(\theta(u)) = q^i$. This says that if $q^{i-1}-1 < u \leqslant q^i-1$ then the ramification group G_u is $\theta(U_K^i)$.

We turn now to the upper numbering of the G_u's. That is, we define a function $\phi = \phi_{K_\pi^n/K}$, corresponding to the extension K_π^n, which satisfies the conditions (a) to (d) above. Namely,

$$\phi(u) = \phi_{K_\pi^n/K}(u) = \int_0^u \frac{dt}{(G:G_t)}.$$

Then $G^v = G_u$ with $v = \phi(u)$. The graph of $\phi(u)$ is shown in Figure 1.

If $q^{i-1}-1 < u \leqslant q^i-1$, then $\phi'(u) = 1/(q^i-q^{i-1})$ and $(U_K : U_K^i) = q^i - q^{i-1}$. So if $i-1 < v \leqslant i$, then $G^v = \theta(U_K^v)$ for $v \leqslant n$.

The general case

(2) *Verification in the general case.*

Having proved Theorem 1 for K_π^n it follows for $K_\pi = \cup K_\pi^n$ by taking projective limits. Hence also for $K_\pi . K_{nr}$, since both extensions have the same intertia subgroup. Since $K_\pi . K_{nr}$ is the maximal abelian extension, the result is true in general.

This concludes the proof of Theorem 1.

COROLLARY. *The jumps in the filtration $\{G^v\}$ of G occur only for integral values of v.*

Proof. This follows from Theorem 1, since it is trivial for filtrations of U_K and Theorem 1 transforms one into the other.

[This result is in fact true for any field which is complete with respect to a discrete valuation and which has perfect residue field (theorem of Hasse-Arf), cf. "Corps Locaux", Chap. IV, V.]

4.2 *Abelian Conductors*

Let L/K be a finite extension and let $\theta : K^* \to G(L/K)$ be the corresponding reciprocity map. There is a smallest number n such that $\theta(U_K^n) = 0$. This number n is called the *conductor* of the extension L/K and is denoted by $f(L/K)$.

PROPOSITION 1. *Let c be the largest integer such that the ramification group G_c is not trivial. Then $f(L/K) = \phi_{L/K}(c)+1$.*

Proof. This is a trivial consequence of Theorem 1 and the fact that the upper numbering is obtained by applying ϕ.

Now let L/K be an arbitrary galois extension. Let $\chi : G \to \mathbf{C}^*$ be a one-dimensional character and let L_χ be the subfield of L corresponding to $\operatorname{Ker}(\chi)$. The field L_χ is a cyclic extension of K and $f(L_\chi/K)$ is called *the conductor of* χ and is denoted by $f(\chi)$.

PROPOSITION 2. *Let $\{G_i\}$ be the ramification subgroups of $G = G(L/K)$ and write $g_i = \operatorname{Card}(G_i)$. Then*

$$f(\chi) = \sum_{i=0}^{\infty}\frac{g_i}{g_0}(1-\chi(G_i))$$

where $\chi(G_i) = g_i^{-1}\sum_{s\in G_i}\chi(s)$ is the "mean value" of χ on G_i.

Proof. We have $\chi(G_i) = 1$ if χ is trivial on G_i (that is, equal to 1 everywhere) and $\chi(G_i) = 0$ if χ is non-trivial on G_i. Hence (the reader is referred to "Corps Locaux", Chaps. IV and VI for the details)

$$\sum_{i=0}^{\infty} \frac{g_i}{g_0}(1-\chi(G_i)) = \sum_{i=0}^{c_\chi} \frac{g_i}{g_0} = \phi_{L/K}(c_\chi)+1,$$

where c_χ is the largest number such that the restriction $\chi|G_{c_\chi} \neq 1$. Now $f(\chi) = f(L_\chi/K)$ is equal to $\phi_{L_\chi/K}(c)+1$, where c is defined as in Prop. 1 for the extension L_χ/K. Since $\phi_{L/K}$ is transitive, it suffices to show that $c = \phi_{L/L_\chi}(c_\chi)$ and this is a consequence of Herbrand's theorem (§ 4.1).

4.3 *Artin's Conductors*

Let L/K be a finite galois extension with Galois group $G = G(L/K)$. Let χ be a character of G (that is, an integral combination of irreducible characters). Artin defined the *conductor* of χ as the number

$$f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0}(\chi(1)-\chi(G_i)).$$

If χ is irreducible of degree 1, this $f(\chi)$ coincides with the previous $f(\chi)$. We define *Artin's character* a_G as follows. For $s \in G$, set

$$a_G(s) = -f.i_G(s) \qquad \text{if } s \neq 1$$
$$a_G(1) = f\sum_{s\neq 1} i_G(s).$$

Here f is the residue degree $[l:k]$ (not to be confused with the conductor's) and i_G is the function defined above.

Proposition 3. *Let* $g = \text{Card}(G)$. *Then*

$$f(\chi) = (a_G, \chi) = \frac{1}{g}\sum_{s\in G} \chi(s)a_G(s).$$

Proof. The proof depends on summation on successive differences $G_i - G_{i+1}$ and is left as an exercise. (See "Corps Locaux", Chap. VI, §2.)

Proposition 4. (a) *Let $K \subset L' \subset L$ be a tower of galois extensions, let χ' be a character of $G(L'/K)$ and let χ be the corresponding character of $G(L/K)$. Then $f(\chi) = f(\chi')$.*

(b) *Let $K \subset K' \subset L$ and let ψ be a character of $G(L/K')$ and let ψ^* be the corresponding induced character of $G(L/K)$. Then*

$$f(\psi^*) = \psi(1).v_K(\mathfrak{d}_{K'/K})+f_{K'/K}.f(\psi),$$

where $f_{K'/K}$ is the residue degree of K'/K and $\mathfrak{d}_{K'/K}$ is the discriminant of K'/K.

Proof. The proof depends on properties of the i_G function and on the relation between the different and the discriminant, and can be found in "Corps Locaux", Chap. VI.

Theorem 2 (Artin). *Let χ be the character of a representation of G. Then $f(\chi)$ is a positive integer.*

Proof. Let χ be the character of the rational representation M of G. It follows from representation theory that

$$\chi(1) = \dim M$$

and

$$\chi(G_i) = \dim M^{G_i}.$$

Thus in

$$\sum \frac{g_i}{g_0}(\chi(1)-\chi(G_i)),$$

each term is positive ($\geqslant 0$) and so $f(\chi) \geqslant 0$.

It remains to be proved that $f(\chi)$ is an integer. According to a theorem of Brauer, χ can be written $\chi = \sum m_i\psi_i^*$ where $m_i \in \mathbf{Z}$ and ψ_i^* is induced by a character ψ_i of degree 1 of a subgroup H_i of G.

Hence, since $f(\psi_i^*) = \psi_i(1)v_K(\mathfrak{d}_{K'/K})+f_{K'/K}.f(\psi_i)$, $f(\psi_i^*)$ is an integer provided that $f(\psi_i)$ is. But since ψ_i has degree 1, $f(\psi_i)$ may be interpreted as an abelian conductor and so is obviously an integer. This proves Theorem 2.

4.4 *Global Conductors*

Let L/K be a finite galois extension of *number fields* and let $G = G(L/K)$ be the Galois group. If χ is a character of G, then we define an ideal $\mathfrak{f}(\chi)$ of K, the *conductor of* χ, as follows. Let $\mathfrak{p}$ be a prime ideal in K and choose a prime ideal $\mathfrak{P}$ in L which divides $\mathfrak{p}$. Let $G_\mathfrak{p} = G(L_\mathfrak{P}/K_\mathfrak{p})$ be the corresponding decomposition subgroup. Let $f(\chi, \mathfrak{p})$ be the Artin conductor of the restriction of χ to $G_\mathfrak{p}$ as defined above. We have $f(\chi, \mathfrak{p}) = 0$ when $\mathfrak{p}$ is unramified. The ideal

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\chi,\mathfrak{p})}$$

is called the (global) conductor of χ.

In this notation, Prop. 4 gives:

Proposition 5. *Let K'/K be a sub-extension of L/K. Let ψ be a character of $H = G(L/K')$ and let ψ^* be the induced character of $G(L/K)$. Then*

$$\mathfrak{f}(\psi^*) = \mathfrak{d}_{K'/K}^{\psi(1)}.N_{K'/K}(\mathfrak{f}(\psi)),$$

where $\mathfrak{d}_{K'/K}$ is the discriminant of K'/K.

We apply Prop. 5 to the case $\psi = 1$ and we denote the induced character ψ^* by $s_{G/H}$ (it corresponds to the permutation representation of G/H). Since $\mathfrak{f}(\psi) = (1)$ we obtain:

Corollary. *We have $\mathfrak{f}(s_{G/H}, L/K) = \mathfrak{d}_{K'/K}$.*

In the case $H = 1$ we have $s_{G/H} = r_G$, the character of the regular representation of G, and the corollary reads

$$\mathfrak{d}_{L/K} = \prod_{\chi} \mathfrak{f}(\chi)^{\chi(1)},$$

where χ runs through the set of irreducible characters of G. This is the "Führerdiskriminantenproduktformel" of Artin and Hasse, which was first proved by analytical methods (L functions). In the abelian case it reads:

$$\mathfrak{d}_{L/K} = \prod_{\chi : G \to \mathbf{C}^*} \mathfrak{f}(\chi).$$

In the quadratic case it reduces to the fact that the discriminant is equal to the conductor.

4.5 *Artin's Representation*

We return to the local case.

THEOREM 3. *Let L/K be a finite galois extension of local fields with Galois group G. Let a_G be the Artin character of G defined above* (*cf.* § 4.3). *Then a_G is the character of a complex linear representation of G called "the" Artin representation.*

Proof. The character a_G takes the same values on conjugate elements and so is a class function. It follows that a_G is a combination $\sum_{\chi} m_{\chi} \chi$, with complex coefficients m_{χ}, of the irreducible characters χ. Since

[Ref. prop 2 (iii) in Local Fields]

$$m_{\chi} = (a_G, \chi) = f(\chi),$$

we know (Prop. 3 and Theorem 2) that m_{χ} is a positive integer. Hence the result.

Now let V_{χ} be an irreducible representation corresponding to χ. We can define Artin's representation A_G by:

$$A_G = \sum f(\chi) . V_{\chi},$$

where the summation is over all irreducible characters χ.

Remark. This construction of A_G is rather artificial. Weil has posed the problem of finding a "natural" A_G.

THEOREM 4. *Let l be a prime number not equal to the residue characteristic. Then the Artin representation can be realized over* $\mathbf{Q}_l$.

Proof. See J-P. Serre, *Annals of Mathematics*, **72** (1960), 406–420, or "Introduction à la théorie de Brauer" *Séminaire I.H.E.S.*, 1965/66.

Examples exist where the Artin representation cannot be realized over $\mathbf{Q}$, $\mathbf{R}$ or $\mathbf{Q}_p$, where p is the residue characteristic. This suggests that there is no trivial definition of the Artin representation.

Assume now that L/K is totally ramified. Let $u_G = r_G - 1$; we have

$u_G(s) = -1$ if $s \neq 1$ and $u_G(s) = \text{Card}(G) - 1$ if $s = 1$. Now $a_G = u_G + b_G$ where b_G is a character of some representation.

Note: $a_G = u_G$ if and only if L/K is tamely ramified. So b_G is a measure of how wild the ramification is.

THEOREM 5. *Let l be a prime number not equal to the residue characteristic. Then there exists a finitely generated, projective* $\mathbf{Z}_l[G]$ *module $B_{G,l}$ with character b_G and this module is unique up to isomorphism.*

Proof. This follows from a theorem of Swan, "Topology", 2 (1963), Theorem 5, combined with Theorem 4 above and the remark that $b_G(s) = 0$ when the order of s is divisible by l. [See also the I.H.E.S. seminar quoted above.]

For applications of Theorem 5 to the construction of invariants of finite G-modules, see M. Raynaud, "Sém. Bourbaki", 1964/65, exposé 286. These invariants play an important role in the functional equation of the zeta functions of curves.

Chapter VII

Global Class Field Theory

J. T. Tate

Throughout these lectures, K will be a global field, as has been defined in Chapter II, § 12. We treat the number field case completely, but in the function field case there is one big gap in our proofs, in that the second inequality and the accompanying key lemma for the existence theorem are proved only for extensions of degree prime to the characteristic. (The reader interested in filling the gap can consult the Artin-Tate notes,† pp. 29–38.)

As in Local Class Field theory, there are several aspects: (1) The cohomology theory of Galois extensions of K. (2) The determination of the abelian extensions of K. (3) L-series analysis.

We will discuss the first two, leaving the third to Heilbronn (Chapter VIII), except for a few remarks.

Sections 1–6 constitute a statement and discussion of the reciprocity law and the main theorems on abelian extensions, with no mention of cohomology. We hope that this preliminary discussion will serve both as orientation and bait for the reader. In sections 7–12 we give the main proofs, based on the determination of the Galois cohomology of idèle classes and the Brauer group of K.

This chapter is strictly limited to the central theorems. In the exercises at the end of the book the reader will find a few concrete examples and further results. There are some references to recent literature scattered in the text but we have made no attempt to give a systematic bibliography. A list of symbols used in this chapter is given at the end.

† Harvard, Dept. of Mathematics, 1961.

1. Action of the Galois Group on Primes and Completions

Let L be a finite Galois extension field of K with Galois group $G = G(L/K)$.

1.1. First of all we have a few lines on our notation and language. If $a \in L$ and $\sigma \in G$, then the action of σ on a will be denoted by σa or a^{σ}, according to the situation. If $\tau \in G$ we use the convention $\sigma(\tau a) = (\sigma\tau)a$ and so $(a^{\tau})^{\sigma} = a^{(\sigma\tau)}$.

A *prime* is an equivalence class of valuations, or a normalized valuation, of K; we usually denote a prime by the letter v or w. A prime may be either *archimedean* or *discrete*; if v is discrete we write $\mathfrak{O}_v$ for its valuation ring and $\mathfrak{P}_v$ for the maximal ideal of $\mathfrak{O}_v$. We reserve the symbol $\mathfrak{P}$ for prime ideals.

Let w be a prime of L, then with the definition $|a|_{\sigma w} = |\sigma^{-1}a|_w$ it follows that σw is another prime of L and $\sigma(\tau w) = (\sigma\tau)w$. If $\mathfrak{O}_w$ is the valuation ring of w, then $\sigma\mathfrak{O}_w = \mathfrak{O}_{\sigma w}$. A Cauchy sequence for w, acted on by σ, gives a Cauchy sequence for σw and conversely a Cauchy sequence for σw, acted on by σ^{-1}, gives a Cauchy sequence for w; so σ induces by continuity an isomorphism $\sigma_w : L_w \xrightarrow{\sim} L_{\sigma w}$ of the completions of L with respect to the primes w and σw respectively. If w is over the prime v of K so is σw and this map is a K_v-isomorphism. Clearly, $\sigma_{\tau w} \circ \tau_w = (\sigma\tau)_w$.

The *decomposition group* G_w of w is the subgroup

$$G_w = \{\sigma \in G \mid \sigma w = w\}$$

of G. Note that

$$G_{\tau w} = \{\sigma \in G \mid \sigma\tau w = \tau w\} = \tau G_w \tau^{-1}, \tag{1}$$

thus the decomposition group of w is determined up to conjugacy by the prime v. By what we have said σ is a K_v-automorphism of L_w if $\sigma \in G_w$ and so we have an injection i of G_w into $G(L_w/K_v)$.

1.2. Proposition. (i) *L_w/K_v is Galois and the injection $i : G_w \to G(L_w/K_v)$ is an isomorphism.*

(ii) *If w and w' are two primes of L over the prime v of K, there exists a $\sigma \in G$ such that $\sigma w = w'$.*

Proof. Letting $[X]$ denote the cardinality of a set X, we have

$$[G_w] \leqslant G(L_w/K_v) \leqslant [L_w : K_v],$$

and these inequalities are equalities if and only if (i) is true. Let $r = (G : G_w)$ and let (σ_i), $1 \leqslant i \leqslant r$, be a system of representatives for the cosets $\sigma_i G_w$ of G_w in G. Put $w_i = \sigma_i w$ for $1 \leqslant i \leqslant r$. These are distinct primes of L lying over v; let w_i for $r+1 \leqslant i \leqslant s$ be the remaining such, if any. Then

$$[G] = r[G_w] = \sum_{i=1}^{r} [G_{w_i}] \leqslant \sum_{i=1}^{r} [L_{w_i} : K_v] \leqslant \sum_{i=1}^{s} [L_{w_i} : K_v] = [L : K] = [G],$$

so we have equality throughout. Hence $r = s$, which implies (ii) and $[G_w] = [L_w : K_v]$, which implies (i). [The fact that the sum of the local degrees is equal to the global degree follows from the bijectivity of the map $L \otimes_K K_v \to \prod_{i=1}^{s} L_{w_i}$ on taking dimensions over K_v; see Chapter II § 10. The surjectivity, which is all we have used, is an easy consequence of the weak approximation theorem.]

Write $\mathfrak{M}_K$ for the set of primes of K. Then, since $\mathfrak{M}_L \to \mathfrak{M}_K$ is surjective (every prime v of K can be extended to a prime w of L), Proposition 1.2 amounts to saying that $\mathfrak{M}_K \simeq \mathfrak{M}_L/G$, i.e. the primes of K are in 1–1 correspondence with the orbits under G of the primes of L, and for each prime w of L, its stabilizer G_w is isomorphic to the Galois group of the corresponding local field extension L_w/K_v.

2. Frobenius Automorphisms

2.1. Suppose that w is a discrete, unramified prime of L over the prime v of K. (This is true of "almost all" primes v, w, i.e. for all but finitely many.) Then

$$(1) \qquad G \supset G_w \simeq G(L_w/K_v) \simeq G(k(w)/k(v)),$$

where $k(v)$ (resp. $k(w)$) denotes the residue class field of K (resp. L) with respect to v (resp. w). Since these residue class fields are finite the Galois group $G(k(w)/k(v))$ is cyclic with a canonical generator,

$$F : x \mapsto x^{Nv},$$

where $Nv = [k(v)]$ is the "absolute norm". Hence we see from (1) that there is a unique element $\sigma_w \in G_w$ which is characterized by the.property

$$\sigma_w \in G_w \quad \text{and} \quad a^{\sigma_w} \equiv a^{Nv} \pmod{\mathfrak{P}_w}$$

for all $a \in \mathfrak{O}_w$. This automorphism σ_w is called the *Frobenius automorphism* associated with the prime w. An immediate consequence of this definition is

2.2. Proposition

$\tau \sigma_w \tau^{-1}$ (see eqn. (2))

$$\sigma_{\tau w} = \tau^{-1} \sigma_w \tau.$$

Thus the Frobenius automorphism is determined by v *up to conjugacy* and we define

$F_{L/K}(v) =$ (conjugacy class of σ_w, w over v) $=$ (the set of σ_w's for w over v).

If S is a finite set of primes of K containing the archimedean primes and the primes ramified in the extension L/K, then $F_{L/K}$ is a map of $\mathfrak{M}_K - S$ into the conjugacy classes of $G(L/K)$.

2.3. Proposition. *Let $\sigma \in F_{L/K}(v)$ have order f, so that it generates the subgroup $<\sigma> = \{1, \sigma, \ldots, \sigma^{f-1}\}$. Then in L, v splits into $[G : <\sigma>]$ factors, each of degree $f = [k(w) : k(v)]$. In particular, v splits completely if and only if $F_{L/K}(v) = 1$, the identity element of G.*

2.4. *Remarks.* This proposition tells us that knowledge of $F_{L/K}$ gives the decomposition law for unramified primes, and more, since it chooses a definite generator for the decomposition group.

Since $F_{L/K}$ is a function to classes of G, to know $F_{L/K}$ it is enough to know $\chi(F_{L/K}(v))$ for all characters χ of G. Accordingly, Artin was led to define his non-abelian L-series in terms of $\chi(F)$, by means of which one can prove the fundamental *Tchebotarev* (= *Čebotarev*) *Density Theorem: Let $\mathscr{C}$ be a conjugacy class in G; the primes v with $F(v) = \mathscr{C}$ have density $[\mathscr{C}]/[G]$.* In particular, for each conjugacy class $\mathscr{C}$, there exists an infinite number of primes v of K such that $F_{L/K}(v) = \mathscr{C}$.

In the cyclotomic case Tchebotarev's theorem is equivalent to the Dirichlet theorem on primes in arithmetic progressions (see 3.4 below).

From Tchebotarev's theorem it follows almost trivially that a finite Galois extension L of K is uniquely determined (up to isomorphism) by the set Spl (L/K) of primes of K which split completely in L (cf. exercise 6). Unfortunately one knows no way to characterize directly, in terms of the arithmetic of K itself, those sets T of primes of K which are of the form Spl (L/K), except in case L is abelian. The decomposition law for abelian extensions, together with the complete classification of such extensions, is given by the main theorem below (§ 5); but no such theorem is known for non-abelian extensions, i.e. "non-abelian class field theory" does not exist. From the abelian theory one can derive decomposition laws of sorts for some soluble extensions (cf. Exercise 2) but this is not what is sought. Recently Shimura ("A reciprocity law in non-solvable extensions", *Crelle's Journal*, **221** (1966), 209–220) has given an explicit decomposition law for certain non-soluble extensions obtained by adjoining to Q the points of order l on a certain elliptic curve. The idea is to relate the behaviour of primes in those extensions to the zeta-function of the curve, and to identify that zeta-function with a modular function, the coefficient of whose q-expansion can be calculated explicitly. The degree of generality of such examples, and whether they will point the way to a general theory, is unclear; but at any rate they are there to test hypotheses against.

3. Artin's Reciprocity Law

3.1. First of all we give some notation. S will usually denote a *finite* set of primes of K including all the archimedean primes. If we are considering a particular finite extension L/K, then S will also include the primes of K

ramified in L. We will denote by I^S the free abelian group on the elements of $\mathfrak{M}_K - S$ (a subgroup of the group of ideals, see Chapter II § 17).

Assume now that L/K is a finite abelian extension. Then the conjugacy classes of $G = G(L/K)$ are single elements and so $F_{L/K}$ is a map from $\mathfrak{M}_K - S$ into G. By linearity we can extend this to a homomorphism (to be denoted by $F_{L/K}$ also) of I^S into G, putting

$$F_{L/K}\Big(\sum_{v \notin S} n_v v\Big) = \prod_{v \notin S} F_{L/K}(v)^{n_v},$$

where the n_v are integers and $n_v = 0$ except for a finite number of the v.

The first proposition of this section concerns the change in the map $F_{L/K}$ when the fields are changed. Suppose that L'/K' and L/K are abelian field extensions with Galois group G' and G respectively, such that $L' \supset L$ and $K' \supset K$, and let θ be the natural map $G' \to G$ (every automorphism of L'/K' induces one of L/K). Let S denote a finite set of primes of K including the archimedean ones and those primes ramified in L' and let S' be the set of primes of K' above those in S. Then

3.2. Proposition. *The diagram*

$$\begin{tikzcd} I^{S'} \arrow[r, "F_{L'/K'}"] \arrow[d, "N_{K'/K}"'] & G' \arrow[d, "\theta"] \\ I^S \arrow[r, "F_{L/K}"] & G \end{tikzcd}$$

commutes, where N denotes "norm".

Proof. By linearity, it is clear that it is enough to check that

$$\theta F_{L'/K'}(v') = F_{L/K}(N_{K'/K} v')$$

for an arbitrary prime v' of K' such that $v' \notin S'$. Let $N_{K'/K} v' = fv$, where v is the prime of K below v'; thus $f = [k(v') : k(v)]$. Let $\sigma' = F_{L'/K'}(v')$ and $\sigma = F_{L/K}(v)$. We must show $\theta(\sigma') = \sigma^f$. Now σ and σ' are determined by their effect on the residue fields. Let w' be a prime of L' above v' and let w be the prime of L below w'. For $x \in k(w) \subset k(w')$ we have

$$x^{\sigma'} = x^{Nv'} = x^{(Nv)^f} = x^{\sigma^f},$$

as required.

If $a \in K^*$ (i.e. a is a non-zero element of K), then we write

$$(a)^S = \sum_{v \notin S} n_v v,$$

where $n_v = v(a)$ for all $v \notin S$; thus $(a)^S$ is an element of I^S.

We can now state the reciprocity law in its crudest form

3.3. Reciprocity Law (Crude form). *If L/K is a finite abelian extension and S is the set of primes of K consisting of the archimedean ones and those ramified in L, then there exists $\varepsilon > 0$ such that if $a \in K^*$ and $|a-1|_v < \varepsilon$ for all $v \in S$, then $F((a)^S) = 1$.*

In words, if $a \in K^*$ is sufficiently near to 1 at all primes in a large enough set S, then $F((a)^S) = \prod_{v \notin S} F(v)^{v(a)} = 1$.

In the number field case the subgroup $(K_v^*)^n$ is open in K^* for all $n > 0$, and we claim that the condition $|a-1|_v < \varepsilon$ can be replaced by $a \in (K_v^*)^n$ for $v \in S$, where $n = [L:K]$. Indeed if the latter is satisfied then, by the weak approximation theorem, there exists $b \in K^*$ such that $|ab^{-n}-1|_v < \varepsilon$ for all $v \in S$, and then

$$F((a)^S) = F((b^n a b^{-n})^S) = F((b)^S)^n F((ab^{-n})^S) = 1.$$

Thus, in the case of number fields, although the set S depends on L, the neighbourhoods of 1 at the primes of S depend only on the degree n of L over K. In particular, for archimedean primes there is no condition needed unless v is real and n is even, in which case the condition $a > 0$ in K_v is sufficient.

Using the approximation theorem in L instead of K, one can replace the condition "a is a local $[L:K]$-th power in S" by "a is a local norm from L to K in S", but for that we shall use the technique of idèles (see 4.4 and 6.4 below). The shift in emphasis from n-th powers to norms was decisive, and is due to Hilbert.

3.4. *Example. The reciprocity law for cyclotomic extensions.* This reciprocity law may be verified directly in the cyclotomic case $k = \mathbf{Q}$, $L = \mathbf{Q}(\zeta)$, where ζ is a primitive m-th root of unity. This particular result will be used later in one of our proofs of the general result (see § 10, below) so we give some details. In the rational case it is conventional to denote primes by p and the associated valuations by v_p. The set S will consist of the archimedean prime and those primes p which divide m (see Chapter III). For $p \notin S$ and w above p, the powers of ζ have *distinct* images in the residue class field $k(w)$, so we have

Proposition.

$$F(v_p)\zeta = \zeta^p \textit{ for all } p \notin S.$$

From this we deduce

Corollary. *If $a \in \mathbf{Z}$, $a > 0$ and $(a, m) = 1$, then $F((a)^S)\zeta = \zeta^a$.*

Consequently, if a is a positive rational number with $|a-1|_p < |m|_p$ for all $p \in S$, then a is a p-adic integer for all p dividing m, and we can write $a = b/c$ with $(b, m) = (c, m) = 1$, and $b \equiv c \pmod{m}$; hence $\zeta^b = \zeta^c$ and so $F((b)^S)\zeta = \zeta^b = \zeta^c = F((c)^S)\zeta$. By linearity this gives $F((a)^S)\zeta = \zeta$ so that $F((a)^S) = 1$.

For another example of an explicit description of $F_{L/K}$, and for the connection between Artin's general reciprocity law and the classical quadratic reciprocity law, see exercise 1.

3.5. *Remark.* The cyclotomic case was easy because one can use the roots of unity to "keep book" on the effect of the F(v)'s for variable v. A similar direct proof works for abelian extensions of complex quadratic fields using division points and modular invariants of elliptic curves with complex multiplication, instead of roots of unity. In the general case no such proof is known (cf. the 12th problem of Hilbert), although Shimura and Taniyama and Weil have made a great contribution, using abelian varieties instead of elliptic curves. (See Shimura-Taniyama, "Complex Multiplication of Abelian Varieties and its Applications to Number Theory", *Publ. Math. Soc. Japan*, No. 6, 1961, and more recently Shimura, "On the Field of Definition for a Field of Automorphic Functions: II", *Annals of Math.* 81 (1965), 124–165.) The proof of the reciprocity law in the general case is very indirect, and can fairly be described as showing that the law holds "because it could not be otherwise".

3.6. *Remark.* In the function field case, as Lang has shown ("Sur les séries L d'une variété algébrique", *Bull. Soc. Math. Fr.* **84** (1956), 385–407), the reciprocity law relates to a geometric theorem about the field $K = k(C)$ of a curve C. Serre has carried out in detail the program initiated by Lang. In his book, "Groupes algébriques et corps de classes", Hermann, Paris (1959), an analogue of the reciprocity law is described as follows. Let $f : C \to G$ be a rational map of a non-singular curve C into a commutative algebraic group G; let S be the finite set of points of C where f is not regular. Then f induces a homomorphism of the group of divisors I^S into G and

THEOREM. *If $\phi \in K$ takes the value 1 to a high order at each point of S, then $f((\phi)) = 1$.*

This theorem is due to Rosenlicht, and independently, but later, Serre. It was Serre and Lang who applied it to class field theory.

3.7. *Definition.* Let K be a global field, S be a finite set of primes of K including all the archimedean ones and G a commutative topological group. A homomorphism $\phi : I^S \to G$ is said to be *admissible* if for each neighbourhood N of the identity element 1 of G there exists $\varepsilon > 0$ such that $\phi((a)^S) \in N$ whenever $a \in K^*$ and $|a-1|_v < \varepsilon$ for all $v \in S$.

If G is a discrete group, we simply take N to be (1). Thus

3.8. *Reformulation of the Reciprocity law: $F_{L/K}$ is admissible.*

In this context the finite group $G = G(L/K)$ is discrete. If G is the circle group, then ϕ is admissible if and only if it is a Grössencharakter (if it maps into a finite subgroup, it is a Dirichlet character). Dirichlet and Hecke

formed their L-series with such characters; Artin was originally forced to produce his reciprocity law in order to show that in the abelian case his L-series defined in terms of characters of the Galois group were really Weber L-series, in other words that $\chi(F(v))$ was admissible for each linear character χ of the abelian Galois group.

4. Chevalley's Interpretation by Idèles

The set of elements of the idèle group J_K (see Chapter II § 16) which have the value 1 at all the v-th components, $v \in S$, is denoted by J_K^S. If $x \in J_K$ it has a non-unit component at only a finite number of v-components; if the (additive) valuation of the v-th component x_v of x is $n_v \in \mathbf{Z}$ we write

$$(x)^S = \sum_{v \notin S} n_v v \in I^S.$$

4.1. PROPOSITION. *Let K and S be as before, G be a complete commutative topological group and ϕ an admissible homomorphism of I^S into G.*

Then there exists a unique homomorphism ψ of $J_K \to G$ such that

(i) *ψ is continuous;*
(ii) $\psi(K^*) = 1$;
(iii) $\psi(x) = \phi((x)^S)$ *for all* $x \in J_K^S$.

Conversely, if ψ is a continuous homomorphism of $J_K \to G$ such that $\psi(K^*) = 1$, then ψ comes from some admissible pair S, ϕ as defined above, provided there exists a neighbourhood of 1 in G in which (1) is the only subgroup.

Remark. It is clear that if such a ψ exists then it induces a continuous homomorphism of the idèle class group $C_K \simeq J_K/K^*$ into G. This induced homomorphism will also be denoted by ψ. Furthermore, if such a ψ exists for a given ϕ and S, then by the unicity statement, it is unchanged if S is enlarged to a bigger set S' and ϕ replaced by its restriction ϕ' to $I^{S'} \subset I^S$. Similarly, two ϕ's on I^S which coincide on $I^{S'}$ for some finite $S' \supset S$ are actually equal on I^S (cf. Exercise 7).

For applications G can be thought of as a discrete group or the circle group.

Proof. Suppose we have an admissible map $\phi : I^S \to G$. If such a ψ were to exist, for any $a \in K^*$ and $x \in J_K$ we would have

$$\psi(x) = \psi(ax) = \psi((ax)_1)\psi((ax)_2),$$

where $(ax)_1$ is the idèle with the same v-component as ax for all $v \in S$ and value 1 elsewhere and $(ax)_2$ is the idèle with the same v-component as ax for all $v \notin S$ and whose v-component is 1 at all $v \in S$ (thus $(ax)_2 \in J_K^S$). By the (weak) approximation theorem (see Chapter II, §6) we can find a sequence

$\{a_n\}$ of elements $a_n \in K^*$, such that $a_n \to x^{-1}$, as $n \to \infty$, at all $v \in S$. Then

$$\psi(x) = \lim_{n\to\infty} \psi((a_n x)_1) . \phi((a_n x)^S) = \lim_{n\to\infty} \phi((a_n x)^S).$$

Hence given ϕ we define a function ψ by

$$(1) \qquad \psi(x) = \lim_{n\to\infty} \phi((a_n x)^S).$$

As $n, m \to \infty$ we have $a_n/a_m \to 1$ at all primes $v \in S$, and consequently

$$\frac{\phi((a_n x)^S)}{\phi((a_m x)^S)} = \phi\left(\left(\frac{a_n}{a_m}\right)^S\right) \to 1$$

in G, because ϕ is admissible. Thus the limit exists, since G is complete, and the limit is independent of the sequence $\{a_n\}$, because it exists for all such sequences. Moreover ψ is continuous. If the components of x are units at primes $v \notin S$, then we have $\psi(x) = \lim \phi((a_n)^S)$; and if in addition the components of x are sufficiently close to 1 at primes $v \in S$, then so will be those of a_n for large n, and by admissibility, $\phi((a_n)^S)$ will be close to 1 in G. The last two conditions (ii) and (iii) are trivially verified by taking $a_n = x^{-1}$ and 1 for all n respectively.

Now suppose we are given a continuous homomorphism $\psi : J_K \to G$ such that $\psi(K^*) = 1$. We will find a set S so that (a) the restriction of ψ to J_K^S comes from a function on I^S and (b) if we call this function ϕ, then ϕ is admissible.

For any finite set S of primes of K let U^S be the set of idèles in J_K for which the v-component is 1 at all $v \in S$ and a unit of K_v for $v \notin S$. By taking S arbitrarily large we can make U^S an arbitrarily small neighbourhood of the identity of J_K. If N is a neighbourhood of (1) we can choose S sufficiently large so that $\psi(U^S) \subseteq N$, since ψ is continuous. Then taking N small enough, we see that $\psi(U^S) = (1)$ for some set S by the "no-small-subgroup" hypothesis. We choose such a set S. Now J_K^S/U^S is canonically isomorphic to I^S and so ψ, when restricted to J_K^S, induces a continuous homomorphism of I^S into G.

It remains to verify that ϕ is admissible; in words, given a neighbourhood N, then $\psi((a)^S) \in N$ whenever $a \in K^*$ is near enough to 1 at all $v \in S$. But in this case $(a)^S$ is near to a in J_K and so by continuity $\psi((a)^S)$ is near to $\psi(a)$, which is 1 since $a \in K^*$.

4.2. Corollary. *The reciprocity law holds for a finite abelian extension L of K if and only if there exists a continuous homomorphism ψ of $J_K \to G(L/K)$ such that*

(i) *ψ is continuous.*

(ii) *$\psi(K^*) = 1$.*

(iii) *$\psi(x) = F_{L/K}((x)^S)$ for all $x \in J_K^S$, where S consists of the archimedean primes of K and those ramified in L.*

Such a map $\psi = \psi_{L/K}$ whose existence we have just postulated is called the *Artin map* associated with the extension L/K. It has been defined as a map $J_K \to G(L/K)$; but since it acts trivially on K^* it may be viewed as a map of the idèle class group $C_K = J_K/K^*$ into $G(L/K)$.

The reciprocity law for finite abelian extensions will be proved later (see § 10). In the meantime certain propositions will be proved and remarks made which depend on its validity. Suppose that L'/K' and L/K are abelian field extensions with Galois groups G' and G respectively and that $L' \supset L$, $K' \supset K$. Let θ be the natural map $G' \to G$. Then in terms of idèles and Artin maps Proposition 3.1 becomes

4.3. Proposition. *If the reciprocity law holds for L/K and L'/K', then*

$$\begin{tikzcd}
J_{K'} \arrow[r, "\psi_{L'/K'}"] \arrow[d, "N_{K'/K}"'] & G' \arrow[d, "\theta"] \\
J_K \arrow[r, "\psi_{L/K}"] & G
\end{tikzcd}$$

is a commutative diagram.

Proof. Let S be a large finite set of primes of K, and S' the set of primes of K' above S. We have then a diagram

$$(2) \qquad \begin{tikzcd}
 & I_{K'}^{S'} \arrow[dr, "F_{L'/K'}"] \arrow[dd] & \\
J_{K'}^{S'} \arrow[ur] \arrow[rr, "\psi_{L'/K'}"'] \arrow[dd, "N_{K'/K}"'] & & G' \arrow[dd, "\theta"] \\
 & I_K^S \arrow[dr, "F_{L/K}"] & \\
J_K^S \arrow[ur] \arrow[rr, "\psi_{L/K}"] & & G
\end{tikzcd}$$

The non-rectangular parallelograms are commutative by the compatibility of ideal and idèle norms, and by Proposition 3.2. The triangles are commutative by (4.2)(iii). Thus the rectangle is commutative, i.e. the restrictions of $\psi_{L/K} \circ N_{K'/K}$ and $\theta \circ \psi_{L'/K'}$ to $J_{K'}^{S'}$ coincide. But those two homomorphisms take the value 1 on principal idèles by 4.2 (ii), so they coincide on $(K')^* J_{K'}^{S'}$, which is a dense subset of $J_{K'}$ by the weak approximation theorem (Chapter II, § 6). Since the two homomorphisms are continuous, they coincide on all of $J_{K'}$ which is what we wished to prove.

For proving Proposition 6.2 below, which is in turn needed for the first of our two proofs of the reciprocity law in §10.4, we need the following

Variant. *Suppose L/K satisfies the reciprocity law, and $K \subset M \subset L$. Then $\psi_{L/K}(N_{M/K} J_M) \subset G(L/M)$.*

Consider diagram (2) with $L' = L$, $K' = M$, but with the upper horizontal arrow $\psi_{L'/K'} = \psi_{L/M}$ removed. It shows that

$$\psi_{L/K}(N_{M/K}J_M^{S'}) \subset G' = G(L/M).$$

Consequently the same is true with $J_M^{S'}$ replaced by $M^*J_M^{S'}$, and since that set is dense in J_M we are done.

4.4. Corollary. *If the reciprocity law holds for L/K, then*

$$\psi_{L/K}(N_{L/K}J_L) = 1.$$

It follows that $\psi_{L/K}(K^*N_{L/K}J_L) = 1$; the next theorem states (among other things) that $K^*N_{L/K}J_L$ is the kernel of $\psi_{L/K}$.

5. Statement of the Main Theorems on Abelian Extensions

5.1. Main Theorem on Abelian Extensions (Takagi-Artin).

(A) *Every abelian extension L/K satisfies the reciprocity law (i.e. there is an Artin map $\psi_{L/K}$).*

(B) *The Artin map $\psi_{L/K}$ is surjective with kernel $K^*N_{L/K}(J_L)$ and hence induces an isomorphism of $C_K/N_{L/K}(C_L)$ on to $G(L/K)$.*

(C) *If $M \supset L \supset K$ are abelian extensions, then the diagram*

$$\begin{tikzcd}
C_K/N_{M/K}C_M \arrow[r, "\psi_{M/K}"] \arrow[d, "j"'] & G(M/K) \arrow[d, "\theta"] \\
C_K/N_{L/K}C_L \arrow[r, "\psi_{L/K}"] & G(L/K)
\end{tikzcd}$$

commutes (where θ is the usual map and j is the natural surjective map which exists because $N_{M/K}C_M \subset N_{L/K}C_L$).

(D) (*Existence Theorem.*) *For every open subgroup N of finite index in C_K there exists a unique abelian extension L/K (in a fixed algebraic closure of K) such that $N_{L/K}C_L = N$.*

The subgroups N of (D) are called *Norm groups*, and the abelian extension L such that $N_{L/K}C_L = N$ is called the *class field* belonging to N. In the number field case every open subgroup of C_K is of finite index in C_K.

5.2. A certain amount of this theorem may be deduced readily from the rest. First, given (A) and (B), then (C) is a special case of 4.3 (put $K' = K$ and $L' = M$).

5.3. Secondly, the uniqueness, though not the existence, of the correspondence given in (D) follows from the rest. Given the existence, let L and L' be two finite abelian extensions of K in a fixed algebraic closure of K and let M be the compositum of L and L' (which is again a finite abelian extension of K). Now consider the commutative diagram above, under (C). Since the horizontal arrows are isomorphisms (by (B)) we see that $\operatorname{Ker}\theta = G(M/L)$ is the isomorphic image, under $\psi_{M/K}$, of the group $N_{L/K}C_L/N_{M/K}C_M$. Thus L, as the fixed field of the group $\operatorname{Ker}\theta$, is uniquely determined as a subfield of M, by $N_{L/K}C_L$. Applying the same reasoning with L replaced by L', we see that if $N_{L'/K'}C_{L'} = N_{L/K}C_L$, then $L = L'$.

For some special examples of class fields (Hilbert class fields) see exercise 3.

For the functorial properties of the Artin map when the ground field K is changed, see 11.5 below.

5.4. The commutative diagram of (C) allows us to pass to the inverse limit (see Chapter III, §1), as L runs over all finite abelian extensions of K. We obtain a homomorphism

$$\psi_K : C_K \to \varprojlim_L G(L/K) \simeq G(K^{ab}/K),$$

where K^{ab} is the maximal abelian extension of K; and then, by (D),

$$G(K^{ab}/K) \simeq \varprojlim_N (C_K/N),$$

where the limit is taken over all open subgroups N of finite index in C_K. Thus we know the Galois groups of all abelian extensions of K from a knowledge of the idèle class group of K. The nature of the homomorphism $\psi_K : C_K \to G(K^{ab}/K)$ is somewhat different in the function field and number field cases. The facts, which are not hard to derive from the main theorem, but whose proofs we omit, are as follows:

5.5. *Function Field Case.* Here the map ψ_K is injective and its image is the dense subgroup of $G(K^{ab}/K)$ consisting of those automorphisms whose restriction to the algebraic closure $\bar{k}$ of the field of constants k is simply an integer power of the Frobenius automorphism F_k (see Artin-Tate notes, p. 76).

5.6. *Number Theory Case.* Here ψ_K is surjective and its kernel is the connected component D_K of C_K. So we have obtained a canonical isomorphism $C_K/D_K \simeq G(K^{ab}/K)$.

However, as Weil has stressed ("Sur la théorie du corps de classes", *J. Math. Soc. Japan*, **3**, 1951), we really want a Galois-theoretic interpretation of the *whole* of C_K. The connected component D_K can be very complicated (see Artin-Tate, p. 82).

5.7. *Example. Cyclotomic Fields.* Consider $\mathbf{Q}^{mc}/\mathbf{Q}$, the maximal cyclotomic extension of $\mathbf{Q}$. Let $\hat{\mathbf{Z}} = \varprojlim_n \mathbf{Z}/n\mathbf{Z}$; by the Chinese remainder theorem this is isomorphic to $\prod_p \mathbf{Z}_p$, where $\mathbf{Z}_p$ is the ring of p-adic integers. $\hat{\mathbf{Z}}$ acts on any abelian torsion group (for $\mathbf{Z}/n\mathbf{Z}$ operates on any abelian group whose exponent divides n) and the invertible elements of $\hat{\mathbf{Z}}$ are those in $\prod_p U_p$, where U_p is the set of p-adic units in $\mathbf{Z}_p$.

Now consider the torsion group μ consisting of all roots of unity. If $\zeta \in \mu$ we can define ζ^u for all $u \in \prod_p U_p$; u induces an automorphism on μ. The idèle group $J_{\mathbf{Q}}$ is isomorphic to the direct product $\mathbf{Q}^* \times \mathbf{R}_+^* \times \prod_p U_p$. (In fact, if $x = \{x_\infty, x_2, x_3, \ldots\} \in J_{\mathbf{Q}}$ we have $x = a.\{t, u_2, u_3, \ldots\}$, where

$$a = (\operatorname{sign} x_\infty) \prod_p p^{v_p(x_p)} \in \mathbf{Q}^*,$$

and where $t > 0$, and $u_p \in U_p$ for $p = 2, 3, \ldots$; moreover, this decomposition is unique, because 1 is the only positive rational number which is a p-adic unit for all primes p.) Hence $C_{\mathbf{Q}}$ is canonically isomorphic to $\mathbf{R}_+^* \times \prod_p U_p$, so there is a map of $C_{\mathbf{Q}}$ onto $\prod_p U_p$, which is the Galois group of the maximal cyclotomic extension.

What in fact happens is the following. If $x \in C_{\mathbf{Q}}$ and $x \mapsto u$ by this map, then $\zeta^{\psi(x)} = \zeta^{u^{-1}}$ (this result is an easy exercise, starting from 3.4, and is independent of parts (B) and (D) of the main theorem). Thus the kernel of ψ is $\mathbf{R}_+^*$, which is the connected component $D_{\mathbf{Q}}$ of $C_{\mathbf{Q}}$. We have now used up the whole of $C_{\mathbf{Q}}/D_{\mathbf{Q}}$; so if we grant part (B) of the main theorem, we see that every abelian extension of $\mathbf{Q}$ must already have appeared as a subfield of $\mathbf{Q}^{\mathrm{mc}}$, and that part (D) holds for abelian extensions of $\mathbf{Q}$.

The connected component $\mathbf{R}_+^*$ of $C_{\mathbf{Q}}$ is uninteresting; similarly, C_K has an uninteresting connected component when K is complex quadratic, essentially because there is only one archimedean prime. It may well be that it is the connected component that prevents a simple proof of the reciprocity law in the general case.

6. Relation Between Global and Local Artin Maps

We continue to deduce results on the assumption that the reciprocity law (but not necessarily the whole main theorem of § 5) is true for an abelian extension L/K.

6.1. For each prime v of K, we let K_v denote the completion of K at v. If L/K is a finite Galois extension, then the various completions L_w with w over v are isomorphic. It is convenient to write L^v for "any one of the completions L_w for w over v", and we write $G^v = G(L^v/K_v)$ for the local Galois group, which we can identify with a decomposition subgroup of G (see 1.2). In the abelian case this subgroup is unique, i.e. independent of the choice of w.

Assume that L/K is abelian and that there is an Artin map

$$\psi_{L/K} : J_K \to G(L/K) = G.$$

For each prime v of K we have

$$\begin{tikzcd} K_v^* \arrow[r, shift left, "i_v"] & J_K \arrow[l, shift left, "j_v"] \arrow[r, "\psi_{L/K}"] & G, \end{tikzcd}$$

where i_v is the mapping of an $x \in K_v^*$ onto the element of J_K whose v component is x and whose other components are 1, and j_v is the projection onto the v-th component. Call $\psi_v = \psi_{L/K} \circ i_v$; so $\psi_v : K_v^* \to G$. In fact

6.2. PROPOSITION. *If* $K_v \subset \mathcal{M} \subset L^v$, *then* $\psi_v(N_{\mathcal{M}/K_v}\mathcal{M}^*) \subset G(L^v/\mathcal{M})$. *In particular,* $\psi_v(K_v^*) \subset G^v$, *and* $\psi_v(N_{L^v/K_v}(L^v)^*) = 1$.

Proof. Let $M = L \cap \mathcal{M}$ be the fixed field of $G(L^v/\mathcal{M})$ in L, so that $G(L/M)$ is identified with $G(L^v/\mathcal{M})$ under our identification of the decomposition group with the local Galois group. Then $\mathcal{M} = M_w$, where w is a prime above v, and the diagram

$$\begin{tikzcd} \mathcal{M} = M_w \arrow[r, "i_w"] \arrow[d, "N_{\mathcal{M}/K_v}"'] & J_M \arrow[d, "N_{M/K}"] \\ K_v \arrow[r, "i_v"] & J_K \end{tikzcd}$$

is commutative. By the 'variant" of 4.3 we conclude that

$$\psi_v(N_{\mathcal{M}/K_v}\mathcal{M}^*) \subset \psi_{L/K} N_{M/K} \subset G(L/M) \simeq G(L^v/\mathcal{M}),$$

6.3. We shall call $\psi_v : K_v^* \to G^v$ the *local Artin homomorphism*, or by its classical name: *norm residue homomorphism*. If $x = (x_v) \in J_K$, then we have

$$x = \lim_S \Big\{ \prod_{v \in S} i_v(x_v) \Big\}$$

and consequently, by continuity, we have

$$\psi_{L/K}(x) = \prod_v \psi_v(x_v)$$

(this product is actually finite since if x_v is a v-unit and v is not ramified, then it is a norm of L^v/K_v). Thus knowledge of all the local Artin maps ψ_v is equivalent to knowledge of the global Artin map $\psi_{L/K}$. Classically, the local maps ψ_v were studied via the global theory and, in particular, were shown to depend only on the local extension L^v/K_v, and not on the global extension L/K from which they were derived. Nowadays one reverses the procedure, giving first a purely local construction (cf. Chapter VI) of maps $\theta_v : K_v^* \to G_v = G(L^v/K_v)$. We will take these maps θ_v from Serre and show that $\prod_v \theta_v$ satisfies the characterizing properties for ψ, in particular, that $\prod_v \theta_v(a) = 1$ for all $a \in K^*$ (see § 10).

The local theory tells us that the Main Theorem of 5.1 is true locally if we replace C_K by K_v^*, ψ by ψ_v and $G(L/K)$ by $G(L^v/K_v)$. In particular

$$K_v^*/NL^{v*} \simeq G(L^v/K_v)$$

and in this isomorphism the ramification groups correspond to the standard filtration of K_v^*/NL^{v*}. Going back to the global theory we get a complete description of prime decomposition in terms of idèle classes, even in the ramified case.

For the question of abelian and cyclic extensions with given local behaviour and the Grunwald-Wang theorem, see Artin-Tate notes Chapter 10, and Wang, "On Grunwald's Theorem", *Annals*, **51** (1950), pp. 471–484.

6.4. We can now give an apparently stronger statement of the reciprocity law formulated in 3.3.

Reciprocity Law (Strong form). *Let L/K be abelian, and let S consist of the archimedean primes of K and those ramified in L. If an element $a \in K^*$ is a norm from L^v for all $v \in S$, then $F_{L/K}((a)^S) = 1$.*

For if $j_v(a)$ is a norm for $v \in S$ we can write $j_v(a) = N_{L^v/K_v}(b_v)$ for some $b_v \in L^v$. Then by Corollary 4.2

$$1 = \psi((a)^S) . \prod_{v \in S} \psi_v(j_v(a)) = F_{L/K}((a)^S) . \prod_{v \in S} \psi_v(N_{L^v/K_v}(b_v)) = F_{L/K}((a)^S),$$

by 6.2.

For the concrete description of the local Artin maps ψ_v by means of the norm residue symbols $(a, b)_v$ in case of Kummer extensions, and the application to the general n-th power reciprocity law, see exercise 2.

7. Cohomology of Idèles

7.1. L/K is a finite Galois extension (not necessarily abelian) with Galois group G. Write A_L for the adèle ring of L; then J_L is the group of invertible elements in $A_L = L \otimes_K A_K$, and G acts on $L \otimes_K A_K$ by $\sigma \mapsto \sigma \otimes 1$; so G acts on J_L.

However, we want to look at the action of G on the cartesian product structure of J_L. Suppose $x \in J_L$, then $x = (x_w)$, where w runs through $\mathfrak{M}_L$; $\sigma \in G$ induces $\sigma_w : L_w \to L_{\sigma w}$ (see 1.1) and $(\sigma x)_{\sigma w} = \sigma_w x_w$, that is, the diagrams

$$\begin{tikzcd} L_w^* \arrow[r, "\sigma_w"] \arrow[d, "i_w"'] & L_{\sigma w}^* \arrow[d, "i_{\sigma w}"] \\ J_L \arrow[r, "\sigma"] & J_L \end{tikzcd} \qquad \begin{tikzcd} L_w^* \arrow[r, "\sigma_w"] & L_{\sigma w}^* \\ J_L \arrow[r, "\sigma"] \arrow[u, "j_w"] & J_L \arrow[u, "j_{\sigma w}"'] \end{tikzcd}$$

commute. (Note that the image of L_w^* in J_L is not a G-invariant subgroup; the smallest such subgroup containing L_w^* is $\prod_{w/v} L_w^*$.)

7.2. Proposition. *Let $v \in \mathfrak{M}_K$ and $w_0 \in \mathfrak{M}_L$ with w_0 over v. Then there are mutually inverse isomorphisms*

$$H^r\left(G, \prod_{w/v} L_w^*\right) \underset{j_{w_0} . \text{res}}{\overset{\text{cores} . i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, L_{w_0}^*)$$

and

$$H^r\left(G, \prod_{w/v} U_w\right) \underset{j_{w_0} . \text{res}}{\overset{\text{cores} . i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, U_{w_0}),$$

where U_w denotes the group of units in L_w.

The assertions remain valid when H^r is replaced by $\hat{H}^r$.

The proof is immediate from Shapiro's lemma (see Chapter IV, § 4) in view of Proposition 1.2 of § 1.

Thus the cohomology groups $H^r(G_w, L_w^*)$ are canonically isomorphic for all w over v, so it is permissible to use the notation $H^r(G^v, (L^v)^*)$ for any one of these.

7.3. Proposition. (a) $J_K \simeq J_L^G$, *the group of idèles of L left fixed by all elements of G.*

(b) $\hat{H}^r(G, J_L) \simeq \coprod_{v \in \mathfrak{M}_K} \hat{H}^r(G^v, (L^v)^*)$,

where $\coprod$ denotes the direct sum.

Proof. (a) is clear from Chapter II, § 19. To prove (b) we observe that

(1) $$J_L = \varinjlim_{S} J_{L,S}, \text{ where } J_{L,S} = \prod_{v \in S}\left(\prod_{w/v} L_w^*\right) \times \prod_{v \notin S}\left(\prod_{w/v} U_w\right)$$

and S is a finite set of primes of K containing all the ramified primes in L/K and the archimedean primes. The limit is taken over an increasing sequence of S with $\lim S = \mathfrak{M}_K$. The cohomology of finite groups commutes with direct limits, and any cohomology theory commutes with products, so it is enough to look at the cohomology of the various parts. By 7.2 and Chapter VI, § 1.4, $\prod_{v \notin S}\left(\prod_{w/v} U_w\right)$ has trivial cohomology if S contains all the ramified primes. Hence

$$\hat{H}^r(G, J_{L,S}) \simeq \prod_{v \in S} \hat{H}^r(G^v, (L^v)^*),$$

by 7.2. Let $S \to \mathfrak{M}_K$; we find

$$\hat{H}^r(G, J_L) \simeq \coprod \hat{H}^r(G^v, (L^v)^*).$$

7.4. Corollary.

(a) $H^1(G, J_L) = 0$.

(b) $H^2(G, J_L) \simeq \coprod_v \left(\dfrac{1}{n_v} \mathbf{Z}/\mathbf{Z}\right)$, *where $n_v = [L^v : K_v]$.*

Here, the determination of H^1 is just Hilbert's "Theorem 90" for the local fields (see Chapter V, § 2.6 and Chapter VI, § 1.4). The second part follows from the determination of the Brauer group of K_v in Chapter VI, § 1.6.

8. Cohomology of Idèle Classes (I), The First Inequality

We recollect the exact sequence $0 \to L^* \to J_L \to C_L \to 0$. The action of G on C_L is that induced by its action on J_L.

8.1. PROPOSITION. $C_K \simeq C_L^G$.

Proof. The above exact sequence gives rise to the homology sequence

$$0 \to H^0(G, L^*) \to H^0(G, J_L) \to H^0(G, C_L) \to H^1(G, L^*),$$

that is

$$0 \to K^* \to J_K \to C_L^G \to 0.$$

8.2. *Remark.* Our object in the abelian case is to define

$$\psi_{L/K} : C_K/N_{L/K}C_L \to G(L/K) = G.$$

By the Proposition above $C_K/N_{L/K}C_L = \hat{H}^0(G, C_L)$, and on the other hand $G = \hat{H}^{-2}(G, \mathbf{Z})$. Comparison with Chapter VI, § 2.1, suggests that the global theorem we want to prove about the cohomology of C_L is essentially the same as the local theorem Serre proves about the cohomology of L^*. This is in fact the case. Abstracting the common features, one gets the general notion of a "class formation". [cf. the Artin-Tate notes.]

We recollect that if G is cyclic and A a G-module the *Herbrand quotient* is defined by $h(G, A) = [H^2(G, A)]/[H^1(G, A)]$ if both these cardinalities $[H^2(G, A)]$ and $[H^1(G, A)]$ are finite (see Chapter IV, § 8).

8.3. THEOREM. *Let L/K be a cyclic extension of degree n. Then $h(G, C_L) = n$.*

Proof. We take a finite set S of primes of K so large that we can write $J_L = L^*.J_{L,S}$, where

$$J_{L,S} = \prod_{v \in S}\Big(\prod_{w/v} L_w^*\Big) \times \prod_{v \notin S}\Big(\prod_{w/v} U_w\Big).$$

More precisely, S is to include the archimedean primes of K, the primes of K ramified in L and all primes of K which "lie below" some primes whose classes generate the ideal class group of L. Denote by T the set of primes of L which are above primes in S. Hence

$$C_L \simeq J_L/L^* \simeq J_{L,S}/(L^* \cap J_{L,S}) = J_{L,S}/L_T$$

where $L_T = L^* \cap J_{L,S}$ is the set of T-units of L, i.e. those elements of L which are units of L_w for $w \notin T$. It follows that

$$h(C_L) = h(J_{L,S})/h(L_T),$$

if the right-hand side is defined (we note that it is impossible to use the above equation with the S missing, since then the right-hand side is not defined).

First of all we determine $h(J_{L,S})$. Since S contains all ramified primes, the group $\prod_{v \notin S}\Big(\prod_{v/w \; w|v} U_w\Big)$ has trivial cohomology, as remarked in 7.3. Hence

$$h(J_{L,S}) = h\Big(\prod_{v \in S}\Big(\prod_{w/v} L_w^*\Big)\Big) = \prod_{v \in S} h\Big(\prod_{w/v} L_w^*\Big);$$

so by 7.2 we have $h(J_{L,S}) = \prod_{v \in S} n_v$, where the n_v are the local degrees (see Chapter VI, § 1.4). This was the "local part" of the proof.

The "global part" consists in determining $h(L_T)$; in order to prove that $h(C_L) = n$ we have to show that $nh(L_T) = \prod_{v \in S} n_v$. We do this by constructing a real vector space, on which G operates, with two lattices such that one has Herbrand quotient $nh(L_T)$ and the other has quotient $\prod_{v \in S} n_v$.

Let V be the real vector space of maps $f: T \to \mathbf{R}$, so $V \simeq \mathbf{R}^t$, where $t = [T]$, the cardinality of T. We make G operate on V by defining $(\sigma f)(w) = f(\sigma^{-1}w)$ (so that $(\sigma f)(\sigma w) = f(w)$), for all $f \in V$, $\sigma \in G$ and $w \in T$. Put $N = \{f \in V | f(w) \in \mathbf{Z}$ for all $w \in T\}$. Clearly, N spans V and is G-invariant. We have $N \simeq \prod_{v \in S}\Big(\prod_{w/v} \mathbf{Z}_w\Big)$, where $\mathbf{Z}_w \simeq \mathbf{Z}$ for all w, and the action of G on N is to permute the $\mathbf{Z}_w$ for all w over a given $v \in S$. Hence.

$$\hat{H}^r(G, N) \simeq \prod_{v \in S} \hat{H}^r\Big(G, \prod_{w/v} \mathbf{Z}_w\Big) \simeq \prod_{v \in S} \hat{H}^r(G^v, \mathbf{Z})$$

by Shapiro's lemma again. Therefore

$$h(N) = \prod_{v \in S} ([\hat{H}^0(G^v, \mathbf{Z})]/[H^1(G^v, \mathbf{Z})] = \prod_{v \in S} n_v.$$

Now define another lattice. Let λ be a map: $L_T \to V$ given by $\lambda(a) = f_a$, where $f_a(w) = \log |a|_w$ for all $w \in T$. The unit theorem (or at any rate its proof!) tells us that the kernel of λ is finite and its image is a lattice M^0 of V spanning the subspace $V^0 = \{f \in V | \sum f(w) = 0\}$.

Since the kernel of λ is finite, $h(L_T) = h(M^0)$ (see Chapter IV, § 8). Now $V = V^0 + \mathbf{R}g$, where g is defined by $g(w) = 1$ for all $w \in S_L$. We define the second lattice M as $M^0 + \mathbf{Z}g$. Then M spans V and both M^0 and $\mathbf{Z}g$ are invariant under G. Hence $h(M) = h(M^0).h(\mathbf{Z}) = nh(M^0) = nh(L_T)$.

Now M, N are lattices spanning the same vector space, so $h(N) = h(M)$ by Chapter IV, § 8. Hence $\prod_v n_v = h(N) = h(M) = nh(L_T)$, as required.

8.4. CONSEQUENCE. *If L/K is cyclic of degree n, then*

$$[J_K/K^*N_{L/K}J_L] \geqslant n.$$

This inequality, called in the old days the second inequality, was always proved by non-analytic methods having their origins in Gauss' theory of the genera of quadratic forms, of which our present ones are an outgrowth. For us it is the *first inequality*, since the other inequality is deduced with the aid of this one.

8.5. CONSEQUENCE. *If L/K is a finite abelian extension and D is a subgroup of J_K such that*

(a) *$D \subset N_{L/K}J_L$,*

(b) *K^*D is dense in J_K,*

then $L = K$.

Proof. We may suppose that L/K is cyclic, since if $L \supset L' \supset K$ and L'/K is cyclic, then $D \subset N_{L/K}J_L \subset N_{L'/K}J_{L'}$. Serre has proved that locally the norms $N_{L_w/K_v}L_w^*$ are open subsets of K_v^* which contain U_v for almost all v; so $N_{L/K}J_L$ (which is simply $\prod_w N_{L_w/K_v}L_w^*$) and $K^*N_{L/K}J_L$ are open, hence closed in J_K, and the latter is dense since its subset K^*D is dense. So it is the whole of J_K, that is, $[J_K/K^*N_{L/K}J_L] = 1$; so $n = 1$ by the previous consequence.

8.6. *Remark.* We emphasize that in the Galois case an element $x = (x_v) \in J_K$ is in $N_{L/K}J_L$ if and only if it is a local norm everywhere, i.e. $x_v \in N_{L^v/K_v}(L^v)$, for all $v \in \mathfrak{M}_K$.

8.7. CONSEQUENCE. *If S is a finite subset of $\mathfrak{M}_K$ and L/K is a finite abelian extension, then $G(L/K)$ is generated by the elements $F_{L/K}(v)$ for $v \notin S$ (i.e. the map $F_{L/K}: I^S \to G(L/K)$ is surjective; cf.* 3.3).

Proof. Take G' as the subgroup of $G(L/K)$ generated by the $F_{L/K}(v)$ with $v \notin S$; let M be the fixed field of G'. For $v \notin S$, the $F_{L/K}(v)$ viewed in $G(M/K) \simeq G/G'$ are all trivial, so for all $v \notin S$, $M_w = K_v$ if $w \in \mathfrak{M}_M$ is over v. Trivially, every element of K_v^* is a norm of this extension.

Take $D = J_K^S$ (idèles with $x_v = 1$ for $v \in S$); every element of D is a local norm, i.e. $D \subseteq N_{M/K}J_M$. By the weak approximation theorem (see Chapter II, § 6) $K^*J_K^S$ is dense in J_K. So by 8.5 we have $M = K$ and G' is the whole of G.

8.8. COROLLARY. *If L is a non-trivial abelian extension of K, there are infinitely many primes v of K that do not split completely (i.e. for which $F_{L/K}(v) \neq 1$).*

For we have just seen that such primes exist outside of any finite set S.

9. Cohomology of Idèle Classes (II), The Second Inequality

Here we deduce what in the non-analytic treatment is the *second inequality*. This inequality can be proved very quickly and easily by analysis (see Chapter VIII, Theorem 5), and classically was called the first inequality. We give Chevalley's proof (*Annals*, 1940).

9.1. THEOREM. *Let L/K be a Galois extension of degree n, with Galois group G. Then*

(1) $[\hat{H}^0(G, C_L)]$ *and* $[\hat{H}^2(G, C_L)]$ *divide* n,
(2) $\hat{H}^1(G, C_L) = (0)$.

Proof. The proof will be in several steps.

Step 1. Suppose that the theorem has been proved when G is cyclic and n is prime. By the Ugly Lemma (see Chapter VI, § 1.5) it follows that $[\hat{H}^0(G, C_L)]$ divides n and $\hat{H}^1(G, C_L) = (0)$. Using this triviality of $\hat{H}^1$, it follows, again by the ugly lemma, that $[\hat{H}^2(G, C_L)]$ divides n.

Step 2. Now we assume that G is cyclic of prime order n; in this case we know that $\hat{H}^0 \simeq \hat{H}^2$ and by the first inequality 8.3 that $[\hat{H}^2] = n[\hat{H}^1]$; so it will be enough to show that $[\hat{H}^0(G, C_L)] = [C_K : N_{L/K}C_L]$ divides n.

We will make the one assumption that in the function field case n is not equal to the characteristic of K. (The other case is treated in the Artin-Tate notes, Chapter 6.)

Step 3. We now show that we may further assume that K contains the n-th roots of unity.

In fact, if we adjoin a primitive n-th root of unity ζ to K, we get an extension $K' = K(\zeta)$ whose degree m divides $(n-1)$, and so is prime to the prime n. So

$$\begin{tikzcd}
L' = LK' \arrow[r, dash, "n"] \arrow[d, dash, "m"'] & K' = K(\zeta) \arrow[d, dash, "m"] \\
L \arrow[r, dash, "n"'] & K
\end{tikzcd}$$

The degree of LK' over K' is n, and L and K' are linearly disjoint over K. So there is a commutative diagram with exact rows (we drop the subscripts since they are obvious):

$$\begin{tikzcd}
C_L \arrow[r] \arrow[d, "\mathrm{Con}"'] & C_K \arrow[r] \arrow[d, "\mathrm{Con}"'] & C_K/NC_L \arrow[r] \arrow[d, "\mathrm{Con}"'] & 0 \\
C_{L'} \arrow[r] \arrow[d, "N"'] & C_{K'} \arrow[r] \arrow[d, "N"'] & C_{K'}/NC_{L'} \arrow[r] \arrow[d, "N"'] & 0 \\
C_L \arrow[r] & C_K \arrow[r] & C_K/NC_L \arrow[r] & 0
\end{tikzcd}$$

Here Con is the Conorm map; and the composite map $N.\mathrm{Con}$ is simply raising to the mth power (see Chapter II, § 19, for this and the definition of the Conorm map). The group C_K/NC_L is a torsion group in which each element has order n, for if $a \in C_K$, then a^n is a norm, i.e. $a^n \in NC_L$. Thus the map $N_{K'/K}\,\mathrm{Con}_{K'/K}: C_K/NC_L \to C_K/NC_L$ is surjective since $(m, n) = 1$. Hence the map $N_{K'/K}: C_{K'}/NC_{L'} \to C_K/NC_L$ is surjective; so if $[C_{K'} : NC_{L'}]$ divides n so does $[C_K : NC_L]$.

Step 4. We are thus reduced to the case where n is a prime and K contains the n-th roots of unity. In fact we shall prove directly in this case the more general result:

Let K contain the n-th roots of unity and L/K be an abelian extension of prime exponent n, with say $G(L/K) = G \simeq (\mathbf{Z}/n\mathbf{Z})^r$. Then

(1) $$[C_K : N_{L/K}C_L] \text{ divides } [L : K] = n^r.$$

For although, as we have just seen, the case of arbitrary r does follow from the case $r = 1$, yet the method to be used does not simplify at all if one puts $r = 1$, and some of the constructions in the proof are useful for large r (see 9.2 and 9.5).

By Kummer Theory (see Chapter III), we know that $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ for some $a_1, a_2, \ldots, a_r \in K$. Take S to be a finite set of (bad) primes, such that

(2) (i) S contains all archimedean primes,
(ii) S contains all divisors of n,
(iii) $J_K = K^* J_{K,S}$ (by making S contain representatives of a system of generators for the ideal class group),
(iv) S contains all factors of the numerator and denominator of any a_i.

Condition (iv) just means that all the a_i are S-units, that is, they belong to $K_S = K \cap J_{K,S}$: they are units for all $v \notin S$.

Write $M = K(\sqrt[n]{K_S})$ for the field obtained from K by adjoining n-th roots of *all* S-units. By the unit theorem the group K_S has a finite basis, so this extension is finite, and M is unramified outside S by Kummer Theory and condition (ii). Now $M \supset L \supset K$ and

$$K_S = M^{*n} \cap K_S \supset L^{*n} \cap K_S \supset K^{*n} \cap K_S = K_S^n.$$

By Kummer theory with $[M:L] = n^t$, $[L:K] = n^r$ (given) and $[M:K] = n^s$ we have

(3) $[K_S : L^{*n} \cap K_S] = n^t$, $[L^{*n} \cap K_S : K_S^n] = n^r$ and $[K_S : K_S^n] = n^s$

respectively. We claim that $s = [S]$, the cardinality of S. By the unit theorem, there are $[S]-1$ fundamental units, and the roots of unity include the n-th roots; so $K_S \simeq \mathbf{Z}^{[S]-1} \times$ (cyclic group of order divisible by n) and

$$[K_S : K_S^n] = n^{[S]} = n^s, \quad \text{where } s = t + r. \tag{4}$$

We recall we want to show that $[C_K : N_{L/K} C_L]$ divides n^r, i.e. divides $[L^{*n} \cap K_S : K_S^n]$. So we need to show that $N_{L/K} C_L$ is fairly large—we have to provide a lot of norms.

If w is a prime of L above a $v \notin S$, then, since M/K is unramified outside S, the Frobenius map $F_{M/L}(w)$ is well-defined. By consequence 8.7, the $F_{M/L}(w)$ generate $G(M/L)$. Choose $w_1, \ldots, w_t$ so that $F_{M/L}(w_i)$ $(i = 1, \ldots, t)$ are a basis for $G(M/L)$, and let $v_1, \ldots, v_t$ be primes of K below them. We assert that $F_{M/L}(w_i) = F_{M/K}(v_i)$ $(i = 1, \ldots, t)$. (In fact, each of the v's is unramified, so $F_{M/K}(v_i)$ is defined). The M/K decomposition group $G_v(M/K)$ is a cyclic subgroup of $(\mathbf{Z}/n\mathbf{Z})^s$, so is either of prime order n or trivial. The w's were chosen so that the $F_{M/L}(w)$ were non-trivial, so the M/L decomposition group $G_w(M/L)$ is non-trivial; so the L/K decomposition group

$$G_v(L/K) \simeq G_v(M/K)/G_w(M/L)$$

is trivial, i.e. v splits completely in L (see Proposition 2). Therefore, $G_{v_i} = G_{w_i}$ and it is generated by the $F_{M/L}(v_i) = F_{M/K}(w_i)$.) Notice also that we have $L_{w_i} = K_{v_i}$ for all $i = 1, \ldots, t$.

Write $T = \{v_1, \ldots, v_t\}$. We claim that

$$(L^*)^n \cap K_S = \{a \in K_S \mid a \in K_v^n \quad \text{for all } v \in T\}. \tag{5}$$

In fact, since $L_w = K_v$ for all $v \in T$ and w above v, it follows trivially that $L^{*n} \cap K_S$ is contained in the right-hand side. Conversely, if $a \in K_S$, then $\sqrt[n]{a} \in M$. If further $a \in K_v^n$ for all $v \in T$, then $\sqrt[n]{a} \in K_v$ for all $v \in T$ and so is left fixed by all $F_{M/K}(v) = F_{M/L}(w)$; these generate $G(M/L)$ so $\sqrt[n]{a} \in L$. This proves (5).

Let

$$E = \prod_{v \in S} K_v^{*n} \times \prod_{v \in T} K_v^* \times \prod_{v \notin S \cup T} U_v, \tag{6}$$

where U_v is the set of v-units in K_v; so $E \subset J_{K,S \cup T}$. Also $E \subset N_{L/K} J_L$ (see Remark 8.6)—for every element of K_v^{*n} is a norm, since $K_v^*/NL_w^* \simeq G_v$ (see Chapter VI, § 2.1), which is killed by n; we have $K_v^* = L_w^*$ for all $v \in T$, and so all the elements of these K_v^* are norms, and the elements of U_v are all norms for v unramified (see Chapter VI, § 1.2, Prop. 1).

Now

$$[C_K/N_{L/K} C_L] = [J_K/K^* N_{L/K} J_L]$$

divides $[J_K : K^*E]$ because $E \subset N_{L/K} J_L$. The set S was chosen ((2)(iii)) so that

$$J_K = K^* J_{K,S} = K^* J_{K,S \cup T}$$

therefore $[C_K/N_{L/K} C_L]$ divides $[K^* J_{K,S \cup T} : K^*E]$. A general formula for indices of groups is

$$[CA : CB][C \cap A : C \cap B] = [A : B],$$

so to prove (1) it will be enough to show that

$$[J_{K,S \cup T} : E]/[K_{S \cup T} : K \cap E] = n^r \tag{7}$$

(where $K_{S \cup T} = K^* \cap J_{K,S \cup T}$).

First, we calculate $[J_{K,S \cup T} : E]$.

$$J_{K,S \cup T} = \prod_{v \in S} K_v^* \times \prod_{v \in T} K_v^* \times \prod_{v \notin S \cup T} U_v,$$

so $[J_{K,S \cup T} : E] = \prod_{v \in S} [K_v^* : (K_v^*)^n]$, by (5). From Chapter VI, § 1.7 (cf. also the Artin-Tate notes, p. xii), we see that the "trivial action" Herbrand quotient $h(K_v^*) = n/|n|_v$ where $|\ |_v$ denotes the normed absolute value. But also $h(K_v^*) = [K_v^* : K_v^{*n}]/n$ because the n-th roots of unity are in K_v^*. This means that $[K_v^* : K_v^{*n}] = n^2/|n|_v$ and

$$[J_{K,S \cup T} : E] = n^{2s} \prod_{v \in S} |n|_v^{-1} = n^{2s}, \text{ by the product formula} \tag{8}$$

since $|n|_v = 1$ if $v \notin S$.

We will also need in a moment the formula

$$[U_v : U_v^n] = n/|n|_v. \tag{9}$$

which follows from the fact that $h(U_v) = 1/|n|_v$ (see Chapter VI, § 1.7).

By (8) we see that to prove (7), it will be enough to show that

$$[K_{S \cup T} : K^* \cap E] = n^{2s-r} = n^{s+t}. \tag{10}$$

As in (4), replacing S by $S \cup T$, we have $[K_{S \cup T} : K_{S \cup T}^n] = n^{s+t}$, so it will be enough to show that $K^* \cap E = K_{S \cup T}^n$.

Trivially, $K^* \cap E \supset K_{S \cup T}^n$, so it remains to prove

$$K^* \cap E \subset K_{S \cup T}^n, \tag{11}$$

and this will result from the following lemma.

9.2. LEMMA. *Let K contain the n-th roots of unity. Let S be a subset of $\mathfrak{M}_K$ satisfying parts* (i), (ii), (iii) *of* (2) *in the above proof, and let T be a set of primes disjoint from S, and independent for K_S in the sense that the map $K_S \to \prod_{v \in T} U_v/U_v^n$ is surjective.*

Suppose that $b \in K^*$ is an n-th power in S, arbitrary in T, and a unit outside $S \cup T$. Then $b \in K^{*n}$.

Proof of Lemma. Consider the extension $K' = K(\sqrt[n]{b})$; it will be enough to deduce that $K' = K$. Put

$$D = \prod_{v \in S} K_v^* \times \prod_{v \in T} U_v^n \times \prod_{v \notin S \cup T} U_v;$$

by arguments similar to ones used before (see after (6)), $D \subset N_{K'/K} J_{K'}$. Therefore, by the first inequality in the form of consequence 8.5, in order to prove that $K' = K$ it is sufficient to prove that $K^* D = J_K$. But by hypothesis, the map $K_S \to \prod_{v \in T} (U_v/U_v^n) \simeq J_{K,S}/D$ is surjective. Hence $J_{K,S} = K_S D$, and $J_K = K^* J_{K,S} = K^* D$ as required.

To deduce (11) from the lemma, we have to check that T is independent for S in the sense of the lemma. Let H denote the kernel of the map $K_S \to \prod_{v \in T} (U_v/U_v^n)$. To prove that map is surjective it suffices to show that $(K_S : H) = \prod_{v \in T} (U_v : U_v^n)$. This latter product is just n^t by (9), because $|n|_v = 1$ for $v \in T$. On the other hand, by (5) we have $H = K_S \cap (L^*)^n$, and consequently $(K_S : H) = n^t$ by (3).

The proof of the theorem is now complete.

9.3. *Remark.* Even the case of the Lemma 9.2 with T empty is interesting. "*If S satisfies conditions* (i), (ii), (iii) *of* (2), *then an S-unit which is a local n-th power at all primes in S is an n-th power*".

9.4. CONSEQUENCE. *If L/K is abelian with Galois group G, and there is an Artin map $\psi : \hat{H}^0(G, C_L) = C_K/NC_L \to G$, then ψ must be an isomorphism.*

In fact, consequence 8.7 of the first inequality already tells us that ψ has to be surjective; if now $[\hat{H}^0(G, C_L)] \leqslant [G]$, then ψ can only be an isomorphism!

9.5. CONSEQUENCE. (Extracted from the proof of Theorem 9.1.) *Let n be a prime and let K be a field, not of characteristic n, containing the n-th roots of unity. Let S be a finite set of primes of K satisfying the conditions* (i), (ii), (iii) *of* (2), *and let $M = K(\sqrt[n]{K_S})$. Then, if the reciprocity law holds for M/K, we have*

$$K^* N_{M/K} J_M = K^* E, \text{ where } E = \prod_{v \in S} (K_v^*)^n \times \prod_{v \notin S} U_v. \tag{12}$$

Consider the case $L = M$ of the proof of 9.1 (so that T is empty, $t = 0$ and $s = r$). Then the E of that proof is as given in (12), and $E \subset N_{M/K} J_M$. By (7) with $L = M$, we have $[J_K : K^* E] = n^s = [M : K]$. On the other hand, if the reciprocity law holds, we know that

$$[C_K : N_{M/K} C_M] = [J_K : K^* N_{M/K} J_M] = n^s;$$

hence (12) must hold.

This result we put into the refrigerator; we will pull it out for the proof of the "existence theorem" in the final section § 12.

9.6. CONSEQUENCE. Let L/K be a finite (not necessarily abelian) Galois extension. Since $H^1(G, C_L) = 0$, the exact sequence $0 \to L^* \to J_L \to C_L \to 0$ gives rise to a very short exact sequence $0 \to H^2(G, L^*) \to H^2(G, J_L)$. Now $H^2(G, J_L) = \coprod_{v \in \mathfrak{M}_K} H^2(G^v, (L^v)^*)$, by Proposition 7.3, so there is an injection

$$0 \to H^2(G, L^*) \to \coprod_{v \in \mathfrak{M}_K} H^2(G^v, (L^v)^*). \tag{13}$$

We shall see later (from the fact that the arrow β_1 in diagram (9) of § 11 is an isomorphism, for example) that the image of this injection consists of those elements in the direct sum, the sum of whose local invariants is 0. We thus obtain a complete description of the structure of the group $H^2(G, L^*)$.

In terms of central simple algebras, (13) gives the *Brauer-Hasse-Noether Theorem, that a central simple algebra over K splits over K if and only if it splits locally everywhere.* In particular, if G is cyclic, $\hat{H}^2 \simeq \hat{H}^0$, and we have the *Hasse Norm Theorem:*

If $a \in K^*$, and L/K is cyclic, then $a \in N_{L/K} L^*$ if and only if $a \in N_{L^v/K_v} L^{v*}$ or all $v \in \mathfrak{M}_K$.

Specializing further, take G of order 2, so $L = K(\sqrt{b})$.

$$N_{L/K}(x + y\sqrt{b}) = x^2 - by^2,$$

so (if the characteristic is not 2) we deduce that a has the form $x^2 - by^2$ if and only if it has this form locally everywhere. It follows that *a quadratic form $Q(x, y, z)$ in three variables over K has a non-trivial zero in K if and only if it has a non-trivial zero in every completion of K.* Extending to n variables, we may obtain the *Minkowski-Hasse Theorem*, that a quadratic form has a zero if and only if it has a zero locally everywhere, see exercise 4.

One may consider the general problem, "if $a \in K^*$ and $a \in NL^{v*}$ for all v, is $a \in NL^*$?" Unfortunately, the answer is not always yes! (See 11.4.)

9.7. We return to the sequence (13). We write $H^2(L/K)$ for $H^2(G, L^*)$ and $H^2(L^v/K_v)$ for $H^2(G^v, L^{v*})$. Thus (13) becomes

$$0 \to H^2(L/K) \to \coprod_v H^2(L^v/K_v). \tag{13'}$$

Serre (Chapter VI, § 1.1, Theorem 3, Corollary 2) has determined $H^2(L^v/K_v)$, it is cyclic of order $n_v = [L^v : K_v]$, with a canonical generator. Thus

$$H^2(G, J_L) = \coprod_v H^2(L^v/K_v) \simeq \coprod_v \left(\frac{1}{n_v}\mathbf{Z}/\mathbf{Z}\right).$$

and

$$0 \to H^2(L/K) \to \coprod_v \left(\frac{1}{n_v}\mathbf{Z}/\mathbf{Z}\right).$$

If $\alpha \in \coprod_v H^2(L^v/K_v)$, or $\alpha \in H^2(L/K)$, we can find its local invariants $\text{inv}_v(\alpha)$ (more precisely $\text{inv}_v(j_v(\alpha))$, where j_v is the projection on the v-component of α), which will determine it precisely.

We are interested in the functorial properties of the map inv_v. Let $L' \supset L \supset K$ be finite Galois extensions with groups

$$G' = G(L'/K),$$

and

$$G = G(L/K) \simeq G'/H,$$

where $H = G(L'/L)$. If $\alpha \in H^2(G, J_L)$, then $\text{infl}(\alpha) \in H^2(G', J_{L'})$ and

$$\text{inv}_v(\text{infl}\,\alpha) = \text{inv}_v(\alpha). \tag{14}$$

Indeed, choosing a prime w' of L' above a prime w of L above v, one reduces this to the corresponding local statement for the tower $L'_{w'} \supset L_w \supset K_v$; cf. Chapter VI, § 1.1.

Thus nothing changes under inflation so we can pass in an invariant manner to the *Brauer group* of K, and get the *local invariants* for $\alpha \in \text{Br}(K) = H^2(\overline{K}/K)$, where $\overline{K}$ is the algebraic closure of K (see Chapter VI, § 1), and more generally for

$$\alpha \in H^2(G_{\overline{K}/K}, J_{\overline{K}}) = \varinjlim_L H^2(G_{L/K}, J_L),$$

where $J_{\overline{K}} = \varinjlim_L J_L$, by definition, the limits being taken over all finite Galois extensions L of K; cf. Chapter V.

If now $\alpha \in H^2(G', J_{L'})$, then $\text{res}^{G'}_H \alpha \in H^2(H, J_{L'})$ and

$$\text{inv}_w(\text{res}^{G'}_H \alpha) = n_{w/v}\,\text{inv}_v(\alpha), \tag{15}$$

where $w \in \mathfrak{M}_L$ lies above $v \in \mathfrak{M}_K$ and $n_{w/v} = [L_w : K_v]$ (again one reduces immediately to the local case, for which see Chapter VI, § 1.1, or Serre's "Corps Locaux", Hermann, (1962), p. 175). Moreover, L/K need not be Galois here.

Finally we mention the result for corestriction, though we will not use it. Again, L/K need not be Galois. If $\alpha' \in H^2(H, J_{L'})$, then $\text{cor}^{G'}_H \alpha' \in H^2(G', J_{L'})$ and

$$\text{inv}_v(\text{cor}^{G'}_H \alpha') = \sum_{w/v} \text{inv}_w(\alpha'), \tag{16}$$

where the sum is over all primes $w \in \mathfrak{M}_L$ over $v \in \mathfrak{M}_K$ (see "Corps Locaux", p. 175).

9.8. COROLLARY. *Let $\alpha \in \text{Br}(K)$ or $H^2(G(\overline{K}/K), J_{\overline{K}})$, where $\overline{K}$ is the separable algebraic closure of K. Let L be an extension of K in $\overline{K}$. Then $\text{res}^{K}_{L}(\alpha) = 0$ if and only if $[L_w : K_v]\,\text{inv}_v(\alpha) = 0$ for every w over v (this is only a finite condition, since almost all the $\text{inv}_v(\alpha)$ are zero).*

In the case when L/K is Galois, there is an exact sequence

$$0 \longrightarrow H^2(L/K) \xrightarrow{\text{infl}} \text{Br}(K) \xrightarrow{\text{res}} \text{Br}(L),$$

and $\alpha \in H^2(L/K)$ if and only if the denominator of $\text{inv}_v(\alpha)$ divides $[L_w : K_v]$ for all w over v.

10. Proof of the Reciprocity Law

10.1. Now let L/K be a finite abelian extension with Galois group G. We recall our discussion in § 6 on local symbols in which we noted that if a global Artin map existed we were able to reduce it to the study of local symbols and remarked that, conversely, if the local Artin maps are defined we could obtain a global Artin map. We propose to carry out this latter program here using the local Artin ("norm residue") maps defined in Chapter VI, § 2.2.

Let the local Artin maps be denoted by $\theta_v : K_v^* \to G^v$; we define a map

$$\theta : J_K \to G$$

by

$$\theta(x) = \prod_{v \in \mathfrak{M}_K} \theta_v(x_v), \quad x \in J_K.$$

This is a proper definition, since (by Chapter VI, § 2.3) $\theta_v(x_v) = F_{L^v/K_v}(v)^{v(x_v)}$ ($v(x_v)$ being the normalized valuation of x_v) when v is unramified, and $v(x_v) = 0$ if $x_v \in U_v$; so $\theta_v(x_v) = 1$ for all but finitely many v. (Indeed, even if L/K were an infinite extension, the product for $\theta(x)$ would be convergent.) It is clear that θ is a continuous map.

Take $S_o \subseteq \mathfrak{M}_K$ as the set of archimedean primes plus the primes ramified in L/K; then $x \in J_K^{S_o}$ implies $\theta(x) = F((x)^{S_o})$. Thus, θ satisfies two of the conditions for an Artin map ((i) and (iii) of Corollary 4.2); the other condition ((ii) of 4.2) is that

$$\theta(a) = \prod_{v \in \mathfrak{M}_K} \theta_v(a) = 1 \quad \text{for all a} \in K^*.$$

So if we can prove this, we will have proved the reciprocity law.

10.2. To prove the reciprocity law, it will be convenient to state two related theorems, and to prove them both at once, gradually extending the cases for which they are true.

THEOREM A. *Every finite abelian extension L/K satisfies the reciprocity law, and the Artin map $\theta : J_K \to G(L/K)$ is given by $\theta = \prod_v \theta_v$.*

THEOREM B. *If $\alpha \in \mathrm{Br}\,(K)$, then $\sum_{v \in \mathfrak{M}_K} \mathrm{inv}_v\,(\alpha) = 0$.*

Remarks. After what has been said above, Theorem A has been whittled down to the assertion that

$$(1) \qquad \prod_{v \in \mathfrak{M}_K} \theta_v(a) = 1 \quad \text{for all } a \in K^*.$$

The sum of Theorem B is finite since $\mathrm{inv}_v\,(\alpha) = \mathrm{inv}_v\,(j_v . \alpha) = 0$ for all but finitely many α.

If $\alpha \in \mathrm{Br}\,(K)$, then $\alpha \in H^2(L/K)$ for some finite extension L/K, i.e. α is split by a finite extension of K.

Logically, the proof is in four main steps.

Step 1. Prove A for an arbitrary finite cyclotomic extension L/K.

Step 2. Deduce B for α split by a cyclic cyclotomic extension.

Step 3. Deduce B for arbitrary $\alpha \in \mathrm{Br}\,(K)$.

Step 4. Deduce A for all abelian extensions.

In practice, we first clarify the relation between Theorems A and B and deduce (step 2) that A implies B for cyclic extensions and (step 4) that B implies A for arbitrary abelian extensions. Then we prove Step 1 directly, and finally push through Step 3, by showing that every element of $\mathrm{Br}\,(K)$ has a cyclic cyclotomic splitting field.

10.3. *Steps 2 and 4. The relation between* A *and* B. A is about $\hat{H}^\circ$ and B is about H^2, so we need a lemma connecting them.

Let L/K be a finite abelian extension with Galois group G. Let χ be a character of G, thus $\chi \in \mathrm{Hom}\,(G, \mathbf{Q}/\mathbf{Z}) = H^1(G, \mathbf{Q}/\mathbf{Z})$, where $\mathbf{Q}/\mathbf{Z}$ is a trivial G-module. If $v \in \mathfrak{M}_K$, denote by χ_v the restriction of χ to the decomposition group G^v. Let δ be the connecting homomorphism

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

If $x = (x_v) \in J_K$, let $\bar{x}$ be its image in $J_K/N_{L/K}J_L \simeq \hat{H}^\circ(G, J_L)$. Then the cup product (see Chapter IV, § 7) $\bar{x} . \delta\chi \in H^2(G, J_L)$.

LEMMA. *For each v we have*

$$\mathrm{inv}_v\,(\bar{x} . \delta\chi) = \chi_v(\theta_v(x_v)),$$

and so

$$\sum_v \mathrm{inv}_v\,(\bar{x} . \delta\chi) = \chi(\theta(x)).$$

Proof. We refer to Chapter VI, § 2.3. The projection $j_v : J_L \to (L^v)^*$ induces a map

$$j_v . \mathrm{res}^G_{G_v} : H^2(G, J_L) \to H^2(G_v, J_L) \to H^2(G_v, (L^v)^*),$$

and as restriction commutes with the cup product, so

$$\begin{aligned} \mathrm{inv}_v\,(\bar{x} . \delta\chi) &= \mathrm{inv}_v\,(j_v . \mathrm{res}^G_{G_v}\,(\bar{x} . \delta\chi)) \\ &= \mathrm{inv}_v\,((j_v . \bar{x}) . \delta\chi_v) \\ &= \mathrm{inv}_v\,(\bar{x}_v . \delta\chi_v) \\ &= \chi_v(\theta_v(x_v)), \end{aligned}$$

the final step coming from Chapter VI, § 2.3.

It follows immediately that

$$\chi(\theta(x)) = \chi\Big(\prod_v \theta_v(x_v)\Big) = \sum_v \chi_v(\theta_v(x_v)) = \sum_v \mathrm{inv}_v\,(\bar{x} . \delta\chi).$$

To check Step 4, apply the lemma with $x = a \in K^* \subseteq J_K$. Denote by $\tilde{a}$ the image of a in $\hat{H}^0(G, L^*)$. Then $\tilde{a} . \delta\chi \in \hat{H}^2(G, L^*) \subseteq \mathrm{Br}\,(K)$, as we need. The image of $\tilde{a} . \delta\chi$ in $H^2(G, J_L)$ is $\bar{a} . \delta\chi$, where $\bar{a}$ is the image of a in $\hat{H}^0(G, J_L)$, and by the above lemma, $\sum_v \mathrm{inv}_v\,(\bar{a} . \delta\chi) = \chi(\theta(a))$; so if Theorem B is true for all $\alpha \in \mathrm{Br}\,(K)$, it follows that $\chi(\theta(a)) = 0$, and since this is true for all χ, that $\theta(a) = 0$. This is Theorem A.

To check Step 2, take L/K cyclic. Choose χ as a generating character, i.e. as an injection of G into $\mathbf{Q}/\mathbf{Z}$. Then cupping with $\delta\chi$ gives an isomorphism $\hat{H}^0 \simeq H^2$, so every element of $H^2(L/K, L^*)$ is of the form $\tilde{a} . \delta\chi$. If Theorem A is true, then by the above lemma

$$\sum_v \mathrm{inv}_v\,(\bar{a} . \delta\chi) = \chi(\theta(a)) = 0$$

for all $a \in K^*$, which is Theorem B.

10.4. *Step 1.* (*Number Field Case.*) We want to prove that if L/K is a cyclotomic extension, then $\prod_v \theta_v(a) = 1$ for all $a \in K^*$.

Let L/K be a finite cyclotomic extension. Then we have $L \subset K(\zeta)$ for some root of unity ζ, and it will suffice to treat the case $L = K(\zeta)$ because of the compatibility of the local symbols θ_v relative to the extensions $(K(\zeta))^v/K_v$ and L^v/K_v; cf. Chapter VI, § 2.4.

Next we reduce to the case $K = \mathbf{Q}$. Suppose that $M = K(\zeta)$, with Galois group G'; define $L = \mathbf{Q}(\zeta)$, with Galois group G. Then $M = LK$, and there is a natural injection $i: G' \to G$ and norm map $N: J_K \to J_{\mathbf{Q}}$. The diagram

$$\begin{tikzcd} J_K \arrow[r, "\theta'"] \arrow[d, "N_{K/\mathbf{Q}}"'] & G' \arrow[d, "i"] \\ J_{\mathbf{Q}} \arrow[r, "\theta"] & G \end{tikzcd}$$

(where $\theta' = \prod_v \theta'_v$, and $\theta = \prod_p \theta_p$) is commutative, since

$$(N_{K/\mathbf{Q}}x)_p = \prod_{v/p} N_{K_v/\mathbf{Q}_p} x_v$$

(see Chapter II, § 11, last display formula) and since the diagrams

$$\begin{tikzcd} K_v^\times \arrow[r, "\theta'_v"] \arrow[d, "N"'] & G'_v \arrow[d, "i"] \\ \mathbf{Q}_p^\times \arrow[r, "\theta_p"] & G_p \end{tikzcd}$$

are commutative whenever v is above p (see Chaper VI, § 2.1, cf. Proposition 3.1 above). Thus $i \circ \theta'(x) = \theta(N_{K/\mathbf{Q}}(x))$ for all $x \in J_K$ and so, in particular, $i \circ \theta'(a) = \theta(N_{K/\mathbf{Q}}(a))$ for all $a \in K$. If Theorem A is true for $L/\mathbf{Q}$, then $\theta(b) = 1$ for all $b \in \mathbf{Q}$, so $\theta'(a) = 1$ for all $a \in K$, because i is injective.

First Proof for $L/\mathbf{Q}$ cyclotomic. We know that the reciprocity law, in the sense of 3.8, holds for $L/\mathbf{Q}$ by computation (see 3.4), i.e. we have an admissible map $F: I^S \to G(L/\mathbf{Q}) = G$, for some S. Using the Chevalley interpretation (Proposition 4.1) we get an Artin map $\psi: J_{\mathbf{Q}} \to G$, and we obtain induced local maps $\psi_p: \mathbf{Q}_p^* \to G_p$ (see § 6). Using Proposition 4.3 we can pass to the limit and take L as the maximal cyclotomic extension $\mathbf{Q}^{\mathrm{mc}}$ of $\mathbf{Q}$. This gives us local maps $\psi_p: \mathbf{Q}_p^{\mathrm{mc}} \to G(\mathbf{Q}_p^{\mathrm{mc}}/\mathbf{Q}_p)$, for all primes p. We want to show that these ψ_p's are the same as the θ_p's of Chapter VI, § 2.2; we do this by using the characterization given by Chapter VI, § 2.8, Proposition 3.

We have to check three things. Firstly, that $\mathbf{Q}_p^{\mathrm{mc}}$ contains the maximal unramified extension $\mathbf{Q}_p^{\mathrm{nr}}$ of $\mathbf{Q}_p$; this follows from Chapter I, § 7, Application. Secondly, if $\alpha \in \mathbf{Q}_p$, then $\psi_p(\alpha) | \mathbf{Q}_p^{\mathrm{nr}} = F^{v_p(\alpha)}$, where $v_p(\alpha)$ is the normalized valuation of α, and F the Frobenius element of $G(\mathbf{Q}_p^{\mathrm{nr}}/\mathbf{Q}_p)$; this is clear. Thirdly, if $\mathcal{M}/\mathbf{Q}_p$ is a finite subextension in $\mathbf{Q}_p^{\mathrm{mc}}$, and $\alpha \in N_{\mathcal{M}/\mathbf{Q}_p}\mathcal{M}^*$, then $\psi_p(\alpha)$ leaves $\mathcal{M}$ pointwise-fixed; this follows from Proposition 6.2. Hence $\psi_p = \theta_p$ for all finite primes p. We must not forget to check that ψ_∞ is the same as θ_∞ (see Chapter VI, § 2.9). By Proposition 6.2, ψ_∞ is a continuous homomorphism of $\mathbf{R}^*$ into $G_\infty = G(\mathbf{C}/\mathbf{R}) \simeq \{\pm 1\}$, and $\psi_\infty(N_{\mathbf{C}/\mathbf{R}}\mathbf{C}^*) = 1$. Hence ψ_∞ and θ_∞ induce maps of $\mathbf{R}^*/\mathbf{R}_+^*$ into $G(\mathbf{C}/\mathbf{R})$ and θ_∞ is onto, so we just have to check that ψ_∞ is onto—in other words, we have to check that ψ_∞ is not the null map.

$\mathbf{C} = \mathbf{R}(i)$, so consider the effect of ψ on $\mathbf{Q}(i) \supset \mathbf{Q}$; the only ramification is at 2 and ∞. Therefore

$$1 = \psi(-7) = \psi_2(-7)\psi_7(-7)\psi_\infty(-7) = \psi_7(7).\psi_\infty(-1),$$

since -7 is a 2-adic norm and so $\psi_2(-7) = 1$. Now $\psi_7(7)$ is the map $i \to i^7 = -i$, so $\psi_\infty(-1)$ is also the map $i \to -i$, i.e. is non-trivial.

Second Proof for $L/\mathbf{Q}$ cyclotomic. We may proceed entirely locally, without using our results of the early sections, but using the explicit local computation of the norm residue symbol in cyclotomic extensions, due originally to Dwork.

Let ζ be a root of unity; by Chapter VI, § 2.9

$$\zeta^{\theta_\infty(x)} = \zeta^{\mathrm{sign}\,(x)}, \quad \text{for } x \in \mathbf{R}^*, \tag{1}$$

and by Chapter VI, § 3.1, if $x \in \mathbf{Q}_p^*$, $x = p^\nu u$, with u a unit in $\mathbf{Q}_p$ and ν an integer

$$\zeta^{\theta_p(p^\nu u)} = \begin{cases} \zeta^{p^\nu}, & \text{when } \zeta \text{ has order prime to } p. \\ \zeta^{u^{-1}}, & \text{when } \zeta \text{ has } p\text{-power order.} \end{cases} \tag{2}$$

We need to check that $\prod_p \theta_p(a) = 1$ for all $a \in \mathbf{Q}^*$ and to do this it is sufficient to show that $\prod_p \theta_p(q) = 1$ for all primes $q > 0$, and that $\prod_p \theta_p(-1) = 1$. Furthermore, it is enough to consider the effect on ζ, an l-th power root of unity (l a prime). One checks explicitly that the effect is trivial, using the tables

$$\zeta^{\theta_p(-1)} = \begin{cases} \zeta^{-1}, & p = \infty \\ \zeta^{-1}, & p = l \\ \zeta, & p \neq l, \infty \end{cases}$$

$$\zeta^{\theta_p(q)} = \begin{cases} \zeta, & p = q = l \\ \zeta, & p \neq l,\ p \neq q \text{ (including the case } p = \infty) \\ \zeta^{q^{-1}}, & p = l,\ p \neq q \\ \zeta^{q}, & p \neq l,\ p = q \end{cases}$$

(Since the Galois group is abelian, it does not matter in what order one applies the automorphisms $\theta_p(-1)$, resp. $\theta_p(q)$.)

10.5. *Step 3.* (*Number Field Case.*) It is enough to show that every element of Br(K) has a cyclic, cyclotomic splitting field. In other words, for every $\alpha \in$ Br(K), there is a cyclic, cyclotomic extension L/K such that for every

$v \in \mathfrak{M}_K$, the local degree $[L^v : K_v]$ is a multiple of the denominator of $\mathrm{inv}_v(\alpha)$ (see Corollary 9.8). Now $\mathrm{inv}_v(\alpha) = 0$ for all but a finite number of primes and so we need only prove the

LEMMA. *Given a number field K of finite degree over* $\mathbf{Q}$, *a finite set of primes S of K, and a positive integer m, there exists a cyclic, cyclotomic extension L/K whose local degrees are divisible by m at the non-archimedean primes of S and divisible by 2 at real archimedean primes v of S (in other words, L is complex).*

Proof. It is sufficient to construct L in the case $K = \mathbf{Q}$ (multiply m by the degree $[K:\mathbf{Q}]$). Take r very large and q an odd prime. The extension $L(q) = \mathbf{Q}(\sqrt[q^r]{1})$ has a Galois group isomorphic to the direct sum of a cyclic group of order $(q-1)$ and cyclic group of order q^{r-1}, so has a subfield $L'(q)$ which is a cyclic cyclotomic extension of $\mathbf{Q}$ of degree q^{r-1}. Now

$$[L(q):L'(q)] = q-1,$$

and so on localizing at a fixed prime $p \neq \infty$ of $\mathbf{Q}$ we have

$$[L(q)^{(p)}:L'(q)^{(p)}] \leqslant (q-1);$$

since $[L(q)^{(p)}:\mathbf{Q}_p] \to \infty$ as $r \to \infty$ (this follows for example from the fact ? that each finite extension of $\mathbf{Q}_p$ contains only a finite number of roots of unity), it follows that $[L'(q)^{(p)}:\mathbf{Q}_p] \to \infty$ as $r \to \infty$. Therefore, since $[L'(q)^{(p)}:\mathbf{Q}_p]$ is always a power of q, it is divisible by a sufficiently large power of q if we take r large enough.

Now let $q = 2$, and put $L(2) = \mathbf{Q}(\sqrt[2^r]{1})$ for r large. $L(2)$ has a Galois group isomorphic to the direct sum of a cyclic group of order 2 and a cyclic group of order 2^{r-2}. Let ζ be a primitive 2^r-th root of unity and set $\xi = \zeta - \zeta^{-1}$ and $L'(2) = \mathbf{Q}(\xi)$. The automorphisms of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ are of the form $\sigma_\mu : \zeta \mapsto \zeta^\mu$ for μ odd, and $\sigma_\mu(\xi) = \zeta^\mu - \zeta^{-\mu}$. Since $\zeta^{2^{r-1}} = -1$, one sees that $\sigma_{-\mu+2^{r-1}}(\xi) = \sigma_\mu(\xi)$; since either μ or $-\mu+2^{r-1}$ is $\equiv 1 \pmod 4$, this implies that the automorphisms of $\mathbf{Q}(\xi)/\mathbf{Q}$ are induced by those σ_μ where $\mu \equiv 1 \pmod 4$ and that they form a cyclic group of order 2^{r-2}. Also, since $\sigma_{-1}\xi = -\xi$, $\mathbf{Q}(\xi)$ is not real, and so its local degree at an infiinte real prime is 2.

Now $[L(2):L'(2)] = 2$, and the same argument as above shows that for $p \neq \infty$ we can make $[L'(2)^{(p)}:\mathbf{Q}_p]$ divisible by as large a power of 2 as we like by taking r large enough.

If now the prime factors of m are $q_1, \ldots, q_n$ and possibly 2, then for large enough r the compositum of $L'(q_1), \ldots, L'(q_n)$ and possibly $L'(2)$ is a complex cyclic cyclotomic extension of $\mathbf{Q}$ whose local degree over $\mathbf{Q}_p$ is divisible by m for all p in a finite set S.

Cyclic cyclotomic extensions seem to be at the heart of all proofs of the general reciprocity law. We have been able to get away with a very trivial

existence lemma for them, because we have at our disposal both cohomology and the local theory. In his original proof Artin used a more subtle lemma; see for example Lang, "Algebraic Numbers", Addison Wesley, 1964, p. 60. (But notice that the necessary hypothesis that $\mathfrak{p}$ be unramified is omitted from the statement there.)

We may prove the reciprocity law for function fields on the same lines, but the special role of "cyclic cyclotomic extensions" in the proof is taken over by "constant field extensions".

Step 3 goes through, if we replace "cyclic cyclotomic extension" by "constant field extension"; we have only to take for the L in the lemma the constant field extension whose degree is m times the least common multiple of the degrees of the primes in S.

For step 1, we check the reciprocity law directly for constant field extensions; in fact, if we denote by σ the Frobenius automorphism of $\bar{k}/k$, where k is the constant field of K, then for each prime v of K the effect of $F(v)$ on $\bar{k}$ is just $\sigma^{\deg v}$, where $\deg v = [k(v):k]$ is the degree of v. Hence the effect on $\bar{k}$ of $\theta(a)$ is $\prod_v \sigma^{v(a)\deg v} = \sigma^{\Sigma v(a) \deg v} = \sigma^{\deg a} = 1$, since $\deg a = 0$ for all $a \in K^*$ (the number of zeros of an algebraic function a is equal to the number of poles).

11. Cohomology of Idèle Classes (III), The Fundamental Class

11.1 Let $E/L/K$ be finite Galois extensions of K; then we have an exact commutative diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
 & 0 \arrow[r] & H^2(L/K, L^*) \arrow[r] \arrow[d] & H^2(L/K, J_L) \arrow[r] \arrow[d] & H^2(L/K, C_L) \arrow[d] \\
(1) & 0 \arrow[r] & H^2(E/K, E^*) \arrow[r] \arrow[d] & H^2(E/K, J_E) \arrow[r] \arrow[d] & H^2(E/K, C_E) \arrow[d] \\
 & 0 \arrow[r] & H^2(E/L, E^*) \arrow[r] & H^2(E/L, J_E) \arrow[r] & H^2(E/L, C_E),
\end{tikzcd}$$

where we have written $H^2(L/K, L^*)$ for $H^2(G(L/K), L^*)$, etc. In this diagram, the vertical lines are inflation-restriction sequences; these are exact since $H^1(E/L, E^*) = (0)$ (Hilbert Theorem 90, Chapter V, § 2.6), $H^1(E/L, J_E) = (0)$ (Corollary 7.4) and $H^1(E/L, C_E) = (0)$ (Theorem 9.1) [see Chapter IV, § 5, Proposition 5]. The horizontal sequences are exact, and come from the sequence $0 \to L^* \to J_L \to C_L \to 0$, since again $H^1(L/K, C_L) = (0)$, etc.

We pass to the limit and let $E \to \bar{K}$, where $\bar{K}$ is the algebraic closure of K, to obtain the new commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & H^2(L/K,L^*) \arrow[r, "\gamma_1"] \arrow[d] & H^2(L/K,J_L) \arrow[r, "\varepsilon_1"] \arrow[d] & H^2(L/K,C_L) \arrow[d] \\
(2)\quad 0 \arrow[r] & H^2(K,\overline{K}^*) \arrow[r, "\gamma_2"] \arrow[d] & H^2(K,J_{\overline{K}}) \arrow[r, "\varepsilon_2"] \arrow[d] & H^2(K,C_{\overline{K}}) \arrow[d] \\
0 \arrow[r] & H^2(L,\overline{K}^*) \arrow[r, "\gamma_3"] & H^2(L,J_{\overline{K}}) \arrow[r, "\varepsilon_3"] & H^2(L,C_{\overline{K}}),
\end{tikzcd}$$

where we have written $H^2(K,\overline{K}^*)$ for $H^2(G(\overline{K}/K),\overline{K}^*)$, etc. Certain of the maps with which we shall be concerned below have been labelled in the diagram.

11.2. We are going to enlarge the above commutative diagram.

For the Galois extension L/K we have the map

$$\mathrm{inv}_1 = \sum_v \mathrm{inv}_v : H^2(L/K,J_L) \to \mathbf{Q}/\mathbf{Z},$$

and Theorem B of 10.2 tells us that the sequence

$$(3)\qquad 0 \longrightarrow H^2(L/K,L^*) \xrightarrow{\gamma_1} H^2(L/K,J_L) \xrightarrow{\mathrm{inv}_1} \mathbf{Q}/\mathbf{Z}$$

is a complex.†

Since $\mathrm{inv}_v(\mathrm{infl}\,\alpha) = \mathrm{inv}_v(\alpha)$ for all $\alpha \in H^2(L/K,J_L)$ (see 9.7, (14)), we have a map $\mathrm{inv}_2 : H^2(K,J_{\overline{K}}) \to \mathbf{Q}/\mathbf{Z}$ such that the diagram

$$\begin{tikzcd}
H^2(L/K,J_L) \arrow[r, "\mathrm{inv}_1"] \arrow[d, "\mathrm{infl}"'] & \mathbf{Q}/\mathbf{Z} \arrow[d, "i"] \\
H^2(K,J_{\overline{K}}) \arrow[r, "\mathrm{inv}_2"] & \mathbf{Q}/\mathbf{Z}
\end{tikzcd}\qquad(4)$$

is commutative, where i is the identity map. Furthermore, the sequence

$$(5)\qquad 0 \longrightarrow H^2(K,\overline{K}^*) \xrightarrow{\gamma_2} H^2(K,J_{\overline{K}}) \xrightarrow{\mathrm{inv}_2} \mathbf{Q}/\mathbf{Z}$$

is a complex.

In a similar manner we have a complex

$$(6)\qquad 0 \longrightarrow H^2(L,\overline{K}^*) \xrightarrow{\gamma_3} H^2(L,J_{\overline{K}}) \xrightarrow{\mathrm{inv}_3} \mathbf{Q}/\mathbf{Z}.$$

But now, $\mathrm{inv}_w(\mathrm{res}\,\alpha) = n_{w/v}\,\mathrm{inv}_v(\alpha)$, where $\alpha \in H^2(K,J_{\overline{K}})$ and w is a prime of L over v of K, and $n_{w/v} = [L_w : K_v]$ (see § 9.7, (15)). Thus we have the commutative diagram

$$\begin{tikzcd}
H^2(K,J_{\overline{K}}) \arrow[r, "\mathrm{inv}_2"] \arrow[d, "\mathrm{res}"'] & \mathbf{Q}/\mathbf{Z} \arrow[d, "n"] \\
H^2(L,J_{\overline{K}}) \arrow[r, "\mathrm{inv}_3"] & \mathbf{Q}/\mathbf{Z},
\end{tikzcd}\qquad(7)$$

as the sum of the local degrees $\sum_{w|v} n_{w/v} = n = [L:K]$.

† i.e. the image of each map is in the kernel of the next.

Now let Image of $\varepsilon_2 = \mathrm{Im}\,\varepsilon_2$ in $H^2(K,C_{\overline{K}})$ be denoted by $H^2(K,C_{\overline{K}})_{\mathrm{reg}}$ and $\mathrm{Im}\,\varepsilon_3$ by $H^2(L,C_{\overline{K}})_{\mathrm{reg}}$. It follows that we have a map β_2 (resp. β_3) induced by inv_2 (resp. inv_3) of $H^2(K,C_{\overline{K}})_{\mathrm{reg}}$ into $\mathbf{Q}/\mathbf{Z}$ (resp. $H^2(L,C_{\overline{K}})_{\mathrm{reg}}$ into $\mathbf{Q}/\mathbf{Z}$). Thus for $a \in H^2(K,C_{\overline{K}})_{\mathrm{reg}}$, we have $\beta_2(a) = \mathrm{inv}_2(b)$, where $\varepsilon_2(b) = a$ (this is independent of the choice of b). We have now explained the two lower layers in diagram (9) below.

↑ since (5) is a complex.

We define

$$(8)\qquad H^2(L/K,C_L)_{\mathrm{reg}} = \{a \in H^2(L/K,C_L) \mid \mathrm{infl}\,a \in H^2(K,C_{\overline{K}})_{\mathrm{reg}}\}.$$

Then $n\beta_2\,\mathrm{infl}\,a = 0$, and so β_2 induces a homomorphism

$$\beta_1 : H^2(L/K,C_L)_{\mathrm{reg}} \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$$

such that

$$\beta_1(a) = \beta_2(\mathrm{infl}\,a).$$

If $a = \varepsilon_1 b$ with $b \in H^2(L/K,J_L)$ then

$$\beta_1(a) = \beta_2(\mathrm{infl}\,b) = \mathrm{inv}_2(\mathrm{infl}\,b) = \mathrm{inv}_1(b).$$

(Note the difference in construction of β_1 and β_2; the point is that $H^2(L/K,C_L)_{\mathrm{reg}} \supset \mathrm{Im}\,\varepsilon_1$ but they will not in general be equal.)

We put all the information from (3)–(8) into (2) to obtain a new commutative (three-dimensional) diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & H^2(L/K,L^*) \arrow[r, "\gamma_1"] \arrow[dd] & H^2(L/K,J_L) \arrow[r, "\varepsilon_1"] \arrow[dd] \arrow[drrr, "\mathrm{inv}_1"'] & H^2(L/K,C_L)_{\mathrm{reg}} \arrow[dd] \arrow[drr, "\beta_1"] & & 0 \arrow[d] \\
 & & & & & \frac{1}{n}\mathbf{Z}/\mathbf{Z} \arrow[dd, "i"] \\
0 \arrow[r] & H^2(K,\overline{K}^*) \arrow[r, "\gamma_2"] \arrow[dd] & H^2(K,J_{\overline{K}}) \arrow[r, "\varepsilon_2"] \arrow[dd] \arrow[drrr, "\mathrm{inv}_2"'] & H^2(K,C_{\overline{K}})_{\mathrm{reg}} \arrow[r] \arrow[dd] \arrow[drr, "\beta_2"] & 0 & \\
 & & & & & \mathbf{Q}/\mathbf{Z} \arrow[dd, "n"] \\
0 \arrow[r] & H^2(L,\overline{K}^*) \arrow[r, "\gamma_3"] & H^2(L,J_{\overline{K}}) \arrow[r, "\varepsilon_3"] \arrow[drrr, "\mathrm{inv}_3"'] & H^2(L,C_{\overline{K}})_{\mathrm{reg}} \arrow[r] \arrow[drr, "\beta_3"] & 0 & \\
 & & & & & \mathbf{Q}/\mathbf{Z}
\end{tikzcd}$$

(9)

in which i is the inclusion map, n is multiplication by n and the "bent" sequences are *complexes*, and the horizontal and vertical sequences are exact.

11.2. (*bis*) We propose to show that

$$(10)\qquad H^2(K, C_{\bar{K}})_{\mathrm{reg}} = H^2(K, C_{\bar{K}}) \simeq \mathbf{Q}/\mathbf{Z}.$$

Now Im (inv$_1$) in $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ is the subgroup $\frac{1}{n_0}\mathbf{Z}/\mathbf{Z}$, where n_0 is the lowest common multiple of all the local degrees of L/K, by Corollary 7.4, and so since Im $\beta_1 \supset$ (inv$_1$) we have the inequalities

$$n \geqslant [H^2(L/K, C_L)] \geqslant [H^2(L/K, C_L)_{\mathrm{reg}}] \geqslant [\mathrm{Im}\,\beta_1] \geqslant [\mathrm{Im}\,(\mathrm{inv}_1)] = n_0,$$

by the second inequality, Theorem 9.1. It follows that *if* $n = n_0$ for this particular finite extension L/K, *then* we have equality throughout, so that β_1 is bijective and the sequence

$$(11)\qquad 0 \longrightarrow H^2(L/K, L^*) \xrightarrow{\gamma_1} H^2(L/K, J_L) \xrightarrow{\mathrm{Inv}_1} \mathbf{Q}/\mathbf{Z}$$

is *exact* (for if $0 = \mathrm{inv}_1(b) = \beta_1\varepsilon_1 b$, then $\varepsilon_1 b = 0$, and $b \in \mathrm{Im}\,\gamma_1$).

Now if L/K is a finite cyclic extension, then $n = n_0$ because the Frobenius elements $F_{L/K}(v)$, whose orders are equal to the local degrees n_v, generate the cyclic group $G(L/K)$ by Consequence 8.7. So if, in particular, the extension L/K is cyclic cyclotomic, then (11) is an exact sequence. But the Lemma of § 10.5 says that the groups $H^2(K, \bar{K}^*)$ and $H^2(K, J_{\bar{K}})$ are the unions (of the isomorphic images under inflation) of the groups $H^2(L/K, L^*)$ and $H^2(L/K, J_L)$ respectively, where L runs over all cyclic cyclotomic extensions of K. Consequently, in our commutative diagram (9) the complexes

$$0 \longrightarrow H^2(K, \bar{K}^*) \xrightarrow{\gamma_2} H^2(K, J_{\bar{K}}) \xrightarrow{\mathrm{Inv}_2} \mathbf{Q}/\mathbf{Z}$$

and

$$0 \longrightarrow H^2(L, \bar{K}^*) \xrightarrow{\gamma_3} H^2(L, J_{\bar{K}}) \xrightarrow{\mathrm{Inv}_3} \mathbf{Q}/\mathbf{Z}$$

are exact. Therefore ker (inv$_2$) = ker (ε_2), so β_2 (and similarly β_3) must be injective maps into $\mathbf{Q}/\mathbf{Z}$. They are surjective, since there exist finite extensions with arbitrarily high local degrees and consequently even inv$_2$ and inv$_3$ are surjective. Hence both β_2 and β_3 are bijective maps. Now, letting L be an arbitrary finite Galois extension, we conclude that β_1 is a bijection:

$$H^2(L/K, C_L)_{\mathrm{reg}} \simeq \frac{1}{n}\mathbf{Z}/\mathbf{Z};$$

but $H^2(L/K, C_L)_{\mathrm{reg}}$ is a subgroup of $H^2(L/K, C_L)$ which has order dividing n. So it is the whole of $H^2(L/K, C_L)$. Letting $L \to \bar{K}$ we see that

$$H^2(L/K, C_{\bar{K}})_{\mathrm{reg}} = H^2(L, C_{\bar{K}}).$$

Thus we can remove the subscripts "reg" from our diagram (9).

Also, we have proved the following

RESULT. *$H^2(L/K, C_L)$ is cyclic of order n, and it has a canonical generator $u_{L/K}$ with invariant $\frac{1}{n}$, i.e.* $\mathrm{inv}_1\,(u_{L/K}) = \frac{1}{n}$.

This element $u_{L/K}$ is called the *fundamental class* of the extension L/K. It was first exhibited by Weil (see the discussion in 11.6 below). The complete determination of the structure of $H^2(L/K, C_L)$ is due to Nakayama. He and Hochschild were the first to give a systematic cohomological treatment of class field theory; see G. Hochschild and T. Nakayama "Cohomology in Class Field Theory", *Annals*, 1952, and the references contained therein.

The two lower layers of diagram (9) and the vertical arrows between them make sense for an arbitrary finite separable extension L/K of finite degree n, and in this more general case, that much of the diagram is still commutative, because the argument showing the commutativity of (7) did not require L/K to be Galois. Using this, and replacing L by K', we see that if $L \supset K' \supset K$ with L/K Galois, then restricting $u_{L/K}$ from L/K to L/K' gives the fundamental class $u_{L/K'}$.

11.3. *Applications*. The results we have obtained show that the idèle classes constitute a class formation. In particular (cf. Chapter IV, § 10) the cup product with the fundamental class $u_{L/K}$ gives isomorphisms

$$\hat{H}^r(G(L/K), \mathbf{Z}) \xrightarrow{\sim} \hat{H}^{r+2}(G(L/K), C_L),$$

for $-\infty < r < \infty$, such that for $L \supset K' \supset K$ with L/K' Galois the diagrams

$$(12)\qquad \begin{tikzcd} \hat{H}^r(G, \mathbf{Z}) \arrow[r, "\sim"] \arrow[d, "\mathrm{res}"'] & \hat{H}^{r+2}(G, C_L) \arrow[d, "\mathrm{res}"'] \\ \hat{H}^r(G', \mathbf{Z}) \arrow[r, "\sim"] & \hat{H}^{r+2}(G', C_L) \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \hat{H}^r(G, \mathbf{Z}) \arrow[r, "\sim"] & \hat{H}^{r+2}(G, C_L) \\ \hat{H}^r(G', \mathbf{Z}) \arrow[r, "\sim"] \arrow[u, "\mathrm{cor}"] & \hat{H}^{r+2}(G', C_L) \arrow[u, "\mathrm{cor}"] \end{tikzcd}$$

are commutative, where $G = G(L/K)$ and $G' = G(L/K')$.

Case $r = -2$. There is a canonical isomorphism (see Chapter IV, § 3)

$$G(L/K)^{\mathrm{ab}} \to C_K/N_{L/K}C_L,$$

which is inverse to the Artin map. Using this as a *definition* in the local case, Serre deduced the formula $\mathrm{inv}\,(\bar{a}\,.\,\delta\chi) = \chi(\theta(a))$ in Chapter VI, § 2.3; we have proved the formula in the global case, so one can reverse the argument. (The isomorphism $G^{\mathrm{ab}} \simeq H^{-2}(G, \mathbf{Z})$ is to be chosen in such a manner that for $\chi \in \mathrm{Hom}\,(G, \mathbf{Q}/\mathbf{Z}) \simeq H^1(G, \mathbf{Q}/\mathbf{Z})$ and $\sigma \in G$, we have $\chi\,.\,\sigma = \chi(\sigma)$ upon identifying $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ with $H^{-1}(G, \mathbf{Q}/\mathbf{Z})$ as usual.)

Reversing the horizontal arrows in (12), with $r = -2$, and letting $L \to \bar{K}$, we obtain the commutative diagrams

$$(13)\qquad \begin{tikzcd} C_K \arrow[r, "\psi"] \arrow[d, "\mathrm{con}"'] & G(K^{\mathrm{ab}}/K) \arrow[d, "V"] \\ C_{K'} \arrow[r, "\psi'"] & G((K')^{\mathrm{ab}}/K') \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} C_K \arrow[r, "\psi"] & G(K^{\mathrm{ab}}/K) \\ C_{K'} \arrow[r, "\psi'"] \arrow[u, "N"] & G((K')^{\mathrm{ab}}/K') \arrow[u] \end{tikzcd},$$

where the ψ's are the Artin maps and V is the "Verlagerung†". The right-hand

† Called the "transfer" in Chapter IV, § 6, *Note* after Prop. 7.

diagram expresses the so-called *translation theorem*, and in fact results also directly from 4.3, which in turn came from an almost obvious property 3.2 of the Frobenius automorphisms $F(v)$. The commutativity of the left-hand diagram (13) can also be proved by a straightforward but somewhat more complicated computation with the Frobenius automorphisms which was first made by Artin in connection with the "principal ideal theorem" (see exercise 3, and Serre, "Corps Locaux", p. 130).

Case $r = -3$. This leads to an isomorphism used by Roquette in Chapter IX, § 2.

11.4. *Application to the Cohomology of* L^*. The general idea is to determine the cohomology of L^* from a knowledge of the cohomology of the idèles and the idèle classes.

Let L/K be a finite extension, with Galois group G. Then the exact sequence $0 \to L^* \to J_L \to C_L \to 0$ gives an exact sequence

$$\to \hat{H}^{r-1}(G, J_L) \xrightarrow{g} \hat{H}^{r-1}(G, C_L) \to \hat{H}^r(G, L^*) \xrightarrow{f} \hat{H}^r(G, J_L) \to \dots$$

in which the kernel of f is isomorphic to the cokernel of g. We know

$$\hat{H}^{r-1}(G, J_L) = \coprod_{v \in \mathfrak{M}_K} \hat{H}^{r-1}(G^v, L^{v*}) = \coprod_{v \in \mathfrak{M}_K} \hat{H}^{r-3}(G^v, \mathbf{Z}).$$

(see Proposition 7.3), and

$$\hat{H}^{r-1}(G, C_L) = \hat{H}^{r-3}(G, \mathbf{Z});$$

so the kernel of

$$f : \hat{H}^r(G, L^*) \to \coprod \hat{H}^r(G^v, L^{v*})$$

is isomorphic to the cokernel of

$$g_1 : \coprod \hat{H}^{r-3}(G^v, \mathbf{Z}) \to \hat{H}^{r-3}(G, \mathbf{Z}).$$

It is easy to see that the map g_1 is given by

$$g_1\left(\sum_v z_v\right) = \sum_v \operatorname{cor}_G^{G_v} z_v.$$

Using the fundamental duality theorem in the cohomology of finite groups, which states that the cup product pairing

$$\hat{H}^r(G, \mathbf{Z}) \times \hat{H}^{-r}(G, \mathbf{Z}) \to \hat{H}^0(G, \mathbf{Z}) \approx \mathbf{Z}/n\mathbf{Z}$$

is a perfect duality of finite groups, one sees that the cokernel of g_1 is the dual of the kernel of the map

$$h : \hat{H}^{3-r}(G, \mathbf{Z}) \to \prod_v \hat{H}^{3-r}(G^v, \mathbf{Z})$$

which is defined by $(h(z))_v = \operatorname{res}_{G_v}^{G}(z)$ for all $v \in \mathfrak{M}_K$.

Case $r = 0$.

$$\operatorname{Ker} f = \left(\frac{a \mid a \in K^*, \ a \text{ is a local norm everywhere}}{a \mid a \in K^*, \ a \text{ is a global norm}}\right),$$

and coker g is dual to $\ker\left(H^3(G, \mathbf{Z}) \xrightarrow{\text{res}} \prod_v H^3(G^v, \mathbf{Z})\right)$. For example, if $G = G^v$ for some v, then this is an injection, so local norms are global norms. If G is cyclic, then $H^3(G, \mathbf{Z}) \approx H^1(G, \mathbf{Z}) = 0$, so local norms are global norms and we recover Hasse's theorem, 9.6. On the other hand, if for instance G is the Vierergruppe, it is possible that G^v is always one of the subgroups of order 2, so $\hat{H}^3(G^v, \mathbf{Z}) = 0$ but $H^3(G, \mathbf{Z}) = \mathbf{Z}/2\mathbf{Z}$. Explicitly, we can consider $\mathbf{Q}(\sqrt{13}, \sqrt{17})/\mathbf{Q}$; here $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1$, and the extension is unramified at 2 because $13 \equiv 17 \equiv 1 \pmod 4$, so all the decomposition groups are cyclic. Thus the set of elements of K^* which are local norms everywhere is not the same as the set of elements of K^* which are global norms (see exercise 5).

Case $r = 3$. $H^3(G, L^*)$ is cyclic of order n/n_0, the global degree divided by the lowest common multiple of the local degrees, generated by $\delta u_{L/K}$ ($\delta : H^2(C_L) \to H^3(L^*)$), the "Teichmüller 3-class". This can be killed by inflation (replace L by a bigger L' so that the n_0 for L' is divisible by n); so $H^3(\bar{K}/K, \bar{K}^*) = 0$.

For a more precise description of the situation, announced at the Amsterdam Congress (*Proc.* II,66-67), see Tate: "The cohomology groups of tori in finite galois extensions of number fields", *Nagoya Math. J.* 27 (1966), 709–719.

Group Extensions. Consider extensions $M/L/K$, where L/K is Galois with group G, and M/K is Galois with group E and M is a class field over L with abelian Galois group A. So $1 \to A \to E \to G \to 1$ is exact. By the Artin isomorphism $A \simeq C_L/N_{M/L}C_M$ (see Theorem A of 10.2 and Consequence 9.4). We want to know about E.

11.5. THEOREM. (i) *Let* $\sigma \in E$ *have image* $\bar{\sigma} \in G$. *Let* $x \in C_L$; *then* $\psi(\bar{\sigma}x) = \sigma\psi(x)\sigma^{-1}$, *where* ψ: $C_L \to A$ *is the Artin map.*

(ii) *Let* $v \in H^2(G, A)$ *be the class of the group extension* E; *then* $v = \psi_*(u_{L/K})$, *where* ψ_* *is the map:* $H^2(G, C_L) \to H^2(G, A)$ *induced by* $\psi : C_L \to A$, *and where* $u_{L/K}$ *is the fundamental class for* L/K.

It is straightforward to see (i). As usual in such cases the situation becomes clearer if we consider an arbitrary field isomorphism $\sigma : M \to M'$ rather than an automorphism. Denoting σL by L' and the restriction of σ to L by $\bar{\sigma}$, we have the picture

$$\begin{tikzcd} M \arrow[r, "\sigma"] \arrow[d, dash] & M' \arrow[d, dash] \\ L \arrow[r, "\bar{\sigma}"] & L' \end{tikzcd},$$

and by transporting the structure of M/L to M'/L' we see that, if $x \in C_L$ and $y \in M$, then $(\psi'(\bar{\sigma}x))(\sigma y) = \sigma(\psi(x)(y))$.

(ii) is non-trivial; Šafarevič did the local case ("On Galois Groups of P-adic Fields", *Doklady*, 1946), but it is really a general theorem about class formations (see Artin-Tate notes, p. 246). We do not prove it here, and will not make any use of the result in these notes.

11.6. Before the structure of $H^2(G, C_L)$ was known, Weil ("Sur la Théorie du Corps de Classes", *J. Math. Soc. Japan*, **3** (1951), 1–35) looked at this situation from the opposite point of view. Taking M to be L^{ab}, the maximal abelian extension of K (so that now $A = G(L^{\text{ab}}/L)$ is a profinite abelian group), Weil asked himself whether there was a group extension $\mathscr{E}$ of $G = G(L/K)$ by C_L which fits into a commutative diagram of the sort

$$\begin{tikzcd}
1 \arrow[r] & C_L \arrow[r] \arrow[d, "\psi_L"] & \mathscr{E} \arrow[r] \arrow[d, "W"] & G \arrow[r] \arrow[d, "\text{id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1,
\end{tikzcd} \tag{14}$$

where $E = G(L^{\text{ab}}/K)$, and if so, to what extent was it unique? In the function field case, ψ_L is for all practical purposes an isomorphism, and the existence of such a diagram is obvious. Moreover, in that case, the group-theoretical transfer map V (Verlagerung) from $\mathscr{E}$ to C_L (which has its image in C_K) gives a commutative diagram

$$\begin{tikzcd}
\mathscr{E} \arrow[r, "V"] \arrow[d, "W"'] & C_K \subset C_L \arrow[d, "\psi_K"] \\
E \arrow[r] & E^{\text{ab}},
\end{tikzcd} \tag{15}$$

as follows from the commutativity of the left-hand diagram (13). Inspired by the case of function fields, Weil proved that also in the number field case a diagram (14) did indeed exist, and was essentially uniquely determined by the condition that (15) (together with its analogues when K is replaced by an arbitrary intermediate field K' between K and L) should be commutative. In particular, the class $u \in H^2(G, C_L)$ of such an extension $\mathscr{E}$ was unique, and that is the way the fundamental class was discovered.

Nowadays one can proceed more directly, simply constructing $\mathscr{E}$ as a group extension of G by C_L corresponding to the fundamental class $u_{L/K}$, and interpreting the unicity as reflecting the fact that $H^1(G, C_L) = 0$ (cf. Artin-Tate, Ch. 14).

The kernel of the map $W: \mathscr{E} \to E$ is the connected component D_L of C_L. As Weil remarks, the search for a Galois-like interpretation of $\mathscr{E}$ (or even a "natural" construction, without recourse to factor systems, of a group $\mathscr{E}$ furnished with a "natural" map $W: \mathscr{E} \to E$) seems to be one of the fundamental problems of number theory.

In support of the idea that $\mathscr{E}$ behaves like a Galois group, Weil also describes how to attach L-series to characters χ of unitary representations of $\mathscr{E}$. These L-series of Weil generalize simultaneously Hecke's L-series "mit Grössencharakteren" (which are obtained from representations which factor through C_K via the arrow V in (15)) and Artin's "non-abelian" L-series (which are obtained from representations which factor through E, or in particular through $G \simeq E/A$, via the arrow W in (15)). (The intersection of Hecke's and Artin's L-series are those of Weber obtained from representations of $E^{\text{ab}} \simeq C_K/D_K$, i.e. from ordinary congruence characters.) Using Brauer's theorem on group characters, Weil shows that his L-series can be expressed as products of (positive or negative) integral powers of Hecke L-series, and are therefore meromorphic.

12. Proof of the Existence Theorem

We still have to prove the Existence Theorem (D) of 5.1. Our proof, more traditional than that used by Serre in Chapter VI, works just as well in the local case.

If H is an open subgroup of C_K of finite index $[C_K : H]$, we say temporarily that H is *normic* if and only if there is an abelian extension L/K such that $H = N_{L/K} C_L$. The existence theorem asserts that every open subgroup H of finite index in C_K is normic. (We have already shown that if L/K is abelian, then $N_{L/K} C_L$ is an open subgroup of C_K of finite index; in fact the normic subgroups are just the inverse images of the open subgroups of $G(K^{\text{ab}}/K)$ under the Artin map $\psi_k: C_K \to G(K^{\text{ab}}/K)$.)

Ψ_K

First, two obvious remarks: If $H_1 \supset H$, and H is normic, then H_1 is normic (the field L corresponding to H has a subfield L_1 corresponding to H_1). If H_1, H_2 are normic, so is $H_1 \cap H_2$ (take as the field the compositum $L_1 L_2$).

Next, we go to 9.5 in order to prove

KEY LEMMA. *Let n be a prime, and K a field not of characteristic n containing the n-th roots of unity. Then every open subgroup H of index n in C_K is normic.*

Proof. In fact, suppose H is open in C_K with $[C_K : H] = n$. Let H' be the inverse image of H in J_K. Then H' is open in J_K, so there is a finite set $S \subset \mathfrak{M}_K$ such that $H' \supset \prod_{v \in S} (1) \times \prod_{v \notin S} U_v = U^S$. Furthermore, H is of index n in C_K, so $H' \supset J_K^n$. Therefore $H' \supset \prod_{v \in S} K_v^{*n} \times \prod_{v \notin S} U_v = E$, say. *
Thus $H = H'/K^* \supset EK^*/K^*$, and from consequence 9.5, it follows that H is normic.

If L is an extension of K, there is a norm map $N: C_L \to C_K$; conversely, if we start with $H \subset C_K$ we get a subgroup $N^{-1}(H) \subset C_L$.

LEMMA. *If L/K is cyclic and $H \subset C_K$, and if $N_{L/K}^{-1}(H) \subset C_L$ is normic for L, then H is normic for K.*

Proof. Write H' for $N_{L/K}^{-1}(H)$ and let M/L be the class field of H'. We claim that M is abelian over K, and $N_{M/K}C_M \subset H$, so H is normic. That $N_{M/K}C_M \subset H$ is clear, since N is transitive; the difficulty is to show that M/K is abelian.

(In point of fact, if something is the norm group from a non-abelian extension, then it is already the norm group from the maximal abelian subextension (see exercise 8). But this has not been proved here—if it had, we would not need L/K to be cyclic, and we would be already finished with the proof of the lemma.)

M/K is a Galois extension since H' is invariant under $G(L/K)$. The Galois group E of M/K is a group extension, $0 \to A \to E \to G \to 1$; since $E/A \simeq G$ is cyclic, it is enough to show that $A = G(M/L)$ is in the centre of E.

We can use the first part of Theorem 11.5. Let ψ be the Artin map $C_L \to A$. To show that A is in the centre, it is enough to check that

$$\psi(x) = \sigma\psi(x)\sigma^{-1} = \psi(\sigma x)$$

for all $x \in C_L$ and $\sigma \in E$. Now $\psi : C_L \to A$ has kernel H', so we want to check that $\sigma x/x \in H'$, which is clear since $N(\sigma x/x) = 1$.

Proof of the Theorem. (In the function field case we can only treat the case in which the index is prime to the characteristic; for the general case, see Artin-Tate, p. 78.)

We use induction on the index of H. If the index is 1 everything is clear. Now let n be a prime dividing the index. Adjoin the n-th roots of unity to K to get K', and replace H by $H' = N_{K'/K}^{-1}(H)$. By the last lemma, it suffices to consider H'. The index of H' divides the index of H; we can assume $(C_{K'} : H') = (C_K : H)$, otherwise H' is normic by induction hypothesis.

So n divides $(C_{K'} : H')$. Take H_1' so that $H_1' \supset H'$and $(C_{K'} : H_1') = n$. By the above Key Lemma, H_1' is normic. Let L be its class field, i.e. $H_1' = N_{L/K'}C_L$. Put $H'' = N_{L/K'}^{-1}(H')$. Then

$$[C_L : H''] < [C_{K'} : H'] = [C_K : H].$$

(For $C_L/H'' \xrightarrow{N_{L/K'}} C_{K'}/H'$ is an injection, whose image is H_1'/H', properly contained in $C_{K'}/H'$.)

Hence H'' is normic by induction hypothesis; L/K' is cyclic, so we can apply the above lemma again; so H' is normic.

LIST OF SYMBOLS

The numbering refers to the section of this Chapter where the symbol was first used.

Note (i) $[A]$ is the cardinality of the set A.
(ii) "$\supset$" denotes inclusion with the possibility of equality.

1.1. K, K^* (non-zero elements of K)
$G(L/K)$, G
$v, v_1 \ldots; w, w_1, \ldots$
$\mathfrak{O}_v$, $\mathfrak{O}_w$
$\mathfrak{P}_v$
K_v, L_w
G_w

1.2. $\mathfrak{M}_K$

2.1. $k(v)$
Nv

2.2. $F_{L/K}(v)$
S

3.1. I^S

3.2. $N_{K'/K}$
$(a)^S$

4. J_K, J_K^S
$(x)^S$

4.1. ψ
C_K
$(x)_S$
U^S

4.2. $\psi_{L/K}$
$\operatorname{Im} \psi$

5.1. Norm group

5.5. $\hat{\mathbf{Z}}$

5.7. $\mathbf{Q}^{\mathrm{mc}}$, $\mathbf{R}_+^*$

6.1. ψ_v

7.1. w/v, $\prod\limits_{w/v}$

7.2. G^v
L^v

7.3. $\coprod$
$J_{K,S}$, $S \subset \mathfrak{M}_K$
$J_{L,S}$, $S \subset \mathfrak{M}_K$
N_v

8.1. $h(G, A)$, $h(A)$
S-units $= K_S$

9.1. Conorm = Con

9.7. inv_v
inv_v (infl)
inv_v (res)
inv_v (cor)
Br (K)

10.1. θ_v, θ Artin maps.

10.3. ., cup-product
G^{ab}