MATHEMATIK DEPARTEMENT ETH ZÜRICH UND
FORSCHUNGSINSTITUT FÜR MATHEMATIK ETH ZÜRICH

Ramaiyengar Sridharan
Chennai Mathematical Institute

2- Torsion in Brauer Groups: A Theorem of Merkurjev

Nachdiplomvorlesung gehalten während
des Wintersemesters 1984-85

in collaboration with

Raman Parimala
Tata Institute of Fundamental Research Bombay

These notes grew out of a Nachdiplomvorlesung" at the ETHZ during Winter 1984-85. We present here a self-contained proof of a theorem of Merkurjev on the 2-torsion of the Brauer group. The paper of Wadsworth entitled Merkurjev's elementary proof of Merkurjev's theorem" served as the main source. To make the notes selfcontained, we have included Kato's proof of the existence of transfer for K_2 of fields and a proof of a theorem of Rosset-Tate on Milnor functors (both avoid the use of Quillen's K-theory). A possible justification for the existence of these notes is the hope that it may be accessible to students with a background in basic algebra.

It is a great pleasure to thank the Forschungsinstitut für Mathematik for its hospitality, and Prof. Eckmann for his kind invitation. We are greatful to Knus, without whose (gentle) persuasion, neither the lectures nor the notes would have existed. We thank Nicollier for his patience in preparing the first draft of the notes, and Frau Aquilino for her excellent typing.

R. Parimala parimala@math.tifr.res.in
http://www.tifr.res.in

R. Sridharan sridhar@cmi.ac.in
http://www.cmi.ac.in

References

1) A.A. Albert: Structure of Algebras, Amer. Math. Soc., Colloqu. Publ. (1939)

2) C. Chevalley: Introduction to the Theory of Algebraic Functions of One Variable, Amer. Math. Soc., Math. Surveys and Monographs, (1951)

3) J.-P. Serre: Corps Locaux, Hermann, Paris, (1962)

4) A.R. Wadsworth: Merkurjev's elementary proof of Merkurjev's theorem, Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983), 741–776, Contemp. Math., 55, Amer. Math. Soc., Providence, R.I., 1986.

5) O. Zariski and P. Samuel: Commutative Algebra, Vol. I + II, Van Nostrand, Princeton, (1958)

Contents

Chapter I: The Brauer group of a field

§ 1. Central simple algebras and Brauer groups

Let K be a field. Let $M_n(K)$ denote the algebra of $n \times n$-matrices with entries in K. We call an algebra A over K a *form* or a *descent* over K of the matrix algebra if for some field extension L/K, $L \otimes_K A \xrightarrow{\sim} M_n(L)$. The algebra $M_n(K)$ has trivially this property. We are interested in the study of nontrivial forms for the matrix algebra. We call an algebra A over K *central* if the centre of A is K, and *simple* if $[A : K] < \infty$ and the only two-sided ideals of A are 0 and A. We shall show that the forms for the matrix algebra are precisely central simple algebras.

Lemma 1.1. *Let A be a central simple algebra over K and B a K-algebra whose only two-sided ideals are 0 and B. Then the only two-sided ideals of $A \otimes_K B$ are 0 and $A \otimes_K B$.*

Proof. By Wedderburn's theorem, $A \xrightarrow{\sim} M_r(D)$, D a division ring, and centre D = centre $M_r(D)$ = centre $A = K$. Since every two-sided ideal of $M_r(D \otimes_K B)$ comes from a two-sided ideal of $D \otimes_K B$, we replace A by D and assume that A is a finite dimensional central division algebra over K. Let $\mathcal{A} \neq 0$ be a two-sided ideal of $A \otimes_K B$. Let $\{e_i\}_{i \in I}$ be a K-basis for B. Every element $a \in \mathcal{A}$, $a \neq 0$, can be uniquely written as $\sum_{i \in J} a_i \otimes e_i$, $J \subset I$, $a_i \in A$. We call $\ell(a) = |J|$. We choose $a \in \mathcal{A}$ with $\ell(a)$ minimal. Replacing a by $(a_{j_o}^{-1} \otimes 1)a$, for some $j_o \in J$, we may assume $a_{j_o} = 1$. For any $d \in A$, $a' = (d \otimes 1)a - a(d \otimes 1) = \sum (da_i - a_i d) \otimes e_i \in \mathcal{A}$ and $\ell(a') < \ell(a)$, a_{j_o} being 1, unless $a' = 0$. Since $\ell(a)$ is minimal, $a' = 0 \Rightarrow da_i = a_i d$ for all $i \in J \Rightarrow a_i \in K$ for all $i \in J \Rightarrow a \in \mathcal{A} \cap 1 \otimes B$. Since B is simple, $\mathcal{A} \cap (1 \otimes B) = 1 \otimes B \Rightarrow 1 \otimes 1 \in \mathcal{A} \Rightarrow \mathcal{A} = A \otimes_K B$. □

Lemma 1.2. *Let A and B be K-algebras, then* centre $(A \otimes_K B) =$
$=$ centre $A \otimes_K$ centre B.

Proof. Clearly, centre $A \otimes_K$ centre $B \subset$ centre $(A \otimes_K B)$. Let $x \in$ centre $(A \otimes_K B)$. Write $x = \sum_i e_i \otimes b_i$, $\{e_i\}_{i \in I}$ a basis of A over K, the condition $(1 \otimes b)x = x(1 \otimes b)$ for all $b \in B$ implies, by the linear independence of $\{e_i\}$, that $bb_i = b_i b$ for all $b \in B$. Thus centre $(A \otimes_K B) \subset A \otimes_K$ centre B. Similarly, centre $(A \otimes_K B)$centre $A \otimes_K B$ so that centre $(A \otimes_K B) \subset (A \otimes_K$ centre $B) \cap$ (centre $A \otimes_K B) \subset$ centre $A \otimes_K$ centre B. □

Proposition 1.3. *If A and B are central simple algebras over K, then $A \otimes_K B$ is a central simple algebra over K.*

Proof. Immediate from Lemma **1.1.** and Lemma **1.2.**. □

Proposition 1.4. *The following are equivalent.*

1) *A is a central simple algebra over K.*

2) *A is form over K for the matrix algebra.*

Proof. Let A be a form over K for the matrix algebra and let L be a field extension of K such that $L \otimes_K A \xrightarrow{\sim} M_n(L)$. Then $[A : K] = [M_n(L) : L] = n^2$. By Lemma **1.2.**,

$$\text{centre}\,(L \otimes_K A) = L \otimes_K \text{centre}\, A = \text{centre}\, M_n(L) = L.$$

Thus $[\text{centre}\, A : K] = [L \otimes_K \text{centre}\, A : L] = 1$ and $\text{centre}\, A = K$. If $\mathcal{A} \neq 0$ is a two-sided ideal of A, then $L \otimes_K \mathcal{A} \neq 0$ is a two-sided ideal of $L \otimes_K A \xrightarrow{\sim} M_n(L)$. Since $M_n(L)$ is simple we must have $L \otimes_K \mathcal{A} = L \otimes_K A$; hence $\mathcal{A} = A$. Suppose now that A is a central simple algebra over K. Let $\overline{K}$ denote the algebraic closure of K. By Lemma **1.1.** and Lemma **1.2.**, $\overline{K} \otimes_K A$ is central simple over $\overline{K}$. Since the only finite dimensional division algebra over an algebraically closed field is itself, it follows, by Wedderburn's theorem, that $\overline{K} \otimes_K A \xrightarrow{\sim} M_n(\overline{K})$. □

Let A be a central simple algebra over K. An extension L/K of fields is called a *splitting field* for A if $L \otimes_K A \xrightarrow{\sim} M_n(L)$. Proposition **1.4.** asserts that every central simple algebra admits of a splitting field. In fact, we have the following

Proposition 1.5. *Every central simple algebra A over K admits of a splitting field L which is a finite extension of K.*

Proof. Let $\overline{K}$ denote the algebraic closure of K and $\varphi : \overline{K} \otimes_K A \xrightarrow{\sim} M_n(\overline{K})$ be an isomorphism of $\overline{K}$-algebras. If $\{e_i\}$, $1 \leq i \leq n^2$ is a K-basis of A and $\varphi(1 \otimes e_i) = \sum_{j,k} \lambda_{ijk} e_{jk}$, $\{e_{jk}\}$, $1 \leq j, k \leq n$ denoting the standard basis of $M_n(\overline{K})$, we set $L = K(\lambda_{ijk})$, $1 \leq i \leq n^2$, $1 \leq j,\ k \leq n$. Then φ induces an L-algebra homomorphism $\tilde{\varphi} : L \otimes_K A \to M_n(L)$. Since $L \otimes_K A$ is simple, $\tilde{\varphi}$ is injective. Since $n^2 = [A : K] = [M_n(L) : L]$, $\tilde{\varphi}$ is an isomorphism. □

The isomorphism classes of central simple algebras over K form a set which we denote by S. The set S is a commutative monoid, with tensor product over K as the operation, and the class of K as the identity element. We introduce an equivalence relation on S as follows. If A is a central simple algebra over K, $A \xrightarrow{\sim} M_r(D_A)$ where D_A is a central division algebra over K, whose isomorphism class is uniquely determined by A. We define $A \sim B$ *(Brauer equivalent)* if and only if $D_A \xrightarrow{\sim} D_B$. We denote by $[A]$, the class of A in $S/_\sim$. We note that if A is Brauer equivalent to B and $[A : K] = [B : K]$, then A is isomorphic to B. Two algebras A and B are Brauer equivalent if and only if $M_r(A) \xrightarrow{\sim} M_s(B)$ for some integers r and s.

The equivalence relation on S is compatible with the monoid structure on S, i.e. $A \sim A', B \sim B' \Rightarrow A \otimes_K B \sim A' \otimes_K B'$. Thus the set $S/_\sim$ is again a commutative

monoid under the operation induced by tensor product over K. We use multiplicative notation for this operation. The identity element is the class of all matrix algebras over K. The following proposition shows that $S/_\sim$ is in fact a group.

Proposition 1.6. *For a central simple algebra A over K, if A^{op} denotes the opposite algebra, then A^{op} is central simple and $[A][A^{\mathrm{op}}] = [K]$ in $S/_\sim$.*

Proof. If A is central simple, clearly A^{op} is again central simple. The maps $A \to \mathrm{End}_K A$, $a \mapsto L_a$ and $A^{\mathrm{op}} \to \mathrm{End}_K A$, $a \mapsto R_a$, L_a, R_a denoting the left and right multiplications, induce a homomorphism $\varphi : A \otimes_K A^{\mathrm{op}} \to \mathrm{End}_K A$, since $L_a \circ R_b = R_b \circ L_a$, $a, b \in A$. Since $A \otimes_K A^{\mathrm{op}}$ is simple (**1.1.**), φ is injective. Further $[A \otimes_K A^{\mathrm{op}} : K] = [A : K]^2 = [\mathrm{End}_K A : K]$ so that φ is surjective and hence an isomorphism. For a choice of basis of A over K, $\mathrm{End}_K A$ is isomorphic to a matrix algebra over K. □

The group $S/_\sim$ is called the *Brauer group of* K, denoted by $\mathrm{Br}(K)$. The assignment $A \mapsto D_A$ yields a bijection between $\mathrm{Br}(K)$ and the set of isomorphism classes of central division algebras over K. Thus the Brauer group classifies finite dimensional central division algebras over K. If K is an algebraically closed field, then $\mathrm{Br}(K)$ is trivial, since the only finite dimensional division algebra over K is itself. If $K = \mathbb{R}$, the field of real numbers, a classical theorem of Frobenius asserts that $\mathrm{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$, the nontrivial class being the class of the real quaternion algebra $\mathbb{H}$. If K is a finite field, in view of a celebrated theorem of Wedderburn, $\mathrm{Br}(K)$ is trivial.

The assignment $K \mapsto \mathrm{Br}(K)$ is functorial. In fact, if $K \hookrightarrow L$ is an injection of fields, we have an induced functorial homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$ defined by $[A] \to [L \otimes_K A]$. We conclude this section by recording a proposition which will be needed later.

Proposition 1.7. *Let $K(X)$ denote the rational function field in the variable X. The inclusion $K \hookrightarrow K(X)$ induces an injection $\mathrm{Br}(K) \hookrightarrow \mathrm{Br}(K(X))$.*

Proof. Let A be a central simple algebra over K such that $K(X) \otimes_K A$ is isomorphic to a matrix algebra over $K(X)$. Let $\varphi : K(X) \otimes_K A \xrightarrow{\sim} M_n(K(X))$ be an isomorphism of $K(X)$-algebras. If K is finite, $\mathrm{Br}(K)$ is trivial so that $A \xrightarrow{\sim} M_n(K)$. Suppose K infinite. Let $\{e_i\}$, $1 \leq i \leq n^2$ be a basis of A over K and let $\varphi(1 \otimes e_i) = \sum_{j,k} \lambda_{ijk} e_{jk}$, $\{e_{jk}\}$, $1 \leq j, k \leq n$, denoting the matrix units in $M_n(K(X))$, $\lambda_{ijk} \in K(X)$. Let $f \in K[X]$ be such that $f \cdot \lambda_{ijk} \in K[X]$ for all i, j and k. Then φ induces a $K[X, 1/f]$-algebra homomorphism $\tilde{\varphi} : K[X, 1/f] \otimes_K A \to M_n(K[X, 1/f])$. Since K is infinite, we can choose $\alpha \in K$ such that $f(\alpha) \neq 0$. Specialising $\tilde{\varphi}$ at α yields a K-algebra homomorphism $A \to M_n(K)$ which is necessarily an isomorphism, since A is central simple over K of dimension n^2. □

§ 2. Existence of Galois splitting fields

We begin with the following two theorems which show how a simple subalgebra sits inside a central simple algebra. The proofs may be found, for example, in the book of Albert.

Theorem 2.1. *Let A be a central simple K-algebra and B a simple subalgebra. Then the commutant $B' = \{a \in A \mid ab = ba \ \forall b \in B\}$ of B is again simple and $[B : K][B' : K] = [A : K]$.*

Theorem 2.2. *Let B be a simple subalgebra of a central simple algebra A. If $\psi : B \to A$ is a K-algebra homomorphism, there exists a unit u of A such that $\psi(x) = uxu^{-1}$ for all $x \in B$. In particular, ψ extends to an inner automorphism of A.*

We call a commutative subring B of A, *a maximal commutative subring* if B is not properly contained in any commutative subring of A. We derive from Theorem **2.1.** the following

Corollary 2.3. *Let L be a subfield of a central simple algebra A over K. Then L is a maximal commutative subring of A if and only if $[A : K] = [L : K]^2$. In particular, a subfield L of a central division algebra D over K is a maximal commutative subfield if and only if $[D : K] = [L : K]^2$.*

Proposition 2.4. *Let A be a central simple algebra over K and L a subfield of A which is a maximal commutative subring. Then L is a splitting field for A.*

Proof. We regard A as the bimodule ${}_AA_L$. The mapping $A \to \mathrm{End}_L A$ given by $a \mapsto L_a$ and mapping $L \to \mathrm{End}_L A$ given by $x \mapsto R_x$ commute to yield an induced homomorphism $\varphi : L \otimes_K A \to \mathrm{End}_L A$. Since the field L is a maximal commutative subring of A, $[L : K]^2 = [A : K] = [A : L][L : K] = n^2$ so that $[L \otimes_K A : L] = n^2 = [\mathrm{End}_L A : L]$. Since $L \otimes_K A$ is central simple over L, φ is indeed an isomorphism. The algebra $\mathrm{End}_L A$ may be identified with $M_n(L)$ through a choice of an L-basis for A. □

Lemma 2.5. *If L is a splitting field for a central simple algebra A over K, then L is a splitting field for A^{op} and for any B Brauer equivalent to A.*

Proof. Let $\varphi : L \otimes A \xrightarrow{\sim} M_n(L)$ be an isomorphism of L-algebras. Then $L \otimes_K A^{\mathrm{op}} \xrightarrow{\sim} (L \otimes A)^{\mathrm{op}} \xrightarrow{\sim} M_n(L)^{\mathrm{op}} \xrightarrow{\sim} M_n(L)$, the last isomorphism being given by matrix transposition. The second assertion follows from the fact that L splits A if and only if L splits D_A. □

In view of Lemma **2.5.**, it makes sense to talk of the splitting field of Brauer class.

Proposition 2.6. *Let A be a central simple algebra over K and L a finite extension of K. Then L is a splitting field for A if and only if there exists a central simple algebra B, Brauer equivalent to A, which contains L as a maximal commutative subring. The algebra B is unique up to isomorphism.*

Proof. If B, B' are two central simple algebras Brauer equivalent to A and both of which contain the field L as a maximal commutative subring, then $[B : K] = [L : K]^2 = [B' : K]$ (see **2.3.**). Thus B and B' are two Brauer equivalent central simple K-algebras of the same rank and hence isomorphic (see after **1.5.**) This proves the uniqueness of B up to isomorphism. Let $B \sim A$ contain L as a maximal commutative subring. Then L splits B by **2.4.** and hence L splits A by **2.5.**.

Suppose A is a central simple algebra over K, split by a finite extension L over K. We may assume without loss of generality, that $A = D$ is a division algebra over K. Since L also splits D^{op}, we have an isomorphism $\varphi : L \otimes_K D^{\mathrm{op}} \xrightarrow{\sim} M_n(L)$. We regard L^n as a bimodule ${}_L L^n_D$ through φ. Let m be the dimension of L^n regarded as a right vector space over D. Then we have an injection $L \hookrightarrow \mathrm{End}_D L^n \xrightarrow{\sim} M_m(D)$. Thus $B = M_m(D)$ is a central simple algebra over K, Brauer equivalent to D, containing L as a subfield. We have $mn^2 = [L^n : D][D : K] = [L^n : K] = n[L : K]$ so that $[L : K] = mn$. Further $[M_m(D) : K] = m^2n^2$. In view of **2.3.**, L is a maximal commutative subring of $M_m(D)$. □

For a central simple algebra A over K, we define *degree* $A = n$ if $[A : K] = n^2$ and *index* $A =$ degree D_A. We note that index A divides degree A.

Corollary 2.7. *Let L be a finite extension of K which splits A. Then* index A *divides* $[L : K]$.

Proof. Let $B \sim A$ contain L as a maximal commutative subring (**2.6.**). Then index $A =$ index $B \mid$ degree $B = [L : K]$. □

Theorem 2.8. *Let D be a central division algebra over K. Then there exists a maximal commutative subfield L of D which is separable over K.*

Proof. Let $[D : K] = n^2$. We prove the theorem by induction on n, the theorem being trivial for $n = 1$. Assume first that D contains an element $c \neq K$, which is not purely inseparable over K. Let $L \neq K$ be a subfield of $K(c)$, containing K and separable over K. If L is a maximal commutative subfield of D, we are through. Otherwise, let D' denote the commutant of L in D. Then, by **2.1.**, D' is a central division algebra over L whose dimension is strictly less than n^2. By induction assumption, D' contains a maximal commutative subfield L' separable over L. Using **2.3.**, it is easy to see that L' is a maximal commutative subfield of

D. Further, L' is separable over K, and the theorem is proved. To exhibit such an element $c \in D$, we take any element $\lambda \in D$, $\lambda \notin K$. The only case to consider is when $\lambda^{p^m} \in K$ for some integer m (otherwise take $\lambda = c$). Let $\lambda^{p^n} \in K$ and $\lambda^{p^{n-1}} \notin K$. Let σ denote the inner automorphism of D given by $\lambda^{p^{n-1}}$. Then $\sigma^p = 1$ so that $(\sigma - 1)^p = 0$ (note that $\operatorname{char} K = p$) and $\sigma - 1 \neq 0$. Let $r \geq 1$ be an integer such that $(\sigma - 1)^r \neq 0$ and $(\sigma - 1)^{r+1} = 0$. Let $y \in D$ be such that $(\sigma - 1)^r(y) \neq 0$. If $a = (\sigma - 1)^{r-1}(y)$ and $b = (\sigma - 1)^r(y)$, then it may be checked that if $c = b^{-1}a$, then $\sigma c = 1 + c$ so that c is not purely inseparable over K. □

Corollary 2.9. *If A is a central simple algebra over K, there exists a finite Galois extension L over K which splits A.*

Proof. We assume, without loss of generality, that A is a central division algebra over K. Let L_1 be a maximal commutative subfield of A, separable over K. By **2.4.**, L_1 splits A. Since any field containing L_1 is again a splitting field for A, we may choose L to be the Galois closure of L_1 over K. □

§ 3. Crossed-Products

Let L be a finite Galois extension of K with Galois group $G(L/K) = G$. Then the action of G on L makes both the additive group L and the multiplicative group $L^* = L \setminus \{0\}$ into $\mathbb{Z}[G]$-modules, $\mathbb{Z}[G]$ denoting the group ring. For any group G and a $\mathbb{Z}[G]$-module M, we shall define, in a later section, the cohomology groups $H^n(G, M)$, for each integer $n \geq 0$. We shall here give an ad hoc definition of $H^2(G, L^*)$.

A *(normalized)* 2*-cocycle* of G with values in L^* is a map $f : G \times G \to L^*$ with the property $f(1, 1) = 1$, and for σ_1, σ_2, $\sigma_3 \in G$,

$$\sigma_1 f(\sigma_2, \sigma_3) f(\sigma_1, \sigma_2, \sigma_3)^{-1} f(\sigma_1, \sigma_2, \sigma_3) f(\sigma_1, \sigma_2)^{-1} = 1.$$

If f is a normalized 2-cocycle, it may be verified that $f(1, \sigma) = f(\sigma, 1) = 1$ for all $\sigma \in G$. The 2-cocycles form an abelian group under the operation

$$(f + g)(\sigma_1, \sigma_2) = f(\sigma_1, \sigma_2) g(\sigma_1, \sigma_2).$$

This group is denoted by $\mathbb{Z}^2(G, L^*)$. A (normalized) 2*-coboundary* is a map $\delta h : G \times G \to L^*$ of the form $(\sigma, \tau) \mapsto \sigma(h(\tau)) h(\sigma\tau)^{-1}$ where $h : G \to L^*$ is a map with $h(1) = 1$. Clearly δh is a 2-cocycle and the 2-coboundaries form a subgroup denoted by $\mathbb{B}^2(G, L^*)$ of $\mathbb{Z}^2(G, L^*)$. Let $H^2(G, L^*) = \mathbb{Z}^2(G, L^*)/\mathbb{B}^2(G, L^*)$. We call $H^2(G, L^*)$ the *second cohomology group* of G with coefficients in L^*.

Let $f \in \mathbb{Z}^2(G, L^*)$. For each $\sigma \in G$, let e_σ denote a symbol. Let (K, G, f) be the free left L-vector space on the set $\{e_\sigma\}$, $\sigma \in G$, as a basis. We define a multiplication on (K, G, f) by setting

$$(\lambda e_\sigma)(\mu e_\tau) = \lambda \sigma(\mu) f(\sigma, \tau) e_{\sigma\tau} \qquad (*)$$

and extending it to (K, G, f) by distributivity. The algebra (K, G, f) so defined is called a *crossed-product* over L.

Proposition 3.1. *The multiplication defined above makes (K, G, f) into a central simple algebra over K. The map $L \to (K, G, f)$, $x \mapsto xe_1$, is an injection of L onto a subfield of (K, G, f) which is a maximal commutative subring. In particular, $[(K, G, f) : K] = [L : K]^2$.*

Proof. The condition $(e_{\sigma_1} e_{\sigma_2}) e_{\sigma_3} = e_{\sigma_1}(e_{\sigma_2} e_{\sigma_3})$ is equivalent to the condition that f is a 2-cocycle. Thus (K, G, f) is an associative algebra. The fact that f is normalized implies that e_1 is the identity element of (K, G, f). Since (K, G, f) is a (left) vector space over L of dimension $|G| = [L : K]$, it follows that

$$[(K, G, f) : K] = [(K, G, f) : L][L : K] = [L : K]^2.$$

Let $x = \sum_{\sigma \in G} x_\sigma$, e_σ, $x_\sigma \in L$ be a central element of (K, G, f). Then, for every $a \in L^*$, the condition $ax = xa$ implies $x_\sigma = 0$ for $\sigma \neq 1$. Thus $x = x_1 e_1$. The condition $xe_\sigma = e_\sigma x$ for all $\sigma \in G$ implies that $\sigma(x_1) = x_1$ for all $\sigma \in G$ so that $x_1 \in K$. We next prove that (K, G, f) is simple. Let $\mathcal{A}$ be a non-zero two-sided ideal of (K, G, f). For $x \in \mathcal{A}$, $x \neq 0$, if $x = \sum_{\sigma \in G} x_\sigma e_\sigma$, we define $\ell(x) =$ the number of $x_\sigma \neq 0$ in this expression. Let $x \in \mathcal{A}$ be an element with $\ell(x)$ minimal. Let σ_o be such that $x_{\sigma_o} \neq 0$. Multiplying x on the left by $x_{\sigma_0}^{-1}$ and on the right by $e_{\sigma_o}^{-1}$, we may assume $x = 1 \cdot e_1 + \sum_{\sigma \neq 1} x_\sigma e_\sigma$. For every $d \in L$, $\ell(dx - xd) < \ell(x)$, unless $dx - xd = 0$. Since $dx - xd \in \mathcal{A}$, it follows that $dx - xd = 0$ for every $d \in L$, i.e. $x_\sigma = 0$ for all $\sigma \neq 1$. Thus $x = e_1 \in \mathcal{A}$ so that $\mathcal{A} = (K, G, f)$. Finally, since $[(K, G, f) : K] = [L : K]^2$, by **2.3.**, it follows that L is a maximal commutative subring of (K, G, f). □

Corollary 3.2. *If $\{e'_\sigma\}_{\sigma \in G}$ are non-zero elements of (K, G, f) satisfying $e'_\sigma x = \sigma(x) e'_\sigma$, then there exist non-zero elements $u_\sigma \in L^*$, for each $\sigma \in G$ such that $e'_\sigma = u_\sigma e_\sigma$.*

Proof. Since $e'_\sigma e_\sigma^{-1}$ commutes with every element of L, L being a maximal commutative subring of (K, G, f), $e'_\sigma e_\sigma^{-1} = u_\sigma \in L^*$. □

The following proposition asserts that the isomorphism class of (K, G, f) is uniquely determined by the cohomology class $[f]$ of f in $H^2(G, L^*)$.

Proposition 3.3. *Let $f, g \in \mathbb{Z}^2(G, L^*)$. Then (K, G, f) and (K, G, g) are isomorphic if and only if $f - g \in \mathbb{B}^2(G, L^*)$.*

Proof. Suppose $f = g + \delta h$ where $h : G \to L^*$ is a map with $h(1) = 1$. Let $\{e_\sigma\}$, $\{e'_\sigma\}$ $\sigma \in G$, be bases of (K, G, f) and (K, G, g) respectively, satisfying $(*)$ with respect to f and g. The map $e_\sigma \mapsto h(\sigma) e'_\sigma$, $x \mapsto x$, $x \in L$ can be verified to induce

an isomorphism of the K-algebras (K, G, f) onto (K, G, g). Suppose conversely that $\varphi : (K, G, f) \to (K, G, g)$ is an isomorphism of K-algebras. Since Le_1' and $\varphi(Le_1)$ are simple subalgebras of (K, G, g), both isomorphic to L, in view of **2.2.**, there exist a unit $u \in (K, G, g)$ such that $\varphi(xe_1) = u(xe_1')u^{-1}$ for all $x \in L$. Replacing φ by $\operatorname{Int} u^{-1} \circ \varphi$, we may assume that $\varphi(xe_1) = xe_1'$. Then, since $\{\varphi(e_\sigma)\}, \sigma \in G$, satisfy $(*)$ there exists $u_\sigma \in L^*$ such that $\varphi(e_\sigma) = u_\sigma e_\sigma'$ with $u_1 = 1$ by **3.2.**. Let $h : G \to L^*$ be defined by $h(\sigma) = u_\sigma$. It is easily verified that $f = g + \delta h$. □

Proposition 3.4. *For $f \in \mathbb{Z}^2(G, L^*)$, the algebra (K, G, f) is isomorphic to a matrix algebra if and only if $f \in \mathbb{B}^2(G, L^*)$.*

Proof. Let $f \in \mathbb{B}^2(G, L^*)$. In view of **3.3.**, it is enough to show that (K, G, f) is a matrix algebra for $f = 1$, the trivial cocycle. The assignment $\varphi(e_\sigma) = \sigma$, $\varphi(x) = R_x$, $x \in L$, R_x denoting multiplication by x, extends to a K-algebra homomorphism $\varphi : (K, G, f) \to \operatorname{End}_K L$, which is indeed an isomorphism. Conversely, if $(K, G, f) \xrightarrow{\sim} M_n(K)$, $n = [L : K]$, since $(K, G, 1) \xrightarrow{\sim} M_n(K)$, it follows from **3.3.** that $f \in \mathbb{B}^2(G, L^*)$. □

Proposition 3.5. *Let $f, g \in \mathbb{Z}^2(G, L^*)$ then the algebra $(K, G, f + g)$ is Brauer equivalent to $(K, G, f) \otimes_K (K, G, g)$.*

Proof. (A sketch of a proof) Let $L = K(\alpha)$ and let $f = x^n + a_{n-1}x^{n-1} + \ldots + a_o \in K[x]$ be the minimal polynomial of α over K. Since f is separable, $f'(\alpha) \neq 0$. The element

$$e = f'(\alpha)^{-1} \sum_{1 \leq i \leq n} a_i \sum_{0 \leq j \leq n-1} \alpha^j \otimes \alpha^{i-1-j}$$

can be verified to be an idempotent of $L \otimes_K L \subset (K, G, f) \otimes_K (K, G, g) = \Lambda$. There exists a map $(K, G, f + g) \to \Lambda$ given by $e_\sigma \mapsto e(e_\sigma^1 \otimes e_\sigma^2)$, $\ell \mapsto e(\ell \otimes 1) = e(1 \otimes \ell)$, $\ell \in L$, e_σ, e_σ^1, e_σ^2 denoting the defining bases of $(K, G, f + g), (K, G, f)$ and (K, G, g) respectively, which induces an isomorphism of $(K, G, f + g)$ onto $e\Lambda e$. We have $e\Lambda e \sim \Lambda$, so that the proposition is proved. □

§ 4. Thee Brauer group is torsion

Let L be a finite Galois extension of K with Galois group $G(L/K) = G$. Let $\operatorname{Br}(L/K)$ be the subset of $\operatorname{Br}(K)$ consisting of those Brauer classes which are split by L. Obviously, $\operatorname{Br}(L/K)$ is a subgroup of $\operatorname{Br}(K)$. For $f \in \mathbb{Z}^2(G, L^*)$, the algebra (K, G, f) is central simple over K and contains L as a maximal commutative subring by **3.1.** and is therefore split by L (**2.4.**). In view of **3.3.**, we have a well-defined map $c : H^2(G, L^*) \to \operatorname{Br}(L/K)$ given by $[f] \mapsto [(K, G, f)]$, which, by **3.5.** is a homomorphism. The map c is injective, by **3.4.**. The map c is also surjective, in view of the following

Proposition 4.1. *Every central simple algebra over K, split by a finite Galois*

extension L/K is Brauer equivalent to a crossed-product over L.

Proof. Let A be a central simple algebra over K, split by a finite Galois extension L of K. In view of **2.6.**, $A \sim B$, where B contains L as a maximal commutative subring. By **2.2.**, every $\sigma \in G(L/K)$ can be extended to an inner automorphism $\operatorname{Int} u_\sigma$ of B, u_σ being a unit of B. We choose $u_1 = 1$. Since $\operatorname{Int}(u_\sigma u_\tau)$ and $\operatorname{Int}(u_{\sigma\tau})$ both extend $\sigma\tau \in G$, it follows that $u_\sigma u_\tau u_{\sigma\tau}^{-1}$ commutes with L and hence belongs to L^*. Let $f(\sigma, \tau) = u_\sigma u_\tau u_{\sigma\tau}^{-1}$, $\sigma, \tau \in G$. Then $f(1,1) = 1$ and the condition $(u_{\sigma_1} u_{\sigma_2}) u_{\sigma_3} = u_{\sigma_1}(u_{\sigma_2} u_{\sigma_3})$ implies that f is a 2-cocycle. The map $e_\sigma \mapsto u_\sigma$, $x \mapsto x$, $x \in L$, $\sigma \in G$ defines a homomorphism φ of (K, G, f) onto A. Since (K, G, f) is simple and $[(K, G, f) : K] = [A : K] = n^2$, φ is indeed an isomorphism. □

Corollary 4.2. *Every central simple algebra over K is Brauer equivalent to a crossed product over some finite Galois extension of K.*

Proof. Immediate from **2.9.** and **4.1.**. □

Thus, we have the following

Theorem 4.3. *Let L be a finite Galois extension of K with Galois group G. Then we have an isomorphism $c : H^2(G, L^*) \xrightarrow{\sim} \operatorname{Br}(L/K)$ given by $[f] \mapsto [(K, G, f)]$.*

Remark. It is not true in general that over a field K, every central division algebra isomorphic to a crossed-product (i.e. every central division algebra contains a maximal commutative subfield, Galois over K). There are counterexamples due to Amitsur (Israel Journal Math., 12 (1972)). However, it is still an open question whether any central division algebra over K of degree p, p a prime, is a crossed-product.

For a central simple algebra A over K, we define the *exponent* of A, abbreviated $\exp A$, to be the order of $[A]$ in $\operatorname{Br}(K)$. The following theorem shows that $\exp A$ is finite for every central simple algebra A over K.

Theorem 4.5. *The group $\operatorname{Br}(K)$ is torsion. In fact, for any central simple algebra A over K, $\exp A$ divides $\operatorname{index} A$; i.e., if $\operatorname{index} A = m$, $A \otimes A \ldots \otimes A$ (m-times) is isomorphic to a matrix algebra over K.*

Proof. Since the exponent and index are Brauer class invariants, it suffices to prove the theorem for a division algebra D. Let $[D : K] = n^2$ so that $\operatorname{index} D = n$. In view of **4.2.**, D is Brauer-equivalent to a crossed product over some finite Galois extension L of K. Let $\varphi : (K, G, f) \to M_m(D)$ be an isomorphism of K-algebras, $G = G(L/K)$, $m \geq 1$. Since L is a maximal commutative subring of (K, G, f), $[L : K]^2 = [(K, G, f) : K] = [M_m(D) : K] = m^2 n^2$ so that $[L : K] = mn$.

We regard L as a maximal commutative subring of $M_m(D)$ through φ. The left $M_m(D)$-module D^m may be regarded as a left vector space over L. Let p be its dimension. Then $[D^m : K] = [D^m : L][L : K]$ so that $mn^2 = pmn \Rightarrow p = n$. For any $\sigma \in G$, $\varphi(e_\sigma) \in M_m(D)$ operates on D^m and $\varphi(e_\sigma)(\lambda x) = \sigma(\lambda)\varphi(e_\sigma)(x)$, for $\lambda \in L$, $x \in D^m$; i.e. $\varphi(e_\sigma)$ is σ-semilinear. For a choice of basis $\{e_i\}$ $1 \leq i \leq n$ of D^m over L, $\{\varphi(e_\sigma)\}\sigma \in G$ can be represented by matrices $T_\sigma \in M_n(L)$. The condition $e_\sigma e_\tau = f(\sigma,\tau) \cdot e_{\sigma\tau}$ translates into the condition $T_\sigma \sigma(T_\tau) = f(\sigma,\tau)T_{\sigma\tau}$ where the action of G on $M_n(L)$ is entry-wise. Let $h(\sigma) = \det T_\sigma, \sigma \in G$. Then $h : G \to L^*$ is a map with $h(1) = 1$. We have $\sigma(h(\tau))h(\sigma) = f(\sigma,\tau)^n h(\sigma\tau)$; i.e. $nf \in \mathbb{B}^2(G, L^*)$. In view of **3.4.**, $[(K, G, f)]^n$ is trivial in $\mathrm{Br}(K)$. Thus $\exp D = \exp(K, G, f)$ divides $n = \mathrm{degree}\, D$. □

§ 5. 2-torsion in the Brauer group - Quaternion algebras

We begin with the following

Lemma 5.1. *Let A be a central simple algebra over K. If p is a prime which divides* $\mathrm{index}\, A$*, then p divides* $\exp A$.

Proof. Since exponent and index are Brauer class invariants, we assume that A is a crossed product over a finite Galois extension L of K. Let $G = G(L/K)$ be the Galois group. Since L splits A, $\mathrm{index}\, A$ divides $[L : K]$ by **2.1.** so that p divides $[L : K] = \mathrm{order\ of}\, G$. Let H be a p-sylow subgroup of G and let L_1 be the fixed field of H, so that $[L_1 : K] = [G : H]$ is coprime to p. We first claim that $L_1 \otimes_K A$ is not a matrix algebra over L_1. For, otherwise, $\mathrm{index}\, A$ would divide $[L_1 : K]$ by **2.1.** so that $p \,|\, [L_1 : K]$ leading to a contradiction. Further, $L \otimes_{L_1} (L_1 \otimes_K A) \simeq L \otimes_K A \xrightarrow{\sim} M_n(L)$ so that $\mathrm{index}\, L_1 \otimes_K A$ divides $[L : L_1] = p^k$, $k \geq 1$. Let $\mathrm{index}\, L_1 \otimes_K A = p^r$, $r \geq 0$. In fact $r \geq 1$ since $L_1 \otimes_K A$ is not a matrix algebra. Since $\exp L_1 \otimes_K A$ divides $\mathrm{index}\, L_1 \otimes_K A$ (**4.5.**), $\exp L_1 \otimes_K A = p^r$, with $r \geq 1$. Since $\mathrm{Br}(K) \to \mathrm{Br}(L)$, induced by $[A] \to [L \otimes_K A]$ is a homomorphism, $\exp_{L_1}(L_1 \otimes_K A)$ divides $\exp A$ so that p divides $\exp A$. □

Let ${}_2\,\mathrm{Br}(K)$ denote the 2-torsion subgroup of $\mathrm{Br}(K)$, i.e. the subgroup of elements of order ≤ 2. Let $[A] \in {}_2\,\mathrm{Br}(K)$. It follows from **5.1.** that $\mathrm{index}\, A$ is a power of 2. An *involution* (of the first kind) of a central simple algebra A over K is an anti-automorphism $\sigma : A \to A$ such that $\sigma^2 = \mathrm{identity}$ and σ is identity on K. An algebra A is *involutorial* if it admits of an involution. If A is involutorial, then $A \xrightarrow{\sim} A^{\mathrm{op}}$ so that $[A] \in {}_2\,\mathrm{Br}(K)$. The next two propositions characterise central simple algebras over K of exponent ≤ 2 as precisely the involutorial algebras over K.

Lemma 5.2. *Let A and B be central simple algebras over K which are Brauer equivalent. If A has an involution, then B has an involution.*

Proof. It is enough th show that if D is a central division algebra over K, then

D has an involution if and only if $M_r(D)$ has an involution. If D has an involution σ, $x \mapsto \sigma(x^t)$ defines an involution of $M_r(D)$, the action of σ on $M_r(D)$ being entry-wise. Suppose $M_r(D)$ has an involution σ. Let $\sigma(e_{ij}) = f_{ji}$, where $\{e_{ij}\}$, $1 \leq i, j \leq r$ are the matrix units of $M_r(D)$. Since σ is an anti-automorphism, it follows that $\{f_{ij}\}$, $1 \leq i, j \leq r$ are again matrix units of $M_r(D)$ so that they generate a K-subalgebra of $M_r(D)$, isomorphic to $M_r(K)$. By **2.2.** there exists a unit $u \in M_r(D)$ such that $f_{ij} = ue_{ij}u^{-1}$, for all i, j. We have $f_{ij} = \sigma(e_{ji}) = ue_{ij}u^{-1}$ and $e_{ji} = \sigma(ue_{ij}u^{-1}) = \sigma u^{-1}ue_{ji}u^{-1}\sigma u$. Thus $v = u^{-1}\sigma u$ commutes with $M_r(K)$ so that v belongs to the commutant of $M_r(K)$ in $M_r(D)$, namely D.

Case 1. Let $u + \sigma u = 0$. Then $v = -1$ and one verifies that $\sigma' = \operatorname{Int} u^{-1} \circ \sigma$ is an involution of $M_r(D)$. Since $\sigma'(e_{ij}) = e_{ji}$, σ' maps $M_r(K)$ onto itself and hence maps the commutant of $M_r(K)$, namely D onto itself and provides an involution of D.

Case 2. Let $u + \sigma u \neq 0$. Then $v \neq -1$ and $1 + v \in D$ is a unit. Thus $u' = u + \sigma u = u(1 + v)$ is a unit of $M_r(D)$ and $\sigma' = \operatorname{Int}(u'^{-1}) \circ \sigma$ defines an involution of $M_r(D)$ which restricts as in case 1 to an involution of D. □

Lemma 5.3 *Let A be an algebra of exponent 2 which is a crossed product over some $L \supset K$. Then A has an involution.*

Proof. Let $A \xrightarrow{\sim} (K, G, f)$ with $G = G(L/K)$, $2f \in \mathbb{B}^2(G, L^*)$. Let $h : G \to L^*$ be a map with $h(1) = 1$ and such that for all $\sigma, \tau \in G$, $f(\sigma, \tau)^2 = \sigma(h(\tau))h(\sigma\tau)^{-1}h(\sigma)$. It is easily verified that the assignment $e_\sigma \mapsto e_\sigma^{-1}h(\sigma)$, $\ell \mapsto \ell$, $\ell \in L$, $\sigma \in G$ induces an involution of (K, G, f). □

We thus have proved the following

Theorem 5.4. *For a central simple algebra A over K, the following are equivalent:*

1) $[A] \in {}_2\operatorname{Br}(K)$

2) *A admits of an involution over K.*

Let D be a central division algebra over K of exponent 2. We have seen that degree D is a power of 2 (**5.1.**) and D admits of an involution. We shall now give examples of algebras of degree 2 over K, the so-called quaternion algebras over K, which come equipped with a canonical involution.

An associative K-algebra generated by two elements ζ, η with relations $\zeta^2 = \zeta + a, \eta^2 = b, \zeta\eta + \eta\zeta = \eta$ with $a, b \in K$, $4a + 1 \neq 0$, $b \neq 0$ is called a *quaternion algebra* over K.

Lemma 5.5 *Central simple algebras over K of rank 4 are precisely the quaternion algebras over K.*

Proof. Let A be a quaternion algebra over K, with generators ζ, η as above. Suppose that the polynomial $x^2 - x - a \in K[x]$ has a root $\lambda \in K$. Then the map

$$\zeta \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & 1-\lambda \end{pmatrix}, \quad \eta \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$$

defines an isomorphism of A with $M_2(K)$. If the polynomial $x^2 - x - a \in K[x]$ is irreducible, since $4a + 1 \neq 0$, the subring $K(\zeta) \subset A$ is a quadratic extension of K which is Galois. Let σ be the nontrivial automorphism of $K(\zeta)$ over K, defined by $\sigma(\zeta) = 1-\zeta$. Let $f \in \mathbb{Z}^2(G, K(\zeta)^*)$ be the 2-cocycle $f(\sigma, \sigma) = b$, $(G = G(K(\zeta)/K))$. Then, the map $e_\sigma \mapsto \eta$, $\ell \mapsto \ell$, $\ell \in K(\zeta)$ induces an isomorphism of (K, G, f) onto A. Hence A is a central simple algebra over K, which is in fact a crossed product over $K(\zeta)$. Let conversely A be any central simple algebra of rank 4 over K. If $A = M_2(K)$, $\zeta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\eta = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ satisfy $\zeta^2 = \zeta$, $\eta^2 = 1$ and $\zeta\eta + \eta\zeta = \eta$ and generate $M_2(K)$ so that $M_2(K)$ is a quaternion algebra. Suppose A is a division algebra over K of rank 4. Let L be a maximal commutative subfield of D, separable over K (see **2.8.**). Let $L = K(\zeta)$ and let $\zeta^2 = \lambda\zeta + h$, λ, $h \in K$. If $\operatorname{char} K = 2$, since ζ is separable, $\lambda \neq 0$. If $\operatorname{char} K \neq 2$, replacing ζ by $\zeta + 1$ if necessary, we assume that $\lambda \neq 0$. We again replace ζ by $\lambda^{-1}\zeta$ and assume that ζ satisfies the equation $\zeta^2 = \zeta + a$, $a \in K$. The condition that ζ is separable over K implies that $4a + 1 \neq 0$. Since A contains the Galois extension L/K, A is a crossed product over L by **5.4.**. Let $e_\sigma = \eta$, where σ is the Galois automorphism $\zeta \mapsto 1 - \zeta$ of L. Then $\eta^2 = e_\sigma^2 = f(\sigma, \sigma) \cdot 1 \in L^*$. Since $f(\sigma, \sigma)$ is a power of e_σ, $f(\sigma, \sigma)$ commutes with e_σ and since it commutes with L, $f(\sigma, \sigma) \in K^*$. Let $b = f(\sigma, \sigma)$. By the definition of η, $\eta\zeta\eta^{-1} = 1 - \zeta$ so that $\zeta\eta + \eta\zeta = \eta$. Thus A is a quaternion algebra over K. $\square$

Let A be a quaternion algebra over K with generators ζ, η as above. Since $\exp A = 1$ or 2, A certainly admits of an involution (see **5.4.**). The assignment $\zeta \mapsto 1-\zeta$, $\eta \mapsto -\eta$ can be extended to an involution $x \mapsto \bar{x}$ of A. This involution has the property that for each $x \in A, N(x) = x\bar{x}$ and $T(x) = x + \bar{x}$ belong to K.

Any involution on A with this property coincides with the involution $x \mapsto \bar{x}$. We call this, the *canonical involution* of A. The map $N : A \to K$ is multiplicative, called the *reduced norm* and the map $T : A \to K$ is additive and is called the *reduced trace*. Since any central simple algebra of rank 4 is either a matrix algebra or a division algebra, a quaternion algebra A is isomorphic to a matrix algebra if and only if there exists a non-zero element $x \in$A such that $Nx = 0$.

Proposition 5.6. *Let A be a quaternion algebra with generators ζ, η with $\zeta^2 = \zeta + a$, $\eta^2 = b$, $\zeta\eta + \eta\zeta = \eta$, $4a + 1 \neq 0$, $b \neq 0$, a, $b \in K$. Then A is a matrix algebra if and only if there exist λ, $\mu \in K$ such that $b = \lambda^2 + \lambda\mu - a\mu^2$.*

Proof. Let $x \in A$ be written, with respect to the basis $(1, \zeta, \eta, \zeta\eta)$ of A as a linear combination $\lambda_1 + \mu_1\zeta + \gamma_1\eta + \delta_1\zeta\eta$, λ_1, μ_1, γ_1, $\delta_1 \in K$. Then

$$N(x) = (\lambda_1^2 + \lambda_1\mu_1 - a\mu_1^2) - b(\gamma_1^2 + \gamma_1\delta_1 - a\delta_1^2).$$

Suppose there exist $\lambda, \mu \in K$ with $b = \lambda^2 + \lambda\mu - a\mu^2$. Then $x = \lambda + \mu\zeta + \eta \neq 0$ and has norm 0. Hence A is a matrix algebra over K. Suppose conversely, that A is a matrix algebra over K. Let $x \in A$, $x \neq 0$ with $Nx = 0$ and let $x = \lambda_1 + h_1\zeta + \gamma_1\eta + \delta_1\zeta\eta$. If the equation $\lambda^2 + \lambda\mu - a\mu^2 = 0$ has a nontrivial solution $\lambda, \mu \in K$, then the algebra $K(\zeta) \xrightarrow{\sim} K[x]/(x^2 - x - a)$ is isomorphic to $K \times K$ so that the norm $N_o : K(\zeta) \to K$ is surjective. In particular, there exists $y = \lambda + \mu\zeta \in K(\zeta)$ such that $N(y) = \lambda^2 + \lambda\mu - a\mu^2 = b$. On the other hand, if the equation $\lambda^2 + \lambda\mu - a\mu^2 = b$ has no nontrivial solution in K, then $K(\zeta)$ is a quadratic extension of K. We have $Nx = 0 \Rightarrow (\lambda_1^2 + \lambda_1\mu_1 - a\mu_1^2) = b(\gamma_1^2 + \gamma_1\delta_1 - a\delta_1^2) \Rightarrow \gamma_1^2 + \gamma_1\delta_1 - a\delta_1^2 \neq 0$, $\gamma_1, \delta_1 \neq 0$ and $b = (\lambda_1^2 + \lambda_1\mu_1 - a\mu_1^2)/(\gamma_1^2 + \gamma_1\delta_1 - a\delta_1^2) = \lambda^2 + \lambda\mu - a\mu^2$ where $\lambda\zeta + \mu = (\lambda_1\zeta + \mu_1)(\gamma_1\zeta + \delta_1)^{-1} \in K(\zeta)$. □

Proposition 5.7. *Let K be a field of characteristic $\neq 2$. Then quaternion algebras over K are precisely algebras generated by ζ, η with the relations $\zeta^2 = a$, $\eta^2 = b$, $\zeta\eta + \eta\zeta = 0$, $a, b \in K^*$. Such an algebra is a matrix algebra if and only if there exist $\lambda, \mu \in K$ such that $b = \lambda^2 - a\mu^2$.*

Proof. Let ζ', η' be generators of A with $\zeta'^2 = \zeta' + a'$, $\eta'^2 = b'$, $\zeta'\eta' + \eta'\zeta' = \eta'$, $1 + 4a'$, $b' \neq 0$ in K. Let $\zeta = \zeta' - 1/2$, $\eta = \eta'$, $a = a' + 1/4$ and $b' = b$. Then ζ, η are the required generators for A. The final assertion is a consequence of **5.6.**. □

Tensor products of quaternion algebras are of degree 2^n and involutorial. The following natural question arises:

Q (1) Is every central simple algebra over a field K of degree 2^n, with an involution, isomorphic to a tensor product of quaternion algebras?

This question has an affirmative answer if $n = 2$ (Albert). However Amitsur-Rowen-Tignol (Israel Journal Math. 33, (1979) have constructed finite dimensional central simple algebras over fields of characteristic $\neq 2$ of degree 2^n, $n \geq 3$, with involutions, which are *not isomorphic* to a tensor product of quaternion algebras.

There is however a weaker question:

Q (2) Is every central simple algebra with an involution, Brauer equivalent to a tensor product of quaternion algebras? (In other words: Is ${}_2\,\mathrm{Br}(K)$ generated by quaternion algebras?)

If $\mathrm{char}\, K = 2$, this question has an affirmative answer, due to Albert. If $\mathrm{char}\, K \neq 2$, it was an open problem, and a consequence of the theorem of Merkurjev is that this is indeed the case.

Chapter II: Cohomology of groups

§ 1. Definition of cohomology groups

Let G be a group and $\mathbb{Z}[G]$ the integral group ring. By a *G-module*, we mean a (left) $\mathbb{Z}[G]$-module. Any abelian group A can be regarded as a G-module by setting $x \cdot a = a$ for all $x \in G$, $a \in A$. Such a G-module is called a *trivial G-module*. In particular, we shall regard $\mathbb{Z}$ as a trivial $\mathbb{Z}[G]$-module. Let H be a subgroup of G and A any H-module. We define on $\mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big)$ a left G-module structure through the right G-module structure of $\mathbb{Z}[G]$; i.e., for $f \in \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big)$, x, $y \in G$, we define $(xf)(y) = f(yx)$. A G-module B is said to be *co-induced from H* if there exists an H-module A and an isomorphism $B \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big)$ of $\mathbb{Z}[G]$-modules. A G-module A is called *co-induced* if it is co-induced from the trivial subgroup (e); i.e., A is isomorphic to $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[G], B\big) = B^*$ for some abelian group B. Every G-module A can be embedded in a co-induced module. In fact, we have a G-homomorphism $i : A \to A^* = \mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[G], A\big)$ given by $a \mapsto f_a$ where $f_a(x) = xa$, $x \in G$, which is clearly injective.

For any G-module A, we set $A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ ($\mathbb{Z}$ being the trivial $\mathbb{Z}[G]$-module). The inclusion

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) = A$$

identifies A^G with the set $\{a \in A \mid xa = a \ \forall x \in G\}$ which is the group of fixed points of A for the action of G.

The *cohomology groups* of G with coefficients in a G-module A are a sequence of abelian groups $H^q(G, A)$, $q = 0, 1 \ldots$ such that

1) $H^0(G, A) = A^G$

2) For any $q \geq 0$ the assignment $A \mapsto H^q(G, A)$ is (covariant) functorial.

2) For any exact sequence

$$0 \to A' \to A \to A'' \to 0$$

of G-modules, there exist *connecting homomorphisms*

$$\delta_q : H^q(G, A'') \to H^{q+1}(G, A')$$

such that the sequence

$$\ldots \to H^q(G, A') \to H^q(G, A) \to H^q(G, A'') \xrightarrow{\delta_q} H^{q+1}(G, A') \to \ldots$$

is exact. Further, δ is functorial for exact sequences; i.e., given a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0
\end{array}$$

of exact sequences of G-modules, the diagram

$$\begin{array}{ccc} H^q(G,A'') & \xrightarrow{\delta_q} & H^{q+1}(G,A') \\ {\scriptstyle H^q(f'')}\downarrow & & {\scriptstyle H^{q+1}(f')}\downarrow \\ H^q(G,B'') & \xrightarrow{\delta_q} & H^{q+1}(G,B') \end{array}$$

commutes.

4)/ For any co-induced module A, $H^q(G,A)=0$ for $q\geq 1$.

Theorem 1.1 *For any group G and any G-module A, cohomology groups $H^q(G,A)$ exist for $q\geq 0$ and are unique up to functorial isomorphisms.*

Proof. We first prove by induction on q the uniqueness up to functorial isomorphisms of the groups $H^q(G,A)$. For $q=0$, this follows from Property 1). Let A be a G-module and $q\geq 1$. We have the following short exact sequence

$$0\to A\overset{i}{\hookrightarrow} A^*\to A'\to 0$$

where i is the embedding of A in the co-induced module $A^*=\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A)$ and $A'=\mathrm{coker}\ i$. If $\left(H^q(G,A),\delta_q\right)$, $\left(\widetilde{H}^q(G,A),\widetilde{\delta}_q\right)$ are two sequences of groups with connecting homomorphisms satisfying 1), 2), 3) and 4) above, we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^G & \longrightarrow & A^{*G} & \longrightarrow & A'^G & \xrightarrow{\delta_0} & H^1(G,A) \longrightarrow H^1(G,A^*)=0 \\ & & \| & & \| & & \| & & \| \\ 0 & \longrightarrow & A^G & \longrightarrow & A^{*G} & \longrightarrow & A'^G & \xrightarrow{\widetilde{\delta}_0} & \widetilde{H}^1(G,A) \longrightarrow \widetilde{H}^1(G,A'^*)=0. \end{array}$$

From this diagram, it is clear that there exists a map $f_1: H^1(G,A)\to\widetilde{H}^1(G,A)$ satisfying $f_1\delta_0(a)=\tilde{\delta}_0(a)$ for all $a\in A'^G$. Since δ_0 and $\widetilde{\delta}_0'$ are functorial in A, f_1 is functorial in A. It is easily verified that f_1 is in fact an isomorphism. By induction, we assume that there is a functorial isomorphism $f_{q-1}: H^{q-1}(G,A)\to\widetilde{H}^{q-1}(G,A)$. We have the following commutative diagram which defines f_q:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^{q-1}(G,A') & \xrightarrow[\sim]{\delta_{q-1}} & H^q(G,A) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_{q-1}} & & \downarrow{\scriptstyle f_q} & & \\ 0 & \longrightarrow & \widetilde{H}^{q-1}(G,A') & \xrightarrow[\sim]{\widetilde{\delta}_{q-1}} & \widetilde{H}^q(G,A) & \longrightarrow & 0 \end{array}$$

Since δ_{q-1}, $\tilde{\delta}_{q-1}$, f_{q-1} are all functorial in A, f_q is again functorial in A.

We *define* $H^q(G,A)=\mathrm{Ext}^q_{\mathbb{Z}[G]}(\mathbb{Z},A)$, the derived functors of the functor

$$A\to\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)=A^G.$$

It follows from standard results of homological algebra that $H^q(G,A)$ satisfies 1), 2) and 3). The fact that $H^q(G,A)$ satisfies 4) follows (by taking $H=(e)$) from the following more general lemma. $\square$

Lemma 1.2. (Shapiro) *Let H be a subgroup of a group G and A an H-module. Then we have isomorphisms $s_A^q : H^q\big(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)\big) \xrightarrow{\sim} H^q(H,A)$, $\forall q \geq 0$, which are functorial in A.*

Proof. Let $\underline{\underline{P}}$ be a $\mathbb{Z}[G]$-free resolution of $\mathbb{Z}$. Since $\mathbb{Z}[G]$ is $\mathbb{Z}[H]$-free, $\underline{\underline{P}}$ is also a $\mathbb{Z}[H]$-free resolution of $\mathbb{Z}$. We have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[H]}\big(\underline{\underline{P}}, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)\big) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[H]}(P, A)$$

of complexes which is functorial in A so that we have induced isomorphisms

$$\mathrm{Ext}^q_{\mathbb{Z}[G]}\big(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big)\big) \xrightarrow{\sim} \mathrm{Ext}^q_{\mathbb{Z}[H]}(\mathbb{Z}A,)$$

which are functorial in A. $\square$

§ 2. The standard complex

By results of homological algebra, for any G-module A, the cohomology groups $H^n(G,A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ can be computed by using any $\mathbb{Z}[G]$-projective resolution of $\mathbb{Z}$. In this section, we give an explicit resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module. Let P_i be the free $\mathbb{Z}$-module on $G^{i+1} = G \times \ldots \times G$ (i-times). We let G operate on P_i by setting $g(g_0, \ldots, g_i) = (gg_0, \ldots, gg_i)$ for $g \in G$, $(g_0, \ldots, g_i) \in G^{i+1}$. The $\mathbb{Z}[G]$-module P_i is free with basis $\{(1, g_1, \ldots, g_i),\ g_j \in G,\ 1 \leq j \leq i\}$. We define homomorphisms $d_i : P_i \to P_{i-1}$, $i \geq 1$ by setting

$$d_i(g_0, \ldots, g_i) = \sum_{0 \leq j \leq i} (-1)^j (g_0, \ldots, \hat{g}_j, \ldots, g_i),$$

which are obviously G-linear. We define $\varepsilon : P_0 \to \mathbb{Z}$ by $\varepsilon(g) = 1$ for all $g \in G$. The sequence

$$\to \ldots \to P_i \to P_{i-1} \to \ldots \to P_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

is indeed a $\mathbb{Z}[G]$-resolution for $\mathbb{Z}$. The fact that $d \circ d = 0$ and that the complex is exact are consequences of the fact that there exist $\mathbb{Z}$-linear maps $h_i : P_i \to P_{i+1}$ (for example, $h_i(g_0, \ldots, g_i) = (s, g_0, \ldots, g_i)$ for a fixed $s \in G$) such that $dh_{i+1} + h_i d =$ identity.

Let A be a G-module. The cohomology groups $H^q(G,A) = \mathrm{Ext}^q_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ can be computed as the homology of the complex

$$\longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A) \xrightarrow{\delta_i} \mathrm{Hom}_{\mathbb{Z}[G]}(P_{i+1}, A) \longrightarrow \ldots,$$

where $\delta_i(f) = f \circ d_{i+1}$. An element of $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A)$ is called an *i-cochain* and can be identified with a map $f : G^{i+1} \to A$ satisfying the condition

$$f(xx_0, xx_1, \ldots, xx_i) = x \cdot f(x_0, \ldots, x_1)$$

for all $x \in G$. Such a map is uniquely determined by its values on the elements of the form $(1, x_1, x_2 \dots x_i)$. We define a function $\tilde{f} : G^i \to A$, associated to an i-cochain f by setting

$$\tilde{f}(x_1, \dots, x_i) = f(1, x_1, x_1x_2, \dots, x_1x_2 \cdots x_i).$$

The map $f \mapsto \tilde{f}$ identifies the group $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A)$ with $\mathrm{Map}(G^i, A)$, elements of which are called the *non-homogeneous cochains*. With this identification, the coboundary $\delta_i : \mathrm{Map}(G^i, A) \to \mathrm{Map}(G^{i+1}, A)$ is given by

$$\begin{aligned} \delta_i(g)(x_1, \dots, x_{i+1}) &= x_1 g(x_2, \dots, x_{i+1}) \\ &\quad + \textstyle\sum_{1 \le j \le i} (-1)^j g(x_1, \dots, x_j x_{j+1}, \dots, x_{i+1}) \\ &\quad + (-1)^{i+1} g(x_1, \dots, x_i). \end{aligned}$$

Let $Z^i(G, A) = \ker \delta_i$ and $B^i(G, A) = \mathrm{im}\, \delta_{i-1}$. Then

$$H^i(G, A) \xrightarrow{\sim} Z^i(G, A)/B^i(G, A).$$

Elements of $Z^i(G, A)$ are called *non-homogeneous cocycles* and those of $B^i(G, A)$ *non-homogeneous coboundaries*.

For $i = 1$, an element of $Z^1(G, A)$ is a map $f : G \to A$ such that, for $x_1, x_2 \in G$,

$$f(x_1x_2) = x_1 f(x_2) + f(x_1).$$

Such an f is called a *crossed homomorphism*. If G acts trivially on A, then crossed homomorphisms are precisely the usual homomorphisms. An element of $B^1(G, A)$ is a map of the form $x \mapsto xa - a$ for some $a \in A$. A (non-homogeneous) 2-cocycle with coefficients in A is a map $f : G \times G \to A$ satisfying.

$$x_1 f(x_2, x_3) - f(x_1x_2, x_3) + f(x_1, x_2x_3) - f(x_1, x_2) = 0.$$

A 2-coboundary is a map $\delta h : G \times G \to A$ given by

$$\delta h(x_1, x_2) = x_1 h(x_2) - h(x_1x_2) + h(x_1),$$

where $h : G \to A$ is any map.

Let f be a 2-cocycle. The cocycle condition on f, written for the triple $(x, 1, 1) \in G^3$ gives $xf(1, 1) = f(1, 1)$. The map $f^* : G^2 \to A$ given by $f^*(x_1, x_2) = f(x_1, x_2) - f(1, 1)$ is verified to be a cocycle with $f^*(1, 1) = 0$. Such a cocycle is called a *normalized* 2-cocycle. Since $f^* = f - \delta h$ where $h(x) = f(1.1)$ for all $x \in G$, every 2-cocycle is cohomologous to a normalized 2-cocycle. It is easily verified that any normalized 2-cocycle satisfies $f(x, 1) = f(1, x) = 0 \ \forall \ x \in G$. The normalized 2-cocycles form a subgroup of $Z^2(G, A)$. If f is a normalized cocycle with $f = \delta h$, then $h(1) = 0$. We call a 2-coboundary *normalized* if it is of the form δh with $h(1) = 0$. Thus $H^2(G, A)$ is isomorphic to the group of normalized cocycles modulo the subgroup of

normalized coboundaries.

§ 3. Galois cohomology of the additive and multiplicative groups Let L/K be a finite Galois extension with Galois group $G = G(L/K)$. Then both L and L^* are G-modules with the action $\sigma \cdot a = \sigma(a)$, for $\sigma \in G$, $a \in L$.

Proposition 3.1. (Hilbert Theorem 90) $H^1(G, L^*) = (0)$.

Proof. Let $f \in Z^1(G, L^*)$ be a 1-cocycle. Since elements of G are linearly independent over L (Dedekind's theorem), there exist a, $b \in L^*$ such that $\sum_{\tau \in G} f(\tau)\tau(b) = a$: For any $x \in G$,

$$xa = \sum_{\tau \in G} xf(\tau) \cdot x\tau(b) = \sum_{\tau \in G} f(x\tau)f(x)^{-1}x\tau(b) = f(x)^{-1} \cdot a,$$

so that $f(x) = xa \cdot a^{-1}$ for all $x \in G$; i.e., $f \in B^1(G, L^*)$. □

Corollary 3.2. *Let L/K be a finite cyclic extension and let σ be a generator of $G(L/K)$. Let a be an element of L^*. Then $N_{L/K}(a) = 1$ if and only if there exists $b \in L^*$ such that $a = \sigma b \cdot b^{-1}$.*

Proof. If $a = \sigma b \cdot b^{-1}$, then $N_{L/K}(a) = a \cdot \sigma(a) \ldots \sigma^{n-1}(a) = 1$ where $n =$ order G. Suppose conversely that $a \in L^*$ with $N_{L/K}(a) = 1$. It is easy to check that the assignment $\sigma \mapsto a$ can be extended to a 1-cocycle $f : G \to L^*$. By **3.1.** above, there exists $b \in L^*$ such that $f(\sigma) = \sigma b \cdot b^{-1}$; i.e. $a = \sigma b \cdot b^{-1}$. □

Proposition *$H^n(G, L) = 0$, for all $n \geq 1$, for any finite Galois extension L/K with $G = G(L/K)$.*

Proof. There exists a normal basis for L/K, i.e., there exists $a \in L$ such that $\{\sigma a \,|\, \sigma \in G\}$ is a basis of L over K. Any $b \in L$ can be uniquely written as $b = \sum_{\sigma \in G} b_\sigma \sigma(a)$. The map $L \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], K)$ given by $b \mapsto (\sigma \mapsto b_{\sigma^{-1}})$ is an isomorphism of G-modules where $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[G], K\big)$ is the module co-induced from K. Hence $H^n(G, L) = 0$ for all $n \geq 1$. □

§ 4. Inflation, restriction and corestriction

Let $f : G \to G'$ be a homomorphism of groups. Let A be a G-module and A' a G'-module. Then A' is a G-module through the homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[G']$ induced by f. Let $\varphi : A' \to A$ be a homomorphism of G-modules. The pair (f, φ) is called a *compatible pair*. They induce, in an obvious manner, homomorphisms $\mathrm{Map}(G'^n, A') \to \mathrm{Map}(G^n, A)$, $n \geq 0$, of complexes and hence homomorphisms $H^n(G', A') \to H^n(G, A)$.

We have the following examples of compatible pairs. Let $f : H \hookrightarrow G$ be the inclusion of a subgroup H in G. Let $\varphi : A \to A$ be the identity map of a G-module A. The homomorphism $H^n(G, A) \to H^n(H, A)$ induced by this compatible pair is called the *restriction homomorphism*, denoted by res. We note that $\text{res} : H^0(G, A) \to H^0(H, A)$ is the inclusion $A^G \hookrightarrow A^H$. Let H be a normal subgroup of G and $\eta : G \to G/H$ the canonical map. For any G-module A, A^H is a G/H-module. Let $\varphi : A^H \hookrightarrow A$ be the inclusion. Then (η, φ) is a compatible pair and the induced homomorphism $H^n(G/H, A^H) \to H^n(G, A)$ is called the *inflation* denoted by inf. We note that $\text{inf} : H^0(G/H, A^H) \to H^0(G, A)$ is the identity: $A^G \to A^G$.

The restriction homomorphism is functorial and commutes with the connecting homomorphisms. More precisely, if $f : A \to A'$ is a homomorphism of G-modules, then the diagram

$$\begin{array}{ccc} H^n(G, A) & \xrightarrow{H^n(G,f)} & H^n(G, A') \\ \downarrow \text{res} & & \downarrow \text{res} \\ H^n(H, A) & \xrightarrow{H^n(H,f)} & H^n(H, A') \end{array}$$

is commutative and if $0 \to A' \to A \to A'' \to 0$ is an exact sequence of G-modules, the diagram

$$\begin{array}{ccc} H^n(G, A'') & \xrightarrow{\delta_n} & H^{n+1}(G, A') \\ \downarrow \text{res} & & \downarrow \text{res} \\ H^n(H, A'') & \xrightarrow{\delta_n} & H^{n+1}(H, A') \end{array}$$

commutes.

Similarly, the inflation is functorial and commutes with connecting homomorphisms. More precisely, if $f : A \to A'$ is a homomorphism of G-modules, then,

$$\begin{array}{ccc} H^n(G/H, A^H) & \xrightarrow{H^n(G/H,f)} & H^n(G/H, A'^H) \\ \downarrow \text{inf} & & \downarrow \text{inf} \\ H^n(G, A) & \xrightarrow{H^n(G,f)} & H^n(G, A') \end{array}$$

commutes and if $0 \to A' \to A \to A'' \to 0$ is an exact sequence of G-modules such that the induced sequence $0 \to A'^H \to A^H \to A''^H \to 0$ is exact, then the diagram

$$\begin{array}{ccc} H^n(G/H, A''^H) & \xrightarrow{\delta_n} & H^{n+1}(G/H, A'^H) \\ \downarrow \text{inf} & & \downarrow \text{inf} \\ H^n(G, A'') & \xrightarrow{\sigma_n} & H^{n+1}(G, A') \end{array}$$

commutes. The proofs of both these statements are by direct verification.

Let A be a G-module and $B = \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big)$ the G-module co-induced from H. We have a homomorphism of G-module $f : A \to B$ given by $a \to f(a)$, $a \in A$ where $f(a)(x) = xa$. We therefore have an induced homomorphism

$$H^n(f) : H^n(G, A) \to H^n(G, B)$$

for all $n \geq 0$. In view of **1.2.**, we have isomorphisms

$$s_A^n : H^n(G, B) \xrightarrow{\sim} H^n(H, A)$$

so that the composite $s_A^n \circ H^n(f)$ is a homomorphism $H^n(G, A) \xrightarrow{\sim} H^n(H, A)$. For $n = 0$, this map is the inclusion $A^G \to A^H$. Since both $H^n(f)$ and s^n are functorial and commute with the appropriate connecting homomorphisms $s_A^n \circ H^n(f)$ is functorial and commutes with connecting homomorphisms. Since $s_A^0 \circ H^0(f) = \mathrm{res}$, it follows that $s_A^n \circ H^n(f) = \mathrm{res}$. We thus have the following

Proposition 4.1. *For any G-module A, the homomorphism*

$$H^n(G, A) \longrightarrow H^n(H, A)$$

defined as the composite $s_A^n \circ H^n(f)$ is the restriction homomorphism.

Proposition 4.2. *Let H be a normal subgroup of G and A a G-module. If $H^i(H, A) = 0$ for $1 \leq i \leq n-1$ (in particular there is no condition if $n = 1$)), then the sequence*

$$0 \longrightarrow H^n(G/H, A^H) \xrightarrow{\inf} H^n(G, A) \xrightarrow{\mathrm{res}} H^n(H, A)$$

is exact.

Proof. The proof is by induction on n. Let $n = 1$ and let $[f] \in H^1(G/H, A^H)$, with $f \in Z^1(G/H, A^H)$ as a representative, such that $\inf [f] = 0$. The cocycle

$$f : G \xrightarrow{\eta} G/H \xrightarrow{f} A^H \xhookrightarrow{i} A$$

being a coboundary, there exists $a \in A$ such that $f(x) = xa - a$ for all $x \in G$. Since $f \mid H$ is zero, $a \in A^H$ is so that $f \in B^1(G/H, A^H)$. Thus $\inf : H^1(G/H, A) \to H^1(G, A)$ is injective. The map $\mathrm{res} \circ \inf$ is zero since the composite $H \hookrightarrow G \to G/H$ is trivial. Let $f \in Z^1(G, A)$ such that $\mathrm{res}\,[f] = 0$. Let $a \in A$ be such that $f(y) = ya - a$ for all $y \in H$. If $f_a : G \to A$ is defined by $x \mapsto xa - a$, $f' = f - f_a$ vanishes on H and $[f'] = [f]$ in $H^1(G, A)$. The map f' induces a 1-cocycle $f'' : G/H \to A^H$ such that $\inf [f''] = [f'] = [f]$.

Suppose $n \geq 1$ and assume by induction that the proposition has been proved for $n - 1$. We have an exact sequence of G-modules

$$0 \longrightarrow A \xrightarrow{i} A^* \longrightarrow A' \longrightarrow 0, \qquad (*)$$

where i is the embedding of A in the co-induced module $A^* = \mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[G], A\big)$. Since $H^1(H, A) = 0$, we have an induced exact sequence

$$0 \longrightarrow H^0(H, A) \longrightarrow H^0(H, A^*) \longrightarrow H^0(H, A') \longrightarrow 0$$

i.e.,

$$0 \longrightarrow A^H \longrightarrow (A^*)^H \longrightarrow (A')^H \longrightarrow 0. \qquad (**)$$

We note that $(*)$ is also an exact sequence of H-modules and

$$A^* = \mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[G], A\big) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\textstyle\bigoplus_{G/H}\mathbb{Z}[H], A) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], \prod_{G/H} A)$$

so that A^* is co-induced as an H-module. We also note that $(**)$ is an exact sequence of G/H-modules and $(A^*)^H \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/H], A)$ is co-induced as a G/H-module. In view of the remarks made earlier in this section on res and inf commuting with connecting homomorphisms, we have the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{n-1}(G/H, A'^H) & \xrightarrow{\inf} & H^{n-1}(G, A') & \xrightarrow{\mathrm{res}} & H^{n-1}(H, A') \\
 & & \downarrow{\scriptstyle \delta_{n-1}} & & \downarrow{\scriptstyle \delta_{n-1}} & & \downarrow{\scriptstyle \delta_{n-1}} \\
0 & \longrightarrow & H^n(G/H, A^H) & \xrightarrow{\inf} & H^n(G, A) & \xrightarrow{\mathrm{res}} & H^n(H, A)
\end{array}$$

The vertical maps are all isomorphisms since $n \geq 2, A^*$ is co-induced both as a G- and H-module and $(A^*)^H$ is co-induced as a G/H-module. The top row is exact, by induction, since $H^i(H, A') \xrightarrow{\sim} H^{i+1}(H, A) = 0$ for $1 \leq i \leq n-2$, A^* being co-induced as an H-module. Hence the bottom row is exact and this completes the proof of the proposition. □

Corollary 4.3. *Let L/K be a finite Galois extension with Galois group G. Let H be a normal subgroup of G and L^H the fixed field of H. Then, the sequence*

$$0 \longrightarrow H^2(G/H, (L^H)^*) \xrightarrow{\inf} H^2(G, L^*) \xrightarrow{\mathrm{res}} H^2(H, L^*)$$

is exact.

Proof. Since H is the Galois group of the extension L/L^H, in view of **3.1.**, $H^1(H, L^*) = 0$ and the corollary is an immediate consequence of the above proposition. □

Let G be a group and H a subgroup of finite index. Let $\{x_i\}_{i\in I}$ be a set of right coset representatives of H in G. We have a G-linear map

$$\varphi : \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big) \longrightarrow A$$

given by $f \mapsto \sum_{i\in I}\ x_i^{-1} f(x_i)$. This map is independent of the choice of representatives. In fact, if $x_i' = h_i x_i$, $h_i \in H$, then,

$$\sum_i (h_i x_i)^{-1}\ f(h_i x_i) = \sum_i x_i^{-1} h_i^{-1}\ f(h_i x_i) = \sum_i x_i^{-1} h_i^{-1} h_i f(x_i) = \sum_i x_i^{-1} f(x_i),$$

f being $\mathbb{Z}[H]$-linear. This homomorphism is functorial in A and induces a functorial homomorphism

$$H^n(\varphi) : H^n\big(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)\big) \to H^n(G, A).$$

Composing this with the functorial isomorphisms

$$(s_A^n)^{-1} : H^n(H, A) \to H^n\big(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)\big)$$

defined in **1.2.**, we obtain a functorial homomorphism $H^n(H, A) \to H^n(G, A)$ for all $n \geq 0$, called the *corestriction*, denoted by cores. It is easily seen that it commutes with the connecting homomorphisms. For $n = 0$, cores : $A^H \to A^G$ is the averaging map $m \to \sum_i x_i m$, $m \in A^H$.

Proposition 4.4. *Let G be a group and H a subgroup of finite index in G. Let A be a G-module. The composite* cores $\circ$ res : $H^q(G, A) \to H^q(G, A)$ *is multiplication by $[G : H]$ for all $q \geq 0$.*

Proof. For $q = 0$, cores $\circ$ res : $A^G \hookrightarrow A^H \to A^G$ is the map $a \mapsto \sum_i x_i a = na$ where $n = [G : h]$, $\{x_i\}$ denoting a set of right coset representatives of H in G. Since both cores $\circ$ res and multiplication by n are functorial and commute with connecting homomorphisms, it follows that cores $\circ$ res is multiplication by $n = [G : H]$ for all q. □

Corollary 4.5. *If G is a finite group of order n and A is any G-module, then $n \cdot H^q(G, A) = 0$ for $q \geq 1$. In particular if A is n-divisible, then $H^q(G, A) = 0$ for $q \geq 1$.*

Proof. We apply Proposition **4.4.** above for $H = (1)$ and note that $H^q(H, A) = 0$ for $q \geq 1$. □

§ 5. The Cup-product

Let G be a group and A and B two G-modules. The $\mathbb{Z}$-module $A \otimes_{\mathbb{Z}} B$ is made into a G-module through the diagonal action; i.e., $x(a \otimes b) = xa \otimes xb$, $x \in G$, $a \in A$, $b \in B$. Throughout this section, unadorned tensor products are taken over $\mathbb{Z}$.

Theorem 5.1. *Let A, B be G-modules and $A \otimes B$ the G-module through the diagonal action of G. Then, for all p, $q \geq 0$, there exist unique homomorphisms*

$$\cup_{p,q} : H^p(G, A) \otimes H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

satisfying the following conditions: (for $a \in H^p(G, A)$, $b \in H^q(G, B)$, $\cup_{p,q}(a \otimes b)$ is denoted by $a \cup b$)

1) *$\cup_{p,q}$ is functorial in A and B.*

2) $\cup_{0,0} : A^G \otimes B^G \to (A \otimes B)^G$ *is given by* $a \otimes b \to a \otimes b$.

3) *If* $0 \to A' \to A \to A'' \to 0$ *is an exact sequence of* G*-modules and* B *is a* G*-module such that the induced sequence*

$$0 \to A' \otimes B \to A \otimes B \to A'' \otimes B \to 0$$

is exact, then the diagram

$$\begin{array}{ccc} H^p(G, A'') \otimes H^q(G, B) & \xrightarrow{\cup_{p,q}} & H^{p+q}(G, A'' \otimes B) \\ \downarrow{\scriptstyle \delta_p \otimes 1} & & \downarrow{\scriptstyle \delta_{p+q}} \\ H^{p+1}(G, A') \otimes H^q(G, B) & \xrightarrow{\cup_{p+1,q}} & H^{p+q+1}(G, A' \otimes B) \end{array} \qquad (*)$$

is commutative for all $p,\ q \geq 0$ *; i.e., for* $a'' \in H^q(G, A'')$ *and* $b \in H^q(G, B)$,

$$\delta_{p+q}(a'' \cup b) = \delta_p(a'') \cup b.$$

4) *If* $0 \to B' \to B \to B'' \to 0$ *is an exact sequence of* G*-modules and* A *a* G*-module such that*

$$0 \to A \otimes B' \to A \otimes B \to A \otimes B'' \to 0$$

is exact, then, the diagram

$$\begin{array}{ccc} H^p(G, A) \otimes H^q(G, B'') & \xrightarrow{\cup_{p,q}} & H^{p+q}(G, A \otimes B'') \\ \downarrow{\scriptstyle 1 \otimes \delta_q} & & \downarrow{\scriptstyle (-1)^p \delta_{p+q}} \\ H^p(G, A) \otimes H^{q+1}(G, B') & \xrightarrow{\cup_{p,q+1}} & H^{p+q+1}(G, A \otimes B') \end{array}$$

is commutative; i.e.

$$\delta_{p+q}(a \cup b'') = (-1)^p a \cup \delta_q(b''),$$

for $a \in H^p(G, A)$, $b'' \in H^q(G, B'')$, *and all* $p,\ q \geq 0$.

Proof. We first prove the uniqueness. Let $\cup$, $\widehat{\cup}$ be two cup-products. By 2), $\cup_{0,0} = \widehat{\cup}_{0,0}$. We shall show that if $\cup_{p,q} = \widehat{\cup}_{p,q}$ for a pair of integers $p,\ q \geq 0$, then $u_{p+1,q} = \widehat{\cup}_{p+1,q}$ and $\cup_{p,q+1} = \widehat{\cup}_{p,q+1}$. An inductive argument shows that $\cup_{p,q} = \widehat{\cup}_{p,q}$ for all $p,\ q$. Suppose $\cup_{p,q} = \widehat{\cup}_{p,q}$ and $A,\ B$ a pair of G-modules. The exact sequence

$$0 \longrightarrow A \xhookrightarrow{i} A^* \longrightarrow A' \longrightarrow 0$$

of G-modules, i being the embedding of A in the co-induced module A^*, is $\mathbb{Z}$-split, the map $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}[G], A\big) \to A$ given by $f \mapsto f(1)$ being a left inverse of i. Hence the sequence

$$0 \to A \otimes B \to A^* \otimes B \to A' \otimes B \to 0$$

is exact. By 3), the diagram

$$\begin{array}{ccc} H^p(G,A')\otimes H^q(G,B) & \xrightarrow{\cup_{p,q}} & H^{p+q}(G,A'\otimes B) \\ \downarrow{\scriptstyle \delta_p\otimes 1} & & \downarrow{\scriptstyle \delta_{p+q}} \\ H^{p+1}(G,A)\otimes H^q(G,B) & \xrightarrow{\cup_{p+1,q}} & H^{p+q+1}(G,A\otimes B) \end{array}$$

is commutative for $\cup$ and $\widehat{\cup}$. For $p \geq 0$, $\delta_p : H^p(G,A') \to H^{p+1}(G,A)$ is surjective since $H^{p+1}(G,A^*) = 0$, so that $\delta_p \otimes 1$ is surjective. The commutativity of the above diagram for $\cup$ and $\widehat{\cup}$ shows that $\cup_{p+1,q} = \widehat{\cup}_{p+1,q}$. Similarly 4) can be used to show that $\cup_{p,q+1} = \widehat{\cup}_{p,q+1}$.

We next prove the existence of the cup-product. Let $a \in H^p(G,A)$, $b \in H^q(G,B)$ with $f \in Z^p(G,A)$, $g \in Z^q(G,B)$ as representatives, respectively. We define $f \cup g \in C^{p+q}(G, A\otimes B)$ by

$$(f\cup g)(x_1,\ldots,x_{p+q}) = f(x_1,\ldots,x_q)\otimes g(x_{p+1},\ldots,x_{p+q})$$

On can verify that $f \cup g$ is a cocycle whose cohomology class is independent of the representatives f, g of a and b, respectively. We define

$$a \cup b = [f \cup g] \in H^{p+q}(G, A\otimes B).$$

It may be verified that this map satisfies the conditions 1) to 4). □

Proposition 5.2. *Let A, B be G-modules. Let H be a subgroup of G. Then, the diagram*

$$\begin{array}{ccc} H^p(G,A)\otimes H^q(G,B) & \xrightarrow{\cup_{p,q}} & H^{p+q}(G,A\otimes B) \\ \downarrow{\scriptstyle \mathrm{res}\otimes\mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ H^p(H,A)\otimes H^{q+1}(H,B) & \xrightarrow{\cup_{p,q+1}} & H^{p+q+1}(H,A\otimes B) \end{array}$$

is commutative; i.e., for $a \in H^p(G,A)$, $b \in H^q(G,B)$, we have

$$\mathrm{res}(a\cup b) = (\mathrm{res}a)\cup(\mathrm{res}b).$$

Proof. For $p = q = 0$, by the definition of $\cup_{0,0}$ and res, the above diagram is commutative. It suffices, by induction, to show that if the above diagram commutes for a pair (p,q), it also commutes for the pairs $(p+1,q)$ and $(p,q+1)$. This is shown by a "dimension shift" argument, as in the proof of the uniqueness of the cup-product, by embedding A (resp. B) in a co-induced module. □

Proposition 5.3. *Let A, B, G, H be as in the above proposition, with $[G:H]$ finite. Then the diagram*

$$\begin{array}{ccccc} H^p(H,A)\otimes H^q(G,B) & \xrightarrow{1\otimes\mathrm{res}} & H^p(H,A)\otimes H^q(H,B) & \xrightarrow{\cup_{p,q}} & H^{p+q}(H,A\otimes B) \\ \downarrow{\scriptstyle \mathrm{cores}\otimes 1} & & & & \downarrow{\scriptstyle \mathrm{res}} \\ H^p(G,A)\otimes H^q(G,B) & = & H^p(G,A)\otimes H^q(G,B) & \xrightarrow{\cup_{p,q}} & H^{p+q+}(G,A\otimes B) \end{array}$$

is commutative, i.e., for $a \in H^p(H, A)$, $b \in H^q(G, B)$,

$$\text{cores}(a \cup \text{ res } b) = (\text{cores } a) \cup b.$$

Proof. For $p = q = 0$, the above diagram reads as

$$\begin{array}{ccccc} A^H \otimes B^G & \xrightarrow{1\otimes \text{res}} & A^H \otimes B^H & \xrightarrow{\cup} & (A \otimes B)^H \\ \downarrow{\scriptstyle \text{cores}\otimes 1} & & & & \downarrow{\scriptstyle \text{res}} \\ A^G \otimes B^G & = & A^G \otimes B^G & \xrightarrow{\cup} & (A \otimes B)^G \end{array}$$

and

$$(\text{cores} \circ \cup \circ 1 \otimes \text{ res})\ (a \otimes b) = \sum x_i(a \otimes b) = \sum x_i a \otimes x_i b = \cup\ (\text{cores} \otimes 1)(a \otimes b)$$

for $a \in A^H$, $b \in B^G$. The general case follows again by dimension shift argument, embedding A (resp. B) in a co-induced module. □

Proposition 5.4. *Let* A, B, C *be a* G*-modules and* $a \in H^p(G, A)$, $b \in H^q(G, B)$ *and* $c \in H^q(G, C)$. *If through the canonical identifications of* $A \otimes B$ *with* $B \otimes A$ *and* $(A \otimes B) \otimes C$ *with* $A \otimes (B \otimes C)$, *we identify the groups* $H^{p+q}(G, A \otimes B)$ *with the groups* $H^{p+q}(G, B \otimes A)$, *resp.* $H^{p+q+v}(G, (A \otimes B) \otimes C)$ *with* $H^{p+q+v}(G, A \otimes (B \otimes C))$, *then,* $a \cup b = (-1)^{pq}(b \cup a)$ *and* $(a \cup b) \cup c = a \cup (b \cup c)$.

Proof. We prove the skew-commutativity of the cup-product, by induction on $p+q$. For $p = q = 0$, the statement is obvious. We assume the result for a pair (p, q) and prove it for $(p + 1, q)$ and $(p, q + 1)$. Embedding A in a co-induced module A^*, with $A' = A^*/A$, we have a surjection $\delta_p : H^p(G, A') \to H^{p+1}(G, A)$. Let $a \in H^{p+1}(G, A)$, $b \in H^q(G, B)$. Let $a = \delta_p a'$ with $a' \in H^p(G, A')$. Then, by induction, we assume $a' \cup b = (-1)^{pq}(b \cup a')$. We have $a \cup b = \delta a' \cup b = \delta(a' \cup b) = (-1)^{pq}\delta(b \cup a') = (-1)^{pq}(-1)^q(b \cup \delta a') = (-1)^{(p+1)q} b \cup a$. Similarly, it can be shown for the pair $(p, q+1)$ by embedding B in a co-induced module that $a \cup b = (-1)^{p(q+1)} b \cup a$. □

§ 6. Profinite cohomology

A *profinite group* is an inverse limit of finite groups. Since any finite group is a compact topological group for the discrete topology, and since an inverse limit is a closed subset of the direct product, it follows that a profinite group is a compact topological group. We recall the following fact from point set topology: For a compact Hausdorff space X, the connected component of any $x \in X$ is the intersection of all compact open subsets of X containing x. The direct product is totally disconnected since the identity element is the intersection of all the open, compact subsets containing it. The same property therefore holds for the profinite groups, so that any profinite group is a compact totally disconnected topological group. The next proposition shows that profinite groups are precisely the compact totally disconnected topological groups.

Proposition 6.1 *Let G be a compact, totally disconnected topological group. Then G is isomorphic to the inverse limit $\varprojlim G/U$, where U runs over the family of all open normal subgroups U of G. (Hence G is profinite since G/U is finite.)*

Proof. Since G is compact, the open subgroups of G are precisely the closed subgroups of finite index. Let $\{U_\alpha\}_{\alpha\in I}$ be the family of all open normal subgroups of G. Since G is compact and totally disconnected, the compact open neighbourhood of e form a fundamental system of neighbourhoods of e. Since in a compact group, any compact open neighbourhood of e contains an open normal subgroup, it follows that $\{U_\alpha\}_{\alpha\in I}$ form a fundamental system of neighbourhoods of e. Since G is Hausdorff, $\cap_{\alpha\in I}U_\alpha = (e)$. The family $\{G/U_\alpha\}_{a\in I}$ is an inverse system of finite groups, the order on I being the inclusion $U_\alpha \subset U_\beta$ in the family $\{U_\alpha\}$. This inverse system is directed since $U_\alpha \cap U_\beta$ again belongs to the family. Let $\widetilde{G} = \varprojlim G/U_\alpha$. The canonical maps $G \to G/U_\alpha$ induce a continuous homomorphism $\phi : G \to \widetilde{G}$. Since $\cap_{\alpha\in I}U_\alpha = (e)$, ϕ is injective. If $(\bar{a}_\alpha) \in \varprojlim G/U_\alpha$ with $a_\alpha \in G$ as representatives, then $\cap_{\alpha\in J}a_\alpha U_\alpha \neq$ for any finite subset J of I. Since G is compact $\cap_{\alpha\in I}a_\alpha U_\alpha \neq$. Let $x \in \cap_{\alpha\in I}a_\alpha U_\alpha$. Then $\phi(x) = (\bar{a}_\alpha)$ so that ϕ is an isomorphism. □

Corollary 6.2. *Let H be a closed subgroup of a profinite group G. Then H is profinite. Further, if H is normal in G, G/H is profinite.*

Proof. Since G is compact, H, being closed in G, is compact. Let $\{U_\alpha\}_{\alpha\in I}$ be the family of open normal subgroups of G. Since $\{H \cap U_\alpha\}_{\alpha\in I}$ is cofinal in the family of open normal (compact) subgroups of H and since $\cap_\alpha(H \cap U_\alpha) = (e)$, H is totally disconnected and hence profinite. Let H be a closed normal subgroup of G. Then G/H is compact. To show that G/H is profinite, it suffices to show that G/H is totally disconnected. Let $x \notin H$. For each $h \in H$, there exists a compact open neighbourhood O_h of h, not containing x, since G is totally disconnected. Then $H \subset U_{h\in H}O_h$ and H being compact, there exist $h_1, \ldots, h_n \in H$ such that $H \subset O_{h_1} \cup O_{h_2} \ldots \cup O_{h_r} = S$. Since S is open, compact, containing H, but not x, it follows that G/H is totally disconnected. □

Example 6.3. Let K be a field and L/K a Galois extension, not necessarily finite. Let $G(L/K)$ be the Galois group. Let $\{K_\alpha\}_{\alpha\in I}$ run through all finite Galois extensions of K, contained in L. Then $G(L/K) = \varprojlim G(K_\alpha/K)$ where the order in I is the inclusion $K_\alpha \subset K_\beta$ of fields. Thus $G(L/K)$ is a profinite group. The open normal subgroups of G are precisely the groups $G(L/K_\alpha)$, $\alpha \in I$.

Let G be a profinite group. A G-module A is called *discrete* if the map $G \times A \to A$, $(x, a) \mapsto xa$ is continuous for the discrete topology of A.

Proposition 6.4. *A G-module is discrete if and only if $A = \cup A^U$, U running over open normal subgroups of G. In particular, any trivial G-module is discrete.*

Proof. Let A be a G-module. For $a, b \in A$, let $V_{a,b} = \{x \in G \mid xa = b\}$. Suppose A is discrete. For any $a \in A$, the map $G \to A$ given by $x \mapsto xa$ is continuous, and A being discrete, for any $b \in B$, $V_{a,b}$ is open. In particular, for every $a \in A$, $V_{a,a}$ is open and hence contains an open normal subgroup U_a and $a \in A^{U_a}$. Hence $A = \cup_a A^{U_a}$. Suppose, conversely that A is a G-module satisfying $A = \cup A^U, U$ running over open normal subgroups of G. For $a \in A$, let U_a denote an open normal subgroup for which $a \in A^{U_a}$. For every $x \in V_{a,b}$, $x \cdot U_a \subset V_{a,b}$ so that $V_{a,b}$ is open. Hence the map $G \times A \to A$, $(x, a) \mapsto xa$ is continuous for the discrete topology of A so that A is discrete. □

Let G be a profinite group and U, U' open normal subgroups of G, with $U' \subset U$. Let A be a discrete G-module. If $\eta_{U,U'} : G/U' \to G/U$ is the canonical map and

$$\phi_{U,U'} : A^U \hookrightarrow A^{U'}$$

is the inclusion, then, the pair $(\eta_{U,U'}, \phi_{U,U'})$ is a compatible pair, in the sense of § 4. This pair induces a homomorphism

$$\inf (U, U') : H^q(G/U, A^U) \to H^q(G/U', A^{U'}).$$

The system $\{H^q(G/U, A^U), \inf\}$ is a direct system of abelian groups. We define the group $H_c^q(G, A)$ to be the direct limit of the system $(H^q(G/U, A^U), \inf)$ and call it the *profinite cohomology* of G with values in the discrete G-module A. Every finite group G is also a profinite group and any G-module A is discrete. Further, $H_c^q(G, A) = H^q(G, A)$ if G is finite.

Let L/K be a Galois extension, not necessarily finite. The Galois group $G(L/K) = G$ is a profinite group, its open normal subgroups being $G(L/L')$ where L' runs over finite Galois extensions of K, contained in L. Since $L = \cup\, L^{G(L/L')} = \cup\, L'$, $L^* = \cup\, L'^*, L'$ running over finite Galois extensions of K contained in L, L and L^* are discrete G-modules.

Proposition 6.5. *Let L/K be a Galois extension. Then $H_c^q\big(G(L/K), L\big) = 0$ for all $q \geq 1$ and $H_c^1\big(G(L/K), L^*\big) = 0$.*

Proof. If L/K is a finite Galois extension, $H_c^q\big(G(L/K), L\big) = H^q\big(G(L/K), L\big) = 0$ and $H_c^1\big(G(L/K), L^*\big) = H^1\big(G(L/K), L^*\big) = 0$, in view of **3.1.** and **3.3.**. The proposition is now a consequence of the definition of profinite cohomology. □

Let G be a profinite group and H a closed subgroup of G. Let A be a discrete H-module. Let $\mathrm{Map}_H(G, A)$ denote the abelian group of all continuous maps $f : G \to A$ satisfying $f(yx) = yf(x)$ for all $y \in H$. We make this group into a G-module by defining $(x'f)(x) = f(xx')$. In view of the following lemma, $\mathrm{Map}_H(G, A)$ is a discrete G-module.

Lemma 6.6. *Let G be a profinite group and A an abelian group with discrete*

topology. Let $f : G \to A$ be a continuous map. Then there exists an open normal subgroup W of G such that $f(xy) = f(x)$ for all $x \in G$, $y \in W$.

Proof. Since A is discrete, $U_a = f^{-1}(a)$, $a \in A$ is an open subset of G. Since G is compact and totally disconnected, open normal subgroups of G form a fundamental system of neighbourhoods of G. Hence $f^{-1}(a) = f^{-1}(a)W_a$ for some open normal subgroup W_a of G. We have an open covering $G = \cup_{a\in A}U_a$ and G being compact, there is a finite covering $G = \cup_{1\leq i\leq n}U_{a_i}$ by disjoint open sets. Then $\cap_{1\leq i\leq n}W_{a_i} = W$ is an open normal subgroup of G. We have $U_{a_i} = U_{a_i} \cdot W_{a_i} \supseteq U_{a_i}W \supseteq U_{a_i}$, so that $U_{a_i} = U_{a_i}W$, $1 \leq i \leq n$. Hence $f(xy) = f(x)$ for all $x \in G$, $y \in W$, ($\{U_{a_i}\}$, $1 \leq i \leq n$, being a covering of G). □

Any discrete G-module isomorphic to $\mathrm{Map}_H(G, A)$ for some discrete H-module A is said to be *co-induced from H*. In particular, if $H = (e)$, modules co-induced from H are called *co-induced*. We note that if G is a finite group, the notion of being co-induced in the profinite sense is the same as being co-induced in the usual sense, since $\mathrm{Map}_H(G, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[H]}\big(\mathbb{Z}[G], A\big)$ as G-modules.

Proposition 6.7. *Let G be a profinite group and A a discrete G-module. Then the groups $H_c^q(G, A)$ satisfy the following conditions:*

1) *$H_c^0(G, A) = \cup A^U$, U running over all the open normal subgroups of G.*

2) *$H_c^0(G, A)$ is functorial in A, for all $q \geq 0$.*

3) *for any exact sequence*

$$0 \longrightarrow A' \xrightarrow{f} A \xrightarrow{g} A'' \longrightarrow 0$$

of discrete G-modules, there exist connecting homomorphisms

$$\delta_q : H_c^q(G, A'') \to H_c^{q+1}(G, A')$$

such that the sequence

$$\ldots \longrightarrow H_c^q(G, A') \xrightarrow{H_c^q(f)} H_c^q(G, A) \xrightarrow{H_c^q(g)} H_c^q(G, A'') \xrightarrow{\delta_q} H_c^{q+1}(G, A') \longrightarrow \ldots$$

is exact. Further, δ_q is functorial.

4) *For any closed subgroup H of G and any discrete H-module A, there exists a functorial isomorphism*

$$s_q : H_c^q\big(G, \mathrm{Map}_H(G, A)\big) \xrightarrow{\sim} H_c^q(H, A)$$

for all $q \geq 0$. In particular, $H_c^q(G, A) = 0$ if A is co-induced and $q \geq 1$.

Proof. All the four statements above are valid if G is finite (see **1.1**). Since the profinite cohomology of G is defined as the direct limit cohomologies of its finite quotients, by functoriality of direct limits and the fact that direct limits commute with exact sequences, it follows that 1) $\Rightarrow$ 4) above are valid for a profinite group G. □

Let $f : G \to G'$ be a continuous homomorphism of profinite groups. Let A (resp. A') be a discrete G (resp. G') module. We regard A' as a G-module through f. Then A' is discrete as a G-module. Let $\phi : A' \to A$ be a G-homomorphism. The pair (f, ϕ) is called a *compatible pair*, in analogy with the case of finite groups. Such a pair gives rise to a homomorphism $H^n(G, A) \to H^n(G', A')$, which may be defined as the direct limit of the corresponding maps of the cohomology of the finite quotients, induced by (f, ϕ).

If H is a closed subgroup of G, then the inclusion $H \overset{I}{\hookrightarrow} G$ and the identity map $A \to A$ form a compatible pair for any discrete G-module A. The induced homomorphism $H_c^q(G, A) \to H_c^q(H, A)$ is called the *restriction*. If H is a closed normal subgroup of $G, G/H$ is profinite (see Corollary**6.2.**) and A^H is a discrete G/H-module. The canonical map $\eta : G \to G/H$ and the inclusion $A^H \hookrightarrow A$ form a compatible pair, giving rise to a homomorphism $H_c^q(G/H, A^H) \to H_c^q(G, A)$ called the *inflation*.

Let H be a closed subgroup of finite index of a profinite group G. One has, as in the finite case, a homomorphism cores: $H_c^q(H, A) \to H_c^q(G, A)$ for any discrete G-module A.

If A, B are discrete A-modules, then $A \otimes_{\mathbb{Z}} B$ is again discrete, for the diagonal action of G. As in the case of finite groups, we can define the cup-product

$$H_c^p(G, A) \times H_c^q(G, B) \overset{\cup_{p,q}}{\longrightarrow} H_c^{p+q}(G, A \otimes_{\mathbb{Z}} B).$$

With these definitions of restriction, corestriction and cup-products, all the statements and proofs of the properties of these maps, given in § 4 and § 5, can be suitably translated into statements and proofs with profinite cohomology replacing the cohomology. From now onwards, we shall use these results for profinite cohomology.

§ 7. Brauer groups as a Galois cohomology

In this section, we prove that the Brauer group of a field is isomorphic to the profinite cohomology group $H_c^2(G(K_s/K), K_s^*)$, K_s denoting a separable closure of K. Let L/K be a finite Galois extension with Galois group $G(L/K) = G$. In view of **4.3.** of Ch. I, we have an isomorphism

$$c_L : H^2(G, L^*) \overset{\sim}{\to} \mathrm{Br}(L/K)$$

given by $[f] \mapsto [(K, G, f)]$, (K, G, f) denoting the crossed product over L associated to the cocycle f. Let $K \subset L' \subset L$ be a tower of Galois extensions of K with

$H = G(L/L')$, so that $G(L'/K) \xrightarrow{\sim} G/H$. Since any central simple algebra over K, split by L', is also split by L, $\mathrm{Br}(L'/K) \hookrightarrow \mathrm{Br}(L/K)$.

Proposition 7.1. *The diagram*

$$\begin{array}{ccc} H^2(G/H, L'^*) & \xrightarrow{c_{L'}} & \mathrm{Br}(L'/K) \\ \downarrow \inf & & \downarrow \\ H^2(G, L^*) & \longrightarrow & Br(L/K) \end{array}$$

is commutative.

Proof. Let $\overline{f} \in Z^2(G/H, L'^*)$. Then, $\inf[\overline{f}] = [f]$, where $f \in Z^2(G, L^*)$ is defined as the composite

$$G \times G \xrightarrow{\eta\times\eta} G/H \times G/H \xrightarrow{\overline{f}} L'^* \times L'^* \hookrightarrow L^* \times L^*.$$

The commutativity of the above diagram is equivalent to $[(K, G, f)] = [(K, G/H, \overline{f})]$ in $\mathrm{Br}(K)$. Let $B = (K, G/H, \overline{f})$ and $A = M_r(B)$ where $r = [L : L']$. Then A is Brauer equivalent to B and $[A : K] = [L : L']^2[L' : K]^2 = [L : K]^2 = [(K, G, f) : K]$. We shall show that (K, G, f) is isomorphic to A. Let $\{t_i\}$, $1 \leq i \leq r$ be a basis of L over L'. For $\sigma \in G$, let

$$\sigma(t_i) = \sum\nolimits_{j=1}^{r} h_{ij}(\sigma)t_j,$$

$h_{ij}(\sigma) \in L'$, $1 \leq i, j \leq r$. Let $\psi(\sigma) = (h_{ij}(\sigma)) \in M_r(L')$. For $\ell \in L$, let

$$\ell t_i = \sum\nolimits_{j=1}^{r} \ell_{ij}(\ell)t_j$$

with $\ell_{ij}(\ell) \in L'$ (i.e., the regular representation of L over L'. It may be verified that there is a homomorphism $(K, G, f) \to A$ induced by the assignment $e_\sigma \mapsto \psi(\sigma)^{-1}e_{\bar{\sigma}}$, $\ell \mapsto (\ell_{ij}(\ell))$. Since $[(K, G, f) : K] = [A, K]$, this homomorphism is indeed an isomorphism. □

Let K_s be a separable closure of K. The set of finite Galois extensions of K inside K_s is a directed set, for the ordering given by inclusion, since the composite of two Galois extensions is again Galois. Since $\mathrm{Br}(K) = \cup_L Br(L/K)$, L running over all finite Galois extensions of K contained in K_s (see **2.9.** of Ch. I), it follows that $\mathrm{Br}(K) = \varinjlim_L \mathrm{Br}(L/K)$. The above proposition shows that we have an isomorphism

$$H_c^2(G(K_s/K), K_s^*) = \varinjlim_L H^2\big(G(L/K), L^*\big) \to \varinjlim_L \mathrm{Br}(L/K) = \mathrm{Br}(K)$$

where the limits are taken over all finite Galois extensions of K contained in K_s.

Chapter III: A cohomological formulation of Merkurjev's theorem

§ 1. The K-groups of Milnor

Let K be a field and let $T(K^*)$ denote the tensor algebra over $\mathbb{Z}$, of the abelian group K^*. Let $K_*(K)$ denote the quotient of $T(K^*)$ by the two-sided ideal I generated by all the elements of the form $a \otimes (1-a)$ for all $a \in K^*$, $a \neq 1$. Since this ideal is homogeneous, $K_*(K)$ is a graded algebra over $\mathbb{Z}$. We write

$$K_*(K) = K_0(K) \oplus K_1(K) \oplus \dots \ .$$

Since I has homogeneous generators of degree 2, $K_0(K) = T_0(K) = \mathbb{Z}$ and $K_1(K) = T_1(K) = K^*$. For $n \geq 2$, $K_n(K)$ is the abelian group generated by $(K^*)^n$ with the relations

$$(a_1, \dots, a_i, a_{i+1}, \dots, a_n) = 0 \quad \text{if} \quad a_i + a_{i+1} = 1,\ 1 \leq i \leq n-1$$

$$(a_1, \dots, a_i a_i', \dots, a_n) = (a_1, \dots, a_i, \dots, a_n) + (a_1, \dots, a_i', \dots, a_n),\ 1 \leq i \leq n.$$

For $a_1, \dots, a_n \in K^*$, the image of $a_1 \otimes \dots \otimes a_n$ in $K_n(K)$ is denoted by $\langle a_1, \dots, a_n \rangle$. Let L/K be a field extension. The inclusion $K^* \hookrightarrow L^*$ induces an algebra homomorphism $K_*(K) \to K_*(L)$. In particular, for all integers $n \geq 0$, we have homomorphisms ext: $K_n(K) \to K_n(L)$ called the *extension* homomorphisms, which are functorial. Let L/K be a finite extension. Then there exist homomorphisms $\mathrm{tr} : K_n(L) \to K_n(K)$ called the *transfer* homomorphisms which are functorial and which satisfy the following

1) *"Projection formula"*

$$\mathrm{tr}\left(\langle x_1, \dots, x_n \rangle \cdot \mathrm{ext}\, \langle y_1, \dots, y_m \rangle\right) = \mathrm{tr}\left(\langle x_1, \dots, x_n \rangle\right) \cdot \langle y_1, \dots, y_m \rangle$$

for $x_i \in L^*$, $1 \leq i \leq n$, $y_j \in K^*$, $1 \leq j \leq m$.

2) $\mathrm{tr} : K_0(L) \to K_0(K)$ is multiplication by $[L : K]$ and $\mathrm{tr} : K_1(L) \to K_1(K)$ is the norm $N_{L/K} : L^* \to K^*$. (See Appendix III for the existence of the transfer homomorphism.)

We note that 2) implies that for any $n \geq 0$, the composite homomorphism

$$\mathrm{tr} \circ \mathrm{ext} : K_n(K) \to K_n(K)$$

is multiplication by $[L : K]$.

We shall be interested only in $K_2(K)$. An element of $K_2(K)$ of the form $\langle a, b \rangle$, $a, b \in K^*$ is called a *symbol*. We list some of the properties of symbols, needed for later use.

Proposition 1.1

i) $\langle a, 1\rangle = \langle 1, a\rangle = 0$

ii) $\langle a^{-1}, b\rangle = \langle a, b^{-1}\rangle = -\langle a, b\rangle$

iii) $\langle a, -a\rangle = 0$

iv) $\langle a, b\rangle = -\langle b, a\rangle$

Proof. $\langle a, 1\rangle = \langle a, 1\rangle + \langle a, 1\rangle \Rightarrow \langle a, 1\rangle = 0$. Similarly $\langle 1, a\rangle = 0$. We have $0 = \langle 1, b\rangle = \langle aa^{-1}, b\rangle = \langle a, b\rangle + \langle a^{-1}, b\rangle$ so that

$$\langle a^{-1}, b\rangle = -\langle a, b\rangle.$$

Similarly $\langle a, b^{-1}\rangle = -\langle a, b\rangle$. To prove iii) we may assume $a \neq 1$. We have

$$\begin{aligned} 0 &= \langle a^{-1}, 1 - a^{-1}\rangle = \langle a^{-1}, (1-a)(-a)^{-1}\rangle \\ &= -\langle a, 1-a\rangle + \langle a, -a\rangle = \langle a, -a\rangle. \end{aligned}$$

To prove iv), we note that

$$\begin{aligned} 0 &= \langle ab, -ab\rangle = \langle a, -a\rangle + \langle a, b\rangle + \langle b, a\rangle + \langle b, -a\rangle \\ &= \langle a, b\rangle + \langle b, a\rangle. \end{aligned}$$

□

§ 2. The norm residue homomorphism

From now onwards, we assume that K is a field of characteristic $\neq 2$. For a pair of elements $a, b \in K^*$, we denote by $(\frac{a,b}{K})$ the quaternion algebra over K defined by the generators ξ, η with relations $\xi^2 = a$, $\eta^2 = b$, $\xi\eta + \eta\xi = 0$.

Proposition 2.1. *The map $K^* \times K^* \to {}_2\,\mathrm{Br}(K)$ given by $(a, b) \mapsto (\frac{a,b}{K})$ induces a homomorphism $\widetilde{\alpha}_K : K_2(K) \to {}_2\,\mathrm{Br}(K)$.*

Proof. We show that in $\mathrm{Br}(K)$

$$[(\frac{a, bb'}{K})] = [(\frac{a, b}{K})] \cdot [(\frac{a, b'}{K})] \qquad (*)$$

for a, b, $b' \in K^*$. If $\sqrt{a} \in K$, then all the three classes above are trivial (**5.7.** of Chapter I). Suppose $\sqrt{a} \notin K$. If σ is the Galois automorphism $\sqrt{a} \mapsto -\sqrt{a}$ of $K(\sqrt{a})$ over K, then, for any $c \in K^*$, the algebra $(\frac{a,c}{K})$ is the crossed product over $K(\sqrt{a})$ corresponding to the cocycle f given by $f(\sigma, \sigma) = c$. Then $(*)$ follows from **3.5.** of Chapter I. The additivity of the map $K^* \times K^* \to {}_2\,\mathrm{Br}(K)$ in the first variable can be checked in a similar manner. Since either $\sqrt{a} \in K^*$ or $1 - a$ is a norm from

the extension $K(\sqrt{a})/K$, it follows from **5.7.** of Chapter I that $(\frac{a,1-a}{K})$ is a matrix algebra. We therefore have a homomorphism $\tilde{\alpha}_K : K_2(K) \to {}_2\,\mathrm{Br}(K)$. □

Let $k_2(K) = K_2(K)/2K_2(K)$. Then $\tilde{\alpha}_K$ induces a homomorphism

$$\alpha_K : k_2(K) \to {}_2\,\mathrm{Br}(K)$$

which is called the *norm residue homomorphism*: Obviously, α_K is functorial in K. The object of these lectures is to prove the following

Theorem 2.2. (Merkurjev) *The map $\alpha_K : k_2(K) \to {}_2\,\mathrm{Br}(K)$ is an isomorphism.*

The surjectivity of the map α_K settles in the affirmative the classical question whether the 2-torsion in the Brauer group of a field is generated by quaternion algebras. The fact that α_K is an isomorphism yields a presentation of ${}_2\,\mathrm{Br}(K)$ in terms of generators and relations. The injectivity of α_K settles in the affirmative a question of Pfister in the theory of quadratic forms. We shall not however discuss this application of Merkurjev's theorem in these lectures.

§ 3. The case of number fields and finite fields

We shall record for further use, the fact that α_K is an isomorphism if K is either a number field or a finite field. We begin with

Lemma 3.1. *If $a, b \in K^*$ are such that $(\frac{a,b}{K})$ is trivial in ${}_2\,\mathrm{Br}(K)$, then $\langle a, b\rangle \in 2K_2(K)$.*

Proof. Suppose $(\frac{a,b}{K}) = M_2(K)$. In view of **5.7.**, Chapter I, there exist λ, $\mu \in K^*$ with $b = \lambda^2 - a\mu^2$. If $\mu = 0$, then $\langle a, b\rangle = \langle a, \lambda^2\rangle = 2\langle a, \lambda\rangle$. If $\lambda = 0, \langle a, b\rangle = \langle a, -a\mu^2\rangle = \langle a, -a\rangle + 2\langle a, \mu\rangle = 2\langle a, \mu\rangle$. Suppose $\lambda\mu \neq 0$. Then $0 = \langle a\mu^2\lambda^{-2}, 1 - a\mu^2\lambda^{-2}\rangle = \langle a\mu^2\lambda^{-2}, b\lambda^{-2}\rangle = \langle a, b\rangle + 2\langle \mu\lambda^{-1}, b\rangle - 2\langle a\mu^2\lambda^{-2}, \lambda\rangle$. □

The above lemma establishes the injectivity of α_K for fields K for which every element of $k_2(K)$ can be represented by a single symbol $\langle a, b\rangle$. This is indeed the case for number fields. The difficulty in the general case is that not every element of $k_2(K)$ can be represented as the class of a single symbol.

Proposition 3.2. *Let K be a number field. Any element of $K_2(K)$ is congruent to a single symbol $\langle a, b\rangle$ modulo $2K_2(K)$.*

For proving this proposition, we need the following

Lemma 3.3. *Let K be any field of characteristic $\neq 2$. If the quadratic form $ax^2 + by^2 - abz^2$ represents zero nontrivially, then $\langle a, b\rangle \in 2K_2(K)$. If $c \in K^*$ is*

represented by $ax^2+by^2-abz^2$, *then there exists* $a' \in K^*$ *such that* $\langle a,b\rangle \equiv \langle a',c\rangle$ *modulo* $2K_2(K)$.

Proof. If $\sqrt{a} \in K^*$, then $\langle a,b\rangle \in 2K_2(K)$ and we may take, for example, $a'=1$. Let $\sqrt{a} \notin K^*$. Let λ, μ, $\nu \in K$, not all zero, such that $a\lambda^2+b\mu^2-ab\nu^2=0$. We note that $\mu^2-a\nu^2 \neq 0$ since otherwise, either $\sqrt{a} \in K$ or $\lambda=\mu=\nu=0$. We have $b=-a\lambda^2(\mu^2-a\nu^2)^{-1}$ so that $\langle a,b\rangle = \langle a,-a\rangle+\langle a,\lambda^2\rangle-\langle a,\mu^2-a\nu^2\rangle \equiv \langle a,\mu^2-a\nu^2\rangle$ mod $2K_2(K)$. Since $(\frac{a,\mu^2-a\nu^2}{K})$ is a matrix algebra, (Chapter I, **5.7.**), it follows from Lemma **3.1.** that $\langle a,\mu^2-a\nu^2\rangle \in 2K_2(K)$ and the first part of the lemma is proved. Let λ, μ, $\nu \in K$ be such that $a\lambda^2+b\mu^2-ab\nu^2=c \in K^*$. Then $b(\mu^2-a\nu^2)=c-a\lambda^2$. If $\mu^2-a\nu^2=0$, then $c=a\lambda^2$ and $\langle a,b\rangle \equiv \langle c,b\rangle = \langle b^{-1},c\rangle$ modulo $2K_2(K)$. Let $\mu^2-a\nu^2 \neq 0$. Then $c^2-a\lambda^2 \neq 0$ and $b=(c-a\lambda^2)(\mu^2-a\nu^2)^{-1}$. We have, $\langle a,b\rangle = \langle a,c-a\lambda^2\rangle - \langle a,\mu^2-a\nu^2\rangle \equiv \langle a,c-a\lambda^2\rangle$ mod $2K_2(K)$, by **3.1.**. Further,

$$\begin{aligned}\langle a,c-a\lambda^2\rangle &= \langle a,c-a\lambda^2\rangle - \langle a\lambda^2c^{-1},1-a\lambda^2c^{-1}\rangle \\ &\equiv \langle a,c-a\lambda^2\rangle - \langle a,(c-a\lambda^2)c^{-1}\rangle + \langle c,(c-a\lambda^2)c^{-1}\rangle \\ &= \langle a,c\rangle - \langle (c-a\lambda^1)c^{-1},c\rangle = \langle ac(c-a\lambda^2)^{-1},c\rangle.\end{aligned}$$

□

Proof of Proposition 3.2. By induction, it is enough to prove that for a, b, c, $d \in K^*$, $\langle a,b\rangle+\langle c,d\rangle \equiv \langle e,f\rangle$ mod $2K_2(K)$, for some $e,f \in K^*$. The quadratic form $q=(ax^2+by^2-abz^2)-(cu^2+dv^2-cdw^2)$ has a nontrivial zero at any real completion of K. In fact, if in a real completion $\widehat{K}$, b is positive (resp. d positive), we may take $x=\sqrt{b}$, $y=0$, $z=1$, $u=v=w=0$ (resp. $u=\sqrt{d}$, $v=0$, $w=1$, $x=y=z=0$), as a nontrivial zero of q. If b and d are both negative, $x=0$, $y=(\sqrt{-b})^{-1}$, $z=0=u$, $v=(\sqrt{-d})^{-1}$, $w=0$ is a nontrivial zero of q. Since q is a form in 6 (≥ 5) variables, q has a nontrivial zero in every non-archimedean completion of K. By Hasse-Minkowski Theorem, q has a nontrivial zero in K. Let λ, μ, ν, λ', μ', $\nu' \in K$ not all zero such that $a\lambda^2+b\mu^2-ab\nu^2=c\lambda'^2+d\mu'^2-cd\nu^2=c_0$. If $c_0=0$, by Lemma **3.3.**, either $\langle a,b\rangle$ or $\langle c,d\rangle$ belongs to $2K_2(K)$ and hence $\langle a,b\rangle+\langle c,d\rangle$ reduces to a single symbol modulo $2K_2(K)$. If $c_0 \neq 0$, again by **3.3.**, $\langle a,b\rangle \equiv \langle a',c_0\rangle$, $\langle c,d\rangle \equiv \langle c',c_0\rangle$ modulo $2K_2(K)$ so that $\langle a,b\rangle+\langle c,d\rangle \equiv \langle a'c',c_0\rangle$ modulo $2K_2(K)$ and the proposition is proved. □

Theorem 3.4. *Let* K *be an algebraic number field. Then the map*

$$\alpha_K : k_2(K) \to {}_2\,\mathrm{Br}(K)$$

is an isomorphism.

Proof. In view of **3.2.** and the remark preceding **3.2.**, injectivity of α_K follows. Let A be a central simple algebra over K with $[A] \in {}_2\,\mathrm{Br}(K)$. By a classical theorem for number fields (see Albert, for instance), we have index $A = \exp A \leq 2$ so that A is either a matrix algebra over K or a matrix algebra over a quaternion algebra over K, so that $[A] \in$ im α_K. Thus α_K is surjective. □

Theorem 3.5. *Let K be a finite field. Then both $K_2(K)$ and $\mathrm{Br}(K)$ are trivial so that α_K is an isomorphism.*

Proof. The fact that $\mathrm{Br}(K)$ is trivial follows from the celebrated theorem of Wedderburn that every finite division ring is commutative. We now show that $K_2(K)$ is trivial. Let c be a generator of the cyclic group K^*. Then K_2 is generated by $\langle c, c\rangle$. Since $\langle c, c\rangle = -\langle c, c\rangle$, it follows that $2\langle c, c\rangle = 0$ and hence $2K_2(K) = 0$. If $\sqrt{c} \in K$, then $\langle c, c\rangle = 2\langle\sqrt{c}, c\rangle \in 2K_2(K) = 0$, so that $K_2(K) = 0$. If $\sqrt{c} \notin K$, then c is a norm from $K(\sqrt{c})/K$, in view of the following lemma, so that $\langle c, c\rangle = 0$ by **3.1.** and $K_2(K) = 0$. □

Lemma 3.6. *Let K be a finite field and L/K a finite extension. Then, the norm map $L^* \to K^*$ is surjective.*

Proof. Consider the sequence

$$1 \longrightarrow K^* \hookrightarrow L^* \xrightarrow{1-\sigma} L^* \xrightarrow{N_{L/K}} K^*$$

where $1-\sigma : L^* \to L^*$ is the map $x \mapsto x(\sigma x)^{-1}$, σ denoting a generator of the Galois group $G(L/K)$ (which is cyclic). By Hilbert Theorem 90 (see **3.2.**, chapter II), the sequence $L^* \xrightarrow{1-\sigma} L^* \xrightarrow{N_{L/K}} K^*$ is exact. If σ is a generator of $G(L/K)$, it follows that $\ker(1-\sigma) = K^*$, and hence the above sequence is exact. A counting argument shows that $|N_{L/K}(L^*)| = |K^*|$ so that $N_{L/K}$ is surjective. □

§ 4. Norm residue homomorphism via Galois cohomology

Let K be a field of characteristic $\neq 2$. Let K_s denote the separable closure of K. The squaring map $K_s^* \xrightarrow{2} K_s^*$ is surjective, with kernel $\mu_2 = (\pm 1)$. Let $G = G(K_s/K)$. We have an exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow K_s^* \xrightarrow{2} K_s^* \longrightarrow 1$$

of discrete G-modules. The above exact sequence gives rise to the following long exact sequence of cohomology groups

$$\begin{aligned} 1 \longrightarrow H_c^0(G, \mu_2) \longrightarrow H_c^0(G, K_s^*) \xrightarrow{2} H_c^0(G, K_s^*) \longrightarrow H_c^1(G, \mu_2) \longrightarrow H_c^1(G, K_s^*) \\ \longrightarrow H_c^1(G, K_s^*) \longrightarrow H_c^2(G, \mu_2) \longrightarrow H_c^2(G, K_s^*) \longrightarrow H_c^2(G, K_s^*) \longrightarrow \dots \end{aligned}$$

Since $H_c^1(G, K_s^*) = 1$ (Proposition **6.4.**, Chapter II), the above sequence breaks up into two exact sequences.

$$1 \longrightarrow \mu_2 \longrightarrow K^* \xrightarrow{2} K^* \xrightarrow{\delta_0} H_c^1(G, \mu_2) \longrightarrow 1$$

$$1 \longrightarrow H_c^1(G, \mu_2) \xrightarrow{\delta_1} H_c^2(G, K_s^*) \xrightarrow{2} H_c^2(G, K_s^*).$$

The map δ_0 induces an isomorphism $K^*/K^{*^2} \xrightarrow{\sim} H^1_c(G,\mu_2) = \mathrm{Hom}_c(G,\mu_2)$ (the group of continuous homomorphisms of G into μ_2), which can be described as follows: For any $b \in K^*$, $\delta_0(\bar{b}) = \chi_b$ where $\chi_b : G \to \mu_2$ is given by $\chi_b(\sigma) = \sigma(\sqrt{b})/\sqrt{b}$. (Note that χ_b is continuous since it is trivial on $H = G(K_s/K(\sqrt{b}))$. With the identification of $H^2_c(G,K^*_s)$ with $\mathrm{Br}(K)$ (see the end of Chapter II), we see that $H^2_c(G,\mu_2) = \ker(\mathrm{Br}(K) \xrightarrow{2} \mathrm{Br}(K))$ can be identified with ${}_2\,\mathrm{Br}(K)$.

We have an isomorphism $\rho : \mu_2 \otimes \mu_2 \xrightarrow{\sim} \mu_2$ given by $\rho(-1 \otimes -1) = -1$, $\rho(1 \otimes -1) = \rho(-1 \otimes 1) = \rho(1 \otimes 1) = 1$, which we regard as an identification of G-modules. The cup-product induces a map

$$K^* \times K^* \to K^*/K^{*^2} \times K^*/K^{*^2} \xrightarrow{\sim} H^1_c(G,\mu_2) \times H^1_c(G,\mu_2) \xrightarrow{\cup}$$
$$H^2_c(G,\mu_2 \otimes \mu_2) \overset{H^2(\rho)}{=} H^2_c(G,\mu_2) \xrightarrow{\sim} {}_2\,\mathrm{Br}(K)$$

which maps $(a,b) \in K^* \times K^*$ to $H^2(\rho)(\chi_a \cup \chi_b) = \chi_a \cup \chi_b$.

Proposition 4.1. *For $a,b \in K^*$, the image of (a,b) in ${}_2\,\mathrm{Br}(K)$ under the above map is the class of the quaternion algebra $(\frac{a,b}{K})$.*

Proof. For any cohomology class $[\tilde{f}] \in H^2_c(G,\mu_2)$, there exists a 2-cocycle $f \in Z^2(G(L/K),L^*)$ for some finite Galois extension L of K such that $[\tilde{f}] = \inf[f]$, $\inf : H^2(G(L/K),L^*) \to H^2_c(G,K^*_s)$ being the inflation homomorphism. Then the isomorphism $H^2_c(G,\mu_2) \xrightarrow{\sim} {}_2\,\mathrm{Br}(K)$ maps $[\tilde{f}]$ into the class of the crossed product $(K,G(L/K),f)$ in $\mathrm{Br}(K)$. To prove the proposition, we first note that if either a or b belongs to K^{*^2}, both $\chi_a \cup \chi_b$ and $(\frac{a,b}{K})$ are trivial. Thus we assume that a and b do not belong to K^{*^2}. Suppose $K(\sqrt{a}) = K(\sqrt{b}) = L$. By the explicit description of the cup-product given in **5.1.** of Chapter II, the cocycle $\chi_a \cup \chi_b$ is given by

$$(\chi_a \cup \chi_b)(\sigma,\tau) = \chi_a(\sigma) \otimes \chi_b(\tau),\ \sigma,\ \tau \in G,$$

i.e.,

$$(\chi_a \cup \chi_b)(\sigma,\tau) = \begin{cases} 1 \otimes 1 & \text{if } \sigma|_L = \tau|_L = \text{identity} \\ 1 \otimes (-1) & \text{if } \sigma| - L = \text{identity},\ \tau|_L \neq \text{identity} \\ (-1) \otimes 1 & \text{if } \sigma|_L \neq \text{identity},\ \tau|_L = \text{identity} \\ (-1) \otimes (-1) & \text{if } \sigma|_L = \tau|_L \neq \text{ identity.} \end{cases}$$

Through the identification of $\mu_2 \otimes \mu_2$ with μ_2, the image of $\chi_a \cup \chi_b$ in $H^2_c(G,\mu_2)$, denoted again by $\chi_a \cup \chi_b$ is in fact $\inf[f]$ where $f \in Z^2(G(L/K),L^*)$ is given by $f(\sigma,\sigma) = -1$, where σ is the non-trivial automorphism of L/K. On the other hand $[(\frac{a,b}{K})] = [(K,G(L/K),g)]$ where $g \in Z^2(G(L/K),L^*)$ is given by $g(\sigma,\sigma) = b$. Let $h : G(L/K) \to L^*$ be the normalized 1-cochain defined by $h(\sigma) = -(\sqrt{b})^{-1}$. Then $f = g \cdot \delta h$ so that $(K,G(L/K),g) \simeq (K,G(L/K),f)$ (**3.3.** of Chapter I). Thus the class of $\chi_a \cup \chi_b$ in ${}_2\,\mathrm{Br}(K)$ is $[(\frac{a,b}{K})]$. Suppose now that $\sqrt{a}$ and $\sqrt{b}$ generate

distinct quadratic extensions of K. Then $L = K(\sqrt{a}, \sqrt{b})$ is a Galois extension of K of degree 4 whose Galois group is the Klein's four group $(1, \sigma_a, \sigma_b, \sigma_a\sigma_b)$ where $\sigma_a(\sqrt{a}) = -\sqrt{a}$, $\sigma_a(\sqrt{b}) = \sqrt{b}$, $\sigma_b(\sqrt{a}) = \sqrt{a}$ and $\sigma_b(\sqrt{b}) = -\sqrt{b}$. For $\sigma, \tau \in G$,

$$(\chi_a \cup \chi_b)(\sigma, \tau) = \begin{cases} 1 \otimes 1 & \text{if} \quad \sigma|_L = \tau|L = \text{identity} \\ 1 \otimes -1 & \text{if} \quad \sigma|_L = \text{identity}, \ \tau|_L = \sigma_b \\ -1 \otimes 1 & \text{if} \quad \sigma|_L = \sigma_a, \tau|_L = \text{identity} \\ -1 \otimes -1 & \text{if} \quad \sigma|_L = \sigma_a, \tau|_L = \sigma_b. \end{cases}$$

Under the identification of $\mu_2 \otimes \mu_2$ with μ_2, the cohomology class of the image of $\chi_a \cup \chi_b$ in $H^2_c(G, \mu_2)$ is the class $\inf[f]$ where $f \in Z^2(G, (L/K), L^*)$ is given by $f(\sigma_a, \sigma_a) = f(\sigma_b, \sigma_b) = f(\sigma_b, \sigma_a) = 1$, $f(\sigma_a, \sigma_b) = -1$. If $\overline{G} = G(K(\sqrt{a})/K)$, we know that $(\frac{a,b}{K}) \simeq (K, \overline{G}, \bar{g})$ where $\bar{g} \in Z^2(\overline{G}, K(\sqrt{a})^*)$ is given by $\bar{g}(\sigma_a, \sigma_a) = b$ (denoting by σ_a, its restriction to $K(\sqrt{a})$). We claim that $[f] = \inf[\bar{g}]$ where inf stands for the inflation homomorphism $H^2(G, K(\sqrt{a})^*) \to H^2(G(L/K), L^*)$. In fact $\inf[\bar{g}] = [g]$ where $g(\sigma_a, \sigma_b) = g(\sigma_b, \sigma_a) = g(\sigma_b, \sigma_b) = 1$, $g(\sigma_a, \sigma_a) = b$. Let $h : G(L/K) \to L^*$ be the normalized 1-cochain defined by $h(\sigma_a) = (\sqrt{b})^{-1}, h(\sigma_b) = 1$, $h(\sigma_a\sigma_b) = -(\sqrt{b})^{-1}$. Then $f = g \cdot \delta h$ and $\chi_a \cup \chi_b = \inf[\bar{g}] = [(\frac{a,b}{K})]$ and this completes the proof of the proposition. □

In view of the above proposition, the map $\beta_K : k_2(K) \to H^2_c(G, \mu_2)$ defined as the composite $k_2(K) \xrightarrow{\alpha_K} {}_2\,\mathrm{Br}(K) \xrightarrow{\sim} H^2_c(G, \mu_2)$ sends $\overline{\langle a, b \rangle}$ to $[\chi_a \cup \chi_b]$. Thus, Merkurjev's theorem can be reformulated as follows.

Theorem 4.2. *Let K be a field of characteristic $\neq 2$. The homomorphism $\beta_K : k_2(K) \to H^2_c(G, \mu_2)$ given by $\overline{\langle a, b \rangle} \to [\chi_a \cup \chi_b]$ is an isomorphism.*

§ 5. A key commutative diagram

We begin with the following

Proposition 5.1. (Arason) *Let G be a group (resp. a profinite group). Let $\chi : G \to \mu_2$ be a nontrivial (continuous) character so that $\chi \in H^1(G, \mu_2)$ (resp. $\chi \in H^1_c(G, \mu_2)$), for the trivial action of G on μ_2. Let $H = \ker \chi$, so that H is a normal subgroup (resp. open normal subgroup) of index 2. We then have an exact sequence*

$$\ldots \longrightarrow H^n(G, \mu_2) \xrightarrow{\text{res}} H^n(H, \mu_2) \xrightarrow{\text{cores}} H^n(G, \mu_2) \xrightarrow{\chi\cup} H^{n+1}(G, \mu_2) \longrightarrow \ldots$$

(resp.

$$\ldots \longrightarrow H^n_c(G, \mu_2) \xrightarrow{\text{res}} H^n_c(H, \mu_2) \xrightarrow{\text{cores}} H^n_c(G, \mu_2) \xrightarrow{\chi\cup} H^{n+1}_c(G, \mu_2) \longrightarrow \ldots).$$

Proof. Let $(1, x)$ be a set of coset representatives of H in G. Let

$$\mu_2^* = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], \mu_2)$$

(resp. $\mathrm{Map}_H(G,\mu_2)$) be the G-module co-induced from H. We then have an exact sequence of G-modules (resp. discrete G-modules)

$$1 \longrightarrow \mu_2 \xrightarrow{i} \mu_2^* \xrightarrow{\pi} \mu_2 \longrightarrow 1$$

where i is the inclusion of μ_2 in μ_2^* and π is defined by $\pi(f) = f(1)\cdot f(x)$. The map π is surjective since $\pi(\chi) = -1$. We have a long exact sequence of (profinite) cohomology groups

$$\begin{array}{ccccccc} \ldots \longrightarrow H^n(G,\mu_2) & \longrightarrow & H^n(G,\mu_2^*) & \longrightarrow & H^n(G,\mu_2) & \xrightarrow{\delta_n} & H^{n+1}(G,\mu_2) \\ & \overset{\text{res}}{\searrow} & \wr\downarrow s^n_{\mu_2} & \overset{\text{cores}}{\nearrow} & & & \\ & & H^n(H,\mu_2) & & & & \end{array}$$

(resp. H_c replacing H everywhere). The only thing that remains to be shown, to complete the proof of the proposition is that δ_n is precisely $\chi\cup$, identifying $\mu_2\otimes\mu_2$ with μ_2. To do this, we use the explicit description of the connecting homomorphism. Let $s:\mu_2\to\mu_2^*$ be the $\mathbb{Z}$-linear section to π given by $s(1)=1, s(-1)=\chi$. Let $[f]\in H^n(G,\mu_2)$ (resp, $H^n_c(G,\mu_2)$) with f as a representative. We have $\delta_n(s\circ f)(G^{n+1})\subset i(\mu_2)$, since $\pi\circ\delta_n(s\circ f) = \delta_n(\pi\circ s\circ f) = 0$. By the definition of connecting homomorphism, $\delta_n([f]) = [i^{-1}\delta_n(s\circ f)]\in H^{n+1}(G,\mu_2)$ (resp. $H_c^{n+1}(G,\mu_2)$). Further,

$$\begin{aligned} \delta_n(s\circ f)(x_1,\ldots,x_{n+1}) &= x_1(s\circ f)(x_2,\ldots,x_{n+1}) \\ &\quad\cdot \prod_{1\le i\le n}[(s\circ f)(x_1,\ldots,x_i\cdot x_{i+1},\ldots,x_{n+1})]^{(-1)^i} \\ &\quad\cdot[(s\circ f)(x_1,\ldots,x_n)]^{(-1)^{n+1}} \\ &= x_1(s\circ f)(x_2,\ldots,x_{n+1})\cdot s(x_1 f(x_2,\ldots,x_{n+1}))^{-1} \end{aligned}$$

since s is $\mathbb{Z}$-linear and $\delta_n f = 1$, f being a cocycle. One can check that for any $r\in\mu_2$ and $x\in G$, $xs(r)\cdot s(r)^{-1} = i\circ\rho(\chi(x)\otimes r)$, $\rho:\mu_2\otimes\mu_2\to\mu_2$ being the isomorphism described in § 4. Let $r = f(x_2,\ldots,x_{n+1})$. Then $\delta_n(s\circ f)(x_1,\ldots,x_{n+1})$ $= i\circ\rho(\chi(x)\otimes r) = i\circ(\chi\cup f)(x_1,\ldots,x_{n+1})$ so that $\delta_n(f) = [\chi\cup f] = \chi\cup[f]$. This completes the proof of the proposition. □

From now onwards, we shall abbreviate $H^n_c(G,\mu_2) = H^n(K)$.

Corollary 5.2. *Let K be a field of characteristic $\neq 2$ and $a\in K^*\setminus K^{*^2}$. Let $\chi_a\in H^1(K)$ be the character corresponding to a. If $L = K(\sqrt{a})$, we have the following exact sequence*

$$\ldots\longrightarrow H^n(K)\xrightarrow{\text{res}} H^n(L)\xrightarrow{\text{cores}} H^n(K)\xrightarrow{\chi_a\cup} H^{n+1}(K)\longrightarrow\ldots\ .$$

Proof. We note that χ_a is a nontrivial character with $\ker\chi_a = G(K_s/L) = G(L_s/L)$. □

Proposition 5.3. *Let K be a field of characteristic $\neq 2$, $a \in K^* \setminus K^{*2}$ and $L = K(\sqrt{a})$. Then, the diagram*

$$\begin{array}{ccccccc} k_1(K) & \xrightarrow{\varphi} & k_2(K) & \xrightarrow{\text{ext}} & k_2(L) & \xrightarrow{\text{tr}} & k_2(K) \\ \downarrow & & \downarrow{\scriptstyle \beta_K} & & \downarrow{\scriptstyle \beta_L} & & \downarrow{\scriptstyle \beta_K} \\ H^1(K) & \xrightarrow{\chi_a \cup} & H^2(K) & \xrightarrow{\text{res}} & H^2(L) & \xrightarrow{\text{cores}} & H^2(K) \end{array} \qquad (*)$$

where, for $b \in K^*$, $\varphi(\bar{b}) = \overline{\langle a, b\rangle}$, and the isomorphism $k_1(K) \xrightarrow{\sim} H^1(K)$ being $\bar{b} \mapsto \chi_b$, is commutative.

To prove the proposition, we begin with the following

Lemma 5.4. *Let L/K be an extension of degree 2. Then $K_2(L)$ is generated by symbols $\langle b, \mu\rangle$, $b \in K^*$, $\mu \in L^*$.*

Proof. Let $\langle \lambda, \mu\rangle \in K_2(L)$. If λ and μ are linearly dependent over K, $\lambda = b\mu$ for some $b \in K^*$. Then $\langle \lambda, \mu\rangle = \langle b\mu, \mu\rangle = \langle -b, \mu\rangle + \langle -\mu, \mu\rangle = \langle -b, \mu\rangle$. Suppose λ and μ are linearly independent over K. Then L/K being of degree 2, $1, \lambda, \mu$ are linearly dependent over K and $1 = b\,\lambda + c\mu$, $b, c \in K^*$. Then $\langle \lambda, \mu\rangle =$
$langleb\lambda, \mu\rangle - \langle b, \mu\rangle = \langle 1 - c\mu, \mu\rangle - \langle b, \mu\rangle = \langle 1 - c\mu, c\mu\rangle - \langle 1 - c\mu, c\rangle - \langle b, \mu\rangle =$
$\langle c, 1 - c\mu\rangle - \langle b, \mu\rangle$. □

Lemma 5.5. *Let L/K be any extension. Then the diagram*

$$\begin{array}{ccc} k_2(K) & \xrightarrow{\text{ext}} & k_2(L) \\ \downarrow{\scriptstyle \beta_K} & & \downarrow{\scriptstyle \beta_L} \\ H^2(K) & \xrightarrow{\text{res}} & H^2(L) \end{array}$$

is commutative.

Proof. For $a, b \in K^*$, res $(\chi_a \cup \chi_b) =$ res $\chi_a \cup$ res χ_b (**5.2.** of Chapter II). Further, for any $c \in K^*$, if c_L denotes c as an element of L, and if $\text{res}_{L/K}$ denotes the restriction $H(K) \longrightarrow H(L)$, then $\text{res}_{L/K}(\chi_c) = \chi_{c_L}$. This is a consequence of the fact that restriction commutes with connecting homomorphisms. Thus β_L ext $(\overline{\langle a, b\rangle}) = \beta_L \overline{\langle a_L, b_L\rangle} = [\chi_{a_L} \cup \chi_{b_L}] = \text{res}_{L/K}[\chi_a \cup \chi_b] = \text{res}_{L/K}\, \beta_K(\overline{\langle a, b\rangle})$. □

Lemma 5.6. *Let L/K be a quadratic extension. Then the diagram*

$$\begin{array}{ccc} k_2(L) & \xrightarrow{\text{tr}} & k_2(K) \\ \downarrow{\scriptstyle \beta_L} & & \downarrow{\scriptstyle \beta_K} \\ H^2(L) & \xrightarrow{\text{cores}} & H^2(K) \end{array}$$

is commutative.

Proof. In view of **5.4.** above, it is enough to show that for $b \in K^*$, $\lambda \in L^*$, $\beta_K \operatorname{tr}(\overline{\langle b_L, \lambda\rangle}) = \operatorname{cores} \circ \beta_L(\overline{\langle b_L, \lambda\rangle})$. By the projection formula,

$$\operatorname{tr}(\overline{\langle b_L, \lambda\rangle}) = \overline{\langle b, N_{L/K}\lambda\rangle}.$$

Thus $\beta_K \operatorname{tr} \overline{\langle b_L, \lambda\rangle} = [\chi_b \cup \chi_{N_{L/K}\lambda}]$. On the other hand, $\operatorname{cores} \circ \beta_L \overline{\langle b_L, \lambda\rangle} = \operatorname{cores}[\chi_{b_L} \cup \chi_\lambda] = \operatorname{cores}[\operatorname{res} \chi_b \cup \chi_\lambda] = [\chi_b \cup \operatorname{cores} \chi_\lambda]$ (**5.3.** of Chapter II). We have $\operatorname{cores} \chi_\lambda = \chi_{N_{L/K}\lambda}$ since corestriction commutes with connecting homomorphisms, i.e., the diagram

$$\begin{array}{ccc} K^* = H^0_c(G(K_s/K), K_s^*) & \xrightarrow{\delta_0} & H^1_c(G(K_s/K), \mu_2) \\ \uparrow{\scriptstyle \text{cores}=N_{l/K}} & & \uparrow{\scriptstyle \text{cores}} \\ L^* = H^0_c(G(L_s/L), L_s^*) & \xrightarrow{\delta_0} & H^1_c(G(L_s/L), \mu_2) \end{array}$$

is commutative. □

Proof of 5.3. By the very definition of φ, the left hand square is commutative. The commutativity of the middle square is proved in **5.5.** and the commutativity of the right hand square is proved in **5.6.**. □

Proposition 5.7. *With the notation of 5.3.,*

a) *the sequence*

$$k_1(K) \xrightarrow{\phi} k_2(K) \xrightarrow{\text{ext}} k_2(L) \xrightarrow{\text{tr}} k_2(K) \qquad (**)$$

is a complex.

b) *If this sequence is exact at $k_2(K)$ for all K and for all quadratic extensions L of K, then β_K is injective for all K.*

c) *If this sequence is exact for all K and all quadratic extensions L of K, then β_K is an isomorphism for all K.*

Proof. a): $\overline{\langle a, b\rangle_L} = \overline{2\langle \sqrt{a}, b_L\rangle} = 0$ in $k_2(L)$. Further, $\operatorname{tr} \circ \operatorname{ext}$ is multiplication by $[L : K] = 2$ (§1 of chapter III) which is zero in $k_2(K)$.
b): Let $\sum_{1\le i\le n} \overline{\langle a_i, b_i\rangle} \in k_2(K)$ be such that $\beta_L(\sum_{1\le i\le n} \overline{\langle a_i, b_i\rangle}) = 0$. To show that $\sum_{1\le i\le n} \overline{\langle a_i, b_i\rangle} = 0$, we proceed by induction on n. If $n = 1$, $\beta_K(\overline{\langle a_1, b_1\rangle}) = [\chi_{a_1} \cup \chi_{b_1}] = 0$ implies that $(\frac{a_1, b_1}{K})$ is a matrix algebra (see **4.1.**). This implies that $\overline{\langle a_1, b_1\rangle} = 0$ by **3.1.**. Let $n > 1$. Let $\beta_K(\sum_{1\le i\le n} \overline{\langle a_i, b_i\rangle}) = 0$. If $\sqrt{a}_n \in K$, then $\overline{\langle a_n, b_n\rangle} = 0$ and we are through by induction. Let $\sqrt{a}_n \notin K$ and let $L = K(\sqrt{a}_n)$. We have $0 = \operatorname{res} \circ \beta_K(\sum_i \langle a_i, b_i\rangle) = \beta_L \cdot \operatorname{ext}(\sum_i \langle a_i, b_i\rangle) = \beta_L(\sum_{1\le i\le n-1} \overline{\langle a_i, b_i\rangle}_L)$, since $\overline{\langle a_n, b_n\rangle}_L = 0$, a_n being a square in L. By induction, β_L is injective on $(n-1)$

symbols so that $\mathrm{ext}_{L/K}\sum\langle a_i, b_i\rangle = 0$. By the assumption of exactness at $k_2(K)$, there exists $b \in K^*$ such that $\sum_i \overline{\langle a_i, b_i\rangle} = \overline{\langle a_n, b\rangle}$. Since $\beta_K(\overline{\langle a_n, b\rangle}) = 0$, it follows that $\overline{\langle a_n, b\rangle} = 0$.

To prove c) we need the following

Lemma 5.8. *Let K be any field and $x \in H_c^2(G(K_s/K), K_s^*)$. Then there exists a finite Galois extension L/K such that if $\mathrm{res}_{L/K}$ denotes the restriction homomorphism $H_c^2(G(K_s/K), K_s^*) \to H_c^2(G(K_s/L), K_s^*)$, then $\mathrm{res}_{L/K}\, x = 0$.*

Proof. By the definition of $H_c^2(G(K_s/K), K_s^*)$, there exists a finite Galois extension L/K such that $x \in$ image of $\inf : H^2(G(L/K), L^*) \to H_c^2(G(K_s/K), K_s^*)$. Since $\mathrm{res} \circ \inf = 0$ (**4.2.** of Chapter II), we have $\mathrm{res}_{L/K}\ x = 0$. □

Corollary 5.9. *Let K be any field of characteristic $\neq 2$ and $x \in H^2(K)$. Then there exists a finite Galois extension L/K such that $\mathrm{res}_{L/K}\, x = 0$.*

Proof. This is immediate from **5.8.** and the fact that the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & H_c^2(G(K_s/K), \mu_2) & \longrightarrow & H_c^2(G(K_s/K)K_s^*) \\ & & \downarrow \mathrm{res} & & \downarrow \mathrm{res} \\ 0 & \longrightarrow & H_c^2(G(K_s/L), \mu_2) & \longrightarrow & H_c^2(G(K_s/L)K_s^*) \end{array}$$

is commutative, with exact rows, for any finite Galois extension L/K. □

Proof of c) of 5.7. In view of b), it suffices to show that under the hypothesis, β_K is surjective. Let $x \in H^2(K)$, $x \neq 0$. Let L/K be a finite Galois extension such that $\mathrm{res}\ x = 0$ in $H^2(L)$ (**5.9.**).
Let $[L : K] = 2^r \cdot m > 1$ with $(2, m) = 1$. Let L_0 be the subfield of L fixed by a 2-sylow subgroup H of $G = G(L/K)$. If $r = 0$, $H = (e)$ and $L = L_0$ and $\mathrm{res}_{L_0/K}(x) = 0 \in H^2(L_0)$ and hence $\mathrm{res}_{L_0/K}(x)$ is in the image of β_{L_0}. Suppose $r > 0$. Let $(e) = H_0 \subset H_1 \subset \ldots \subset H_r = H$ be such that H_i/H_{i-1} is of order 2, $1 \leq i \leq r$. Let L_i be the fixed field of H_{r-i}, $1 \leq i \leq r$. We then have a tower of fields $L_0 \subset L_1 \subset \ldots \subset L_r = L$ of successive quadratic extensions. We denote by $\mathrm{res}_{L_i/K}$ the restriction homomorphism $H^2(K) \to H^2(L_i)$. The diagram

$$\begin{array}{ccccccc} k_1(L_{i-1}) & \xrightarrow{\varphi} & k_2(L_{i-1}) & \xrightarrow{\mathrm{ext}} & k_2(L_i) & \xrightarrow{\mathrm{tr}} & k_2(L_{i-1}) \\ \downarrow \wr & & \downarrow \beta_{L_{i-1}} & & \downarrow \beta_{L_i} & & \downarrow \beta_{L_{i-1}} \\ H^1(L_{i-1}) & \longrightarrow & H^2(L_{i-1}) & \xrightarrow{\mathrm{res}} & H^2(L_i) & \xrightarrow{\mathrm{cores}} & H^2(L_{i-1}) \end{array}$$

is commutative with exact rows (by hypothesis and **5.3.** of Chapter III). We have that $\mathrm{res}_{L_r/K}(x) = \mathrm{res}_{L/K}(x) = 0$ trivially belongs to $\mathrm{im}\,\beta_{L_r}$. We show that if $\mathrm{res}_{L_i/K}(x)$ is in the image of β_{L_i}, then, $\mathrm{res}_{L_{i-1}/K}(x)$ belongs to the image of $\beta_{L_{i-1}}$.

This would prove that $\mathrm{res}_{L_0/K}(x)$ belongs to $\mathrm{im}\,\beta_{L_0}$. Let $\mathrm{res}_{L_i/L}(x) = \beta_{L_i}(y)$ for $y \in k_2(L_i)$. Then we have $0 = \mathrm{cores} \circ \mathrm{res}_{L_i/L_{i-1}} \circ \mathrm{res}_{L_{i-1}/K}(x) = \mathrm{cores} \circ \mathrm{res}_{L_i/K}(x) = \mathrm{cores}\ \beta_{L_i}(y) = \beta_{L_{i-1}}\ \mathrm{tr}(y)$. Since $\beta_{L_{i-1}}$ is injective (in view of b)), $\mathrm{tr}\ y = 0$. The top row being exact, $y = \mathrm{ext}\ z$, for some $z \in k_2(L_{i-1})$. Since $\beta_{L_{i-1}} z$ and $\mathrm{res}_{L_{i-1}/K}\ x$ have the same image $\mathrm{res}_{L_i/K}\ (x)$ in $H^2(L_i)$, $\beta_{L_{i-1}}(z) - \mathrm{res}_{L_i/K}\ (x)$ comes from $H^1(L_{i-1}) \simeq k_1(L_{i-1})$. Thus there exists $\tilde{z} \in k_2(L_{i-1})$ such that $\beta_{L_{i-1}}(\tilde{z}) = \beta_{L_{i-1}}(z) - \mathrm{res}_{L_{i-1}/K}\ (x)$ so that $\mathrm{res}_{L_{i-1}/K}\ (x) \in\ \mathrm{Im}\,\beta_{L_{i-1}}$. Thus $\mathrm{res}_{L_0/K}(x) = \beta_{L_0}(z)$ for some $z \in k_2(L_0)$. The diagram

$$\begin{array}{ccccc} k_2(K) & \xrightarrow{\mathrm{ext}} & k_2(L_o) & \xrightarrow{\mathrm{tr}} & k_2(K) \\ \downarrow{\scriptstyle \beta_K} & & \downarrow{\scriptstyle \beta_{L_0}} & & \downarrow{\scriptstyle \beta_K} \\ H^2(K) & \xrightarrow{\mathrm{res}} & H^2(L_0) & \xrightarrow{\mathrm{cores}} & H^2(K) \end{array}$$

is commutative. The left hand side square commutes by **5.5.**. The right hand side square commutes, in view of a theorem of Rosset-Tate (cf. Appendix IV).

Also $\mathrm{cores}_{L_0/K} \circ \mathrm{res}_{L_0/K}$ = multiplication by $[L_0 : K]$ = identity since $H^2(K)$ is 2-torsion and $[L_0 : K]$ is coprime to 2. Thus $x = \mathrm{cores} \circ \mathrm{res}_{L_0/K}(x) =\ \mathrm{cores}\ \beta_{L_0}(z) = \beta_K\,\mathrm{tr}(z)$ so that β_K is surjective. □

Thus, to prove Merkurjev's theorem, one needs to establish the exactness of the sequence $(**)$ of **5.7.** for all fields K and all quadratic extensions L of K. The exactness at $k_2(L)$ can be derived from the following *Hilbert Theorem 90* for K_2.

Theorem 5.10. (Suslin-Merkurjev) *Let K be a field of characteristic $\neq 2$ and $L = L(\sqrt{a})$ a quadratic extension of K. Let σ be a generator of $G(L/K)$. Then the sequence*

$$K_2(L) \xrightarrow{1-\sigma} K_2(L) \xrightarrow{\mathrm{tr}} K_2(K)$$

is exact, where $(1-\sigma)(\langle b, c\rangle) = \langle b, c\rangle\ -\ \langle \sigma b, \sigma c\rangle$.

Corollary 5.11. *The sequence $K_2(K) \xrightarrow{\mathrm{ext}} k_2(L) \xrightarrow{\mathrm{tr}} k_2(K)$ is exact.*

Proof. Let $\bar{r} \in k_2(L)$ with $r \in K_2(L)$ as a representative such that $\mathrm{tr}(\bar{r}) = 0$. Let $\mathrm{tr}\, r = 2\theta$, $\theta \in K_2(K)$. We have $\mathrm{tr} \circ \mathrm{ext}\,\theta = 2\theta$. Thus $\mathrm{tr}(r - \mathrm{ext}\,\theta) = 0$. Replacing r by $r - \mathrm{ext}\,\theta$, we may assume that $\mathrm{tr}\, r = 0$. By **3.1.**, $r = (1-\sigma)(\beta)$, $\beta \in K_2(L)$. In view of **5.4.** of Chapter III, β may be written as a sum $\sum_{i=1}^n \langle b_i, \lambda_i\rangle$, $b_i \in K^*$, $\lambda_i \in L^*$. Thus $r = \sum_{i=1}^n \{\langle b_i, \lambda_i\rangle + \langle b_i, \sigma\lambda_i\rangle - 2\langle b_i, \sigma\lambda_i\rangle\} \equiv \sum_{i=1}^n \langle b_i, N_{L/K}\lambda_i\rangle \mathrm{mod}\ 2K_2(L), = \mathrm{ext}_{L/K} \sum_{i=1}^n \langle b_i, N_{L/K}\lambda_i\rangle$. □

In the next two chapters, we prove Theorem **5.10.** above and the exactness at $k_2(K)$ of the sequence $(**)$ of **5.7.**. This would complete the proof of Merkurjev's theorem. □

Chapter IV: "Hilbert Theorem 90" for K_2

§ 1. Function field of a conic

In this section, K denotes a field of characteristic $\neq 2$. For $a, b \in K^*$, the projective conic $C = C_{a,b}$ defined over K is the set of zeros of $aX^2 + bY^2 - Z^2$ in $\mathbb{P}^2(\bar{K})$, $\bar{K}$ denoting the algebraic closure of K. The polynomial $aX^2 + bY^2 - 1 \in K[X, Y]$ is irreducible in $\tilde{K}[X, Y]$ for any field extension $\tilde{K}$ of K, so that if

$$R = K[X, Y]/(aX^2 + bY^2 - 1)$$

is the coordinate ring of the affine conic $aX^2 + bY^2 - 1$, then

$$\tilde{K} \otimes_K R \hookrightarrow \tilde{K}[X, Y]/(aX^2 + bY^2 - 1)$$

is a domain.

The *function field of* C is, by definition, the quotient field of R and is denoted by $K(C)$. Let x, $y \in R$ denote the images of X, Y respectively. Then $K(C)$ is a quadratic extension generated by y of the field $K(x)$ of rational functions in x so that $K(C)$ is an algebraic function field in one variable over K.

Proposition 1.1. *The following conditions are equivalent:*

i) *$K(C)$ is a purely transcendental extension of K.*

ii) *C has a K-rational point, i.e., there exist λ, μ, $\nu \in K$ not all zero such that $a\lambda^2 + b\mu^2 - \nu^2 = 0$.*

iii) *The quaternion algebra $(\frac{a,b}{K})$ is a matrix algebra.*

Proof. The fact that i) and ii) are equivalent is a consequence of **5.7.** of Chapter I.
iii) $\Rightarrow$i): Let $(\frac{a,b}{K})$ be a matrix algebra. Then by **5.7.**, $b = \mu^2 - a\lambda^2$, λ, $\mu \in K$. Let $t = \frac{1+\mu y}{x+\lambda y}$. It is easily verified that $K(C) = K(t)$.
i) $\Rightarrow$ iii): Let $K(C)$ be a rational function field in one variable over K. Since in $K(C), a = (\frac{1}{x})^2 - b(\frac{Y}{x})^2$, it follows by **5.7.** of Chapter I that $(\frac{a,b}{K(C)}) = (\frac{a,b}{K}) \otimes_K K(C)$ is a matrix algebra. Then $(\frac{a,b}{K})$ is a matrix algebra by **1.7.** of Chapter I. □

We say that a conic $C = C_{a,b}$ is *split over* K if any one of the equivalent conditions of the above proposition is satisfied. An extension $\widetilde{K}$ of K is said to *split* C if C is split over $\widetilde{K}$.

Lemma 1.2. *The ring $R = K[x, y]$ is the integral closure of $K[x]$ in $K(C)$.*

Proof. Since y is integral over $K[x]$, R is integral over $K[x]$. Let $\lambda + \mu y \in K(C)$, λ, $\mu \in K(x)$, be integral over $K[x]$. Then $\lambda - \mu y$ is also integral over $K[x]$, so that

2λ and $(\lambda^2 - b^{-1}\mu^2)(1 - ax^2) \in K(x)$ and are integral over $K[x]$. Since $K[x]$ is integrally closed in $K(x)$, 2λ and $(\lambda^2 - b^{-1}\mu^2)(1 - ax^2)$ belong to $K[x]$. Thus λ and $\mu^2(1 - ax^2)$ belong to $K[x]$. Since $1 - ax^2$ has distinct roots in $\bar{K}$, it follows that $\mu^2 \in K[x]$ and hence $\mu \in K[x]$. Thus $\lambda + \mu y \in R$. □

Lemma 1.3. *The field K is algebraically closed in $K(C)$.*

Proof. Let $\alpha = f_0(x) + f_1(x)y \in K(C)$ be algebraic over K with $f_0(x)$, $f_1(x) \in K(x)$. Then $f_0(x) - f_1(x)y$ is also algebraic over K so that $2f_0(x)$ and $(f_0(x))^2 - (f_1(x))^2\ b^{-1}(1 - ax^2)$ are algebraic over K. It follows that $f_0(x) \in K$ and $f_1(x) = 0$ so that $\alpha \in K$. □

§ 2. Discrete valuations of function fields

Let K be any field. A *discrete valuation* v of K is a surjective homomorphism $v : K^* \to \mathbb{Z}$ such that for a, b, $a + b \in K^*$, $v(a + b) \geq \min(v(a), v(b))$. If v is a discrete valuation of K, the *valuation ring* $\mathfrak{O}_v$ of v is the set

$$\mathfrak{O} = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\},$$

which in fact is a subring of K since for a, $b \in \mathfrak{O}_v$, either $a + b = 0$ or $v(a + b) \geq \min\,(v(a), v(b)) \geq 0$, so that $a + b \in \mathfrak{O}_v$. The ring $\mathfrak{O}_v$ has a unique non-zero prime ideal $\mathfrak{p}_v$ defined by $\mathfrak{p}_v = \{x \in K^* \mid v(x) > 0\} \cup \{0\}$. If π is any element of K^* with $v(\pi) = 1$, then $\mathfrak{p}_v = \mathfrak{O}_v \cdot \pi$ so that $\mathfrak{p}_v$ is a principal ideal. Such an element π is called a *uniformising parameter* for v. The group $\mathfrak{O}_v \setminus \mathfrak{p}_v = \{x \in K^* \mid v(x) = 0\}$ is precisely the group of invertible elements of $\mathfrak{O}_v$, called the units of v. The ring $\mathfrak{O}_v$ is a local principal ideal domain and every nonzero element of K can be written as $u\pi^n$, $u \in \mathfrak{O}_v \setminus \mathfrak{p}_v$ and π a parameter for v. The field $K_v = \mathfrak{O}_v/\mathfrak{p}_v$ is called the *residue class field* of the valuation v.

Let K be a field with a discrete valuation v. Let L be any extension of K. If w is a discrete valuation of L such that $\mathfrak{O}_w \cap K = \mathfrak{O}_v$, then w is called an extension of v (denoted w/v). If w is an extension of v, then $\mathfrak{p}_w \cap K = \mathfrak{p}_v$. If π_v is a parameter for v and $w(\pi_v) = e$, e is called the *ramification index* of w over v and denoted by $e(w/v)$. We note that e is independent of the choice of the parameter and for any $x \in K^*$, $w(x) = ev(x)$.

Proposition 2.1. *Let A be a Dedekind domain and K its quotient field. If v is a discrete valuation of K, such that $A \subset \mathfrak{O}_v$, then there exists a unique non-zero prime ideal $\mathfrak{p}$ of A such that $A_\mathfrak{p} = \mathfrak{O}_v$. Conversely, any nonzero prime ideal $\mathfrak{p}$ of A defines a discrete valuation $v_\mathfrak{p}$ of K whose valuation ring is $A_\mathfrak{p}$. In fact, if $x \in K^*$ and $xA = \prod \mathfrak{p}^{n_\mathfrak{p}(x)}$, $\mathfrak{p}$ running over the set of all the prime ideals of A, then, $x \mapsto n_\mathfrak{p}(x) = v_\mathfrak{p}(x)$ is the required valuation. The assignment $\mathfrak{p} \mapsto v_\mathfrak{p}$ is in fact a bijection between the set of non-zero prime ideals of A and the set of discrete valuations of K such that $v(x) \geq 0$ for all $x \in A$.*

Proposition 2.2. *Let A be a Dedekind domain with quotient field K. Let L/K be a finite separable extension. If B is the integral closure of A in L, then, B is a Dedekind domain whose quotient field is L. If $\mathfrak{p}$ is any non-zero prime ideal of A, then $\mathfrak{p}B \neq B$ and if $\mathfrak{p}B = \prod \mathfrak{P}^{e_\mathfrak{p}}$, the valuations of L extending $v_\mathfrak{p}$ are precisely the valuations $w_\mathfrak{P}$ corresponding to those prime ideals $\mathfrak{P}$ of B with $e_\mathfrak{P} > 0$. We have $e(w_\mathfrak{P}/v_\mathfrak{p}) = e_\mathfrak{P}$. If $f_\mathfrak{P} = [B/\mathfrak{P} : A/\mathfrak{p}]$, then, $[L : K] = \sum_{e_\mathfrak{P}>0} e_\mathfrak{P} \cdot f_\mathfrak{P}$. If L/K is Galois, then $G(L/K)$ operates on B and operates transitively on the set $\{\mathfrak{P} \mid e_\mathfrak{P} > 0\}$. If $\sigma\mathfrak{P}_i = \mathfrak{P}_j$, then, $w_{\mathfrak{P}_j} \circ \sigma = w_{\mathfrak{P}_i}$ and $\mathfrak{O}_{w_{\mathfrak{P}_j}} = \sigma(\mathfrak{O}_{w_{\mathfrak{P}_i}})$. For any $x \in B$, $N_{L/K}(x) \in A$ and*

$$\overline{N_{L/K}(x)} = \prod_{e_\mathfrak{P}>0} N_{B/\mathfrak{P}/A/\mathfrak{p}}(\overline{x})^{e_\mathfrak{P}}$$

where bar denotes 'reduction modulo $\mathfrak{p}$' on the left hand side and 'reduction modulo $\mathfrak{P}$' on the right hand side.

The proof of **2.1.** is straightforward and the proof of **2.2.** may be found in 'Commutative Algebra' vol. I, Chapter V, by Zariski and Samuel (see also Appendix I).

Proposition 2.3. *Let $K(x)$ denote the field of rational function in one variable over K. The only discrete valuations v of $K(x)$ which are trivial on K (i.e. $v(\lambda) = 0 \; \forall \; \lambda \in K^*$) are the valuations v_p for each prime $p \in K[x]$ and v_∞ defined as follows:*

$$v_p(f) = n,\ f \in K[x],\ p^n | f,\ p^{n+1} \not| f, \quad v_\infty(f) = -\deg f, f \in K[x].$$

Proof. The field $K(x)$ is the quotient field of the Dedekind domain $K[x]$. Let v be any discrete valuation of $K(x)$ trivial on K. If $v(x) \geq 0$, then $\mathfrak{O}_v \supset K[x]$ so that by (2.1), $v = v_p$ defined as above for some prime p of $K[x]$. If $v(x) < 0$, then $v(1/x) > 0$ and $\mathfrak{O}_v \supset K[1/x]$. Since $1/x$ is a prime in $K[1/x]$, it follows that $v = v_{1/x} = v_\infty$, defined as above. □

We note that $\mathfrak{O}_{v_p} = K[x]_{(p)}$, $\mathfrak{p}_{v_{(p)}} = p \cdot K[x]_{(p)}$ so that $K(x)_{v_p} = K[x]_{(p)}/p \cdot K[x]_{(p)} \simeq K[x]/(p)$. Thus $[K(x)_{v_p} : K] = \deg p$ which is called *the degree of the valuation* v_p. We have $\mathfrak{O}_{v_\infty} = K[1/x]_{(1/x)}$ and $\mathfrak{p}_{v_\infty} = 1/x \cdot K[1/x]_{(1/x)}$ so that $[K(x)_{v_\infty} : K]$ (which is called the *degree* of v_∞) $= 1$.

Let $C = C_{a,b}$ be a conic defined over K. Then $K(C)$ is a quadratic extension of $K(x)$ and the integral closure of $K[x]$ in $K(C)$ is $R = K[x, y] = K[X, Y]/(aX^2 + bY^2 - 1)$. The only discrete valuations of $K(C)$ trivial on K are extensions of the valuations v_p or v_∞ of $K(x)$. In view of **2.2.** above, there are at the most two valuations of $K(C)$ extending any valuation of $K(x)$. For any valuation w of $K(C)$, we define

$$\deg w = [\mathfrak{O}_w/\mathfrak{p}_w : K] = [\mathfrak{O}_w/\mathfrak{p}_w : \mathfrak{O}_v/\mathfrak{p}_v] \cdot [\mathfrak{O}_v/\mathfrak{p}_v : K]$$

(where w extends v). Thus $\deg v \mid \deg w$. We denote by $\mathfrak{P}_K(C)$ the set of discrete valuations of $K(C)$ trivial on K and by $\mathfrak{P}_K$ the set of discrete valuations of $K(x)$ trivial on K.

Proposition 2.4. *Let $K(C)$ be the function field of a conic $C = C_{a,b}$ defined over K and L/K a quadratic extension. For any $v \in \mathfrak{P}_K(C)$, if w is an extension of v to $L(C)$, then $e(w/v) = 1$. The inclusions $L \hookrightarrow L(C)_w, K(C)_v \hookrightarrow L(C)_w$ induce an isomorphism $L \otimes_K K(C)_v \xrightarrow{\sim} \coprod_{w/v} L(C)_w$. If v has two distinct extensions to $L(C)$ and if $\sigma \in G(L/K)$ is the nontrivial element, then, $\sigma \otimes 1$ on $L \otimes K(C)_v$ transports under this isomorphism into the map $(\bar{x}, \bar{y}) \mapsto (\overline{\sigma y}, \overline{\sigma x})$, x, $y \in L(C)$ belonging to the corresponding valuation rings.*

Proof. Let v be a discrete valuation of $K(C)$ trivial on K. We take $R = K[X,Y]/(aX^2 + bY^2 - 1)$, $S = L[X,Y]/(aX^2 + bY^2 - 1)$ if v is an extension of a valuation v_p of $K(X)$ where p is a prime in $k[X]$ and

$$\begin{aligned} R &= K[1/X, Y/X]/(a + b(Y/X)^2 - (1/X)^2), \\ S &= L[1/X, Y/X]/(a + b(Y/X)^2 - (1/X)^2 - (1/X)^2) \end{aligned}$$

if v is an extension of v_∞ of $K(X)$. Then S is the integral closure of R in $L(C)$. Let v define the prime ideal $\mathfrak{p}$ of R, and let $\mathfrak{p}S = \prod_{\mathfrak{P} \supset \mathfrak{p}} \mathfrak{P}^{e\mathfrak{P}}$. Then $L \otimes_K R/\mathfrak{p} \simeq S/\mathfrak{p}S \simeq \prod_{\mathfrak{P} \supset \mathfrak{p}} S/\mathfrak{P}^{e\mathfrak{P}}$. Since L is a separable extension of K, $L \otimes R/\mathfrak{p}$ has no nilpotent elements so that $e_\mathfrak{P} = e(w_\mathfrak{P}/v_\mathfrak{p}) = 1$ and we have the isomorphism $L \otimes K(C)_v = L \otimes R/\mathfrak{p} \simeq \prod_{\mathfrak{P} \supset \mathfrak{p}} S/\mathfrak{P} = \prod_{w/v} L(C)_w$. The effect of the transport of $\sigma \otimes 1$ on $\prod_{w/v} L(C)_w$ can be easily computed to be that given in the proposition. □

Proposition 2.5. *Let $C = C_{a,b}$ be a conic defined over K. For any $f \in K(C)^*$, the set $\{v \in \mathfrak{P}_K(C) \mid v(f) \neq 0\}$ is finite. If $f \in K(C)^*$ is such that $v(f) \geq 0$ for all valuations $v \in \mathfrak{P}_K(C)$, then, $f \in K^*$.*

Proof. We know in view of **2.2.** above that every $v \in \mathfrak{P}_K(C)$ is either an extension of the valuation v_∞ of $K(x)$ or corresponds to a non-zero prime ideal $\mathfrak{P}$ of $K[X,Y]/(aX^2 + bY^2 - 1) = R$. Let $fR = \prod \mathfrak{P}^{v_\mathfrak{P}(f)}$. Then the set of valuations $v \in \mathfrak{P}_K(C)$ such that $v(f) \neq 0$ is contained in the set $\{v_\mathfrak{P} \mid \mathfrak{P} \ni f\} \cup$ extensions of v_∞, which is finite. For any $v \in \mathfrak{P}_K(C)$ extending v_p of $K(x)$, $\mathfrak{O}_v \supset K[x,y]$ and for any $v \in \mathfrak{P}_K(C)$ extending v_∞ of $K(x)$, $\mathfrak{O}_v \supset K[1/x, y/x]$. Since every $v \in \mathfrak{P}_K(C)$ is given by a prime ideal of $K[x,y]$ or a prime ideal of $K[1/x, y/x]$ and since for any Dedekind domain A, $\cap A_\mathfrak{p}$, $\mathfrak{p}$ running over the set of all the non-zero prime ideals of A, coincides with A, $\cap_{v \in \mathfrak{P}_K(C)} \mathfrak{O}_v = K[x,y] \cap K[1/x, y/x] = K$. □

Proposition 2.6. *Let $C = C_{a,b}$ be a conic defined over K. For any valuation v of $K(C)$, the residue field $K(C)_v$ splits C. Further, if C is non-split over K, degree v is even, for any $v \in \mathfrak{P}_K(C)$.*

Proof. If $\mathfrak{O}_v \supset K[x,y]$ and $\bar{x}$, $\bar{y}$ denote the images of x, y in $K(C)_v$, then $a\bar{x}^2 + b\bar{y}^2 =$

1 so that $(\frac{a,b}{K(C)_v})$ is trivial, by **5.7.** of Chapter I, and in view of **1.1.** of Chapter III, $K(C)_v$ splits C. If $\mathfrak{O}_v \supset K(1/x, y/x], v$ is an extension of v_∞, and if $\tilde{x}$, $\tilde{y}$ are the images of $1/x, y/x$ in $K(C)_v$, then $\tilde{x} = 0$ and $\tilde{y}^2 = -a/b$, so that $(\frac{a,b}{K(C)_v})$ is again trivial.

Suppose C is non-split over K. Then $\sqrt{a} \notin K$ and $K(C)_v \neq K$, in view of the above. Since $K(C)_v$ splits C, $b = N_{K(C)_v(\sqrt{a})/K(C)_v}(\beta)$ for some $\beta \in K(C)_v(\sqrt{a})$ so that $N_{K(C)_v(\sqrt{a})/K}\beta = N_{K(C)_v/K}(b) = = b^{\text{degw}} = N_{K(\sqrt{a})/K}(N_{K(C)_v(\sqrt{a})/K(\sqrt{a})}(\beta))$. Thus b^{degw} is a norm from $K(\sqrt{a})$. On the other hand, b^2 is a norm from $K(\sqrt{a})$. If $\deg w$ were odd, this would imply that b is a norm from $K(\sqrt{a})$ so that C is split over K, contradicting our assumption that C is non-split. Thus $\deg w$ is even. □

§ 3. Divisors on a conic

Let K be a field of char $\neq 2$ and $C = C_{a,b}$ a conic defined over K. A *divisor* of $K(C)$ is a formal linear combination $\sum_{v \in \mathfrak{P}_K(C)} n_v v$, $n_v \in \mathbb{Z}$ being zero for all but a finitely many v. The divisors form an abelian group $\text{Div}(K(C))$ which is in fact the free abelian group on $\mathfrak{P}_K(C)$. For any divisor $D = \sum n_v v$, we define the *support* of D, denoted by *supp* D, to be the set $\{v \in \mathfrak{P}_K(C) \mid n_v \neq 0\}$. The divisor D is said to be *non-negative* (notation $D \geq 0$) if $n_v \geq 0$ for all $v \in \mathfrak{P}_K(C)$. The *degree* of a *divisor* D, denoted $\deg D$, is $\sum n_v \deg v$. The map $D \mapsto \deg D$ is obviously a homomorphism $\text{Div}(K(C)) \to \mathbb{Z}$. Let $\text{Div}_0(K(C))$ denote the kernel of this homomorphism. For any $f \in K(C)^*$, we define the divisor of f, denoted by $\text{div}(f)$, as $\sum_{v \in \mathfrak{P}_K(C)} v(f) \cdot f$. The fact that $\text{div}(f)$ is a divisor follows from (2.5) above. The map $K(C)^* \stackrel{\text{div}}{\to} \text{Div}(K(C))$ given by $f \mapsto \text{div}(f)$ is a homomorphism.

Proposition 3.1. *The image* $\text{div}(K(C)^*)$ *is contained in* $\text{Div}_0(K(C))$.

To prove the proposition, we need the following

Lemma 3.2. *Let $C = C_{a,b}$ be a conic defined over K and L/K a quadratic extension. Then, the map $\mathfrak{P}_K(C) \to \text{Div}(L(C))$ given by $v \mapsto \sum_{w/v} w$ induces a homomorphism $\text{Div}(K(C)) \stackrel{\text{ext}}{\longrightarrow} \text{Div}(L(C))$ which satisfies $\deg(\text{ext}D) = \deg D$ for all $D \in \text{Div}(K(C))$.*

Proof. It is obviously enough to check that for any valuation v of the field $K(C)$, $\deg(\sum_{w/v} w) = \deg v$. We have $[L : K] \sum_{w/v} \deg w = \sum_{w/v} [L : K][L(C)_w : L] = \sum_{w/v} [L(C)_w : K] = \sum_{w/v} [L(C)_w : K(C)_v][K(C)_v : K] = (\sum_{w/v} f(w/v)) \deg v = [L : K] \deg v$ in view of **2.2**, since by **2.4.** $e(w/v) = 1$. Thus $\sum_{w/v} \deg w = \deg v$. □

Proof of Proposition 3.1. Let L be a quadratic extension of K which splits C. In view of the above lemma, we replace $K(C)$ by $L(C)$ and assume that $K(C) = K(t)$ the rational function field in one variable t over K. For $f, g \in K(t), f, g \neq 0$, it is

easy to verify that $\sum v_p(f/g) = -v_\infty(f/g)$, so that $\deg(\operatorname{div}(f/g)) = 0$. □

Let $D = \sum n_v v$ be a divisor and let

$$\mathcal{L}(D) = \{f \in K(C)^* \mid \operatorname{div} f + D \geq 0\} \cup \{0\}.$$

Using the fact that $v(f+g) \geq \min(v(f), v(g))$ for $f,\ g,\ f+g \in K(C)^*$, and $v(\lambda f) = v(f)$ for $\lambda \in K^*,\ f \in K(C)^*$, for any $v \in \mathfrak{P}_K(C)$, it follows that $\mathcal{L}(D)$ is a K-vector space.

Lemma 3.3 *Let L/K be any quadratic extension. Then for any $D \in \operatorname{Div}(K(C))$, $\dim_L \mathcal{L}(\operatorname{ext} D) = \dim_K \mathcal{L}(D)$.*

Proof. Since for any $f \in K(C)$ and valuations $v \in \mathfrak{P}_K(C)$, $w \in \mathfrak{P}_L(C)$, w extending v, $w(f) = v(f)$ (cf. **2.4.** above), the inclusion $K(C) \hookrightarrow L(C)$ induces a K-linear map $\mathcal{L}(D) \to \mathcal{L}(\operatorname{ext} D)$. Since L and $K(C)$ are linearly disjoint over K, any set of elements of $\mathcal{L}(D)$ linearly independent over K is linearly independent over L so that $\dim_L \mathcal{L}\ (\operatorname{ext} D) \geq \dim_K \mathcal{L}(D)$. We shall show that $\mathcal{L}(D)$ generates $\mathcal{L}(\operatorname{ext} D)$ as a vector space over L and this will complete the proof of the lemma. Let $\{e_j\}\ 1 \leq j \leq 2$ be a K-basis for L and let $f \in \mathcal{L}(\operatorname{ext} D)$. We write $f = f_1 e_1 + f_2 e_2$, $f_1,\ f_2 \in K(C)$. Then, if $g_j = \operatorname{tr}_{L/K}(f e_j) = \sum_i f_i \operatorname{tr}_{L/K}(e_i e_j)$, we can write $f_i = \sum b_{ij} g_j$, $b_{ij} \in K$ since the matrix $(\operatorname{tr}(e_i e_j))$ is invertible (L/K being separable). We have $v(f_i) \geq \min_j v(g_j) \geq \min_{j, w/v} w(g_j) \geq \min_{w/v} w(f)$ (since $g_j = f e_j + \sigma f \cdot \sigma e_j$, σ denoting the nontrivial element of $G(L/K)$), $\min_{w/v} w(f) \geq -n_v$ where $D = \sum n_v v$. Thus $f_i \in \mathcal{L}(D)$. □

Lemma 3.4. *For any divisor D of $K(C)$, $\mathcal{L}(D)$ is a finite dimensional vector space over K.*

Proof. We first show that the dimension of $\mathcal{L}(0)$ is 1. Let $f \in K(C)^*$ with $\operatorname{div} f \geq 0$, i.e. $v(f) \geq 0$ for every $v \in \mathfrak{P}_K(C)$. By **2.5.** $f \in K^*$, so that $\mathcal{L}(0) = K$. To prove the lemma, it is sufficient to show that $\mathcal{L}(D)$ is finite dimensional if and only if $\mathcal{L}(D + w)$ is finite dimensional for $w \in \mathfrak{P}_K(C)$. We have a homomorphism $\mathcal{L}(D + w) \to K(C)_w$ given by sending $f \in \mathcal{L}(D + w)$ to the class of $f \cdot \pi^{n_w + 1}$ in $K(C)_w$, where $D = \sum n_v v$. Let E denote the image of this map. Then E is finite dimensional and the kernel of this map is $\mathcal{L}(D)$ so that we have an exact sequence of K-vector spaces

$$0 \to \mathcal{L}(D) \to \mathcal{L}(D + w) \to E \to 0.$$

This shows that $\mathcal{L}(D)$ is finite dimensional if and only if $\mathcal{L}(D + w)$ is finite dimensional. □

Lemma 3.5. *Let D, D' be two divisors of $K(t)$ which are "linearly equivalent" (i.e. $D - D' = \operatorname{div} g$ for some $g \in K(t)^*$). Then $\mathcal{L}(D) \xrightarrow{\sim} \mathcal{L}(D')$.*

Proof. Let $D = D' + \operatorname{div} g$, $g \in K(t)^*$. Then the map $K(C) \to K(C)$ given by $f \mapsto fg$ induces an isomorphism $\mathcal{L}(D) \xrightarrow{\sim} \mathcal{L}(D')$. □

Lemma 3.6 *Let D be a divisor of degree 0 of the rational function field $K(t)$. Then $D = \operatorname{div} f$ for some $f \in K(t)^*$.*

Proof. Let $D = \sum_p n_p v_p + n_\infty v_\infty$, v_p, $v_\infty \in \mathfrak{P}_K$ defined as in **2.3.**. Since $\deg D = 0$, $\sum n_p \deg p + n_\infty = 0$. Let $f = \prod_p^{n_p}$. By definition $v_p(f) = n_p$ and $v_\infty(f) = -\sum n_p \deg p = n_\infty$. Thus $D = \operatorname{div}(f)$. □

Proposition 3.7. *Let D be a divisor of the rational function field $K(t)$ of degree ≥ 0. Then $\dim \mathcal{L}(D) = 1 + \deg D$.*

Proof. Let $\deg D = n \geq 0$. Then $D - nv_t$ has degree 0 and hence is the divisor of a function (see **3.6.**). Thus $\mathcal{L}(D) \xrightarrow{\sim} \mathcal{L}(nv_t)$, by **3.5.** above. We need only to show that $\dim \mathcal{L}(nv_t) = 1 + n$. Every element of $\mathcal{L}(nv_t)$ is of the form f/t^i, $0 \leq i \leq n$, with $\deg f \leq i$. This K-subspace of $K(t)$ has dimension $1 + n$. □

Theorem 3.8. *Let $C = C_{a,b}$ be a conic defined over K. Then, for any divisor D of C, we have $\dim \mathcal{L}(D) = 1 + \deg D$ if $\deg D \geq 0$ and $\dim \mathcal{L}(D) = 0$ if $\deg D < 0$.*

Proof. Let L/K be a quadratic extension of K which splits C. By **3.2.** and **3.3.** above, we may replace K by L and assume that $K(C) = K(t)$, the field of rational functions in one variable. The first claim follows from **3.6.** above. Let $D = \sum n_v v$ be a divisor with $\deg D < 0$. If $f \in \mathcal{L}(D)$, $f \neq 0$, $v(f) \geq -n_v$ so that $\deg \operatorname{div}(f) = \sum v(f) \cdot \deg v \geq -\sum n_v \deg v = -\deg D > 0$, a contradiction. Thus $\mathcal{L}(D) = 0$. □

Corollary 3.9. *Let $C = C_{a,b}$ be a conic defined over K. Then any divisor of degree zero is the divisor $\operatorname{div} g$ for some $g \in K(C)^*$.*

Proof. If D is a divisor with $\deg D = 0$, then $\dim \mathcal{L}(D) = 1$. Let $f \in \mathcal{L}(D)$ with $f \neq 0$. Then $\operatorname{div} f + D \geq 0$. Since $\deg(\operatorname{div} f) = \deg D = 0$, it follows that $\operatorname{div} f + D = 0$ i.e. $D = -\operatorname{div}(f) = \operatorname{div}(1/f)$. □

§ 4. Proof of Hilbert Theorem 90 for K_2

Proposition 4.1. *Let K be any field of characteristic $\neq 2$ and L/K any quadratic extension. The sequence $K_2(L) \xrightarrow{1-\sigma} K_2(L) \xrightarrow{\mathrm{tr}} K_2(K)$ is a complex.*

Proof. Since $K_2(L)$ is generated by elements of the form $\langle b, \lambda \rangle$, $b \in K^*$, $\lambda \in L^*$ (see **5.4.** of Chapter III), it is enough to prove that $\mathrm{tr} \circ (1 - \sigma)(\langle b, \lambda \rangle) = 0$. We have

$\mathrm{tr} \circ (1-\sigma)(\langle b, \lambda\rangle) = \mathrm{tr}\langle b, \lambda(\sigma\lambda)^{-1}\rangle = \langle b, N(\lambda(\sigma\lambda)^{-1})\rangle = \langle b, 1\rangle = 1.$ □

Proposition 4.2. *The sequence* $K_2(L) \xrightarrow{1-\sigma} K_2(L) \xrightarrow{tr} K_2(K)$ *is exact if the map* $N_{L/K} : L^* \longrightarrow K^*$ *is surjective.*

Proof. By **4.1.** above, we have an induced homomorphism

$$\widetilde{\mathrm{tr}} : K_2(L)/(1-\sigma)K_2(L) \to K_2(K)$$

induced by transfer. Let $N_{L/K} : L^* \to K^*$ be surjective. We construct an inverse to $\widetilde{\mathrm{tr}}$. We define $\varphi : K^* \times K^* \to K_2(L)/(1-\sigma)K_2(L)$ by $(b, c) \mapsto \overline{\langle \lambda, c\rangle}$ where $\lambda \in L^*$ is such that $N_{L/K}(\lambda) = b$. We note that φ is well-defined. In fact $N_{L/K}(\lambda) = N_{L/K}(\lambda')$ implies that $N_{L/K}(\lambda\lambda'^{-1}) = 1$ so that by the classical Hilbert Theorem 90 (**3.2.** of Chapter II), there exists $\mu \in L^*$ such that $\lambda\lambda'^{-1} = \mu(\sigma\mu)^{-1}$. Then $\langle \lambda, c\rangle - \langle \lambda', c\rangle = \langle \lambda\lambda'^{-1}, c\rangle = \langle \mu(\sigma\mu)^{-1}, c\rangle = (1-\sigma)\langle \mu, c\rangle \in (1-\sigma)K_2(L)$. Obviously φ is biadditive so that we have an induced homomorphism

$$\varphi : K^* \otimes_{\mathbb{Z}} K^* \to K_2(L)/(1-\sigma)K_2(L).$$

We claim that for any $b \in K^*$, $b \neq 1$, $\varphi(b \otimes (1-b)) = 0$; i.e. the symbol $\langle \lambda, 1-b\rangle \in (1-\sigma)K_2(L)$ if $\lambda \in L^*$ is such that $N_{L/K}(\lambda) = b$. Let $\sqrt{b} \in K^*$. Then $\langle \lambda, 1-b\rangle = \langle \lambda, 1+\sqrt{b}\rangle + \langle \lambda, 1-\sqrt{b}\rangle = \langle \lambda/-\sqrt{b}, 1+\sqrt{b}\rangle + \langle \lambda/\sqrt{b}, 1-\sqrt{b}\rangle$. Since $N_{L/K}(\lambda/\pm\sqrt{b}) = 1$, $\lambda/-\sqrt{b} = \mu(\sigma\mu)^{-1}$, $\lambda/\sqrt{b} = \nu(\sigma\nu)^{-1}$. Thus $\langle \lambda, 1-b\rangle = (1-\sigma)\langle \mu, 1+\sqrt{b}\rangle + (1-\sigma)\langle \mu, 1-\sqrt{b}\rangle \in (1-\sigma)K_2(L)$.
Suppose $\sqrt{b} \in L^*$, $\sqrt{b} \notin K^*$. Then $\langle \lambda, 1-b\rangle = \langle \lambda, 1+\sqrt{b}\rangle + \langle \lambda, 1-\sqrt{b}\rangle = \langle \lambda, 1+\sqrt{b}\rangle - \langle \sigma\lambda, 1-\sqrt{b}\rangle + \langle \sigma\lambda, 1-\sqrt{b}\rangle + \langle \lambda, 1-\sqrt{b}\rangle = (1-\sigma)\langle \lambda, 1+\sqrt{b}\rangle + \langle \lambda\sigma\lambda, 1-\sqrt{b}\rangle = (1-\sigma)\langle \lambda, 1+\sqrt{b}\rangle + 2\langle \sqrt{b}, 1-\sqrt{b}\rangle = (1-\sigma)\langle \lambda, 1+\sqrt{b}\rangle \in (1-\sigma)K_2(L)$. Suppose $\sqrt{b} \notin L^*$. Then $L = K(\sqrt{a})$ and $K(\sqrt{b})$ are both Galois over L and are linearly disjoint over K. Let $\widetilde{L} = K(\sqrt{a}, \sqrt{b})$. Then $\widetilde{L}/K$ is Galois and the Galois group is generated by the automorphisms σ_a, σ_b where $\sigma_a(\sqrt{a}) = -\sqrt{a}$, $\sigma_a(\sqrt{b}) = \sqrt{b}$, $\sigma_b(\sqrt{a}) = \sqrt{a}$, $\sigma_b(\sqrt{b}) = -\sqrt{b}$ so that $\sigma_a|_L = \sigma$. By Hilbert Theorem 90 for the extension $\widetilde{L}/K(\sqrt{b})$, we have $\lambda/-\sqrt{b} = \sigma_a(\widetilde{\lambda})\widetilde{\lambda}^{-1}$ for some $\widetilde{\lambda} \in \widetilde{L}^*$. By the projection formula for transfer (§ 1 of Chapter III), we have $\langle \lambda, 1-b\rangle = \langle \lambda, N_{L/L}(1+\sqrt{b})\rangle = \mathrm{tr}_{\widetilde{L}/L}\langle \lambda, 1+\sqrt{b}\rangle = \mathrm{tr}_{\widetilde{L}/L}\langle \sigma_a(\widetilde{\lambda}), 1+\sqrt{b}\rangle - \mathrm{tr}_{\widetilde{L}/L}\langle \widetilde{\lambda}, 1+\sqrt{b}\rangle = \mathrm{tr}_{\widetilde{L}/L} \circ \sigma_a\langle \widetilde{\lambda}, 1+\sqrt{b}\rangle - \mathrm{tr}_{\widetilde{L}/L}\langle \widetilde{\lambda}, 1+\sqrt{b}\rangle = \sigma \circ \mathrm{tr}_{\widetilde{L}/L}\langle \widetilde{\lambda}, 1+\sqrt{b}\rangle - \mathrm{tr}_{\widetilde{L}/L}\langle \widetilde{\lambda}, 1+\sqrt{b}\rangle \in (1-\sigma)K_2(L)$, the last equality being valid since for $\mu \in L^*$, $\widetilde{\mu} \in \widetilde{L}^*$,

$$\begin{aligned}
\mathrm{tr}_{\widetilde{L}/L} \circ \sigma_a\langle \mu, \widetilde{\mu}\rangle &= \mathrm{tr}_{\widetilde{L}/L}\langle \sigma\mu, \sigma_a\widetilde{\mu}\rangle \\
&\quad \langle \sigma\mu, N_{\widetilde{L}/L}\sigma_a\widetilde{\mu}\rangle \\
&\quad \langle \sigma\mu, \sigma_a\widetilde{\mu} \cdot \sigma_b\sigma_a\widetilde{\mu}\rangle \\
&\quad \langle \sigma\mu, \sigma_a\widetilde{\mu} \cdot \sigma_a\sigma_b\widetilde{\mu}\rangle \\
&\quad \langle \sigma\mu, \sigma_a N_{\widetilde{L}/L}(\widetilde{\mu})\rangle \\
&\quad \sigma \circ \mathrm{tr}_{\widetilde{L}/L}\langle \mu, \widetilde{\mu}\rangle.
\end{aligned}$$

This completes the proof of Proposition **4.2.** □

For any field K of characteristic $\neq 2$ and a quadratic extension L/K, we define

$$V(K) = \ker \mathrm{tr} \,/\, \mathrm{im}(1-\sigma),$$

where $\mathrm{tr} : K_2(L) \to K_2(K)$ and $(1-\sigma) : K_2(L) \to K_2(L)$ are as defined earlier. Let E/K be any extension such that $L \not\subset E$ so that EL/E is a quadratic extension of E. We denote by σ the automorphism of EL/E induced by the nontrivial automorphism of σ of L/K. We obtain a complex

$$K_2(EL) \xrightarrow{1-\sigma} K_2(EL) \xrightarrow{tr} K_2(E)$$

and the following diagram is commutative.

$$\begin{array}{ccccc} K_2(EL) & \xrightarrow{1-\sigma} & K_2(EL) & \xrightarrow{\mathrm{tr}} & K_2(E) \\ \uparrow{\scriptstyle \mathrm{ext}} & & \uparrow{\scriptstyle \mathrm{ext}} & & \uparrow{\scriptstyle \mathrm{ext}} \\ K_2(L) & \xrightarrow{1-\sigma} & K_2(L) & \xrightarrow{\mathrm{tr}} & K_2(K). \end{array}$$

We therefore have an induced homomorphism $V(K) \to V(E)$. The strategy for proving Hilbert Theorem 90 for K_2 is to construct an extension E/K such that $L \not\subset E$ and such that

1) $V(K) \to V(E)$ is injective,

2) $N_{EL/E} : (EL)^* \to E^*$ is surjective.

Then, by **4.2.** above, $V(E) = 0$ so that $V(K) = 0$.
To construct such a field E, we begin with the following

Theorem 5.4. *Let K be a field of characteristic $\neq 2$ and L a quadratic extension of K. Let $C = C_{a,b}$ be a conic defined over K, split by L. Then L is not contained in $K(C)$ and the map $V(K) \to V(K(C))$ is injective.*

We postpone the proof of this theorem to § 5 and § 6 and complete the proof of Hilbert Theorem 90 for K_2. We begin with the following

Lemma 4.4. *Let $C = C_{a,b}$ be a conic defined over K and $\widetilde{K}$ any extension of K. Then $\widetilde{K} \otimes_K K(C)$ is an integral domain whose quotient field is isomorphic to $\widetilde{K}(C)$.*

Proof. Since $aX^2 + bY^2 - 1$ is irreducible over any extension of K, $\widetilde{K}[X,Y]/(aX^2 + bY^2 - 1)$ is an integral domain with quotient field $\widetilde{K}(C)$. We have homomorphisms $\widetilde{K}[X,Y]/(aX^2 + bY^2 - 1) = \widetilde{K} \otimes K[X,Y]/\ (aX^2 + bY^2 - 1) \to \widetilde{K} \otimes K(C) \to \widetilde{K}(C)$, the composite being the inclusion of $\widetilde{K}[X,Y]/aX^2 + bY^2 - 1)$ in its quotient field. Thus all the maps above are injections so that $\widetilde{K} \otimes K(C)$ is a domain with quotient field $\widetilde{K}(C)$. □

Proof of Theorem 5.10. Let $K(\sqrt{a})$. For any finite subset $I = \{b_1, b_2, \ldots, b_n\}$ of K^*, we have, by iterated applications of **4.10.** above, that $\otimes_{1\leq j\leq n} K(C_{a,b_j})$ is an integral domain whose quotient field is denoted by K_I. (We note that if $I' = \{b_1, \ldots, b_{n-1}\}$, then, K_I is the function field of the conic C_{a,b_n} over $K_{I'}$). The set $\mathcal{J}$ of finite subsets of K^* is directed with inclusion of subsets as ordering. We note that if $I_1 \subset I_2$, $K_{I_1} \subset K_{I_2}$. Let $K_1 = \varinjlim_{I\in\mathcal{J}} K_I$. We have an inclusion $K_I \subset K_1$. Since L splits C_{a,b_i}, the map $V(K) \to V(K(C_{a,b_i}))$ is injective, by **4.3.** above. Since L is not contained in $K(C_{a,b_i})$, $L \not\subset K_1$. Thus the map $V(K) \to V(K_1)$ is defined and is injective since K_1 is a direct limit of successive function fields. Further, any $b \in K^*$ is a norm in the extension $LK(C_{a,b})/K(C_{a,b})$ since L splits $C_{a,b}$, so that K^* is contained in $N_{LK_1/K_1}(K_1^*)$ and $V(K) \to V(K_1)$ is injective. Replacing K by K_1, we construct a field K_2 such that $L \not\subset K_2$, $V(K_1) \to V(K_2)$ is injective and $K_1^* \subset N_{LK_2/K_2}(K_2^*)$. Iterating this procedure, we get a sequence of fields $K = K_0 \subset K_1 \subset \ldots$. Let $E = \varinjlim_n K_n$. Then $L \not\subset E$ and $V(K) \to V(E)$ is injective since $V(K) \to V(K_n)$ is injective for all n. Further, if $\lambda \in E$, then $\lambda \in K_n$ for some n. By the very construction of K_{n+1}, $\lambda \in N_{LK_{n+1}/K_{n+1}}(LK_{n+1}) \subset N_{LE/E}(LE)$. Thus $N : (LE)^* \to E^*$ is surjective and $V(E) = 0$ by **4.3.**. Hence $V(K) = 0$ and this completes the proof of the theorem. □

§ 5. An analogue of an exact sequence of Bass-Tate for conics

Let K be a field with a discrete valuation v. We have a map $\varphi : K^* \times K^* \to K_v^*$ (K_v denoting the residue field $\mathfrak{O}_v/\mathfrak{p}_v$ of v) given by $(a,b) \mapsto (-1)^{v(a)v(b)}\overline{(a^{v(b)})b^{v(a)})}$ where bar denotes reduction modulo the maximal ideal $\mathfrak{p}_v$ of $\mathfrak{O}$. We note that $\{(-1)^{v(a)v(b)}a^{-v(b)}b^{v(a)}\} = 0$ so that the map is indeed defined. It is easily verified that φ is biadditive and that $\varphi(a, 1-a) = 1$ for $a \in K^*$, $a \neq 1$. Thus we have an induced homomorphism $T_v : K_2(K) \to K_1(K_v) = K_v^*$ called the *tame symbol*. We record the following two properties of the tame symbol.

5.1. If π is a parameter for v, u, u' units of v, then

a) $T_v(<\pi, u>) = \overline{u}$

b) $T_v(<u, u'>) = 1$.

Let $C = C_{a,b}$ be a conic defined over K. We shall assume, from now on that $\operatorname{Char} K \neq 2$. For each $v \in \mathfrak{P}_K(C)$, we have a homomorphism $T_v : K_2(K(C)) \to K_1(K(C)_v)$. These homomorphisms give rise to a homomorphism

$$T = (T_v) : K_2(K(C)) \to \prod_v K_1(K(C)_v).$$

The image of T is, in view of **2.5.**, contained in $\coprod_v K_1(K(C)_v)$.

If C is a split conic, so that $K(C) = K(t)$ is the rational function field in one variable, we have the following

Theorem 5.2. *The sequence*

$$0 \to K_2(K) \to K_2(K(t)) \xrightarrow{T} \coprod_{v \in \mathfrak{P}_K} K_1(K(t)_v) \xrightarrow{N} K_1(K) \to 0$$

is split exact, where $N = \left(N_{K(C)_v/K}\right)$.

See Appendix II for a proof of this theorem. The aim of this section is to prove a partial analogue of the above exact sequence for any conic, not necessarily split. More precisely we prove the following

Theorem 5.3. *Let* $C = C_{a,b}$ *be a conic defined over* K. *The sequence*

$$K_2(K(C)) \xrightarrow{T} \coprod_{v \in \mathfrak{P}_K(C)} K_1(K(C)_v) \xrightarrow{N} K_1(K) \qquad (*)$$

is exact.

Proposition 5.4 *The sequence* $(*)$ *is a complex.*

To prove this proposition, we need the following

Lemma 5.5. *Let* ℓ/k *be a quadratic extension with 2 invertible in* k. *If* v *is any discrete valuation of* k, *the following diagram is commutative.*

$$\begin{array}{ccc} K_2(\ell) & \xrightarrow{(T_w)} & \coprod_{w/v} \ell_w^* \\ \downarrow \mathrm{tr} & & \downarrow \left(N_{\ell_w/k_v}\right) = N \\ K_2(k) & \xrightarrow{T_v} & k_v^* \end{array}$$

Proof.
Case 1. Suppose there is only one extension w of v to ℓ with $e(w/v) = 2$. Then $k_v = \ell_w$ by **2.2.**. Let B be the integral closure of $\mathfrak{O}_w$ in ℓ. Then there exists a parameter π_w of w in B, since $\mathfrak{O}_w = B$. Let $\pi_w^2 + a\pi_w + b = 0$ be the integral equation satisfied by π_w over $\mathfrak{O}_v$. If $a = 0$, then $\pi_w^2 = -b \in k$ and $-b = \pi_v$ is a parameter for v. If $a \neq 0$, it may be checked that $\pi_w + a/2 \in \mathfrak{O}_w$ is a parameter for w whose square $-b + a^2/4$ belongs to k and is a parameter for v. Thus we assume, without loss of generality, that π_w is a parameter for w with $\pi_w^2 = \pi_v \in k$ a parameter for v. Since $K_2(\ell)$ is generated by $\langle a, b\rangle$, $a \in l$, $b \in k$, it is sufficient to check the commutativity of the above diagram for elements of the form $\langle u, u'\rangle$, $\langle u, \pi_v\rangle$, $\langle \pi_w, u'\rangle$, $\langle \pi_w, \pi_v\rangle$ where u is a unit of w and $u' \in k$ is a unit of v.

$$
\begin{array}{lcl}
N \circ T_w(\langle u, u' \rangle) & = & 0 \\
T_v \circ \mathrm{tr}(\langle u, u' \rangle) & = & T_v(\langle N_{\ell/k} u, u' \rangle) \quad \text{(projection formula)} \\
 & = & 0 \quad \text{since } N_{\ell/k} u \text{ is a unit for } v. \\
N \circ T_w(\langle u, \pi_v \rangle) & = & N_{\ell_w/k_v}(\overline{u}^{-2}) = \overline{u}^{-2} \\
T_v \circ \mathrm{tr}(\langle u, \pi_v \rangle) & = & T_v(\langle N_{\ell/k} u, \pi_v \rangle) = \overline{N_{\ell/k} u} - 1 \\
 & = & N_{\ell_w/k_v}(\overline{u})^{-2} = \overline{u}^{-2} \quad \text{(in view of } \mathbf{2.2.}) \\
N \circ T_w(\langle \pi_w, u' \rangle) & = & N_{\ell_w/k_v}(\overline{u}') = \overline{u}' \\
T_v \circ \mathrm{tr}(\langle \pi_w, u' \rangle) & = & T_v(\langle N_{\ell/k} \pi_w, u' \rangle) \\
 & = & T_v(\langle -\pi_v, u' \rangle) \\
 & = & \overline{u'}.
\end{array}
$$

We have $\langle \pi_w, \pi_v \rangle = \langle \pi_w, (-\pi_w)^2 \rangle = 2\langle \pi_w, -\pi_w \rangle = 0$.

Case 2. Suppose there is only one extension w of v to ℓ with $e(w/v) = 1$. Then $[\ell_w : k_v] = 2$ and if π is a parameter for v in k , π is also a parameter for w. If suffices to check the commutativity of the above diagram for elements $\langle \pi, u \rangle$ where $u \in \ell^*$ is a unit for w.

$$
\begin{array}{lcl}
N \circ T_w(\langle \pi, u \rangle) & = & N_{\ell_w/k_v}(\overline{u}) \\
T_v \circ \mathrm{tr}(\langle \pi, u \rangle) & = & T_v(\langle \pi, N_{\ell/k} u \rangle) \\
 & = & \overline{N_{\ell/k} u} = N_{\ell_w/k_v}(\overline{u}) \qquad (\text{see } \mathbf{2.2.}).
\end{array}
$$

Case 3. Let w_1, w_2 be distinct extensions of v to ℓ. Then $e(w_i/v) = 1$ and $[\ell_{w_i} : k_v] = 1$. Let $\sigma \in G(\ell/k)$ be a generator so that $w_2 = w_1 \circ \sigma$ (see **2.2**). Let π be a parameter for v in k. Then π is a parameter for both w_1 and w_2. It suffices to check the commutativity of the diagram for elements of $K_2(\ell)$ of the form $\langle u, b \rangle, \langle \pi, b \rangle$ where $u \in k^*$ is a unit for v and $b \in \ell^*$ any element.

$$
\begin{array}{lcl}
N \circ T_w(\langle u, b \rangle) & = & N\big(\overline{u}^{-w_1(b)}, \overline{u}^{-w_2(b)}\big) \\
 & = & \big(\overline{u}^{-w_1(b)}, \overline{u}^{-w_2(b)}\big)\big(\overline{u}^{-w_2(b)}, \overline{u}^{-w_1(b)}\big) \qquad (\text{see } \mathbf{2.4.}) \\
 & = & \overline{u}^{-(w_1(b)+w_2(b))} \in k_v^* \\
 & = & \overline{u}^{-vNb}. \\
T_v \circ \mathrm{tr}(\langle u, b \rangle) & = & T_v(\langle u, Nb \rangle) = \overline{u}^{-vNb}. \\
N \circ T_w(\langle \pi, b \rangle) & = & N\big((-1)^{w_1(b)} \pi^{-w_1(b)} b), (-1)^{w_2(b)} \pi^{-w_2(b)} b\big) \\
 & = & \overline{(-1)^{vNb} \pi^{-vNb} Nb} \qquad (\text{see } \mathbf{2.4.}) \\
T_v \circ \mathrm{tr}(\langle \pi, b \rangle & = & T_v(\langle \pi, Nb \rangle) \\
 & = & \overline{(-1)^{vNb} \pi^{-vNb} Nb}.
\end{array}
$$

□

Proof of 5.4. Let $t \in K(C)$ be such that $K(C)$ is a quadratic extension of $K(t)$. For any $v \in \mathfrak{P}_K$, there are at the most two valuations w in $\mathfrak{P}_K(C)$ extending v. We

claim that the following diagram is commutative:

$$\begin{array}{ccccc} K_2(K(C)) & \xrightarrow{(T_w)} & \coprod_{w/v} K_1(K(C)_w) & \xrightarrow{N} & K_1(K) \\ \downarrow{\scriptstyle \mathrm{tr}} & & \downarrow{\scriptstyle N} & & \| \\ K_2(K(t)) & \xrightarrow{Tv} & K_1(K(t)_v) & \xrightarrow{N} & K_1(K) \end{array}$$

The right hand side diagram commutes since norm is transitive. The commutativity of the left hand square is a consequence of **5.5.** above. The bottom row is exact by **5.2.**. Hence the top row is a complex. Hence the sequence $(*)$ of **5.3.** is a complex. □

Proof of Theorem 5.3. If C is a conic split over K, then exactness of $(*)$ follows from **5.2.**. We therefore assume that C is non-split. Let $\eta = (\eta_v)_{v\in\mathfrak{P}_K(C)}$, be an element of $\coprod_{v\in\ \mathfrak{P}_K(C)} K_1(K(C)_v)$ with $\prod_v N_{K(C)_v/K}(\eta_v) = 1$. We need to show that $\eta \in \operatorname{im} T$. Let

$$\mathfrak{A}(K(C)) = \coprod_{v\in\mathfrak{P}_K(C)} K_1(K(C)_v).$$

We say that for $\eta, \eta' \in \mathfrak{A}(K(C))$, $\eta \sim \eta'$ if and only if $\eta\eta'^{-1} \in \operatorname{im} T$. For any $\eta \in \mathfrak{A}(K(C))$, we define

$$\operatorname{supp}\eta = \{v \in \mathfrak{P}_K(C) \ \mid \ \eta_v \neq 1\},$$

so that if $\eta = 1$, $\operatorname{supp}\eta = \emptyset$. We define $\operatorname{rk}\eta = (d,\ k)$ where $d = \max_{v\in\operatorname{supp}\eta}\{\deg v\}$, and k is the number of v in $\operatorname{supp}\eta$ with degree $v = d$. If $\eta = 1$, we set $\operatorname{rk}\eta = (0,\ 0)$. We introduce the lexicographic ordering on the set of pairs $(d,\ k)$, i.e., $(d,\ ,k) < (d', k')$ if $d < d'$ or if $d = d'$, $k < k'$. The proof of **5.3.** is immediate if we prove the following:

Step 1. If $\eta \in \mathfrak{A}(K(C))$ with $\operatorname{rk}\eta \leq (2,\ 2)$, then $\prod_v N_{K(C)_v/K}(\eta) = 1$ implies that $\eta \sim 1$.

Step 2. For any $\eta \in \mathfrak{A}(K(C))$, there exists $\eta' \in \mathfrak{A}(K(C))$ such that $\eta \sim \eta'$ and $\operatorname{rk}\eta' \leq (2,\ 2)$.

To prove Step 1, we need the following lemma which is of independent interest.

Lemma 5.6. *Let K_1, K_2 be quadratic extensions of a field K. If $\beta_i \in K_i$ are such that $N_{K_1/K}(\beta_1) = N_{K_2/K}(\beta_2)$, then, there exists $\gamma \in (K_1 \otimes_K K_2)^*$ and $\mu \in K^*$ such that $N_{K_1\otimes K_2/K_1}(\gamma) = \mu\beta_1$, $N_{K_1\otimes K_2/K_2}(\gamma) = \mu\beta_2$.*

Proof. Suppose $K_1 \otimes_K K_2$ is a field. Then $K_1 \otimes_K K_2$ is a Galois extension of K which is the composite of K_1 and K_2 whose Galois group is generated by $\sigma_1 \otimes 1$ and

$1 \otimes \sigma_2$ where $\sigma_i \in G(K_i/K)$ are the generators, $i = 1, 2$. Let $\widetilde{K}$ be the fixed field of $\sigma_1 \otimes \sigma_2$. We have

$$N_{K_1 \otimes K_2/\tilde{K}}(\beta_1 \otimes \beta_2^{-1}) = (\beta_1 \otimes \beta_2^{-1})(\sigma_1\beta_1 \otimes \sigma_2\beta_2^{-1}) = N_{K_1/K}(\beta_1) \otimes N_{K_2/K}(\beta_2^{-1}) = 1,$$

by hypothesis. By Hilbert Theorem 90 for $K_1 \otimes K_2/\widetilde{K}$ (**3.2.**, Chapter III) there exists $\delta \in (K_1 \otimes K_2)^*$ with $\beta_1 \otimes \beta_2^{-1} = \delta \cdot (\sigma_1 \otimes \sigma_2)(\delta^{-1})$. Let $\gamma = (\beta_1 \otimes 1) \cdot (\sigma_1 \otimes \sigma_2)(\delta) = (1 \otimes \beta_2)\delta$ and $\mu = N_{K_1 \otimes K_2/K_1}(\gamma)(\beta_1^{-1} \otimes 1)$. Then $(1 \otimes \sigma_2)(\mu) = \mu$. Since K_1 and K_2 are respectively the fixed fields of $K_1 \otimes K_2$ under $\sigma_1 \otimes 1$ and $1 \otimes \sigma_2$, we get, using the expressions for γ that:

$$\begin{aligned}
\mu &= N_{K_1 \otimes K_2/K_1}((\sigma_1 \otimes \sigma_2)(\delta)) \cdot (\beta_1 \otimes 1) \quad (\in K_1 \otimes 1) \\
&= (\sigma_1 \otimes \sigma_2)(\delta) \cdot (1 \otimes \sigma_2)(\sigma_1 \otimes \sigma_2)(\delta) \cdot (\beta_1 \otimes 1) \\
&= (\sigma_1 \otimes \sigma_2)(\delta) \cdot (\beta_1 \otimes 1)(\sigma_1 \otimes 1)(\delta) \\
&= (1 \otimes \beta_2) \cdot \delta(\sigma_1 \otimes 1)(\delta) \\
&= (1 \otimes \beta_2^{-1}) \cdot N_{K_1 \otimes K_2/K_2}(\gamma) \quad (\in \otimes K_2)\cdot
\end{aligned}$$

Thus $\mu \in K_1 \otimes 1 \cap 1 \otimes K_2 = K$. We have

$$\begin{aligned}
N_{K_1 \otimes K_2/K_1}(\gamma) &= (\beta_1 \otimes 1)\mu \\
N_{K_1 \otimes K_2/K_1}(\gamma) &= (1 \otimes \beta_2)\mu.
\end{aligned}$$

This proves the lemma if $K_1 \otimes_K K_2$ is a field. If $K_1 \otimes_K K_2$ is not a field, $K_1 \otimes_K K_2 \simeq K_1 \times K_1$ (K_1 being isomorphic to K_2 over K) and the automorphism $\sigma : (x, y) \mapsto (y, x)$ of $K_1 \times K_1$ has for its fixed field $\widetilde{K}_1 = \{(x, x) \mid x \in K_1\} \subset K_1 \times K_1$ which is isomorphic to K_1. It is trivially checked that any element of $K_1 \times K_1$ which is of norm 1 over $\tilde{K}_1$ is of the form $\mu(\sigma\mu)^{-1}$ for some $\mu \in (K_1 \times K_1)^*$. The proof of the lemma in this case is on the same lines as before. □

Proof of Step 2. Let $v_1, v_2 \in \mathfrak{P}_K(C)$ be such that $v_1 \neq v_2$, $\deg v_i = 2$ and $\operatorname{supp} \eta \subset \{v_1, v_2\}$. (Note that K being infinite, there are infinitely many valuations of $K(x)$ of degree 1 and C being nonsplit over K, every extension to $K(C)$ of a valuation of degree one of $K(x)$ of degree 2). Let $K_1 = K(C)_{v_1}$, $K_2 = K(C)_{v_2}$. Then K_1 splits C (**2.6.**) and we have the following diagram which is commutative in view of Lemma **5.5.** above.

$$\begin{array}{ccccc}
K_2(K_1(C)) & \xrightarrow{T} & \coprod_{v \in \mathfrak{P}_k(C)}(K_1 \otimes K(C)_v)^* & \xrightarrow{N} & K_1 \\
\downarrow{\scriptstyle \mathrm{tr}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\
K_2(K(C)) & \xrightarrow{T} & \coprod_{v \in \mathfrak{P}_k(C)}(K(C)_v)^* & \longrightarrow & K
\end{array}$$

(We note that $K_1 \otimes_K K(C)_v \simeq \coprod_{w/v} K_1(C)_w$ in view of **2.4.** and $\mathfrak{A}(K_1(C))$ is thus indexed by $\mathfrak{P}_K(C)$.)

Since $\eta \in \mathfrak{A}(K(C))$ is such that $N(\eta) = 1$, $N_{K_1/K}(\eta_{v_1}^{-1}) = N_{K_1/K}(\eta_{v_2})$. By the above lemma **5.6.** on norms, there exist $\mu \in K^*$, $\nu \in K_1 \otimes K_2$ such that $N_{K_1 \otimes K_2/K_1(\nu)} = \mu\,\eta_{v_1}^{-1}$, $N_{K_1 \otimes K_2/K_2}(\nu) = \mu\,\eta_{v_2}$. We define $\widetilde{\eta} \in \mathfrak{A}(K_1(C))$ as follows: the component of

$\widetilde{\eta}$ in $K_1 \otimes K(C)_{v_1} \simeq K_1 \otimes K_1$ is (μ^{-1}, η_{v_1}), the component of $\widetilde{\eta}$ in $K_1 \otimes K(C)_{v_2} \simeq K_1 \times K_2$ is ν and every other component of $\widetilde{\eta}$ is 1. Then $N(\widetilde{\eta}) = \mu^{-1}\eta_{v_1} \cdot N_{K_1 \otimes K_2/K_1}(\nu) = 1$. Since the top row is exact by **5.2.**, C being split by K_1, there exists $\delta \in K_2(K_1(C))$ such that $T(\delta) = \widetilde{\eta}$. We have $T \circ \mathrm{tr}(\delta) = N \circ T(\delta) = N(\widetilde{\eta}) \in \mathfrak{A}(K(C))$ where $N(\widetilde{\eta})_{v_1} = \mu^{-1}\,\eta_{v_1}$, $N(\widetilde{\eta})_{v_2} = \mu\,\widetilde{\eta}_{v_2}$ and $N(\widetilde{\eta})_v = 1$ if $v \neq v_1, v_2$. On the other hand, since $v_1 - v_2 \in \mathrm{Div}(K(C))$ has degree zero, in view of **3.9.**, there exists a function $g \in K(C)^*$ such that $\mathrm{div}\, g = v_1 - v_2$. Then $T(\langle g, \mu\rangle)$ has component μ in K, and μ^{-1} in K_2. Thus $T(\mathrm{tr}(\delta) - \langle g.\mu\rangle) = \eta$ and this proves Step 2. □

To prove Step 1, we begin with the following

Lemma 5.7. *Let C be a conic defined over K and $v \in \mathfrak{P}_K(C)$, $D \in \mathrm{Div}(K(C))$ are such that $\deg D = \deg v$ and $v \notin \mathrm{Supp}\, D$. Then, the map $\mathcal{L}(D) \to K(C)_v$ given by $f \mapsto \overline{f}$, the class of f modulo $\mathfrak{p}_v$, is a surjective homomorphism whose kernel is $\mathcal{L}(D - v)$.*

Proof. Since $v \notin \mathrm{Supp}\, D$, for any $f \in \mathcal{L}(D)$, $v(f) \geq 0$ so that there is a well-defined map $\varphi : \mathcal{L}(D) \to K(C_v)$ which is obviously a homomorphism of K-vector spaces. We have $\ker \varphi = \{f \in \mathcal{L}(D) \mid v(f) \geq 1\} \cup \{0\} = \mathcal{L}(D - v)$. By **3.8.**, $\dim_K \mathcal{L}(D) = 1 + \deg D$ (since $\deg D = \deg v \geq 1$) and $\dim_K \mathcal{L}(D - v) = 1, \deg(D - v)$ being zero. Hence $\dim(\mathrm{im}\, \varphi) = \deg D = \deg v = [K(C)_v : K]$. Thus φ is surjective. □

Lemma 5.8. *Let $\eta \in \mathfrak{A}(K(C))$ be such that rank $\eta = (2n, k)$, $n \geq 1$. Then there exists $g \in K(C)*$ such that $v_1(g) = 0$ and the image of g in $K(C)_{v_1}$ is η_{v_1} and such that $\mathrm{Supp}(\mathrm{div}\, g)$ consists of valuations of degrees $< 2n - 1$.*

Proof. We have already remarked that there are an infinity of $v \in \mathfrak{P}_K(C)$ with $\deg v = 2$. Choose $w_1, w_2 \in \mathfrak{P}_K(C)$ with $w_1 \neq w_2$ and $\deg w_i = 2$, $i = 1, 2$. We have $v_1 \neq w_1$ since $n > 1$ and $\deg nw_1 = \deg v_1 = 2n$. Since $v_1 \notin \mathrm{Supp}(nw_1)$, the map $\varphi : \mathcal{L}(nw_1) \to K(C)_{v_1}$ defined as in **5.7.** above is surjective. Since $v_1 \neq w_1$, for any $h \in \mathcal{L}(w_1)$ $h \neq 0$ $v_1(h) \geq 0$ and the map $\psi : \mathcal{L}(w_1) \to K(C)_{v_1}$ defined by $h \mapsto \eta_{v_1}\bar{h}$ is a well-defined homomorphism of k-vector spaces. We claim that ψ is injective. In fact, if $h \in \mathcal{L}(w_1)$, $h \neq 0$, $\eta_{v_i}\bar{h} = 0$ implies that $\bar{h} = 0$, i.e., $v_1(h) \geq 1$. Thus $\ker \psi = \mathcal{L}(w_1 - v_1)$. Since $\deg(w_1 - v_1) = 2 - 2n < 0$, by **3.8.**, $\ker \psi = 0$. Thus $\dim_K(\psi(\mathcal{L}(w_1))) = \dim_K(\mathcal{L}(w_1)) = 1 + \deg w_1 = 3$. Since φ is surjective, we have $\dim_K \varphi^{-1}(\psi(\mathcal{L}(w_1))) \geq 3$. We have two subspaces $\varphi^{-1}\psi(\mathcal{L}(w_1))$ and $\mathcal{L}(nw_1 - w_2)$ of $l(nw_1)$ which is of dimension $1 + 2n$ over K such that $\dim_K \varphi^{-1}\psi(\mathcal{L}(w_1)) \geq 3$ and $\dim_K \mathcal{L}(nw_1 - w_2) = 2n - 1$. These two subspaces necessarily intersect nontrivially. Let $g \neq 0$ be in this intersection. We claim that $\varphi(\widetilde{g}) \neq 0$. Indeed, if $\varphi(\widetilde{g}) = 0$, then $\widetilde{g} \in \mathcal{L}(nw_1 - v_2)$ and since $\widetilde{g} \in \mathcal{L}(nw_1 - w_2)$ by choice, $wide\widetilde{g} \in \mathcal{L}(nw_1 - w_2 - v_1)$. Since $\deg(nw_1 - w_2 - v_1) = -2 < 0$, it follows by **3.8.** that $\widetilde{g} = 0$, a contradiction. Thus $0 \neq \varphi\widetilde{g}) = \eta_{v_1}\overline{\widetilde{h}}$ for some $\widetilde{h} \in \mathcal{L}(w_1)$, $\widetilde{h} \neq 0$. Let $g = \widetilde{g} \cdot \widetilde{h}^{-1} \in K(C)$. Then $\eta_{v_1} = \bar{g} \in K(C)_{v_1}$ and $\mathrm{Supp}(\mathrm{div}\, g) = \mathrm{Supp}(\mathrm{div}\, \widetilde{g} - \mathrm{div}\, \widetilde{h}) \subset \mathrm{Supp}(\mathrm{div}\, \widetilde{g} \cup \mathrm{Supp}(\mathrm{div}\, \widetilde{h}.$

Since $\widetilde{g} \in \mathcal{L}(nw_1 - w_2)$, we have $w_1(\widetilde{g}) \cdot \deg w_1 \geq -2n$. Since by **3.1.**, $\deg(\operatorname{div} \widetilde{g}) = 0$, it follows that $\operatorname{Supp}(\operatorname{div} \widetilde{g})$ contains no valuation of degree $> 2n$. Since $\widetilde{h} \in \mathcal{L}(w_1)$ with $\deg w_1 = 2$, and by **3.1.**, $\deg(\operatorname{div} \widetilde{h}) = 0$, $\operatorname{Supp} \widetilde{h}$ contains at the most one other valuation of degree 2. It follows that $\operatorname{Supp}(\operatorname{div} g)$ contains valuations of degree at the most $2n - 2$. This proves the lemma. □

Proposition 5.9. *Let C be any conic, non split, over K, and let $\eta = (\eta_v) \in \mathfrak{A}(K(C))$ be such that $\operatorname{rk} \eta = (d, k)$ with $d > 2$. Then there exists $\eta' \in \mathfrak{A}(K(C))$ such that $\eta' \sim \eta$ and $\operatorname{rk} \eta' < \operatorname{rk} \eta$.*

Proof. Let $v_1 \in \mathfrak{P}_K(C)$ with $\deg v_1 = d = 2n\,(n > 1)$ and $v_1 \in \operatorname{Supp} \eta$. Let $v_2 \in \mathfrak{P}_K(C)$ be such that $\deg v_2 = 2$. Since $\deg(v_1 - nv_2) = 0$, there exists by (3.9) $f \in K(C)^\star$ such that $v_1 - nv_2 = \operatorname{div} f$. Let $g \in K(C)^\star$ be chosen as in (5.8) above with respect to v_1. Since $operatornameSuppT(\langle f, g \rangle) \subset \operatorname{Supp}(\operatorname{div} g) \cup \operatorname{Supp}(\operatorname{div} g)$, it follows that $\operatorname{Supp} T(\langle f, g \rangle)$ consists of valuations of degree at the most $d - 2$. We have $v_1(f) = 1$ and $v_1(g) = 0$ with $\bar{g} = n_{v_1}$, so that $T_{v_1}(\langle f, g \rangle) = \eta_{v_1}$. Let $\eta' = \eta \cdot T(\langle f, g \rangle)$. Then $rk\eta' < rk\eta$ and $\eta' \sim \eta$. This proves the proposition. □

Proposition 5.10 *Let C be a non-split conic over K. Let $\eta \in \mathfrak{A}(K(C))$ be such that $rk\eta = (2, k)$ with $k \geq 3$. Then there exists $\eta' \in \mathfrak{A}(K(C))$ with $\eta \sim \eta'$ and such that* $\operatorname{rk}\, \eta' < \operatorname{rk}\, \eta$.

Proof. We choose v_1, v_2, $w \in \mathfrak{P}_K(C)$ contained in $\operatorname{Supp} \eta$ such that $\deg v_1 = \deg v_2 = \deg w = 2$ and v_1, v_2, w distinct. Since $\deg(v_i - w) = 0$, $i = 1, 2$, by **3.9.**, it follows that $v_i - w = \operatorname{div} f_i$ for $f_i \in K(C)^*$. Thus $f_i \in \mathcal{L}(w)$, $i = 1, 2$. By **5.7.** above, the map $f \mapsto \bar{f}$ of $\mathcal{L}(w) \to K(C)_{v_i}$ is surjective for $i = 1, 2$. Thus there exist $g_i \in \mathcal{L}(w_i)$, $g_i \neq 0$ such that $\overline{g_i} = \eta_{v_i}$, $i = 1, 2$ in $K(C)_{v_i}$. We note that f_1 and g_1 (resp. f_2 and g_2) are linearly independent over K. In fact, if $\mu f_1 + \nu g_1 = 0$, μ, $\nu \in K$, then $v_1(f_1) = 0$ so that $\nu \cdot g_1(v_1) = \nu \eta_{v_1} = 0$, i.e., $\nu = 0$. (For any $v \in \mathfrak{P}_K(C)$ and $f \in \mathfrak{O}_v \subset K(C)^*$, $f(v)$ denotes $\bar{f}$, the image of f in $K(C)_v$). Since $f_1(v_2) \neq 0$, and $\mu \cdot f_i(v_2) = 0$, $\mu = 0$.

Since by (3.8) $\dim_K \mathcal{L}(w) = 1 + \deg w = 3$, the 2-dimensional subspaces generated by f_1, g_1 and f_2, g_2 intersect nontrivially. Let $h \neq 0$ be in this intersection. Let $h = \mu_1 f_1 + \nu_1 g_1 = \mu_2 f_2 + \nu_2 g_2$, μ_i, $\nu_i \in K$.

Case 1. $\nu_1 = 0$. Then $\nu_2 \neq 0$ since otherwise $\operatorname{div} f_1 = \operatorname{div} f_1$, a contradiction. Since $v_2(f_1) = 0$, $v_2(f_2) = 1$, we have

$$\begin{aligned} T_{v_2}(\langle f_2, \mu_1/\nu_2 \cdot f_1 \rangle) &= \mu_1/\nu_2 \cdot f_1(v_2) &&= h(v_2)/\nu_2 \\ &= \mu_2/\nu_2 \cdot f_2(v_2) &&+ g_2(v_2) \\ &= g_2(v_2) \\ &= \eta_{v_2}. \end{aligned}$$

Further, $\operatorname{Supp} T(\langle f_2, \mu_1/\nu_2 \cdot f_1 \rangle) \subset (\operatorname{Supp}(\operatorname{div} f_1) \cup \operatorname{Supp}(\operatorname{div} f_2) = \{v_1, v_2, w\}$. Thus $\eta' = \eta \cdot T(\langle f_2, \mu_1/\nu_2 \cdot f_1 \rangle)^1$ has the property $\eta \sim \eta'$ and $\operatorname{rk}\, \eta' < \operatorname{rk}\, \eta$.

Case 2. $\nu_2 = 0$. The argument is similar to Case 1.

Case 3. $\nu_1\nu_2 \neq 0$. We first note that $\mathrm{Supp}(\mathrm{div}\, f_i) = \{w,\, v_i\}$. Since $f_i(v_i) = 0$ and $g_i(v_i) = \bar{g}_i = n_{v_i}$, $h(v_i)$ is defined and equals $\mu_i f_i(v_i) + \nu_i g_i(v_i) = \nu_i \eta_{v_i} \neq 0$, so that $v_i(h) = 0$, $i = 1, 2$. Thus $v_i \notin \mathrm{Supp}(\mathrm{div}\, h)$. Since $h \in \mathcal{L}(w)$, $\mathrm{div}\, h + w = D \geq 0$, i.e., $\mathrm{div}\, h = D - w$ so that D is a positive divisor with $\deg D = \deg w = 2$. Thus $D = w' \in \mathfrak{P}_K(C)$ with $\deg w' = 2$. (Note that w' may be equal to w.) Thus $\mathrm{Supp}\, h = \{w, w'\}$. Consider $\langle f_i/h, h/\nu_i\rangle \in K_2(K(C))$, $i = 1, 2$. Then $\mathrm{Supp}\, T(\langle f_i/h, h/\nu_i\rangle) \subset \mathrm{Supp}(\mathrm{div}\, f_i/h) \cup \mathrm{Supp}(\mathrm{div}\, h) \subset \{v_1, v_2, w, w'\}$ and $T_{v_i}\langle f_i/h, h/\nu_i\rangle = h(v_i)/\nu_i = \eta_{v_i}$, f_i/h being a parameter for v_i, since $v_i(h) = 0$ and $\mathrm{div}\, f_i = v_i - w$. Let $\eta' = \eta \cdot T(\langle f_1/h, h/\nu_1\rangle + \langle f_2/h, h/\nu_2\rangle)^{-1}$. Then $\mathrm{Supp}\, \eta' \subset (\mathrm{Supp}\, \eta \setminus \{v_1, v_2\}) \cup \{w'\}$. Since $\deg w' = 2$, we get $\mathrm{rk}\, \eta' < \mathrm{rk}\, \eta$ and the proposition is proved. □

Proof of Step 1. Immediate from **5.9.** and **5.10.** above. □

§ 6. Injectivity of the map $V(K) \to V(K(C_{a,b}))$

Let $C = C_{a,b}$ be a conic defined over K and L/K a quadratic extension which splits C. Since by **1.3.**, K is algebraically closed in $K(C)$, L is not contained in $K(C)$ and $L(C)$ is a quadratic extension of $K(C)$. Let $\sigma \in G(L/K)$ be a generator. Then σ also generates $G(L(C)/K(C))$. Since L splits C, $L(C)$ is isomorphic to $L(t)$, the field of rational functions in one variable t.

Proposition 6.1. *The diagram*

$$
\begin{array}{ccccccccc}
 & & & & & & & & 1 \\
 & & & & & & & & \downarrow \\
 & & & & K_2(K(C)) & \xrightarrow{T} & \coprod_{v\in\mathfrak{P}(C)} K(C)_v^* & \xrightarrow{N} & K^* \\
 & & & & \downarrow{\scriptstyle \mathrm{ext}} & (3) & \downarrow{\scriptstyle \mathrm{ext}} & (5) & \downarrow{\scriptstyle \mathrm{ext}} \\
0 & \longrightarrow & K_2(L) & \xrightarrow{\mathrm{ext}} & K_2(L(C)) & \xrightarrow{T} & \coprod_{v\in\mathfrak{P}(C)} (L\otimes K(C)_v)^* & \xrightarrow{N} & K^* \\
 & & \downarrow{\scriptstyle 1-\sigma} & (1) & \downarrow{\scriptstyle 1-\sigma} & (4) & \downarrow{\scriptstyle 1-\sigma} & & \\
0 & \longrightarrow & K_2(L) & \xrightarrow{\mathrm{ext}} & K_2(L(C)) & \xrightarrow{T} & \coprod_{v\in\mathfrak{P}(C)} (L\otimes K(C)_v)^* & & \\
 & & \downarrow{\scriptstyle \mathrm{tr}} & (2) & \downarrow{\scriptstyle \mathrm{tr}} & & & & \\
 & & K_2(K) & \xrightarrow{\mathrm{ext}} & K_2(K(C)) & & & &
\end{array}
$$

is commutative where T is the tame symbol (T_w), (identifying $L \otimes K(C)_v$ with $\coprod_{w/v} L(C)_w$ as in the proof of Step 2 of (5.3) of this chapter). Further, the rows are exact, the first two columns are complexes and the last two columns are exact.

Proof. The exactness of the top row is a consequence of **5.3.** and the exactness

of the second and the third rows follows from **5.2.** since $L(C) = L(t)$. The first column on the left is a complex, in view of **4.1**. To show the exactness of the third column from the left, we note that if $L \otimes K(C)_v$ is a field, then $\sigma \otimes 1$ is the Galois automorphism of $L \otimes K(C)_v$ over $K(C)_v$ so that the fixed field for $\sigma \otimes 1$ is $K(C)_v$. If $L \otimes K(C)_v$ is not a field, then $K(C)_v \hookrightarrow L \otimes K(C)_v \simeq K(C)_v \times K(C)_v$, the inclusion being $x \to (x, x)$ and $\sigma \otimes 1$ on $L \otimes K(C)_v$ acts as $(x, y) \to (y, x)$ on this product so that the fixed set for $\sigma \otimes 1$ is again $K(C)_v$. This shows that the third column is exact: the exactness of the right most column is trivial.

Commutativity of (1) is clear. To check the commutativity of (2) we need only to observe that $K_2(L)$ is generated by $\langle a, b\rangle$, $a \in L^*$, $b \in K^*$ and $N_{L/K}(a) = N_{L(C)/K(C)}(a)$. The square (3) is commutative since $L(C)/K(C)$ is such that $e(w/v) = 1$ for w/v (see **2.4.**). The commutativity of (5) is a consequence of the fact that the norm commutes with base change. Finally, we check that the square (4) is commutative. Suppose $v \in \mathfrak{P}_K(C)$ has a unique extension w in $\mathfrak{P}_L(C)$. It is enough to check that the diagram

$$\begin{array}{ccc} K_2(L(C)) & \xrightarrow{T_w} & L(C)_w^* \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ K_2(L(C)) & \xrightarrow{T_w} & L(C)_w^* \end{array}$$

commutes. Let π be a parameter for w. Then $\sigma\pi$ is again a parameter for w. We use that $K_2(L(C))$ is generated by $\langle \pi, u\rangle$, $\langle u', u\rangle$ where u, u' are units for w. We have

$$\sigma \circ T_w(\langle \pi, u\rangle) = \sigma(\overline{u}),$$

$$T_w \circ \sigma(\langle \pi, u\rangle) = T_w(\langle \sigma\pi, \sigma u\rangle) = \overline{\sigma u} = \sigma\overline{u},$$

$$\sigma \circ T_w(\langle u', u\rangle)) = 0 = T_w((\langle \sigma u', \sigma u\rangle)) = T_w \circ \sigma(\langle u'u\rangle).$$

Suppose $w_1, w_2 \in \mathfrak{P}_L(C)$ are two distinct extensions of $v \in \mathfrak{P}(C)$. We need to check that the diagram

$$\begin{array}{ccc} K_2(L(C)) & \xrightarrow{(T_{w_i})} & L(C)_{w_1}^* \oplus L(C)_{w_2}^* \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma\otimes 1} \\ K_2(L(C)) & \xrightarrow{(T_{w_i})} & L(C)_{w_1}^* \oplus L(C)_{w_2}^* \end{array}$$

commutes, where $\sigma \otimes 1$ is the isomorphism $(\overline{x}, \overline{y}) \to (\overline{\sigma y}, \overline{\sigma x})$ (see (2.4)). Let $\pi \in K(C)$ be a parameter for v. Then π is a parameter for w_1 and w_2. We have $K_2(K(C))$ generated by $\langle \pi, a\rangle$ and $\langle u, a\rangle$ where $a \in L(C)^*$ and $u \in K(C)$ is a unit for v. We have

$$\begin{aligned}(\sigma \otimes 1) \circ (T_{w_i})(\langle \pi, a\rangle) &= (\sigma \otimes 1)(\overline{(-1)^{w_1(a)\cdot\pi^{-w_1(a)}\cdot a}}, \overline{(-1)^{w_2(a)\cdot\pi^{-w_2(a)}\cdot a}}) \\ &= (\overline{(-1)^{w_2(a)\cdot\pi^{-w_2(a)}\cdot\sigma a}}, \overline{(-1)^{w_1(a)\cdot\pi^{-w_1(a)}\cdot\sigma a}}).\end{aligned}$$

$$
\begin{aligned}
(T_{w_i}) \circ \sigma(\langle \pi, a\rangle) &= (T_{w_i})\langle \pi, \sigma a\rangle \\
&= (\overline{(-1)^{w_1\sigma a}\cdot \pi^{-w_1\sigma a}\cdot \sigma a}\,,\ \overline{(-1)^{w_2\sigma a}\cdot \pi^{-w_2\sigma a}\cdot \sigma a}), \\
&= (\sigma \otimes 1)\cdot (T_{w_i})(\langle \pi, a\rangle)\ ,
\end{aligned}
$$

since $w_1 \circ \sigma = w_2$, $w_2 \circ \sigma = w_1$.

$$
\begin{aligned}
(\sigma \otimes 1) \circ (T_{w_i})(\langle u, a\rangle) &= (\sigma \otimes 1)(\overline{u^{-w_1(a)}}\,,\ \overline{u^{-w_2(a)}}) \\
&= (\overline{u^{-w_2(a)}}\,,\ \overline{u^{-w_1(a)}})\,.
\end{aligned}
$$

$$
\begin{aligned}
(T_{w_i}) \circ (\sigma \otimes 1)(\langle u, a\rangle) &= (T_{w_i})(\langle u, \sigma a\rangle) \\
&= (\overline{u^{-w_1\sigma a}}\,,\ \overline{u^{-w_2\sigma a}}) \\
&= (\overline{u^{-w_2\sigma a}}\,,\ \overline{u^{-w_1\sigma a}})\,.
\end{aligned}
$$

This shows that the square (4) is commutative and completes the proof of the proposition. □

Proof of Theorem 4.3. As we remarked earlier, K being algebraically closed in $K(C)$, $L \not\subset K(C)$ so that the map $V(K) \to V(K(C))$ is defined. The method of proof involves diagram–chasing in the diagram **6.1.**. Let $\overline{x}_1 \in V(K) = \ker \mathrm{tr} \,/\, \mathrm{im}(1-\sigma)$ with $x_1 \in K_2(L)$ as a representative, i.e. $\mathrm{tr}\, x_1 = 0$. Suppose the image of $\overline{x}_1$ in $V(K(C))$ is zero, i.e. $\mathrm{ext}\, x_1 = x_2 \in K_2(L(C))$ belongs to $(1-\sigma)\cdot K_2(L(C))$. We need to show that $x_1 \in (1-\sigma)\cdot K_2(L)$, in order to check the injectivity of the map $V(K) \to V(K(C))$. Let $x_3 \in K_2(L(C))$ be such that $(1-\sigma)x_3 = x_2$. Let $x_4 = T(x_3)$. Then $(1-\sigma)x_4 = (1-\sigma)T(x_3) = T\sigma(1-\sigma)(x_3) = T(x_2) = T \circ \mathrm{ext}\, x_1 = 0$. The third column being exact, there exists $x_5 \in \coprod_v K(C)_v^*$ such that $\mathrm{ext}\, x_5 = x_4$. We have $Nx_4 = N$
$circTx_3 = 0$. Thus $\mathrm{ext} \circ Nx_5 = N \circ \mathrm{ext}\, x_5 = Nx_4 = 0$. Thus $Nx_5 = 0$. The top row being exact, there exists $x_6 \in K_2(K(C))$ such that $Tx_6 = x_5$. Let $\mathrm{ext}\, x_6 = x_7$. Then $Tx_7 = T \circ \mathrm{ext}\, x_6 = \mathrm{ext} \circ Tx_6 = \mathrm{ext}\, x_5 = x_4$ and hence $T(x_3 - x_7) = 0$. Thus there exists $x_8 \in K_2(L)$ such that $\mathrm{ext}\, x_8 = x_3 - x_7$. We have $(1-\sigma)x_7 = (1-\sigma)\mathrm{ext}\, x_6 = 0$ and hence $(1-\sigma)\mathrm{ext}\, x_8 = (1-\sigma)(x_3) = x_2$. Thus $\mathrm{ext}(1-\sigma)(x_8) = \mathrm{ext}\, x_1$. Since $\mathrm{ext} : K_2(L) \to K_2(L(C))$ is injective, $(1-\sigma)(x_8) = x_1$ so that $\overline{x}_1 = 0$ in $V(K)$. This completes the proof of the theorem. □

Chapter V: Kernel of ext : $k_2(K) \to k_2(K(\sqrt{a}))$

§ 1. An analogue of the tame symbol for cohomology

The aim of this section is to prove the following

Proposition 1.1. *Let K be a field with a discrete valuation v. Suppose K and K_v are of characteristic $\neq 2$. Then there exists a homomorphism $\partial_v : H^2(K) \to H^1(K_v)$ (see § 5 of Ch. III for notation) satisfying the following properties:*

(1) $\partial_v(\chi_\pi \cup \chi_u) = \chi_{\overline{u}}$

(2) $\partial_v(\chi_u \cup \chi_{u'}) = 0$

for any uniformising parameter π for v and units u, u' for v, $\overline{u}$ denoting the residue class of u modulo $\mathfrak{p}_v$.

Remark. The existence of ∂_v would have been immediate if Merkurjev's theorem had been granted. In fact, then, ∂_v is the transport of the tame symbol T_v under the isomorphism $\beta_K : k_2(K) \xrightarrow{\sim} H^2(K)$. We prove **1.1.** directly, since we need it in the proof of Merkurjev's theorem.

For the proof of **1.1.**, we need some generalities on complete discrete valuated fields.

Let K be a field with a discrete valuation v. The map $K \to \mathbb{R}^+$ given by $x \mapsto (1/2)^{v(x)}$, $x \neq 0$ and $0 \mapsto 0$ defines a norm on K and hence a metric. We say that K is *complete with respect to* $\boldsymbol{v}$ if K is complete with respect to this norm. Given a field K with a discrete valuation v, there exists an extension field $\widehat{K}$ of K with a discrete valuation $\widehat{v}$ such that $\widehat{v}$ is an extension of v and $\widehat{K}$ is complete with respect to $\widehat{v}$ and such that K is dense in $\widehat{K}$. The pair $(\widehat{K}, \widehat{v})$ is called the *completion* of (K, v). We shall abbreviate $(\widehat{K}, \widehat{v})$ by $\widehat{K}$. We recall that if $\widehat{K}$ is the completion of K for the discrete valuation v, $\mathfrak{O}_v \hookrightarrow \mathfrak{O}_{\widehat{v}}$, $\mathfrak{p}_v \hookrightarrow \mathfrak{p}_{\widehat{v}}$, $\mathfrak{p}\mathfrak{O}_{\widehat{v}} = \mathfrak{p}_{\widehat{v}}$ (and hence a parameter of v is a parameter for $\widehat{v}$). The canonical map $\mathfrak{O}_v/\mathfrak{p}_v \to \mathfrak{O}_{\widehat{v}}/\mathfrak{p}_{\widehat{v}}$ is an isomorphism.

Let K be a field which is complete with respect to a discrete valuation v and L/K a finite extension. Then it is well–known (Zariski–Samuel, Commutative Algebra Vol. II) that there is a unique extension w of v to L. We say that L/K is *unramified* if $e(w/v) = 1$ and L_w/K_v is separable. We need the following two theorems whose proofs can be found in the Appendix I.

Theorem 1.2. *Let K be a field, complete with respect to a discrete valuation v and K_s a separable closure of K. Then there exists a subfield K_{nr} of K_s containing K (called the maximal unramified extension of K) such that any finite extension L/K, contained in K_s and unramified over K is contained in K_{nr}. If L/K is a finite Galois unramified extension and w the extension of v to L then L_w/K_v is Galois*

and the natural map $G(L/K) \to G(L_w/K_v)$ is an isomorphism. Thus we have an isomorphism $G(K_{nr}/K) \xrightarrow{\sim} G((K_v)_s/K_v)$ of profinite groups.

Theorem 1.3. *Let K be a field, complete with respect to a discrete valuation v and D a central division algebra over K, with $[D : K] = n^2$, $(n, \text{char } K_v) = 1$. Then D contains a maximal commutative subfield L unramified over K. In particular, if* char $K_v \neq 2$, *and if we identify* $\text{Br}(K)$ *with $H_c^2(G(K_s/K), K_s^*)$ and $H_c^2(G(K_{nr}/K), K_{nr}^*)$ as a subgroup of $H_c^2(G(K_s/K), K_s^*)$, under inflation, then ${}_2\text{Br}(K)$ is contained in $H_c^2(G(K_{nr}/K), K_{nr}^*)$.*

Proof of 1.1. We first assume that K is complete with respect to v. The valuation $v : K^* \to \mathbb{Z}$ extends to a surjective homomorphism $v : K_{nr}^* \to \mathbb{Z}$, induced by the unique valuations $L^* \to \mathbb{Z}$, L/K being a finite extension contained in K_{nr}which are extensions of v. This homomorphism v is a continuous $G(K_{nr}/K)$–morphism, $\mathbb{Z}$ being regarded as a trivial $G(K_{nr}/K)$–module. From now on, we write $G(K_{nr}/K) = G_{nr}$. We have a homomorphism $v : H_c^2(G_{nr}, K_{nr}^*) \to H_c^2(G_{nr}, \mathbb{Z})$ induced by v. The exact sequence

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

of trivial G_{nr}–modules gives rise to the exact sequence

$$H_c^1(G_{nr}, \mathbb{Q}) \longrightarrow H_c^1(G_{nr}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H_c^2(G_{nr}, \mathbb{Z}) \longrightarrow H_c^2(G_{nr}, \mathbb{Q}/\mathbb{Z})\,.$$

In view of **4.5.** of Ch. II extended to profinite cohomology, $H_c^1(G_{nr}, \mathbb{Q}) = 0 = H_c^2(G_{nr}, \mathbb{Q})$, so that δ is an isomorphism. We define

$$\widetilde{\partial}_v = \delta^{-1} \circ v : H_c^2(G_{nr}, K_{nr}^*) \longrightarrow H_c^1(G_{nr}, \mathbb{Q}/\mathbb{Z}).$$

Since char $K \neq 2$, ${}_2\text{Br}(K) \xrightarrow{\sim} H^2(K) \hookrightarrow H_c^2(G(K_s/K), K_s^*)$ and since, further, char $K_v \neq 2$, $H^2(K) \hookrightarrow H_c^2(G_{nr}, K_{nr}^*)$ (**1.3.** above). We restrict $\widetilde{\partial}_v$ to $\widetilde{\partial}_v : H^2(K) \to H_c^1(G_{nr}, \mathbb{Q}/\mathbb{Z})$. The isomorphism $c : G_{nr} \xrightarrow{\sim} G((K_v)_s/K_v)$ of **1.3.** yields an isomorphism $\widetilde{c} : H_c^1(G_{nr}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H_c^1(G(K_v/K), \mathbb{Q}/\mathbb{Z})$. The image of $\widetilde{c} \circ \widetilde{\partial}_v$ is contained in the 2–torsion of $H_c^1(G((K_v)_s/K_v), \mathbb{Q}/\mathbb{Z})$. We have an exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{2} \mathbb{Q}/\mathbb{Z} \longrightarrow 0, \quad -1 \mapsto [1/2]$$

of trivial $G((K_v)_s/K_v)$–modules with $\mathbb{Q}/\mathbb{Z}$ divisible. Hence $H^1(K_v)$ can be identified with the 2–torsion subgroup of $H_c^1(G((K_v)_s/K_v), \mathbb{Q}/\mathbb{Z})$. Through this identification, we have a map $\widetilde{c} \circ \widetilde{\partial}_v : H^2(K) \to H^1(K_v)$ which we call ∂_v. We verify that ∂_v satisfies (1) and (2).

Let π be a uniformizer for v and u a unit of v. We first show that the extension $K(\sqrt{u})/K$ is unramified. Since char $K_v \neq 2$ and K is complete, by Hensel's lemma, roots of the polynomial $x^2 - \overline{u}$ in K_v can be lifted to $\mathfrak{O}_v$. Let $x^2 - u$ be irreducible in $K[x]$. Then $x^2 - \overline{u}$ is irreducible in $K_v[x]$. The integral closure of $\mathfrak{O}_v$ in the quadratic extension$K(\sqrt{u})$ of K is $\mathfrak{O}[\sqrt{u}]$ and is the valuation ring of the extension of v to $K(\sqrt{u})$. The corresponding residue field is $\mathfrak{O}[\sqrt{u}]/\mathfrak{p}_v\mathfrak{O}[\sqrt{u}] \xrightarrow{\sim} K_v(\sqrt{\overline{u}})$ which is

a separable quadratic extension of K_v, 2 being invertible in K_v. Thus $K(\sqrt{u})/K$ is unramified.

The quaternion algebra $(\frac{\pi,u}{K})$ corresponding to the element $\chi_\pi \cup \chi_u$ in $H^2(K)$ has $K(\sqrt{u})/K$ as an unramified splitting field and its cohomology class in $H^2(G_{nr}, K_{nr}^*)$ is (see proof of **5.5.**, Ch. I) $\inf[f]$, where $f \in Z^2(G(K(\sqrt{u})/K), K(\sqrt{u})^*)$ is the cocycle $f(\sigma,\sigma) = \pi$, $\sigma \in G(K(\sqrt{u})/K)$ being the generator. The diagram

$$\begin{array}{ccc} H^2(G_{nr}, K_{nr}^*) & \xrightarrow{v} & H^2(G_{nr}, \mathbb{Z}) \\ \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} \\ H^2(G(K(\sqrt{u})/K),\, K(\sqrt{u})^*) & \xrightarrow{v} & H^2(G(K(\sqrt{u})/K), \mathbb{Z}) \end{array}$$

is commutative since inf is functorial. Thus $v \circ \inf[f] = \inf \circ v[f] = \inf[\widetilde{f}]$, $\widetilde{f} \in Z^2(G(K(\sqrt{u})/K, \mathbb{Z})$ being the cocycle $\widetilde{f}(\sigma,\sigma) = v(\pi) = 1$. If $\widetilde{g} \in Z^1(G(K(\sqrt{u})/K), \mathbb{Q}/\mathbb{Z})$ is given by $\widetilde{g}(\sigma) = [1/2] \in \mathbb{Q}/\mathbb{Z}$, it is easily verified that $\delta \inf[\widetilde{g}] = \inf[\widetilde{f}] = v \circ \inf[f]$. Under the isomorphism $c : G_{nr} \xrightarrow{\sim} G((K_v)_s/K_v)$, σ corresponds to the nontrivial automorphism $\overline{\sigma}$ of $K_v(\sqrt{u})$ over K_v and $\widetilde{c}(\inf[\widetilde{g}]) = \inf([h]) \in H^1(K_v)$ where $h \in Z^1(G((K_v)_s/K_v), \mu_2)$ is the cocycle $h(\widetilde{\sigma}) = -1$, i.e., $\inf([h]) = \chi_{\overline{u}}$. Thus $\partial_v(\chi_\pi \cup \chi_u) = \partial_v(\inf[f]) = \chi_{\overline{u}}$, which proves (1). One similarly verifies (2).

If K is not complete with respect to v, let $\widehat{K}$ denote the completion of K with respect to v. The inclusion $K \hookrightarrow \widehat{K}$ induces a homomorphism $s : \mathrm{Br}(K) \to \mathrm{Br}(\widehat{K})$ which, in turn, induces a homomorphism $s : H^2(K) \to H^2(\widehat{K})$. Since $s(\frac{a,b}{K}) = (\frac{a,b}{\widehat{K}})$, we have, $s(\chi_a \cup \chi_b) = \chi_a \cup \chi_b \in H^2(\widehat{K})$. With the canonical identification $K_v = \widehat{K}_v$, we define $\partial_v : H^2(\widehat{K}) \to H^1(K_v)$ as the composite $\partial_{\widehat{v}} \circ s$. Since a parameter (resp. unit) for v remains a parameter (resp. unit) for $\widehat{v}$, it follows that ∂_v satisfies (1) and (2). □

§ 2. A weak form of a theorem of Bloch

Proposition 2.1. *Let K be a field of characteristic $\neq 2$. If $\beta_K : k_2(K) \to H^2(K)$ is injective, and if $K(X_1, \ldots, X_n)$ the rational function field in n variables, then, $\beta_{K(X_1,\ldots,X_n)}$ is injective.*

Proof. By induction on n, it is enough to show that if β_K is injective, then $\beta_{K(X)}$ is injective, $K(X)$ denoting the rational function field in one variable over K. By **5.2.** of Ch. IV, we have a split exact sequence

$$0 \longrightarrow K_2(K) \xrightarrow{\mathrm{ext}} K_2(K(X)) \xrightarrow{T} \coprod_{v \in \mathfrak{P}_K} K_1(K(X)_v) \xrightarrow{N} K_1(K) \longrightarrow 0 \ .$$

Since tensor product commutes with split exact sequences, tensoring the above se-

quence with $\mathbb{Z}/2\mathbb{Z}$ we get an exact sequence

$$0 \longrightarrow k_2(K) \longrightarrow k_2(K(X)) \xrightarrow{T} \coprod_{v\in\mathfrak{P}_K} k_1(K(X)_v) \xrightarrow{N} k_1(K) \longrightarrow 0 \ .$$

In the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & k_2(K) & \xrightarrow{\text{ext}} & k_2(K(X)) & \xrightarrow{T} & \coprod_{v\in\mathfrak{P}_K} k_1(K(X)_v) \\ & & \downarrow{\scriptstyle \beta_K} & & \downarrow{\scriptstyle \beta_{K(X)}} & & \downarrow{\scriptstyle \theta=(\theta_v)} \\ 0 & \longrightarrow & H^2(K) & \xrightarrow{\text{ext}} & H^2(K(X)) & \xrightarrow{\partial=(\partial_v)} & \coprod_{v\in\mathfrak{P}_K} H^1(K(X)_v) \end{array}$$

the map $H^2(K) \xrightarrow{\text{ext}} H^2(K(X))$ is defined by the commutativity of the diagram

$$\begin{array}{ccc} H^2(K) & \xrightarrow{\text{ext}} & H^2(K(X)) \\ \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} \\ {}_2\mathrm{Br}(K) & \xrightarrow{\text{ext}} & {}_2\mathrm{Br}(K(X)) \end{array}$$

where the map on the last line is induced by $[A] \mapsto [K(X) \otimes A]$ and θ is induced by the isomorphisms $\theta_v : k_1(K(X)_v) \xrightarrow{\sim} H^1(K(X)_v)$, $\theta_v(\overline{x}) = \chi_x$. The right hand side square is commutative in view of **1.1.**. The left hand side square is clearly commutative. The map ext : $H^2(K) \to H^2(K(X))$ is injective, in view of **1.7.** of Chapter I. Let $x \in k_2(K(X))$ be such that $\beta_{K(X)}(x) = 0$. Then $\theta \circ T(x) = \partial \circ \beta_{K(X)}(x) = 0$. Since θ is injective, $T(x) = 0$. Since the top row is exact, there exists $y \in k_2(K)$ such that $\text{ext}\, y = x$. We have $\text{ext} \circ \beta_K(y) = \beta_{K(X)} \circ \text{ext}(y) = 0$. Since ext is injective, $\beta_K(y) = 0$ and β_K being injective, $y = 0$. Thus $x = \text{ext}\, y = 0$. □

Remark 2.2. The above proposition is only a part of theorem of Bloch which asserts that the kernel and cokernel of β_K map isomorphically onto the kernel and cokernel of $\beta_{K(X)}$.

§ 3. A criterion for the vanishing of a sum of symbols

Proposition 3.1. *Let K be a field of characteristic $\neq 2$. Let $\{b_1, \ldots, b_n\} \subset K^*$ be such that $\{\overline{b}_1, \ldots, \overline{b}_n\} \subset K^*/K^{*2}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$. Let $c_i \in K^*$, $1 \leq i \leq n$. Then the following conditions are equivalent.*

1) $\sum_{1\leq 1\leq n} \overline{\langle b_i, c_i\rangle} = 0$ *in $k_2(K)$, bar denoting modulo $2K_2(K)$.*

2) *There exists an integer $m \geq n$ and elements $b_{n+1}, \ldots, b_m$ in K^* such that*

   a) *$\{\overline{b}_1, \ldots, \overline{b}_m\}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$.*

b) *Setting* $c_{n+1} = \cdots = c_m = 1$ *and* $b_S = \prod_{i\in S} b_i$, *for each non–empty subset* S *of* $\{1, \ldots, m\}$, *there exists a* $\nu_S \in K^*$ *which is a norm from* $K(\sqrt{b_S})$ *and such that*

$$c_i = \prod_{i\in S} \nu_S, \quad 1 \leq i \leq m \ .$$

3) *Same statement as 2) with the last condition replaced by*

$$\overline{c}_i = \prod_{i\in S} \overline{\nu}_S, \quad 1 \leq i \leq m \ ,$$

bar denoting modulo K^{*2}.

Proof. Trivially 2) $\Rightarrow$ 3). We show that 3) $\Rightarrow$ 2). Let $c_i = \prod_{i\in S} \nu_S \cdot \mu_i^2$, $\mu_i \in K^*$, $1 \leq i \leq m$. We set $\nu'_S = \nu_S$ if $|S| \geq 2$, $\nu'_{\{i\}} = \nu_i \mu_i^2$, $1 \leq i \leq n$. Then $c_i = \prod_{i\in S} \nu'_S$ and ν'_S is obviously a norm from $K(\sqrt{b_S})$.
2) $\Rightarrow$ 1). Since $c_{n+1} = \cdots = c_m = 1$, we have

$$\begin{aligned} \textstyle\sum_{1\leq i\leq n} \overline{\langle b_i, c_i\rangle} &= \sum_{1\leq i\leq m} \overline{\langle b_i, c_i\rangle} \\ &= \textstyle\sum_{1\leq i\leq m} \sum_{i\in S} \overline{\langle b_i, \nu_S\rangle} \\ &= \textstyle\sum_S \overline{\langle b_S, \nu_S\rangle} \\ &= 0 \ , \end{aligned}$$

since ν_S is a norm from $K(\sqrt{b_S})$ (see **3.1.** of Ch. III).
1) $\Rightarrow$ 3). Let $\sum_{1\leq i\leq n} \overline{\langle b_i, c_i\rangle} = 0$. Then

$$\sum_{1\leq i\leq n} \overline{b}_i \otimes \overline{c}_i = \sum_{i\leq j\leq r} \overline{\mu}_j \otimes (1 - \overline{\mu}_j)$$

for some $r \geq 1$ and $\mu_j \in K^*$, $\mu_j \neq 1$ and μ_j non squares in K^*. We extend $\{\overline{b}_1, \ldots, \overline{b}_n\}$ to the set $\{\overline{b}_1, \ldots, \overline{b}_m\}$, $m \geq n$, of linearly independent elements in K^*/K^{*2} over $\mathbb{Z}/2\mathbb{Z}$ generating a subspace containing $\{\overline{\mu}_1, \ldots, \overline{\mu}_r\}$. We define S_j as the set of the indices i, $i \leq m$, such that $\overline{b}_i$ occurs in the expression for $\overline{\mu}_j$ in terms of the basis $\{\overline{b}_1, \ldots, \overline{b}_m\}$. Then $\overline{\mu}_j = \overline{b}_{S_j}$, i.e. $\mu_j = b_{S_j} \cdot \nu_j^2$, $\nu_j \in K^*$. For any nonempty subset $S \subset \{1, \ldots, m\}$, we define $\nu_S = 1$ if $S \neq S_j$ for every j, $1 \leq j \leq r$ and

$$\nu_S = \prod_{\substack{k\in\{1,\ldots,r\} \\ S_k = S_j}} (1 - \nu_k),$$

if $S = S_j$ for some j, $1 \leq j \leq r$. Then $\nu_S \in N_{K(\sqrt{b_S})/K}(K(\sqrt{b_S})^*)$. We set $c_i = 1$ for $n+1 \leq i \leq m$. We verify that $\overline{c}_i = \prod_{i\in S} \overline{\nu}_S$, $1 \leq i \leq m$. To do this, it is enough to check that

$$\sum_{1\leq i\leq m} (\overline{b}_i \otimes \overline{c}_i) \ = \ \sum_{1\leq i\leq m} (\overline{b}_i \otimes \overline{\prod_{i\in S} \nu_S})$$

(with the convention that the product over an empty set is 1), since $\{\overline{b}_i\}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$. However

$$\begin{aligned}\sum_{1\le i\le m}(\overline{b}_i\otimes\overline{c}_i) &= \textstyle\sum_{1\le j\le r}\overline{\mu}_j\otimes(1-\overline{\mu}_j)\\ &= \textstyle\sum_{1\le j\le r}\overline{b}_{S_j}\otimes(1-\overline{\mu}_j)\\ &= \textstyle\sum_S(\overline{b}_S\otimes\prod_{\substack{j\in\{1,\dots,r\}\\ S=S_j}}(1-\overline{\mu}_j)\\ &= \textstyle\sum_S(\overline{b}_S\otimes\overline{\nu}_S)\\ &= \textstyle\sum_{1\le i\le m}\overline{b}_i\otimes(\prod_{i\in S}\overline{\nu}_S)\ .\end{aligned}$$

□

Remark 3.2. We note that any element $\overline{x}\in k_2(K)$ has a representative $x\in K_2(K)$ with $x=\sum_{1\le i\le m}\langle b_i,c_i\rangle$ where $\{\overline{b}_i\}_{1\le i\le m}$ in K^*/K^{*2} are linearly independent over $\mathbb{Z}/2\mathbb{Z}$. Thus the above proposition is indeed a criterion for the vanishing of an element of $K_2(K)$.

§ 4. Construction of a universal field

Theorem 4.1. *Let K be a field of characteristic $\neq 2$. Let $L=K(\sqrt{a})$ be a quadratic extension of K. Let $\{b_i,c_i\}$, $1\le i\le n$ be elements of K^* such that the images of $\{b_1,\dots,b_n\}$ in K^*/K^{*2} and L^*/L^{*2} are linearly independent over $\mathbb{Z}/2\mathbb{Z}$. Let $\operatorname{ext}\sum_{1\le i\le n}\overline{\langle b_i,c_i\rangle}=0$ in $k_2(L)$. Then there exists a field E obtained from the prime field of K by successive purely transcendental and quadratic extensions, an element $A\in E$ with $\sqrt{A}\notin E$, elements $\{B_i,C_i\}$, $1\le i\le n$ in E such that $\operatorname{ext}\sum\overline{\langle B_i,C_i\rangle}=0$ in $k_2(E(\sqrt{A}))$, homomorphisms $\varphi_i: k_i(E)\to k_i(K)$, $i=1,2$ such that $\varphi_1(\overline{A})=\overline{a}$, $\varphi_2(\sum\overline{\langle B_i,C_i\rangle})=\sum\overline{\langle b_i,c_i\rangle}$ and such that the diagram*

$$\begin{array}{ccc} k_1(E) & \longrightarrow & k_2(E) \\ \downarrow{\scriptstyle\varphi_1} & & \downarrow{\scriptstyle\varphi_2} \\ k_1(K) & \longrightarrow & k_2(K), \end{array} \qquad \begin{array}{ccc} \overline{B} & \longmapsto & \overline{\langle A,B\rangle} \\ & & \\ \overline{b} & \longmapsto & \overline{\langle a,b\rangle} \end{array}$$

is commutative.

Before proving the theorem, we record some facts on the theory of places.

A *place* of a field K into a field F is a ring homomorphism $\varphi:\mathfrak{O}\to F$ where $\mathfrak{O}$is a subring of K such that for $x\in K$, either $x\in\mathfrak{O}$ or $x^{-1}\in\mathfrak{O}$ and $\varphi(x^{-1})=0$. We introduce a symbol ∞ and write $\varphi(x)=\infty$ if $x\in K$, $x\notin\mathfrak{O}$ and denote a place by $\varphi: K\to F\cup\infty$. The ring $\mathfrak{O}$ is a local ring whose unique maximal ideal $\mathfrak{p}$ is $\ker\varphi$. We call $\mathfrak{O}$ the *valuation ring of the place*. The homomorphism φ induces an isomorphism of $\mathfrak{O}/\mathfrak{p}$ onto a subfield of F. The group K^*/U, where U is the

group of invertible elements of $\mathfrak{O}$, is an ordered abelian group and the canonical map $K^* \to K^*/U$ is in fact a valuation (not necessarily discrete). Conversely, any valuation of a field into an ordered abelian group gives rise to a place, so that the notions of places and valuations are equivalent. We shall not go into details of this correspondence. We record, however, the following facts which will be needed in the sequel.

The valuation ring $\mathfrak{O}$ of a place $\varphi : K \to F \cup \infty$ has K as its quotient field and is integrally closed in K. If v is a discrete valuation of a field K, the canonical map $\mathfrak{O}_v \to K_v$ defines a place on K. Let $\varphi : K \to F \cup \infty$ be a place and $K' \supset K$, $F' \supset F$. A place $\varphi' : K' \to F' \cup \infty$ is called an *extension* of φ if $\varphi'|_K = \varphi$.

Lemma 4.2.[1] *Let $\varphi_1 : K \to K_1 \cup \infty$, $\varphi_2 : K_1 \to K_2 \cup \infty$ be two places. Then there exists a place $\varphi : K \to K_2 \cup \infty$ satisfying $\varphi(x) = \varphi_2(\varphi_1(x))$ whenever the right hand side is defined. The place φ is called the composition of φ_1 and φ_2, denoted by $\varphi_2 \circ \varphi_1$.*

Proof. Let $\mathfrak{O}_1$ be the valuation ring φ_1 and $\mathfrak{O}_2$ the valuation ring of φ_2. Let $\varphi_1^{-1}(\mathfrak{O}_2) = \mathfrak{O}$. Then $\mathfrak{O} \subset \mathfrak{O}_1$ is a subring which contains $\mathfrak{p} = \varphi_1^{-1}(\mathfrak{p}_2) \supset \varphi_1^{-1}(0) = \mathfrak{p}_1$ where $\mathfrak{p}_i$ are the maximal ideals of $\mathfrak{O}_i$. We show that the homomorphism $\varphi : \mathfrak{O} \to K_2$ defined by $\varphi(x) = \varphi_2(\varphi_1(x))$ is a place of K. Let $x \in K$, $x \notin \mathfrak{O}$. If $x \notin \mathfrak{O}_1$, then $x^{-1} \in \mathfrak{O}_1$ and $\varphi_1(x^{-1}) = 0$, so that $x^{-1} \in \mathfrak{p}_1 \subset \mathfrak{O}$ and $\varphi(x^{-1}) = \varphi_2(\varphi_1(x^{-1})) = 0$. If $x \in \mathfrak{O}_1$, $x \notin \mathfrak{p}_1$, since $\mathfrak{p}_1 \subset \mathfrak{O}$. Thus $x^{-1} \in \mathfrak{O}_1$ and $\varphi_1(x^{-1}) = \varphi_1(x)^{-1}$. Since $x \notin \mathfrak{O}$, $\varphi_1(x) \notin \mathfrak{O}_2$ so that $\varphi_1(x)^{-1} \in \mathfrak{O}_2$ and $\varphi_2(\varphi_1(x)^{-1}) = 0$. Thus $x^{-1} \in \mathfrak{O}$ and $\varphi(x^{-1}) = 0$. Thus φ is indeed a place with $\ker \varphi = \mathfrak{p}$. Further, if $x \in K$ is such that $\varphi_2(\varphi_1(x))$ is defined, then $x \in \mathfrak{O}$, so that φ has properties required by the lemma. □

Proposition 4.3. *Let $\varphi : K \to F \cup \infty$ be a place and $\lambda_1, \ldots, \lambda_n \in F$. Then there exists a place $\varphi' : K(X_1, \ldots, X_n) \to F \cup \infty$ (where $K(X_1, \ldots, X_n)$ is the rational function field) extending φ such that $\varphi(X_i) = \lambda_i$.*

Proof. We suppose, by induction on n, that there is a place

$$\varphi_1 : K(X_1, \ldots, X_{n-1}) \to F \cup \infty$$

extending φ such that $\varphi_1(X_i) = \lambda_i$, $1 \leq i \leq n-1$. We define the place

$$\varphi_2 : K(X_1, \ldots, X_{n-1})(X_n) \to K(X_1, \ldots, X_{n-1}) \cup \infty$$

to be the place associated to the discrete valuation $v_{(X_n - \lambda_n)}$ of the function field $K(X_1, \ldots, X_{n-1})(X_n)$ over $K(X_1, \ldots, X_{n-1})$, i.e., φ_2 is given by the map $K(X_1, \ldots, X_{n-1})[X_n]_{(X_n - \lambda_n)} \to K(X_1, \ldots, X_{n-1})$, $X_n \mapsto \lambda_n$ and identity on

[1] We thank Prof. A. Rosenberg for drawing our attention to this lemma.

$K(X_1, \ldots, X_{n-1})$. Let $\varphi' = \varphi_1 \circ \varphi_2$ as in **4.2.** above. Then $\varphi' : K(X_1, \ldots, X_n) \to F \cup \infty$ has the required properties. $\square$

Lemma 4.4. *Let $\varphi : K \to F \cup \infty$ be a place. Let* char $F \neq 2$ *and $A \in K^*$ an element with $\varphi(A) = a \in F^*$. Suppose $\sqrt{A} \notin K$. If $\sqrt{a}$ denotes a square root of a in F_s, then, there exists a place $\varphi' : K(\sqrt{A}) \to F(\sqrt{a}) \cup \infty$ extending φ with $\varphi'(\sqrt{A}) = \sqrt{a}$.*

Proof. The integral closure of $\mathfrak{O}$ in $K(\sqrt{A})$ contains $\mathfrak{O}[\sqrt{A}]$. In fact, it is equal to $\mathfrak{O}[\sqrt{A}]$ since 2 is a unit of $\mathfrak{O}$ and $\mathfrak{O}$ is integrally closed in K. For, if $\lambda + \mu\sqrt{A} \in K(\sqrt{A})$ is integral over $\mathfrak{O}$, with $\lambda, \mu \in K$, then 2λ and $\lambda^2 - \mu^2 A$ belong to $\mathfrak{O}$ and hence $\lambda, \mu \in \mathfrak{O}$. Let $\mathfrak{p} = \ker \varphi$ and $\overline{\mathfrak{O}} = \mathfrak{O}/\mathfrak{p}$. Then φ can be viewed as the canonical map $\mathfrak{O} \to \overline{\mathfrak{O}}$ composed with an inclusion $\varphi_1 : \overline{\mathfrak{O}} \to F$. Since $\mathfrak{O}[\sqrt{A}]$ is free over $\mathfrak{O}$ with $(1, \sqrt{A})$ as a basis, we have an isomorphism

$$\alpha : \mathfrak{O}[\sqrt{A}]/\mathfrak{p}\mathfrak{O}[\sqrt{A}] \xrightarrow{\sim} \mathfrak{O}/\mathfrak{p} \otimes \mathfrak{O}[\sqrt{A}] \xrightarrow{\sim} \overline{\mathfrak{O}}[X]/(X^2 - a).$$

If $\sqrt{a} \notin \overline{\mathfrak{O}}$, $X^2 - a$ is irreducible in $\overline{\mathfrak{O}}[X]$ and the map $X \mapsto \sqrt{a}$ yields an isomorphism $\theta : \overline{\mathfrak{O}}[X]/(x^2 - a) \xrightarrow{\sim} \overline{\mathfrak{O}}(\sqrt{a})$ which is a quadratic extension of $\overline{\mathfrak{O}}$. Thus $\mathfrak{p}\mathfrak{O}[\sqrt{A}]$ is a maximal ideal of $\mathfrak{O}[\sqrt{A}]$ and the composite map

$$\varphi' : \mathfrak{O}[\sqrt{A}] \xrightarrow{\eta} \mathfrak{O}[\sqrt{A}]/\mathfrak{p}\mathfrak{O}[\sqrt{A}] \xrightarrow{\theta \circ \alpha} \overline{\mathfrak{O}}(\sqrt{a}) \xrightarrow{\varphi_1} F(\sqrt{a})$$

(η being the canonical map), can be verified to be a place extending φ which maps $\sqrt{A}$ to $\sqrt{a}$. If $\sqrt{a} \in F$, then $\overline{\mathfrak{O}}[X]/(X^2 - a) \xrightarrow{\beta}{\sim} \overline{\mathfrak{O}} \times \overline{\mathfrak{O}}$. Let $(\beta \circ \alpha)^{-1}(\overline{\mathfrak{O}}, 0) = \mathfrak{p}_1, (\beta \circ \alpha)^{-1}(0, \overline{\mathfrak{O}}) = \mathfrak{p}_2$. Let $\eta_i : \overline{\mathfrak{O}} \times \overline{\mathfrak{O}} \to \overline{\mathfrak{O}}$ be two projections. Then $\{\mathfrak{p}_i\}, i = 1, 2$, are maximal ideals of $\mathfrak{O}[\sqrt{A}]$ containing $\mathfrak{p} \cdot \mathfrak{O}[\sqrt{A}]$ and the maps

$$\mathfrak{O}[\sqrt{A}] \xrightarrow{\eta} \mathfrak{O}[\sqrt{A}]/\mathfrak{p}\mathfrak{O}[\sqrt{A}] \xrightarrow{(\eta_i \circ \beta \circ \alpha)} \overline{\mathfrak{O}} \xrightarrow{\varphi_1} F$$

yield places of $K(\sqrt{A})$ extending φ, mapping $\sqrt{A}$ to $\sqrt{a}$, respectively. $\square$

Proposition 4.5. *Let $\varphi : K \to F \cup \infty$ be a place. Then there exist homomorphisms $\varphi_i : k_i(K) \to k_i(F)$, $i = 1, 2$ satisfying $\varphi_1(\overline{b}) = \overline{\varphi(b)}$, $\varphi_2(\overline{\langle b_1, b_2 \rangle}) = \overline{\langle \varphi(b_1), \varphi(b_2) \rangle}$, whenever b, b_1, $b_2 \in \mathfrak{O} \setminus \mathfrak{p}$, $\mathfrak{O}$ being the valuation ring of φ and $\mathfrak{p} = \ker(\varphi_{|\mathfrak{O}})$.*

Proof. Let $\{\pi_j\}_{j \in J}$ be a family of elements of K^* whose images in $(K^*/U)/(K^*/U)^2$ form a $\mathbb{Z}/2\mathbb{Z}$–basis. Clearly, every element $b \in K^*$ can be written as a product $b = u \cdot \pi_{j_1} \cdot \ldots \cdot \pi_{j_k} \cdot c^2$ where $u \in U = \mathfrak{O} \setminus \mathfrak{p}$ and $c \in K^*$. In this expression, u is uniquely determined modulo U^2, and the subset $\{j_1, \ldots, j_k\} \subset J$ is unique (uniqueness of u modulo U^2 is a consequence of the fact that $\mathfrak{O}$ is integrally closed in K). We define $\varphi_1 : k_1(K) \to k_1(F)$ by $\varphi_1(\overline{b}) = \overline{\varphi(u)}$, bar denoting modulo squares. We note that if $b \in U$, then $\varphi_1(\overline{b}) = \overline{\varphi(b)}$. If $\overline{b'} = \overline{b}$ and $b' = u' \pi_{i_1} \cdot \ldots \cdot \pi_{i_k} \cdot c'^2$, then $u = u' d^2$, $d \in U$ so that $\overline{\varphi(u)} = \overline{\varphi(u')\varphi(d)^2} = \overline{\varphi(u')}$. Thus φ_1 is well–defined

and is clearly a homomorphism. We define a map $\varphi_2 : k_2(K) \to k_2(F)$ as follows: Let $b = u\pi_{j_1}\cdot\ldots\cdot\pi_{j_k}\cdot c^2$, $b' = u'\pi_{i_1}\cdot\ldots\cdot\pi_{i_\ell}\cdot c'^2$. The map $r : K^* \times K^* \to k_2(F)$ given by $(b, b') \mapsto \overline{\langle\varphi(u), \varphi(u')\rangle}$ is well–defined and biadditive. We show that $r(b, 1-b) = 0$ if $b \in K^*$, $b \neq 1$.

Case 1. Let $b \in \mathfrak{O}$ so that $\varphi(b) \in F$. If $\varphi(b) = 0$, then $1 - b \in U$ and $\varphi(1-b) = 1$. Then $r(b, 1-b) = \overline{\langle\varphi(u), \varphi(1-b)\rangle} = \overline{\langle\varphi(u), 1\rangle} = 0$. If $\varphi(b) = 1$, then $b \in U$ and $r(b, 1-b) = \overline{\langle\varphi(b), \varphi(u')\rangle} = \overline{\langle 1, \varphi(u')\rangle} = 0$ where $1 - b = u'\cdot\pi_{j_1}\cdot\ldots\cdot\pi_{j_k}\cdot c^2$. If $\varphi(b) \neq 0,\ 1$, then $\varphi(1-b) \neq 0,\ 1$ and $b,\ 1-b$ both belong to U so that $r(b, 1-b) = \overline{\langle\varphi(b), 1 - \varphi(b)\rangle} = 0$.

Case 2. Let $b \in K \setminus \mathfrak{O}$. Then $b^{-1} \in \mathfrak{O}$ and $\varphi(b^{-1}) = 0$. Thus $1 - b^{-1} \in U$. If $b = u\cdot\pi_{j_1}\cdot\ldots\cdot\pi_{j_k}\cdot c^2$, then $1 - b = -u\cdot(1 - b^{-1})\cdot\pi_{j_1}\cdot\ldots\cdot\pi_{j_k}\cdot c^2$ with $u\cdot(1 - b^{-1}) \in U$. Thus $r(b, 1-b) = \overline{\langle\varphi(u), \varphi(-u(1-b^{-1}))\rangle} = \overline{\langle\varphi(u), -\varphi(u)\rangle} + \overline{\langle\varphi(u), \varphi(1-b^{-1}))\rangle} = 0 + \overline{\langle\varphi(u), 1\rangle} = 0$.

Thus we have a homomorphism $K_2(K) \to k_2(F)$ which vanishes on $2k_2(K)$ and induces a homomorphism $\varphi_2 : k_2(K) \to k_2(F)$. □

Proof of 4.1. By **3.1.**, there exist elements $b_{n+1}, \ldots, b_m \in L^*$ such that $\{\overline{b}_1, \ldots, \overline{b}_m\}$ in L^*/L^{*2} are linearly independent over $\mathbb{Z}/2\mathbb{Z}$ and for each subset $S \subset \{1, \ldots, m\}$, an element

$$\nu_S \;=\; (x_S + \sqrt{a}\,y_S)^2 - b_S\cdot(z_S + \sqrt{a}\,w_S)^2,$$

$x_S,\ y_S,\ z_S,\ w_S \in K$ and such that

$$c_i \;=\; \prod_{i\in S} \nu_S, \quad 1 \le i \le m,$$

where $b_S = \prod_{i\in S} b_i$ and $c_i = 1$, $n+1 \le i \le m$. Let $b_i = u_i + \sqrt{a}\,v_i$, $n+1 \le i \le m$, $u_i, v_i \in K$. Let K_0 be the prime field of K. Let K_1 be the rational function field obtained from K_0 by adjoining the variables A, $\{B_i, C_i\}$, $1 \le i \le n$, $\{U_i, V_i\}$, $n+1 \le i \le m$, $\{X_S, Y_S, Z_S, W_S\}$, S running over non–empty subsets of $\{1, \ldots, m\}$. By **4.3.**, the inclusion $K_0 \hookrightarrow K$ can be extended to a place $\psi_1 : K_1 \to K \cup \infty$ with $\psi_1(A) = a$, $\psi_1(B_i) = b_i$, $\psi_1(C_i) = c_i$, $1 \le i \le n$, $\psi_1(U_i) = u_i$, $\psi_1(V_i) = v_i$, $n+1 \le i \le m$, $\psi_1(X_S) = x_S$, $\psi_1(Y_S) = y_S$, $\psi_1(Z_S) = z_S$, $\psi_1(W_S) = w_S$, S running over non–empty subset of $\{1, \ldots, m\}$. By **4.4.**, ψ_1 can be extended to a place $\psi_2 : K_1(\sqrt{A}\,) \to L \cup \infty$ with $\psi_2(\sqrt{A}\,) = \sqrt{a}$. (We note that since $\sqrt{a} \notin L$, we may choose $\psi_2(\sqrt{A}\,) = \sqrt{a}$.)

In $K_1(\sqrt{A}\,)$, we define $B_i = U_i + \sqrt{A}\,V_i$, $n+1 \le i \le m$, $B_S = \prod_{i\in S} B_i$, $N_S = (X_S + \sqrt{A}\,Y_S)^2 - B_S(Z_S + \sqrt{A}\,W_S)^2$, for $S \subset \{1, \ldots, m\}$, $S \neq \emptyset$. We shall construct an extension E of K_1 such that $\sqrt{A} \notin E$ and such that $\sum_{1\le i\le n} \overline{\langle B_i, C_i\rangle} = 0$ in $k_2(E(\sqrt{A}\,))$. In view of **3.1.**, it is sufficient to construct an extension E of K_1 with $\sqrt{A} \notin E$ such that $\{\overline{B}_1, \ldots, \overline{B}_m\} \subset E(\sqrt{A}\,)^*/E(\sqrt{A}\,)^{*2}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$ and such that $C_i = \prod_{i\in S} N_S\cdot D^2$ for some $D \in E(\sqrt{A}\,)^*$, $1 \le i \le m$. The construction of such an E is as follows.

We write $\prod_{i\in S} N_S = R_i + \sqrt{A}\,T_1$, with $R_i, T_i \in K_1$. Since R_i, T_i are polynomials in X_S, Y_S, Z_S, W_S, U_i and V_i, $\psi_1(R_i)$, $\psi_1(T_i) \in K$. Since $\psi_2(B_i) = b_i$, $1 \le i \le m$, $\psi_2(B_S) = b_s$ and $\psi_2(N_S) = \nu_S$ for every $S \subset \{1, \dots, m\}$, $S \neq \emptyset$. We have $c_i = \prod_{i\in S} \nu_S = \psi_2(\prod_{i\in S} N_S) = \psi_2(R_i + \sqrt{A}\,T_i) = \psi_1(R_i) + \sqrt{a}\psi_1(T_i)$. Since $c_i \in K$ and $\sqrt{a} \notin K$, it follows that $\psi_1(R_i) = c_i$, $\psi_1(T_i) = 0$. Let $M_i = R_i^2 - AT_i^2$. We denote by E, the field obtained from K_1 by adjoining $\sqrt{M}_1, \dots, \sqrt{M}_m$ and $\sqrt{\frac{R_1+\sqrt{M}_1}{2C_1}}$, .., $\sqrt{\frac{R_m+\sqrt{M}_m}{2C_m}}$. Since $\psi_2(M_i) = \psi_2(R_i^2 - AT_i^2) = c_i^2$, we can extend in view of (4.4) ψ_2 to a place $\psi_3 : K_1(\sqrt{M}_1, \dots, \sqrt{M}_m) \to K \cup \infty$ such that $\psi_3(\sqrt{M}_i) = c_i$. Then $\psi_3(\frac{R_i+\sqrt{M}_i}{2C_i}) = \frac{2c_i}{2c_i} = 1$ and once again ψ_3 can be extended in view of **4.4.** to a place $\psi_4 : E \to K \cup \infty$. We claim that $\sqrt{A} \notin E$. Otherwise, $\sqrt{A}$ would belong to the valuation ring of ψ_4 and hence $\psi_4(\sqrt{A}\,) \in K$ would be a square root of a, contradicting the assumption $\sqrt{a} \notin K$. The place ψ_4 can be extended in view of (4.4) to a place $\psi_5 : E(\sqrt{A}\,) \to L \cup \infty$. Since $\psi_5(B_i) = b_i$ and $\{\overline{b}_i\}$, $1 \le i \le m$ are linearly independent in L^*/L^{*2} over $\mathbb{Z}/2\mathbb{Z}$, it follows that $\{\overline{B}_1, \dots, \overline{B}_m\}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$ in $E(\sqrt{A}\,)^*/E(\sqrt{A}\,)^{*2}$. Further, if $\alpha_i = \sqrt{\frac{R_i+\sqrt{M}_i}{C_i}}$, then $(\prod_{i\in S} N_S)/C_i = (R_i + \sqrt{A}\,T_i)/C_i = (\alpha_i + \frac{\sqrt{A}T_i}{2\alpha_i C_i})^2$ so that $\overline{C_i} = \prod_{i\in S} N_S$ in $E(\sqrt{A}\,)^*/E(\sqrt{A}\,)^{*2}$. Thus $\sum_{1\le i\le n} \overline{\langle B_i, C_i\rangle} = 0$ in $k_2(E(\sqrt{A}\,))$. The place $\psi_4 : E \to K \cup \infty$ which maps A to a gives rise, in view of **4.5.**, to a homomorphism $\varphi_i : k_i(E) \to k_i(K)$ such that $\varphi_1(A) = a$, $\varphi_2(\sum_{1\le i\le n} \overline{\langle B_i, C_i\rangle}) = \sum_{1\le i\le n} \overline{\langle b_i, c_i\rangle}$ and obviously the diagram in **4.1.** This completes the proof of **4.1.**. □

§ 5. Proof of the exactness of $k_1(K) \longrightarrow k_2(K) \longrightarrow k_2(K(\sqrt{a}))$

We have the following commutative diagram

$$\begin{array}{ccccccc} k_1(K) & \xrightarrow{\varphi} & k_2(K) & \xrightarrow{\text{ext}} & k_2(L) & \xrightarrow{\text{tr}} & k_2(K) \\ {\scriptstyle\wr}\downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\beta_K} & & \downarrow{\scriptstyle\beta_L} & & \downarrow{\scriptstyle\beta_K} \\ H^1(K) & \xrightarrow{\chi_a\cup} & H^2(K) & \xrightarrow{\text{res}} & H^2(L) & \xrightarrow{\text{cores}} & H^2(K) \end{array}$$

with the bottom row exact (**5.3.** of Ch. III), where $L = K(\sqrt{a})$.

Lemma 5.1. *If β_K is injective, then β_L is injective for any quadratic extension L of K.*

Proof. Let $x_1 \in K_2(L)$ be such that $\beta_L(x_1) = 0$. Then $\beta_K \circ \text{tr}(x_1) =$ cores $\circ\, \beta_L(x_1) = 0$. Since β_K is injective, $\text{tr}(x_1) = 0$. By **5.11.** of Ch. III, there exists $x_2 \in k_2(K)$ such that ext $x_2 = x_1$. We have res $\circ\, \beta_K(x_2) = \beta_L \circ \text{ext}(x_2) = \beta_L(x_1) = 0$. Since the bottom row is exact, there exists $x_3 \in H^1(K)$ such that $\chi_a \cup x_3 = \beta_K(x_2)$. Let $\theta x_4 = x_3$. Then $\beta_K(x_2 - \varphi x_4) = 0$. Since β_K is injective, $x_2 = \varphi(x_4)$ and $x_1 =$ ext $x_2 =$ ext $\varphi x_4 = 0$. Thus β_L is injective. □

Lemma 5.2. *If β_K is injective, then, for any quadratic extension L of K, the top*

row of the diagram above is exact.

Proof. Since exactness at $k_2(L)$ is already proved in **5.11.** of Ch. III, it is enough to check the exactness at $k_2(K)$. Let $x_1 \in k_2(K)$ with ext $x_1 = 0$. Then res $\circ\, \beta_K(x_1) = \beta_L \circ$ ext $x_1 = 0$. Since the bottom row is exact, there exists $x_2 \in H^1(K)$ such that $\beta_K(x_1) = \chi_a \cup x_2$. Let $\theta(x_3) = x_2$. Then $\beta_K(x_1 - \varphi(x_3)) = 0$. Since β_K is injective, $x_1 = \varphi(x_3)$. □

Theorem 5.3. *Let K be a field of characteristic $\neq 2$ and $L = K(\sqrt{a})$ any quadratic extension. Then the sequence $k_1(K) \xrightarrow{\varphi} k_2(K) \xrightarrow{\text{ext}} k_2(L)$ is exact.*

Proof. Let $x \in k_2(K)$ with $\text{ext}(x) = 0$. Let $\sum_{1\leq i\leq n} \langle b_i, c_i\rangle \in K_2(K)$ be a representative of x. We may assume that $\{\overline{b}_1 \ldots, \overline{b}_n\} \subset K^*/K^{*2}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$. In fact, if $b_k = \mu^2 \cdot b_1^{\varepsilon_1} \cdot \ldots \cdot b_k^{\varepsilon_k} \cdot \ldots \cdot b_n^{\varepsilon_n}$, $\mu \in K^*$, $\varepsilon_i = 0$ or 1, $\varepsilon_k = 0$, then $\sum_{1\leq i\leq n} \overline{\langle b_i, c_i\rangle} = \sum_{1\leq i\leq n,\, i\neq k} \overline{\langle b_i, c_k^{\varepsilon_i} c_i\rangle}$. We may also assume that $\{b_1, \ldots, b_n\} \subset L^*/L^{*2}$ are linearly independent over $\mathbb{Z}/2\mathbb{Z}$. If, for example,

$$b_1 = (\mu + \nu\sqrt{a})^2 b_2^{\varepsilon_2} \cdot \ldots \cdot b_n^{\varepsilon_n},$$

$\varepsilon_i = 0$ or 1 and μ, $\nu \in K$, then $\mu\nu = 0$. If $\nu = 0$, $b_1 = \mu^2 b_2^{\varepsilon_2} \cdot \ldots \cdot b_n^{\varepsilon_n}$ contradicting the linear independence of $\{\overline{b}_1, \ldots, \overline{b}_n\} \subset K^*/K^{*2}$ over $\mathbb{Z}/2\mathbb{Z}$. Thus $\mu = 0$, and $b_1 = a \cdot \nu^2 \cdot b_2^{\varepsilon_2} \cdot \ldots \cdot b_n^{\varepsilon_n}$ and $\sum_{1\leq i\leq n} \langle b_i, c_i\rangle = \langle a, c_1\rangle + \sum_{1\leq i\leq n} \overline{\langle b_i, c_1^{\varepsilon_i} \cdot c_i\rangle}$. Since ext $\overline{\langle a, c_1\rangle} = 0$, ext $\sum_{2\leq i\leq n} \overline{\langle b_i, c_1^{\varepsilon_i} \cdot c_i\rangle} = 0$ and $\sum_{2\leq i\leq n} \overline{\langle b_i, c_1^{\varepsilon_i} \cdot c_i\rangle}$ is of the form $\overline{\langle a, b\rangle}$ if and only if $\sum_{1\leq i\leq n} \overline{\langle b_i, c_i\rangle}$ is of the form $\overline{\langle a, b'\rangle}$.

Thus we assume, without loss of generality that $x = \sum_{1\leq i\leq n} \overline{\langle b_i, c_i\rangle}$ with the images of $\{b_1, \cdots_n\}$ in K^*/K^{*2} and in L^*/L^{*2} linearly independent over $\mathbb{Z}/2\mathbb{Z}$. Let E be an extension of the prime field K_0 of K constructed by successive quadratic and purely transcendental extensions as in **4.1.** with respect to $\sum \langle b_i, c_i\rangle \in K_2(K)$ and the quadratic extension L/K. Since β_{K_0} is injective (**3.4.** or **3.5.** of Ch. IV) β_E is injective, in view of **5.1.** and **2.1.**. Hence by **5.2.**, the sequence

$$k_1(E) \xrightarrow{\varphi} k_2(E) \xrightarrow{\text{ext}} k_2(E(\sqrt{A}\,)$$

is exact. Let $y \in k_1(E)$ be such that $\varphi(y) = \sum_{1\leq i\leq n} \overline{\langle B_i, C_i\rangle}$. Since the diagram

$$\begin{array}{ccc} k_1(E) & \xrightarrow{\varphi} & k_2(E) \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ k_1(K) & \xrightarrow{\varphi} & k_2(K) \end{array}$$

is commutative, $\varphi_2 \circ \varphi(y) = \varphi_2(\sum_{1\leq i\leq n} \overline{\langle B_i, C_i\rangle}) = \sum_{1\leq i\leq n} \overline{\langle b_i, c_i\rangle} = \varphi \circ \varphi_1(y) = \overline{\langle \mathrm{a}, \mathrm{z}\rangle}$ where $\overline{z} = \varphi_1(y)$ and the theorem is proved. □

Appendix I: Existence of unramified splitting fields

§ 1. Some generalities on integral extensions

Let $A \subset B$ be commutative rings. An element $b \in B$ is said to be *integral* over A if b satisfies a monic polynomial $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, $a_i \in A$. The extension B/A is said to be an *integral extension* if every element of B is integral over A. If B/A is any extension, the set of all elements of B integral over A is a subring of B called the *integral closure* of A in B. If $A \subset B \subset C$ with B an integral extension of A and C an integral extension of B, then C is an integral extension of A (see Zariski–Samuel, Commutative Algebra Vol. 1). An integral domain A is said to be *integrally closed* if its integral closure in its quotient field coincides with A. (For example, a unique factorization domain is integrally closed.)

A *discrete valuation ring* is an integrally closed Noetherian domain which has a unique non–zero prime ideal. We record the following (see Zariski–Samuel, Commutative Algebra Vol. 1).

Proposition 1.1. *For a Noetherian domain A, the following conditions are equivalent.*

1. *A is a discrete valuation ring.*
2. *A is a local ring with its maximal ideal principal.*
2. *A is a local principal ideal domain.*

Let A be a discrete valuation ring and π a generator of its maximal ideal. Then every element of A can be written uniquely as $u\pi^n$ where u a unit of A. If K is the quotient field of A, the map $v : K^* \to \mathbb{Z}$ given by $v(a) = n$ where $a = u \cdot \pi^n$, u a unit of A, is a discrete valuation of K whose valuation ring is A. Conversely, the valuation ring of any discrete valuation of a field is a discrete valuation ring, whose maximal ideal is generated by any parameter of the valuation. We note that if A is a discrete valuation ring with quotient field K, A is a maximal subring of K; i.e. $A \subseteq B \subseteq K$, B a ring implies that $A = B$ or $K = B$.

A *Dedekind domain* is a Noetherian integrally closed domain in which every non–zero prime ideal is maximal. We have the following equivalent characterizations of a Dedekind domain.

Proposition 1.2. *For a noetherian domain A, the following are equivalent:*

1) *A is a Dedekind domain.*

2) *For any non–zero prime ideal $\mathfrak{p}$ of A, $A_{\mathfrak{p}}$ is a discrete valuation ring.*

3) *The non–zero fractionary ideals of A (i.e. finitely generated A–submodules of the quotient field of A) form a group under multiplication.*

Corollary. *If A is a Dedekind domain, any non–zero ideal of A can be uniquely written as a finite product $\prod \mathfrak{p}_i^{e_i}$ of prime ideals of A.*

For proofs of **1.2.**, see, for instance, Zariski–Samuel, Commutative Algebra Vol. 1.

Proposition 1.3. *Let A be a Dedekind domain with quotient field K. For any non–zero prime ideal $\mathfrak{p}$ of A let v denote the discrete valuation of K whose valuation ring is $A_\mathfrak{p}$. The map $\mathfrak{p} \mapsto v_\mathfrak{p}$ is a bijection between the set of non–zero prime ideals of A and the set of discrete valuations of K which are non–negative on A.*

Proof. The assignment $\mathfrak{p} \mapsto v_\mathfrak{p}$ is clearly injective. Let v be a discrete valuation of K, non–negative on A. Let $\mathfrak{p} = \{x \in A \mid v(x) > 0\}$. Then $\mathfrak{p} = \mathfrak{p}_v \cap A$, where $\mathfrak{p}_v$ is the maximal ideal of the valuation ring $\mathfrak{O}_v$. Since v is non–trivial, $\mathfrak{p} \neq 0$ and $A_\mathfrak{p} \subset \mathfrak{O}_v$ so that $A_\mathfrak{p} = \mathfrak{O}_v$. □

Lemma 1.4. *Let A be a Dedekind domain with quotient field K. Let L/K be a finite extension and let B be the integral closure of A in L. Then L is the quotient field of B. If B is of finite type over A, then B is a Dedekind domain.*

Proof. Let $b \in L$ and let $b^n + \lambda_1 b^{n-1} + \cdots + \lambda_n = 0$ with $\lambda_i \in K$, $\lambda_n \neq 0$. Clearing the denominators of λ_i, we see that there exists a $\nu \in A$, $\nu \neq 0$ such that νb is integral over A so that $\nu b \in B$. Thus L is the quotient field of B. If B' is the integral closure of B in L, B' is integral over B and B integral over A so that B' is integral over A which implies that $B' = B$. Thus B is integrally closed. Suppose B is of finite type over A. If $\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \cdots \subset \mathfrak{A}_n \subset \ldots$ is a chain of ideals in B, since B is noetherian as an A–module and $\mathfrak{A}_i$ are A–submodules of B, the chain terminates at a finite stage. Thus B is noetherian. Finally we show that every non–zero prime ideal of B is maximal. This is a consequence of the following three lemmas and the fact that every non–zero prime ideal of A is maximal. □

Lemma 1.5. *Let $A \subset B$ be commutative rings with B integral over A. If $\mathfrak{m}$ is any maximal ideal of B, then $\mathfrak{m} \cap A$ is a maximal ideal of A.*

Proof. We have an inclusion $A/\mathfrak{m} \cap A \hookrightarrow B/\mathfrak{m}$ and $B/\mathfrak{m}$ is integral over $A/\mathfrak{m} \cap A$. Replacing A by $A/\mathfrak{m} \cap A$ and B by $B/\mathfrak{m}$, it is enough to prove that if B is a field integral over a subring A, then A is a field. Let $a \in A$, $a \neq 0$. The element $a^{-1} \in B$ satisfies a monic polynomial

$$(a^{-1})^n + a_1(a^{-1})^{n-1} + \cdots + a_n = 0$$

with $a_i \in A$, so that $a^{-1} = -(a_n a^{n-1} + \cdots + a_1) \in A$. Thus A is a field. □

Lemma 1.6. *Let $A \hookrightarrow B$ be integral domains with B integral over A. Then the intersection of every non–zero prime ideal of B with A is non–zero.*

Proof. Let $\mathfrak{P}$ be a non–zero prime ideal of B. Let $b \in \mathfrak{P}$, $b \neq 0$. Let $b^n + a_{n-1}b^{n-1} + \cdots + a_n = 0$ be the monic polynomial satisfied by b over A. Since B is a domain, we may assume that $a_n \neq 0$. Then $a_n = -(b^n + a_1 b^{n-1} + \cdots + a_{n-1}) \in \mathfrak{P} \cap A$. □

Lemma 1.7. *Let $A \hookrightarrow B$ be an integral extension. Let $\mathfrak{p} \subsetneqq \mathfrak{q}$ be prime ideals of B.Then $\mathfrak{p} \cap A$ and $\mathfrak{q} \cap A$ are prime ideals of A with $\mathfrak{p} \cap A \subsetneqq \mathfrak{q} \cap A$.*

Proof. For any prime ideal of B, its intersection with A is clearly a prime ideal of A. Replacing A by $A/\mathfrak{p} \cap A$ and B by $B/\mathfrak{p}$, it is sufficient to prove that for any non–zero prime ideal $\mathfrak{q}$ of B, $\mathfrak{q} \cap A$ is non–zero. This is a consequence of **1.6.**. □

Proposition 1.8. *Let A be a Dedekind domain with quotient field K. Let L/K be a separable extension and B the integral closure of A in L. Then B is a module of finite type over A and hence a Dedekind domain.*

Proof. In view of **1.4.**, L is the quotient field of B. Let $\{b_1, \ldots, b_n\} \subset B$ be a K–basis of L. For any $\lambda \in B$, the conjugates of λ in an algebraic closure of L are integral over A so that $\mathrm{tr}_{L/K}\,\lambda$ is integral over A (tr denoting the trace) and hence belongs to A, A being integrally closed. Let $b \in B$ with $b = \sum_i \lambda_i b_i$, $\lambda_i \in K$. Then $\mathrm{tr}_{L/K}\, bb_j = \sum_i \lambda_i \,\mathrm{tr}_{L/K}\, b_i b_j$. The elements $\mathrm{tr}_{L/K}\, b_i b_j$, $\mathrm{tr}_{L/K}\, bb_j$ belong to A. Let $\delta = \det(\mathrm{tr}_{L/K}\, b_i b_j)$. Since L/K is separable, $\delta \neq 0$ and $\lambda_i \in 1/\delta \cdot A$, for all i. Thus B is contained in $\sum_i Ab_i/\delta$. Since A is noetherian, B is finitely generated as an A–module. □

Proposition 1.9. *Let A be a Dedekind domain with quotient field K. Let L/K be a finite extension and B the integral closure of A in L. Suppose B is a finitely generated A–module. Then B is a Dedekind domain. If $\mathfrak{p}$ is a non–zero prime ideal of A, $\mathfrak{p}B \neq B$ and the valuations of L extending $v_\mathfrak{p}$ are precisely given by $\{v_\mathfrak{P}\}$ where $\mathfrak{P}$ runs over the prime ideals of B containing $\mathfrak{p}$. Let $\mathfrak{p}B = \prod_{\mathfrak{P} \supset \mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$. Then $e_\mathfrak{P} = e(v_\mathfrak{P}/v_\mathfrak{p})$ and if $f_\mathfrak{P}$ is the degree field extension, then $[L : K] = \sum_{\mathfrak{P} \supset \mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}$.*

Proof. In view of **1.4.**, B is a Dedekind domain. To prove the proposition, we may localize A at $\mathfrak{p}$, replace B by $S^{-1}B$ where $S = A \setminus \mathfrak{p}$ and assume that A is a discrete valuation ring. Since A is an A–module of finite type, by Nakayama lemma $\mathfrak{p}B \neq B$. If $\mathfrak{P}$ is any non–zero prime ideal of B, $\mathfrak{P} \cap A$ is a maximal ideal of A (**1.5.**) and hence is equal to $\mathfrak{p}$. Thus $B_\mathfrak{P} \supset A$ and $v_\mathfrak{P}$ is an extension of the valuation $v_\mathfrak{p}$ of K. If w is any extension of $v_\mathfrak{p}$ to L, $\mathfrak{O}_w \supset A$ and since $\mathfrak{O}_w$ is integrally closed in L, $\mathfrak{O}_w \supset B$. Thus w is a valuation of L, non–negative on B so that by **1.3.**, $w = v_\mathfrak{P}$ for some prime ideal $\mathfrak{P}$ of B. Since $\mathfrak{p}B_\mathfrak{P} = \mathfrak{P}^{e_\mathfrak{P}} B_\mathfrak{P}$, we have $e(v_\mathfrak{P}/v_\mathfrak{p}) = e_\mathfrak{p}$. The residue class field of $v_\mathfrak{p}$ is $B_\mathfrak{P}/\mathfrak{P}B_\mathfrak{P} \simeq B/\mathfrak{P}$. Since A is a (local) principal ideal domain and B

a torsion free A–module of finite type, B is free as an A–module and its rank is $[L:K]$. Thus $[L:K] = [B:A] = [B/\mathfrak{p}B : A/\mathfrak{p}] = \sum_{\mathfrak{P}\neq 0}[B/\mathfrak{P}^{e_\mathfrak{P}} : A/\mathfrak{p}]$, since, by chinese reminder theorem, $B/\mathfrak{p}B \simeq \prod_{\mathfrak{P}\neq 0} B/\mathfrak{P}^{e_\mathfrak{P}}$, as $A/\mathfrak{p}$–vector spaces. We have a composition series $B/\mathfrak{P}^{e_\mathfrak{P}} \supset \mathfrak{P}/\mathfrak{P}^{e_\mathfrak{P}} \supset \cdots \supset \mathfrak{P}^{e_\mathfrak{P}-1}/\mathfrak{P}^{e_\mathfrak{P}} \supset 0$ whose successive quotients $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ are isomorphic to $B/\mathfrak{P}$, (since $\mathfrak{P}^2 \subset \mathfrak{A} \subset \mathfrak{P}^{i+1} \Rightarrow \mathfrak{A} = \mathfrak{P}^i$ or $\mathfrak{A} = \mathfrak{P}^{i+1}$). Thus

$$[B/\mathfrak{P}^{e_\mathfrak{P}} : A/\mathfrak{p}] = e_\mathfrak{P}[B/\mathfrak{P} : A/\mathfrak{p}] = e_\mathfrak{P} f_\mathfrak{P} \text{ and } [L:K] = \sum_{\mathfrak{P}\neq 0} e_\mathfrak{P} f_\mathfrak{P} \ .$$

□

Corollary 1.10. *With the notations of 1.9., for $x \in B$, $N_{L/K}(x) \in A$ and*

$$\overline{N_{L/K}(x)} \ = \ \prod_{\mathfrak{P}\supset\mathfrak{p}} N_{B/\mathfrak{P}/A/\mathfrak{p}}(\overline{x})^{e_\mathfrak{P}} \ ,$$

bar denoting reduction modulo $\mathfrak{p}$ on the left hand side and reduction modulo $\mathfrak{P}$ on the right hand side.

Proof. We may assume as before that A is a discrete valuation ring so that B is free over A of rank $[L:K]$. Since any A–basis of B is a K–basis for L, for any $x \in B$,

$$\begin{aligned} \overline{N_{L/K}(x)} \ = \ \overline{N_{B/A}(x)} \ &= \ N_{B/\mathfrak{p}B/A/\mathfrak{p}}(\overline{x}) \ = \ \textstyle\prod_{\mathfrak{P}\neq 0} N_{B/\mathfrak{P}^{e_\mathfrak{P}}/A/\mathfrak{p}}(\overline{x}) \\ &= \ \textstyle\prod_{\mathfrak{P}\neq 0} N_{B/\mathfrak{P}/A/\mathfrak{p}}(\overline{x})^{e_\mathfrak{P}} \end{aligned}$$

since the factors of the composition series

$$B/\mathfrak{P}^e\mathfrak{P} \supset \mathfrak{P}/\mathfrak{P}^{e_\mathfrak{P}} \supset \cdots \supset 0$$

are invariant under multiplication by x. □

Proposition 1.11. *Let A be a Dedekind domain with quotient field K and L/K a finite Galois extension. Let B be the integral closure of A in L. The group $G(L/K)$ operates on B and acts transitively on the set of prime ideals $\mathfrak{P}$ of B containing a given non–zero prime ideal $\mathfrak{p}$ of A. If $\mathfrak{P}$, $\mathfrak{P}'$ are prime ideals containing $\mathfrak{p}$, $e_\mathfrak{P} = e_{\mathfrak{P}'}$, $f_\mathfrak{P} = f_{\mathfrak{P}'}$, and $[L:K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$ where $e_\mathfrak{p} = e_\mathfrak{P}$, $f_\mathfrak{p} = f_\mathfrak{P}$ for any $\mathfrak{P} \supset \mathfrak{p}$ and $g_\mathfrak{p}$ = number of prime ideals of B containing $\mathfrak{p}$.*

Proof. If $x \in B$ and $\sigma \in G(L/K)$, σx is integral over A and hence belongs to B. Thus $G(L/K)$ operates on B and hence on the set of prime ideals of B containing $\mathfrak{p}$. Let $\mathfrak{P}, \mathfrak{P}'$ be prime ideals of B containing $\mathfrak{p}$. Suppose $\mathfrak{P} \not\subset \sigma\mathfrak{P}'$ for every $\sigma \in G(L/K)$. Then $\mathfrak{P} \not\subset \cup_{\sigma\in G(L/K)} \sigma\mathfrak{P}'$ (any ideal contained in the union of prime ideals is contained in one of them). Let $x \in \mathfrak{P}$ such that $\sigma x \notin \mathfrak{P}'$ for every

$\sigma \in G(L/K)$. Then $N_{L/K}x = \prod_{\sigma \in G(L/K)} \sigma(x) \in \mathfrak{P} \cap A = \mathfrak{p} \subset \mathfrak{P}'$ so that $\sigma x \in \mathfrak{P}'$ for some σ, leading to a contradiction. Thus $\mathfrak{P} = \sigma\mathfrak{P}'$ for some $\sigma \in G(L/K)$. The rest of the assertions is clear, in view of **1.9.**. □

§ 2. Complete valuated fields

Let K be a field, complete with respect to a discrete valuation v. As remarked in Ch. V, this means that K is complete with respect to the norm defined by $\|x\| = (1/2)^{v(x)}$, $x \neq 0$ and $\|0\| = 0$. Clearly, the valuation ring $\mathfrak{O}_v$ is closed in K and hence is complete.

Let L/K be a finite extension. The map $v' : L^* \to \mathbb{Z}$ given by $v'(x) = v(N_{L/K}(x))$ is a homomorphism. If $x \in K^*$, $v'(x) = n \cdot v(x)$ where $n = [L : K]$, so that $v'(L^*) \supset n\mathbb{Z}$. Let d be a positive generator of $v'(L^*)$. Then $d|n$ and the map $w : L^* \to \mathbb{Z}$ defined by $w(x) = 1/d \cdot v(N_{L/K}(x))$ is a surjective homomorphism. We shall in fact show that w is the unique discrete valuation of L which extends v and $d = [\overline{L} : \overline{K}]$, bar denoting the corresponding residue fields.

Lemma 2.1. *Let L/K be a finite extension. Then there exists a unique discrete valuation w of L which extends v and L is complete with respect to w.*

Proof. Let $K \subset L_0 \subset L$ be such that L_0/K is separable and L/L_0 purely inseparable. In view of **1.9.**, there exists a discrete valuation v_0 of L_0 extending v. Let $[L : L_0] = p^n = q$ where char $K = p$. Then for any $x \in K$, $x^q \in L_0$ and the map $v_1 : L^* \to \mathbb{Z}$ given by $v_1(x) = v_0(x^q)$ is a homomorphism which satisfies $v_1(x+y) \geq \min(v_1(x), v_1(y))$. If $v_1(L^*) = d\mathbb{Z}$, then $d \neq 0$ and $w = \frac{1}{|d|} \cdot v_1$ is a discrete valuation of L extending v_0 and hence v. The uniqueness of w is a consequence of the following lemma, noting that K is complete and that any two discrete valuations w_1, w_2 of L (extending v) giving rise to equivalent norms are equal. □

Lemma 2.2. *Let K be a field complete for a discrete valuation v. Let v be a finite dimensional vector space over K. If $\| \ \|_1$, $\| \ \|_2$ are two norms on V such that $\|\lambda x\|_i = \|\lambda\| \, \|x\|_i$, $i = 1, 2$, for $x \in V$, $\lambda \in K$, then $\| \ \|_1$ and $\| \ \|_2$ are equivalent, $\| \ \|$ denoting the norm on K induced by the valuation v.*

Lemma 2.3. *Let K be a field complete for a discrete valuation v. Let L/K be a finite extension and let w be the unique extension of v to L. Then $\mathfrak{O}_w$ is the integral closure of $\mathfrak{O}_v$ in L. Further $\mathfrak{O}_w$ is a free $\mathfrak{O}_v$–module of rank equal to $[L : K]$ and $[L : K] = ef$ where $e = e(w/v)$ and $f = [\overline{L} : \overline{K}]$ bar denoting the corresponding residue fields.*

Proof. Let B be the integral closure of A in L. Let π be a uniformizing parameter for v and let $\{b_i\}_{i \in I}$ by elements of B whose images in $B/\pi B$ form a basis of $B/\pi B$ over $\mathfrak{O}_v/(\pi) = \overline{K}$. We shall show that $\{b_i\}_{i \in I}$ form a basis of B over $\mathfrak{O}_v$. Let

$\sum_i a_i b_i = 0$, $a_i \in \mathfrak{O}_v$. Multiplying this equation by a suitable power of π, we may assume that $\overline{a}_i \neq 0$ for some i (bar denotes "modulo π"). Reducing modulo π, there is a relation of linear dependence of $\{\overline{b_i}\}$ over $\overline{K}$, leading to a contradiction. Thus $\{b_i\}_{i\in I}$ are linearly independent over $\mathfrak{O}_v$ and hence over K so that $|I| \leq [L:K] = n$. We write $I = \{1, 2, \ldots, r\}$. Let B_0 be the $\mathfrak{O}_v$–submodule of B generated by $\{b_i\}$. Let $b \in B$. Then $\overline{b} = \sum \overline{a}_i \overline{b}_i$, $\overline{a}_i \in \overline{K}$. Then $b - \sum a_i b_i = \pi b^{(1)}$, $b^{(1)} \in B$, a_i denoting lifts in $\mathfrak{O}_v$ of $\overline{a}_i$. Repeating the same argument, replacing b by $b^{(1)}$, and using induction, we have

$$b = \sum_{1\leq i\leq r} A_i^{(n)} b_i + \pi^n \cdot b^{(n)}$$

where $b^{(n)} \in B$ and $\{A_i^{(m)}\}$ is a Cauchy sequence in $\mathfrak{O}_v$. Since $\mathfrak{O}_v$ is complete, there exists $\widetilde{a}_i \in \mathfrak{O}_v$ with $\widetilde{a}_i = \lim A_i^{(m)}$. Then $b = \sum \widetilde{a}_i b_a \in B_0$ so that $B = B_0$. Thus B is finitely generated over $\mathfrak{O}_v$ and hence by **1.4.**, B is a Dedekind domain. Every prime ideal $\mathfrak{p}$ of B gives rise to a discrete valuation $v_\mathfrak{p}$ of B (see **1.3.**) with valuation ring $B_\mathfrak{p} \supset \mathfrak{O}_v$ and $v_\mathfrak{p}$ lies over v. Since there is a unique extension of v to L, B is local and hence by (**1.2.**, 2)), B is a discrete valuation ring, so that $B = \mathfrak{O}_w$. The rest of the assertions of Lemma **2.3.** follows from **1.9.**. □

Proposition 2.4. *Let K be a field, complete with respect to a discrete valuation v and L/K a finite extension. If w denotes the unique extension of v to L, then, $w = (1/f)v(N_{L/K}(x))$ where $f = [\overline{L} : \overline{K}]$, bar denoting the corresponding residue fields.*

Proof. We first assume that L/K is normal. If σ is any K–automorphism of L, $w = w \circ \sigma$ since $w \circ \sigma$ is again an extension of v. Thus, for any $x \in L$, $w(x) = \frac{1}{[L:K]} w(N_{L/K} x) = \frac{e(w/v)}{[L:K]} v(N_{L/K}(x)) = (1/f)\cdot v(N_{L/K}(x))$ where $f = [\overline{L} : \overline{K}]$, since $e(w/v)f = [L : K]$, by **2.3.**. Suppose L/K is not necessarily normal and let L'/K be the normal closure of L/K. Let w' be the extension of v to L'. For any finite extension M'/M of complete discrete valuated fields, let $e(M'/M)$ denote the ramification and $f(M'/M)$ the degree of the residue field extension. Then $e(L'/K) = e(L'/L)\cdot e(L/K)$ and $f(L'/K) = f(L'/L)\cdot f(L/K)$. Further, by the previous case, $w'(x) = (1/f(L'/K))\cdot v(N_{L'/K}(x))$ for $x \in L'$. For $x \in L$, we have $e(L'/L)w(x) = w'(x) = \frac{1}{f(L'/K)} v(N_{L'/K}(x)) = \frac{1}{f(L'/K)} v(N_{L/K}(x^{[L':L]})) = \frac{[L':L]}{f(L'/K)} v(N_{L/K}(x)) = \frac{e(L'/L)\cdot f(L'/L)}{f(L'/L)\cdot f(L/K)} \cdot v(N_{L/K}(x))$. It follows that $w(x) = (1/f(L/K))\cdot v(N_{L/K}(x))$ and this proves the proposition. □

§ 3. Existence of maximal unramified extensions of complete fields

Let K be a field, complete for a discrete valuation v and L/K a finite extension. We say that L/K is *unramified* if $e(w/v) = 1$ and $[\overline{L} : \overline{K}]$ separable, $\overline{L}/\overline{K}$ denoting the corresponding residue fields.

We shall show that any finite extension ℓ of $\overline{K}$ corresponds to an unramified exten-

sion L/K, unique up to K–isomorphisms, such that $\overline{L}$ is $\overline{K}$–isomorphic to ℓ. We begin with the following

Lemma 3.1. (Hensel) *Let K be a field complete with respect to a discrete valuation v and let $\overline{K}$ denote the residue field $\mathfrak{O}_v/(\pi)$. Let $f \in \mathfrak{O}_v[x]$ such that $\overline{f} \in \overline{K}[x]$ has a simple root $\lambda \in \overline{K}$. Then there exists a unique $x \in \mathfrak{O}_v$ such that $f(x) = 0$ and $\overline{x} = \lambda$.*

Proof. We first prove the uniqueness. Let $x,\ x' \in \mathfrak{O}_v$ be such that $\overline{x} = \overline{x}' = \lambda$ and $f(x) = f(x') = 0$. Let $f(X) = (X - x)g(X)$, $g(X) \in \mathfrak{O}_v[X]$ and $\overline{g}(\lambda) \neq 0$. Then $f(x') = (x' - x)g(x') = 0$. Since $\overline{g(x')} = \overline{g}(\overline{x}') = \overline{g}(\lambda) \neq 0,\ g(x')$ is a unit of $\mathfrak{O}_v$ so that $x - x' = 0$. We now prove the existence of a root of f whose reduction modulo π is λ. Let $x_1 \in \mathfrak{O}_v$ be any lift of λ so that $f(x_1) \in \pi \cdot \mathfrak{O}_v$. Suppose, by induction, that x_n is chosen in $\mathfrak{O}_v$ so that $\overline{x}_n = \lambda$ and $f(x_n) \in \pi^n \cdot \mathfrak{O}_v$. We shall show that x_{n+1} can be chosen in $\mathfrak{O}_v$ so that $\overline{x}_{n+1} = \lambda$ and $f(x_{n+1}) \in \pi^{n+1}\mathfrak{O}_v$. Let $f'(x)$ denote the derivative of f. Since λ is a simple root of $\overline{f}$, $\overline{f'}(\lambda) \neq 0$ so that $f'(x_n)$ is a unit of $\mathfrak{O}_v$. Let $h = -f(x_n) \cdot (f'(x_n))^{-1}$. Then $h \in \pi^n \mathfrak{O}_v$ and $f(x_n + h) = f(x_n) + hf'(x_n) + h^2 \cdot \nu$ where $\nu \in \mathfrak{O}_v$. Since $f(x_n) + hf'(x_n) = 0,\ f(x_n + h) = h^2\nu \in \pi^{n+1}\mathfrak{O}_v$. We take $x_{n+1} = x_n + h$. The sequence $\{x_n\}$ is a Cauchy sequence in $\mathfrak{O}_v$ for the metric induced by v and hence converges to an element x in $\mathfrak{O}_v,\ \mathfrak{O}_v$ being closed in K. Then $f(x) = \lim_n f(x_n) = 0$ and $\overline{x} = \overline{x - x_n} + \overline{x}_n = \lambda$. This proves the lemma. □

Lemma 3.2. *Let $\mathfrak{O}$ be a discrete valuation ring with maximal ideal $\mathfrak{p}$ and residue class field $\overline{\mathfrak{O}} = \mathfrak{O}/\mathfrak{p}$. If $f \in \mathfrak{O}[X]$ is monic and such that $\overline{f} \in \overline{\mathfrak{O}}[X]$ is irreducible, then $\mathfrak{O}[X]/(f)$ is a discrete valuation ring.*

Proof. Let K be the quotient field of $\mathfrak{O}$. Since $\overline{f}$ is irreducible , f, being monic, is irreducible in $\mathfrak{O}[X]$. Since $\mathfrak{O}$ is a principal ideal domain, $\mathfrak{O}[X]$ is a u.f.d. so that f is a prime and $\mathfrak{O}[X]/(f)$ is a domain. Since $\mathfrak{O}[X]/(f)$ is integral over $\mathfrak{O}$, if $\mathfrak{m}$ is any maximal ideal of $\mathfrak{O}[X]/(f)$, by **1.5.**, $\mathfrak{m} \cap \mathfrak{O}$ is a maximal ideal of $\mathfrak{O}$ and hence $\mathfrak{m} \cap \mathfrak{O} = \mathfrak{p}$. Thus the image $\widetilde{(\mathfrak{p}, f)}$ of $(\mathfrak{p}, f)$ in $\mathfrak{O}[X]/(f)$ is contained in $\mathfrak{m}$. We have $\mathfrak{O}[X]/(\mathfrak{p}, f) \simeq \overline{\mathfrak{O}}[X]((\overline{f})$ which is a field and hence $\widetilde{(\mathfrak{p}, f)}$ is maximal in $\mathfrak{O}[X]/(f)$. Thus $\mathfrak{m} = \widetilde{(\mathfrak{p}, f)}$ is generated by π, a generator of $\mathfrak{p}$ in $\mathfrak{O}$. Thus $\mathfrak{O}[X]/(f)$ is a local noetherian domain whose maximal ideal is principal and hence by **1.1.** is a discrete valuation ring. □

Proposition 3.3. *Let K be a complete discrete valuated field with residue field $\overline{K}$. Let $k'/\overline{K}$ be a finite separable extension. Then there exists a finite unramified extension K'/K such that $\overline{K}'$ is $\overline{K}$–isomorphic to k'.*

Proof. Let $k' = \overline{K}(x)$ and let $f \in \mathfrak{O}[X]$ be a monic lift of the minimal polynomial of x over $\overline{K}$, $\mathfrak{O}$ being the valuation ring of K. Let K' be the quotient field of $\mathfrak{O}[X]/(f)$. By **3.2.**, $\mathfrak{O}[X]/(f)$ is a discrete valuation ring such that its maximal

ideal is generated by a parameter in K. Since $\mathfrak{O}[X]/(f)$ is of finite type over $\mathfrak{O}$ and is integrally closed in K', $\mathfrak{O}[X]/(f)$ is the integral closure of $\mathfrak{O}$ in K'. Since every valuation of K' extending the valuation of K is given by the prime ideals of $\mathfrak{O}[X]/(f)$ containing $\mathfrak{p}$, the maximal ideal of $\mathfrak{O}$, (**1.9.**), it follows that there is a unique extension of the valuation of K to K' whose valuation ring is $\mathfrak{O}[X]/(f)$. Since a parameter of K generates the maximal ideal of $\mathfrak{O}[X]/(f)$, $e(K'/K) = 1$. Further, $\mathfrak{O}[X]/(f)/(\mathfrak{m}, f) = \mathfrak{O}/\mathfrak{m}[X]/(\overline{f}) = \overline{K}[X]/(\overline{f}) = k'$ which is separable over $\overline{K}$ so that K'/K is unramified, whose residue field is $\overline{K}$–isomorphic to k'. □

Lemma 3.4. *Let K'/K be a finite unramified extension with residue field $k'/\overline{K}$, constructed in 3.3.. If K''/K is any finite extension with k'' as the residue field, the set of K–isomorphisms of K' into K'' is in bijection with the set of $\overline{K}$–isomorphisms of k' into k''.*

Proof. Let A be the valuation ring of K, $A' = A[X]/(f)$ the valuation ring of K' and A'' the valuation ring of K''. Since K is complete, by **2.3.**, A' and A'' are, respectively, the integral closures of A in K' and K'' and $\mathrm{Hom}_{K-\mathrm{alg}}(K', K'') = \mathrm{Hom}_{A-\mathrm{alg}}(A', A'')$. If $\mathfrak{p}$ is the maximal ideal of A and $\mathfrak{m}'$, $\mathfrak{m}''$ the maximal ideals of A' and A'', respectively, since $f(\mathfrak{p}A') \subset \mathfrak{p}A''$, $f(\mathfrak{m}') \subset \mathfrak{m}''$ and we have a canonical homomorphism $\theta : \mathrm{Hom}_{A-\mathrm{alg}}(A', A'') \to \mathrm{Hom}_{\overline{K}-\mathrm{alg}}(k', k'')$. Every A-algebra homomorphism $A' \to A''$ determines, and is determined by an element $y \in A''$ with $f(y) = 0$. Since $k' = \overline{k}[X]/(\overline{f})$, every $\overline{K}$–isomorphism of k' into k'' determines and is determined by an $\overline{y} \in k''$ with $\overline{f}(\overline{y}) = 0$. Since $\overline{f}$ is separable, by **3.2.**, K'' being complete, every root of $\overline{f}$ can be lifted to a root of f in A''. Thus θ is a bijection. □

Corollary 3.5. *Let K be a complete discrete valuated field with residue field $\overline{K}$. Let k'/K be a finite separable extension. Then there exists an unramified extension K'/K, unique up to K–isomorphism, with residue field $\overline{K}$-isomorphic to k'. In fact, K'/K is Galois if and only if $k'/\overline{K}$ is Galois and in this case $G(K'/K) \xrightarrow{\sim} G(k'/\overline{K})$* ***canonically****.*

Proof. Immediate from **3.3.** and **3.4.**. □

Let K be a complete discrete valuated field. Let K_s denote a separable closure of K. If L, L', contained in K_s are finite unramified extensions of K, the composite LL' in K_s is unramified over K. In fact, if $\overline{L}$, $\overline{L}'$ are the residue fields of L and L', respectively, $\overline{L}\,\overline{L}'$ is separable over $\overline{K}$. If L''/K is the unramified extension whose residue field is $\overline{L}\,\overline{L}'$, the $\overline{K}$–injections $\overline{L} \hookrightarrow \overline{L}\,\overline{L}'$ and $\overline{L}' \hookrightarrow \overline{L}\,\overline{L}'$ yield K–injections $L \hookrightarrow L'$ and $L' \hookrightarrow L''$ and hence $LL' \hookrightarrow L''$. Since L''/K is unramified, $e(L''/K) = e(L''/LL') \cdot e(LL'/K) = 1$ and hence $e(LL'/K) = 1$. Further $\overline{LL'} \subset \overline{L}'' = \overline{L}\,\overline{L}'$ is separable over $\overline{K}$. Thus LL' is unramified over K. Let K_{nr} denote the union of all finite unramified extensions of K contained in K_s. The canonical isomorphisms

$G(L(K) \to G(\overline{L}/\overline{K})$ where L/K is a finite Galois unramified extension of K yield an isomorphism $G(K_{nr}/K) \simeq G(\overline{K}_s/\overline{K})$ of profinite groups. We thus have the following

Theorem 3.6. *Let K be a field, complete with respect to a discrete valuation v and K_s a separable closure of K. Then there exists a subfield K_{nr} of K_s containing K (called the* ***maximal unramified extension of K****) such that every finite unramified extension L/K contained in K_s is contained in K_{nr}. Further if L/K is a finite Galois unramified extension of K contained in K_s, there is a canonical isomorphism $G(L/K) \to G(\overline{L}/\overline{K})$, bar denoting the residue fields. We thus have an isomorphism $G(K_{nr}/K) \xrightarrow{\sim} G(\overline{K}_s/\overline{K})$ of profinite groups.*

§ 4. Unramified splitting fields for division algebras

Let K be a field and A a central simple algebra over K. We define a map Nrd : $A \to K$, called the *reduced norm*, as follows. Let L be a splitting field of A and let $\varphi : L \otimes_K A \xrightarrow{\sim} M_n(L)$, an isomorphism of L–algebras. For $x \in A$, we define Nrd $x = \det \varphi(1 \otimes x)$. If $\varphi' : L \otimes A \xrightarrow{\sim} M_n(L)$ is another isomorphism, $\varphi' \circ \varphi^{-1}$ is an automorphism of $M_n(L)$ which is inner (Ch. I, **2.2.**) and if $\varphi' \circ \varphi^{-1} = \text{Int } \alpha,\ \alpha \in GL_n(L),\ \det \varphi(1 \otimes x) = \det(\alpha^{-1}\varphi'(1 \otimes x)\alpha) = \det \varphi'(1 \otimes x)$, so that Nrd x is independent of the isomorphism φ. Since the determinant map is invariant under base change, it is easy to verify that Nrd x is independent of the splitting field L chosen. Let L/K be a Galois splitting field for A and let $\varphi : L \otimes_K A \simeq M_n(L)$ be an isomorphism of L–algebras. Then, for any $\sigma \in G(L(K),\ \varphi \circ (\sigma \otimes 1) \circ \varphi^{-1} \circ \sigma^{-1}$ is an L–algebra automorphism of $M_n(L)$ and hence $\varphi \circ (\sigma \otimes 1) \circ \varphi^{-1} \circ \sigma^{-1} = \text{Int } \alpha_\sigma,\ \alpha_\sigma \in GL_n(L)$. Then $\sigma(\det\ \varphi(1 \otimes x)) = \det\ \sigma\varphi(1 \otimes x) = \det\ \alpha_\sigma \varphi(1 \otimes x)\alpha_\sigma^{-1} = \det\ \varphi(1 \otimes x)$, so that $\det\ \varphi(1 \otimes x) \in K$. Thus we have a well–defined map Nrd : $A \to K$ which is multiplicative; i.e., $\text{Nrd}(xy) = \text{Nrd } x \cdot \text{Nrd } y$. We may verify the following properties of the reduced norm.

(1) If $a \in M_n(K)$, Nrd $a = \det a$.

(2) If $x \in D,\ D$ a central division algebra over K, Nrd $x = (N_{K(x)/K}(x))^\ell$ where $\ell = n/[K(x) : K]$, where $n^2 = [D : K]$. In particular, if L is a maximal commutative subfield of D containing $x,$ Nrd $x = N_{L/K}x$.

(3) $\text{Nrd}(\lambda x) = \lambda^n \text{ Nrd } x,\ \lambda \in K,\ x \in D$ where $[D : K] = n^2$.

Let K be a field complete for a discrete valuation v. Let D be a central division algebra of dimension n^2 over K. We define a map $v' : D^* \to \mathbb{Z}$ by $v'(x) = v(\text{Nrd } x)$. Clearly, v' is a homomorphism and for $x \in K^*,\ v'(x) = n \cdot v(x)$ so that $v'(K^*) \subset n\mathbb{Z}$. Let $v'(D^*) = d\mathbb{Z}$ with d positive. Then the map $w : D^* \to \mathbb{Z}$ defined by $w(x) = (1/d)v(\text{Nrd } x)$ is a surjective homomorphism. For $x \in K^*,\ w(x) = (n/d)v(x)$.

Lemma 4.1. *For $x, y \in D^*$ with $x + y \in D^*,\ w(x + y) \geq \min(w(x), w(y))$.*

Proof. For any $x \in D$, $\text{Nrd}\, x = N_{L/K}x$ where L is a maximal commutative subfield of D containing x. If w' denotes the unique extension of v to L, $w'(x) = (1/f)v(N_{L/K}(x)) = (1/f)v(\text{Nrd}\, x) = (d/f)w(x)$, $f = [\overline{L} : \overline{K}]$. For $x, y \in D$, let L be a maximal commutative subfield of D containing $x^{-1}y$. Then $w(1 + x^{-1}y) = (f/d)w'(1 + x^{-1}y) \geq \min((f/d)w'(1), (f/d)w'(x^{-1}y)) = \min(w(1), w(x^{-1}y))$ so that $w(x + y) = w(x) + w(1 + x^{-1}y) \geq w(x) + \min(w(1), w(x^{-1}y)) \geq \min(w(x), w(y))$. □

Lemma 4.2. *Let $\mathfrak{O}_D = \{x \in D \mid w(x) \geq 0\} \cup \{0\}$. Then $\mathfrak{O}_D$ is a subring of D. Let $\pi \in \mathfrak{O}_D$ be such that $w(\pi) = 1$. Then $\pi\mathfrak{O}_D = \mathfrak{O}_D\pi$ and every left– or right–ideal of $\mathfrak{O}_D$ is a two-sided ideal generated by a power of π. Every element of $\mathfrak{O}_D$ not in $\pi\mathfrak{O}_D$ is a unit of $\mathfrak{O}_D$.*

Proof. Let $x \in D^*$ and let w' be the extension of v to $K(x)$. Then $w(x) = n' \cdot w'(x)$ for some $n' \in \mathbb{Z}$, $n' \geq 0$. Thus $\mathfrak{O}_D \cap K(x =) = \mathfrak{O}_{w'}$. Since $\mathfrak{O}_{w'}$ is the integral closure of $\mathfrak{O}_v$ in $K(x)$, (see **2.3.**) it follows that $\mathfrak{O}_D$ consists of precisely the elements of D integral over $\mathfrak{O}_v$. The fact that $\mathfrak{O}_D$ is a subring of D follows from the formal properties of valuations, satisfied by w. For $\lambda \in \mathfrak{O}_D$, $\pi\lambda = (\pi\lambda\pi^{-1})\pi$ with $w(\pi\lambda\pi^{-1}) = w(\lambda) \geq 0$ so that $\pi\mathfrak{O}_D = \mathfrak{O}_D\pi$. The rest of the assertions of the lemma is trivial. □

We call w the *extension of* V to D. We define a map $\| \| : D \to \mathbb{R}^+$, by $x \mapsto (1/2)^{w(x)}$ if $x \neq 0$ and $0 \mapsto 0$. It is easily checked that $\| \|$ is a norm. Since K is complete, the topology on Ddefined by this norm is in fact the product topology on K^{n^2}, where $[D : K] = n^2$. If $K \subset L \subset D$ where L is a commutative subfield, then L is closed in D and the restriction of the norm $\| \|$ to L is equivalent to the norm on L induced by the unique extension of v to a valuation of L.

Lemma 4.3. *Let K be a complete discrete valuated field with residue field $\overline{K}$ and let* char $\overline{K} = p$. *Let D be a finite dimensional central division algebra over K such that $[D : K] = n^2$ with $n > 1$ and $(n, p) = 1$ (no condition on n if* char $\overline{K} = 0$*). Then D contains a subfield $L \supsetneqq K$, unramified over K.*

Proof. Suppose such a field L does not exist. Then for every commutative subfield $K \subset L \subset D$, the residue field $\overline{L}$ of L for the unique extension of the valuation of K coincides with $\overline{K}$. For, if $\overline{L} \supsetneqq \overline{K}$, since $[\overline{L} : \overline{K}]$ divides $[L : K]$ (see **2.3.**) which is coprime with char $\overline{K}$, $\overline{L}/\overline{K}$ is separable and can be lifted (see **3.3.**) to an unramified extension L_0/K contained in L, with $[L_0 : K] = [\overline{L} : \overline{K}]$. Let w be an extension of v to D and let $\pi \in D$ be such that $w(\pi) = 1$. Let $b \in \mathfrak{O}_D$ and $L = K(b)$. If w' is the extension of v to $K(b)$, since $v(N_{L/K}(x)) = v(\text{Nrd}\, x)$, $e = \sqrt{[D : K]}/[L : K]$, it follows, in view of **2.4.**, that $w'(b) \geq 0$. Since the residue field of $K(b)$ coincides with $\overline{K}$, there exists $a \in \mathfrak{O}_v$ such that $w'(b - a) \geq 0$. Hence $w(b - a) > 0$ so that there exists $b_1 \in \mathfrak{O}_D$ such that $b - a = \pi b_1$. Repeating the argument, replacing b by

b_1, for each integer N, one has

$$b = a + \pi a_1 + \pi^2 a_2 + \cdots + \pi^{N-1} \cdot a_{N-1} + \pi^N \cdot b_N$$

with $a_i \in \mathfrak{O}_v$, $b_N \in \mathfrak{O}_D$. Since the subfield $K(\pi)$ of D is complete and $w''(\pi) > 0$ where w'' is the extension of v to $K(\pi)$, the Cauchy sequence $\{A_N\}$, where $A_N = a + \pi a_1 + \cdots + \pi^N a_N$, converges to an element of $K(\pi)$ so that $b \in K(\pi)$. Thus $\mathfrak{O}_D \subset K(\pi)$ and $D \subset K(\pi)$ contradicting the hypothesis that $n > 1$. □

Proposition 4.4. *With the same hypothesis as in (4.3), D contains a maximal commutative subfield, unramified over K.*

Proof. By **4.3.**, there exists $K \subsetneqq K' \subset D$ such that K'/K is unramified. Let $D' =$ commutant of K' in D. Then $[D : K] = [D' : K][K' : K]$ (Ch. I, **2.1.**) and hence D' is a central division algebra over K' of dimension $[D : K]/[K' : K]^2$. By induction on $[D : K]$, D' contains a maximal commutative subfield L' unramified over K'. We have $[L' : K]^2 = [L' : K']^2[K' : K]^2 = [D' : K'][K' : K]^2 = [D : K]$ so that L' is a maximal commutative subfield of D. Further L'/K is unramified since L'/K' and K'/K are unramified. □

Appendix II: A theorem of Bass–Tate

Let K be a field. The *Milnor ring* $K_*(K)$ is, by definition, the quotient $T(K^*)/I$ where I is the two–sided ideal of the tensor algebra $T(K^*)$ of the $\mathbb{Z}$–module K^* generated by all elements of the form $a \otimes (1-a)$, for all $a \in K^*$, $a \neq 1$. Since $T(K^*)$ is graded and I is homogeneous, $K_*(K)$ is graded. Let $K_n(K)$ denote the image of $T_n(K^*)$ in $K_*(K)$. Then $K_*(K) = K_0(K) \oplus K_1(K) \oplus \dots$. We have $K_0(K) \simeq \mathbb{Z}$, $K_1(K) \simeq K^*$ and $K_2(K)$ is the group defined in Chapter III. We denote the image of $(a_1 \otimes \cdots \otimes a_n)$ in $K_n(K)$ by $\langle a_1, \dots, a_n \rangle$. The multiplication in $K_*(K)$ is induced by the maps $K_n(K) \times K_m(K) \to K_{n+m}(K)$ given by $(\langle a_1, \dots, a_n \rangle, \langle b_1, \dots, b_m \rangle) \mapsto \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle$. We note that for $a, b \in K^*$, $\langle a \rangle + \langle b \rangle = \langle a \cdot b \rangle$, $-\langle a \rangle = \langle a^{-1} \rangle$ and $\langle a \rangle \cdot \langle b \rangle = \langle a, b \rangle$. The ring $K_*(K)$ is generated by all elements of of the form $\langle a_1, \dots, a_n \rangle$. We have $\langle a_i, \dots, a_n \rangle = 0$ whenever $a_i + a_{i+1} = 1$, for some i, since $\langle a_i, a_{i+1} \rangle = \langle a_i, 1 - a_i \rangle = 0$ and $\langle a_1, \dots, a_n \rangle = \langle a_1, \dots, a_{i-1} \rangle \langle a_i, a_{i+1} \rangle \langle a_{i+2}, \dots, a_n \rangle$.

Lemma 1. *1) For $\xi \in K_n(K)$, $\eta \in K_m(K)$, $\xi\eta = (-1)^{mn}\eta\xi$; i.e. $K_*(F)$ is a graded commutative algebra.*
2) $\langle a_1, \dots, a_n \rangle = 0$ whenever $a_1 + a_2 + \cdots + a_n = 0$ or 1.

Proof. 1) is a consequence of the fact that $\langle a, b \rangle = -\langle b, a \rangle$ in $K_2(K)$ (**1.1.** of Ch. III). The claim 2) is true for $n \leq 2$ since $\langle 1 \rangle = 0$, $\langle a, -a \rangle = 0$ for $a \in K^*$ and $\langle a, 1-a \rangle = 0$ for $a \in K^*$, $a \neq 1$. We prove 2) by induction on n, $n \geq 3$. If $a_1 + a_2 = 0$, $\langle a_1, \dots, a_n \rangle = \langle a_1, a_2 \rangle \cdot \langle a_3, \dots, a_n \rangle = 0$. If $a_1 + a_2 \neq 0$, then $a_1(a_1+a_2)^{-1} + a_2(a_1+a_2)^{-1} = 1$ and hence $\langle a_1(a_1+a_2)^{-1}, a_2(a_1+a_2)^{-1} \rangle = 0$, i.e. $\langle a_1, a_2 \rangle + \langle a_1 + a_2, a_1 + a_2 \rangle - \langle a_1, a_1 + a_2 \rangle - \langle a_1 + a_2, a_2 \rangle = 0$. Multiplying this equation by $\langle a_3, \dots, a_n \rangle$, and noting that $\langle a_1 + a_2, a_3, \dots, a_n \rangle = 0$, by induction, we have $\langle a_1, \dots, a_n \rangle = -\langle a_1 + a_2 \rangle \cdot \langle a_1 + a_2, a_3, \dots, a_n \rangle + \langle a_1 \rangle \cdot \langle a_1 + a_2, a_3, \dots, a_n \rangle - \langle a_2 \rangle \cdot \langle a_1 + a_2, a_3, \dots, a_n \rangle = 0$. □

Lemma 2. *Let K be a field with a discrete valuation v. Let π be a parameter for v. Then $K_n(K)$ is generated by elements of the form $\langle \pi, u_2, \dots, u_n \rangle$ and $\langle u_1, \dots, u_n \rangle$ where u_i, $1 \leq i \leq n$ are units for the valuation.*

Proof. Every element of K^* can be written as $u\pi^n$ where u is a unit for the valuation and $n \in \mathbb{Z}$. We have the switching rule $\langle a, b \rangle = -\langle b, a \rangle$ in $K_2(K)$. Further, $\langle \pi, \pi \rangle = \langle \pi, -\pi \rangle + \langle \pi, -1 \rangle = \langle \pi, -1 \rangle$. Since $\langle a_1, \dots, a_n \rangle$ is additive in each component, the lemma is immediate. □

Theorem 3. (Existence of the "tame symbol") *Let K be a field with a discrete valuation v. There exists a unique homomorphism $T_v : K_n(K) \to K_{n-1}(K_v)$, $n \geq 1$ satisfying*

$$T_v\langle \pi, u_2, \dots, u_n \rangle \;=\; \langle \overline{u}_2, \dots, \overline{u}_n \rangle,$$

where π is a parameter for v and u_i, $2 \leq i \leq n$ are units of v. Further,

$T_v\langle u_1,\dots,u_n\rangle = 0$ *if* u_i *are units of* v *for* $1 \le i \le n$.

Proof. We first prove the uniqueness of T_v. Let π be a parameter of v and $u_1, u_2, \dots, u_n$ units of v. Then πu_1 is again a parameter of v so that $T_v\langle \pi u_1, u_2, \dots, u_n\rangle = \langle \overline{u}_2, \dots, \overline{u}_n\rangle$. Since $\langle \pi u_1, u_2, \dots, u_n\rangle = \langle \pi, u_2, \dots, u_n\rangle + \langle u_1, \dots, u_n\rangle$, $T_v\langle \pi u_1, u_2, \dots, u_n\rangle = \langle \overline{u}_2, \dots, \overline{u}_n\rangle + T_v\langle u_1, \dots, u_n\rangle$ so that $T_v\langle u_1, \dots, u_n\rangle = 0$. Since $\langle \pi, u_2, \dots, u_n\rangle$ and $\langle u_1, \dots, u_n\rangle$ generate $K_n(F)$, the uniqueness of T_v follows.

To show the existence of T_v, it is enough to define a $\mathbb{Z}$–multilinear map

$$\varphi : K^* \times \cdots \times K^* \to K_{n-1}(K_v),$$

such that $\varphi(a_1, \dots, a_n) = 0$ whenever $a_i + a_{i+1} = 1$ for some i, $1 \le i \le n-1$ and $\varphi(\pi, u_2, \dots, u_n) = \langle \overline{u}_2, \dots, \overline{u}_n\rangle$, whenever π is a parameter for v and $u_2, \dots, u_n$ units of v. Let $K_*(K_v)\langle X\rangle$ denote the graded polynomial ring over $K_*(K_v)$ in the variable X; i.e., $X\xi = (-1)^m \xi X$, $\xi \in K_m(K_v)$ and $X^m \cdot X^n = X^{m+n}$. To any element

$$(\pi^{r_1} u_1, \dots, \pi^{r_n} u_n) \in K^* \times \cdots \times K^*,$$

we associate the element $\prod_{1\le i\le n}(Xr_i + \langle \overline{u}_i\rangle) \in K_*(K_v)\langle X\rangle$. Let

$$\prod_{1\le i\le n}(Xr_i + \langle \overline{u}_i\rangle) = X^n\varphi_0 + X^{n-1}\varphi_1 + \cdots + \varphi_n$$

where $\varphi_i \in K_i(K_v)$. Thus each φ_i is a map $K^* \times \cdots \times K^* \to K_i(K_v)$. We claim that φ_i is additive in each component. We show, for instance, that φ_i is additive in the first component. Let $\prod_{2\le i\le n}(Xr_i + \langle \overline{u}_i\rangle) = X^{n-1}\psi_0 + X^{n-2}\psi_1 + \cdots + \psi_{n-1}$, $\psi_i \in K_i(K_v)$. We have $\varphi_i(\pi^{r_1+r_1'} u_1 u_1', u_2, \dots, u_n) =$ coefficient of X^{n-i} in the polynomial $(X(r_1 + r_1') + \langle \overline{u_1 u_1'}\rangle)(X^{n-1}\psi_0 + \cdots + \psi_{n-1}) =$ $(r_1 + r_1')\psi_{i+1} + (-1)^{n-i}\langle \overline{u_1 u_1'}\rangle\psi_i = (r_1\psi_{i+1} + (-1)^{n-i}\langle \overline{u}_1\rangle\psi_i) + (r_1'\psi_{i+1} + (-1)^{n-i}\langle \overline{u}_1'\rangle\psi_i)$ $= \varphi_i(\pi^{r_1} u_1, u_2, \dots, u_n) + \varphi_i(\pi^{r_1'} u_1', u_2, \dots, u_n)$. Let

$$\prod_{1\le i\le n}(Xr_i + \langle \overline{u}_i\rangle) = X\widetilde{\varphi} + \varphi_n$$

where $\widetilde{\varphi} = X^{n-1}\varphi_0 + \cdots + \varphi_{n-1}$. We define $\varphi(\pi^{r_1} u_1, \dots, \pi^{r_n} u_n) = \widetilde{\varphi}(\langle -1\rangle) = \langle -1\rangle^{n-1} \cdot \varphi_0 + \langle -1\rangle^{n-2}\varphi_1 + \cdots + \varphi_{n-1}$. Since each φ_i is additive in each component, φ is additive in each component. We have $\varphi_i(\pi, u_2, \dots, u_n) = 0$ for $i \ne n-1$ and $\varphi_{n-1}(\pi, u_2, \dots, u_n) = \langle \overline{u}_2, \dots, \overline{u}_n\rangle$ so that $\varphi(\pi, u_2, \dots, u_n) = \langle \overline{u}_2, \dots, u_n\rangle$. It remains to show that $\varphi(\pi^{r_1} u_1, \dots, \pi^{r_n} u_n) = 0$ whenever $\pi^{r_i} u_i + \pi^{r_i+1} u_{i+1} = 1$ for some i, $1 \le i \le n-1$. We check this when $\pi^{r_1} u_1 + \pi^{r_2} u_2 = 1$. Then $\min(r_1, r_2) \le 0$.

a) Let $r_1 = r_2 = 0$. Then $u_1 + u_2 = 1$ and

$$\prod_{1\le i\le n}(Xr_i + \langle u_i\rangle) = \langle \overline{u}_1, \overline{u}_2\rangle \cdot \prod_{3\le i\le r}(Xr_i + \langle \overline{u}_i\rangle) = 0,$$

since $\langle \overline{u}_1, \overline{u}_2\rangle = \langle \overline{u}_1, -\overline{u}_1\rangle = 0$.

b) $r_1 = 0$, $r_2 > 0$. Then $u_1 + \pi^{r_2} u_2 = 0$, $\overline{u}_1 = 1$ and

$$\prod_{1 \le i \le n} (Xr_i + \langle \overline{u}_i \rangle) = \langle \overline{1} \rangle \cdot \prod_{2 \le i \le n} (Xr_i + \langle \overline{u}_i \rangle) = 0.$$

c) $r_1 > 0$, $r_2 = 0$ similar to b)

d) $r_1 < 0$. In this case $r_2 = r_1 = r < 0$ and $u_1 + u_2 = \pi^{-r}$ so that $\overline{u}_1 + \overline{u}_2 = 0$. Thus $\prod_{1 \le i \le n}(Xr_i + \langle \overline{u}_i \rangle) = (Xr_1 + \langle \overline{u}_1 \rangle)(Xr_2 + \langle -\overline{u}_1 \rangle) \prod_{3 \le i \le n}(Xr_i + \langle \overline{u}_i \rangle) = \{X^2 r^2 + Xr(\langle -\overline{u}_1 \rangle - \langle \overline{u}_1 \rangle) + \langle \overline{u}_1, -\overline{u}_1 \rangle\} \prod_{3 \le i \le n}(Xr_i + \langle \overline{u}_i \rangle) =$
$X(Xr^2 + \langle -\overline{1} \rangle r) g(X)$ where $g(X) = \prod_{3 \le i \le n}(Xr_i + \langle \overline{u}_i \rangle)$ and $\widetilde{\varphi}(\langle -\overline{1} \rangle) = \langle (-1)^{r^2 + r} \rangle g(\langle -\overline{1} \rangle) = \langle \overline{1} \rangle \cdot g(\langle -1 \rangle) = 0$. Finally, if π' is any other parameter for v with $\pi' = \pi^{n_1} u_1$, u_1 a unit of v and $u_2, \ldots, u_n$, units of v, then $\varphi(\pi', u_2, \ldots, u_n) = \varphi(\pi, u_2, \ldots, u_n) + \varphi(u_1, u_2, \ldots, u_n) = \langle \overline{u}_2, \ldots, \overline{u}_n \rangle$.

□

Lemma 4. *Let K be a field with a discrete valuation v and π a parameter for v. The homomorphism $K^* \to K_v^*$ given by $\pi^n \cdot u \mapsto \overline{u}$, u a unit of v, induces a ring homomorphism $\psi_v : K_*(K) \to K_*(K_v)$.*

Proof. The map $\pi^n u \to \overline{u}$ clearly defines a ring homomorphism $T(K^*) \xrightarrow{\widetilde{\psi}_v} T(K_v^*)$. If $\pi^{r_1} u_1 + \pi^{r_2} u_2 = 1$, $\widetilde{\psi}_v(\pi^{r_1} u_1 \otimes \pi^{r_2} u_2) = \overline{u}_1 \otimes \overline{u}_2$ whose image in $K^*(K_v)$ is $\langle \overline{u}_1, \overline{u}_2 \rangle$ which can be verified to be zero, as in the proof of Theorem 3. Thus $\widetilde{\psi}_v$ induces a ring homomorphism $\psi_v : K_*(K) \to K_*(K_v)$.

Let $K(X)$ denote the field of rational functions in one variable over K. If, for any prime $p \in K[X]$, v_p denotes the discrete valuation of $K(X)$ corresponding to p and v_∞ the discrete valuation of $K(X)$ corresponding to $1/X$, we have the following sequence of abelian groups

$$0 \longrightarrow K_n(K) \xrightarrow{\text{ext}} K_n(K(X)) \overset{T=(T_{v_p})}{\longrightarrow} \coprod_p K_{n-1}(K[X]/(p)) \longrightarrow 0.$$

The map T is in fact into the direct sum $\coprod_p K_{n-1}(K[X]/(p))$ since for any element $f \in K(X)^*$, f is a unit for all but a finite number of v_p (**2.5.** of Ch. IV). We shall show that this is a split exact sequence. Since $\psi_{v_X} \circ \text{ext} = \text{identity}$, we see that ext is a direct injection. Thus the sequence is split exact, provided it is exact. For $\lambda \in K^*$, $v_p(\lambda) = 0$ for every prime p of $K[X]$ so that $T_{v_p}\langle \lambda_1, \ldots, \lambda_n \rangle = 0$ for $\lambda_i \in K^*$, $1 \le i \le n$. Thus $T \circ \text{ext} = 0$ showing that the above is a complex. We have an induced homomorphism

$$\widetilde{T} : K_n(K(X))/\text{ext } K_n(K) \to \coprod_p K_{n-1}(K[X]/(p))$$

We shall show that $\widetilde{T}$ is an isomorphism, thereby showing the exactness of the sequence. In what follows, we shall identify $K_n(K)$ as a subgroup of $K_n(K(X))$ through ext.

Let G_d be the subgroup of $K_n(K(X))$ generated by all elements of the form $\langle f_1, \ldots, f_n\rangle$, $f_i \in K[X]$, degree $f_i \leq d$. Then $\{G_d\}_{d\in\mathbb{Z}^+}$ is a filtration of $K_n(K(X))$; i.e. $G_0 \subset G_1 \subset \cdots \subset G_{i+1} \subset \ldots$ and $\cup_i G_i = K_n(K(X))$. Further $G_0 = K_n(F)$. $\square$

Lemma 5. *For all $d \geq 0$, G_d is generated by $\langle f_1, \ldots, f_n\rangle$, with $d \geq \deg f_1 > \deg f_2 > \cdots > \deg f_m = 0 = \deg f_{m+1} \ldots$ for some m, $1 \leq m \leq n$ and f_i monic irreducible for $1 \leq i \leq m-1$.*

Proof. Using the additivity of $\langle \ldots \rangle$ in each component and the anticommutativity of K_*, we see that every element of G_d is a linear combination of elements of the form $\langle f_1, \ldots, f_n\rangle$ where $d \geq \deg f_1 \geq \cdots \geq \deg f_n$; where f_i are monic irreducible or constants. The lemma now follows from the following $\square$

Lemma 6. *Let $g_1, g_2 \in K[X]$ with $\deg g_1 = \deg g_2 = s$. Then $\langle g_1, g_2\rangle$ is a sum of symbols $\langle f, g\rangle$ with $\deg f$, $\deg g \leq s$ and at the most one of f and g has degree s.*

Proof. If $g_2 = \lambda g_1$, with $\lambda \in K^*$, then $\langle g_1, g_2\rangle = \langle g_1, -\lambda\rangle$. If $g_2 \neq \lambda g_1$ for any $\lambda \in K^*$, replacing g_1 and g_2 by scalar multiples, we may assume g_1 and g_2 are monic and $g_1 - g_2 = g \neq 0$. Then $\deg g < s$ and $g_1/g - g_2/g = 1$. Thus $\langle g_1/g, -g_2/g\rangle = 0$; i.e. $\langle g_1, g_2\rangle = \langle g, g_2\rangle + \langle g_1, -g\rangle - \langle g, -g\rangle$ with $\deg g < s$. $\square$

If p is any irreducible polynomial of degree d, any polynomial of degree $< d$ is coprime with p so that the map $T_{v_p} : G_d \to K_{n-1}(K[X]/(p))$ vanishes on G_i, $i < d$; and we have an induced homomorphism $T^i_{v_p} : G_d/G_i \to K_{n-1}(K[X]/(p))$. We denote by T_{v_p} the map $T^{d-1}_{v_p}$.

Lemma 7. *The map $G_d/G_{d-1} \xrightarrow{(T_{v_p})} \coprod_{\deg p=d} K_{n-1}(K[X]/(p))$ is an isomorphism.*

Proof. We construct an inverse to (T_{v_p}) as follows: For any monic irreducible $p \in K[X]$, we define a map $(K[X]/(p))^* \times \cdots \times (K[X]/(p))^* \to G_d/G_{d-1}$ ($n-1$ copies of $(K[X]/(p))^*$) by $\langle \overline{h}_1, \ldots, \overline{h}_{n-1}\rangle \mapsto \langle p, h_1, \ldots, h_{n-1}\rangle \bmod G_{d-1}$ where $h_i \in K[X]$ are the unique polynomials of degree $< d$ whose classes modulo p are $\overline{h}_i$, $1 \leq i \leq n-1$. If $\overline{h}_i + \overline{h}_{i+1} = 1$, then $h_i + h_{i+1} = 1$ since $\deg h_i < d$ so that $\langle p, h_1, \ldots, h_{n-1}\rangle = 0$. Let $h_i h_i' = \lambda p + h$ with $\deg h < d$, then $\deg \lambda < d$ and $\langle p, h_1, \ldots, h, \ldots, h_{n-1}\rangle = \langle p, h_1, \ldots, h_i, \ldots, h_{n-1}\rangle + \langle p, \ldots h_i', \ldots, h_{n-1}\rangle + \langle p, h_1, \ldots, 1 - \frac{\lambda p}{h_i h_i'}, \ldots, h_{n-1}\rangle$.
Since $1 = \lambda p/h_i h_i' + h/h_i h_i'$, we have

$$\begin{aligned} 0 &= \langle \lambda p/h_i h_i', h_i, \ldots, 1 - \lambda p/h_i h_i', \ldots, h_{n-1}\rangle \\ &= \langle p, h_i, \ldots, 1 - \tfrac{\lambda p}{h_i h_i'}, \ldots, h_{n-1}\rangle + \langle \lambda/h_i h_i', h_1, \ldots, h/h_i h_i', \ldots, h_{n-1}\rangle \\ &\equiv \langle p, h_1, \ldots, 1 - \tfrac{\lambda p}{h_i h_i'}, \ldots, h_{n-1}\rangle \bmod G_{d-1}. \end{aligned}$$

Thus

$$\langle p, h_1, \ldots, h, \ldots, h_{n-1}\rangle$$

$$\equiv \langle p, h_1, \ldots, h_i, \ldots, h_{n-1}\rangle + \langle p, h_1, \ldots, \ , \ldots, h_i', \ldots, h_{n-1}\rangle \text{ modulo } G_{d-1}.$$

Thus φ_p induces a homomorphism $\varphi_p : K_{n-1}(K[X]/(p) \to G_d/G_{d-1}$. Obviously φ_p satisfies the condition $T_{v_p} \circ \varphi_p =$ identity and $T_{v_p'} \circ \varphi_p = 0$ if $p \neq p'$. Thus the map $\varphi = (\varphi_p) : \coprod_{\deg p=d} K_{n-1}(F[X]/(p)) \to G_d/G_{d-1}$ is injective. To prove the lemma, it is enough to check that φ is surjective. Let $\langle f_1, \ldots, f_n\rangle$ be an element of G_d such that f_i is a monic irreducible polynomial of degree d and deg $f_i < d$, for $i \geq 2$. Then $\varphi_{v_{f_1}}\langle \overline{f}_2, \ldots, \overline{f}_n\rangle = \langle f_1, \ldots, f_n\rangle$ modulo G_{d-1}. Since by Lemma 5, such $\langle f_1, \ldots, f_n\rangle$ generate G_d, Lemma 7 follows. □

We claim the map

$$T^0_{v_p} : G_d/G_0 \coprod_{\deg p \leq d} K_{n+1}(K[X]/(p))$$

is an isomorphism. We have the following commutative diagram

$$\begin{array}{ccc} G_i/G_{i-1} & \xrightarrow[\sim]{(T_{v_p})} & \coprod_{\deg p=d} K_{n-1}(K[X]/(p)) \\ \downarrow & & \downarrow i \\ G_d/G_0 & \xrightarrow{T^0_{v_p}} & \coprod_{\deg p \leq d} K_{n-1}(K[X]/(p)) \end{array}$$

For $\overline{x} \in G_d/G_0$, there exists $x \in G_i$, a representative of $\overline{x}$ with $x \neq G_{i+1}$ so that $T^0_{v_p}(\overline{x}) = i \circ (T_{v_p})(\overline{x}) \neq 0$. Further any element of $K_{n-1}(K[X]/(p))$ with deg $p = 1$ has a preimage $\overline{x} \in G_i/G_{i-1}$ and is hence in the image of $T^0_{v_p}$. Thus $T^0_{v_p}$ is an isomorphism. Taking the direct limit over d, we get: $\widetilde{T} : k_n(K[X])/K_n(K) \xrightarrow{\sim} K_{n-1}(K[X]/(p))$ is an isomorphism. We thus have proved the following

Theorem 8. *The sequence*

$$0 \longrightarrow K_n(K) \xrightarrow{ext} K_n(K(X)) \xrightarrow{T=(T_{v_p})} \coprod_p K_{n-1}([X]/(p)) \longrightarrow 0$$

is a split exact sequence.

Corollary 9. *Let $q \in K[X]$ be a monic irreducible polynomial of degree d. Then $K_{n-1}([X]/(q))$ $(n \geq 2)$ is generated by elements of the form $\langle \overline{g}_1, \ldots \overline{g}_{n-1}\rangle$, where $d >$ deg $g_1 > \cdots >$ deg $g_m = 0 =$ deg$_{m+1} = \cdots =$ deg g_n, for some $0 \leq m \leq n$ and g_i monic irreducible in $K[X]$ for $1 \leq i \leq m-1$.*

Proof. The map $T^0_{v_p} : G_d/G_0 \to \coprod_{\deg p \leq d} K_{n-1}(K[X]/(p))$ is an isomorphism so that we have a surjective homomorphism $G_d \to K_{n-1}(K[X]/(q))$. By Lemma 5, we have a set of generators of G_d of the form $\langle f_1, \ldots, f_n\rangle$ where $d \geq$ deg $f_1 >$ deg $f_2 >$

$\cdots > \deg f_m = 0 = \cdots = \deg f_n$, with f_i monic irreducible for $1 \leq i \leq m-1$. We note that if $f_1 \neq q, T^0_{v_p}\overline{\langle f_1, \ldots, f_n\rangle} = 0$. If $f_1 = q$, $T^0_{v_p}\overline{\langle f_1, \ldots, f_n\rangle} = \langle \overline{f}_2, \ldots, \overline{f}_n\rangle$. This proves the corollary. □

We denote by $\mathfrak{P}$ the set of all discrete valuations of $K(X)$ over K. Let $v \in \mathfrak{P}$. The inclusions $K \hookrightarrow K(X)$ and $K \hookrightarrow K(X)_v$ induce ring homomorphisms ext : $K_*(K) \to K_*(K(X))$ and $K_*(K) \to K_*(K(X)_v)$. We regard $K_*(K(X))$ and $K_*(K(X)_v)$ as right $K_*(K)$–modules through these homomorphisms. The tame symbol $T_v : K_*(K(X)) \to K_*(K(X)_v)$ is $K_*(K)$–linear. In fact, if $v = v_p$, for units $u_i \in K(X)^*$ for v_p, $2 \leq i \leq n$ and $a_i \in K^*$, $1 \leq i \leq n$,

$$\begin{aligned} T_{v_p}(\langle p, u_2, \ldots, u_n\rangle \cdot \langle a_1, \ldots, a_m\rangle) &= T_{v_p}\langle p, u_2, \ldots, u_n, a_1, \ldots, a_m\rangle \\ &= \langle \overline{u}_2, \ldots, \overline{u}_n, a_1, \ldots, a_m\rangle \\ &= T_{v_p}\langle p, u_2, \ldots, u_n\rangle \cdot \langle a_1, \ldots, a_m\rangle. \end{aligned}$$

A similar argument holds for $v = v_\infty$. For $v = v_\infty$, we have $K \simeq K[1/X]/(1/X) \simeq K(X)_{v_\infty}$ so that ext : $K_*(K) \to K_*(K(X)_{v_\infty})$ is an isomorphism. In view of Theorem 8, we have the following diagram

$$\begin{array}{ccc} K_{n+1}(K(X))/\mathrm{ext}\, K_{n+1}(K) & \xrightarrow{\overline{T}} & \coprod_{v\in\mathfrak{P},\, v\neq v_\infty} K_n(K(X)_v) \\ \downarrow{\scriptstyle T_{V_\infty}} & & \downarrow{\scriptstyle N=(N_v)} \\ K_n(K(X)_{v_\infty}) & \xrightarrow{-\mathrm{ext}^{-1}} & K_n(X) \end{array}$$

where for each $n \geq 0$, $v \neq v_\infty$, the group homomorphism $N_v : K_n(K(X)_v) \to K_n(K)$ is defined by $N = (N_v) = -(\mathrm{ext})^{-1} \circ T_{v_\infty} \circ \overline{T}^{-1}$. Thus N_v is a uniquely determined homomorphism for every $v \neq v_\infty$. We define $N_{v_\infty} : K_n(K(X)_{v_\infty}) \to K_n(K)$ to be $(\mathrm{ext})^{-1}$. We thus have, for each valuation $v \in \mathfrak{P}$, a homomorphism $N_v : K_*(K(X)_v) \to K_*(K)$ of graded groups.

Proposition 10. *1) (Projection formula) For any valuation $v \in \mathfrak{P}$, the map $N_v : K_*(K(X)_v) \to K_*(K)$ is $K_*(K)$–linear; i.e.$N_v(\xi\eta) = N_v(\xi)\eta$ for $\eta \in K_*(K)$ $\xi \in K_*(K(X)_v)$.*

2) For $\eta \in K_n(K(X))$ $(n \geq 1)$, $\sum_{v\in\mathfrak{P}} N_v T_v(\eta) = 0$.

3) For each $v \in \mathfrak{P}$, let $f_v : K_n(K(X)_v) \to K_n(K)$ be homomorphisms such that f_{v_∞} = identity (identifying $K(X)_{v_\infty}$ with K) and $\sum_{v\in\mathfrak{P}} f_v \circ T_v(\beta) = 0$ for every $\beta \in K_{n+1}(K(X))$. Then $f_v = N_v$, for all v.

Proof. 1) follows from the fact that $\widetilde{T}$, T_{v_∞} and ext : $K_*(K) \to K_*(K(X)_{v_\infty})$ are $K_*(K)$–linear. Since $N \circ \widetilde{T}(\eta) = -N_{v_\infty} \circ T_{v_\infty}(\eta)$, $\forall\, \eta \in K_{n+1}(K(X))$,
$\sum_{v\in\mathfrak{P}} N_v T_v(\eta) = 0$ and 2) follows. 3) is a consequence of the fact that $f = (f_v)_{v\neq v_\infty}$ has the property $f \circ \widetilde{T} = -N_{v_\infty} \circ T_{v_\infty} \circ \widetilde{T}^{-1} = N$. □

Theorem 11. *The sequence*

$$0 \to K_n(K) \xrightarrow{\text{ext}} K_n(K(X)) \xrightarrow{T} \coprod_{v\in\mathfrak{P}} K_{n-1}(K(X)_v) \xrightarrow{N} K_{n-1}(K) \to 0$$

is split exact, for all $n \geq 1$.

Proof. We have already seen that ext is a direct injection and the sequence is exact at $K_n(K(X))$, using Theorem 8. By Proposition 10, it follows that $N \circ T = 0$. Let $x \in \coprod_{v\in\mathfrak{P}} K_{n-1}(K(X)_v)$ with $N(x) = 0$. Since

$$(T_v)_{v\neq v_\infty} : K_n(K(X)) \to \coprod_{v\neq v_\infty} K_{n-1}(K(X)_v)$$

is surjective, we may assume that $x \in K_{n-1}(K(X)_{v_\infty})$. Then $N_{v_\infty}(x) = 0$ implies that $x = 0$ since $N_{v_\infty} = \text{ext}^{-1}$ is an isomorphism. Further N_{v_∞} is an isomorphism implies that N is surjective, and the exactness of the sequence is proved. That the sequence is split follows from the fact that the sequence of Theorem 8 is split exact and $N_{v_\infty} : K_{n-1}(K(X)_{v_\infty}) \to K_{n-1}(K)$ is an identification. □

Proposition 12. *For any* $v \in \mathfrak{P}$, *the map* $N_v : K_0(K(X)_v) \to K_0(K) = \mathbb{Z}$ *is multiplication by* $\deg v = [K(X)_v : K]$.

Proof. The map $T_v : K_1(K(X)) = K(X)^* \to K_0(K(X)_v) = \mathbb{Z}$ is the valuation map $v : K(X)^* \to \mathbb{Z}$. We have N_{v_∞} = identity since $[K(X)_{v_\infty} : K] = 1$ and $\sum_{p\in\mathfrak{P}} \deg p \cdot v_p(f) = \deg f = -v_\infty(f) = -\deg v_\infty \cdot v_\infty(f)$ so that by 3) of Proposition 10, N_v is the multiplication by $\deg v$. □

Proposition 13. *The map* $N_v : K_1(K(X)_v) \to K_1(K)$, $v \in \mathfrak{P}$ *is the norm* $N_{K(X)_{v_\infty}/K}$.

Proof. We have $N_{K(X)_v/K}$ = identity. In view of 3) of Proposition 11, it is enough to check that for $f, g \in K[X]$, f, g monic irreducible, $\prod_{v\in\mathfrak{P}} N_{K(X)_v/K} T_v\langle f, g\rangle = 1$. If g is a constant, then $T_v\langle f, g\rangle = g^{v(f)} \in K^*$ so that $\prod_{v\in\mathfrak{P}} N_{K(X)_v/K} T_v\langle f, g\rangle = g^{\sum \deg v \cdot v(f)} = g^{\deg(\text{div}(f))=1}$ (**3.1.** of Ch. IV). If f, g are both non constant and $f = g$, $\langle f, f\rangle = \langle f, -1\rangle$ so that $\prod_{v\in\mathfrak{P}} N_{K(X)_v/K} T_v\langle f, f\rangle = 1$. Let f, g be monic irreducible with $f \neq g$. Then $T_v\langle f, g\rangle = 1$ for $v \neq v_f$, v_g or v_∞. We have $T_{v_f}\langle f, g\rangle = \overline{g} \in [K[X]/(f))^*$ and $T_{v_\infty}\langle f, g\rangle = (-1)^{\deg f \cdot \deg g} \in K^*$. In fact, if

$$f = X^m + a_{m-1}X^{m-1} + \cdots + a_0 = X^m \cdot u,$$

$u = (1 + \frac{a_{m-1}}{X} + \cdots + \frac{a_0}{X^m})$, $v_\infty(f) = m$ with $\overline{u} = 1$. Similarly, if $\deg g = m'$ and $g = X^{m'} \cdot u'$, then, $v_\infty(g) = m'$ with $\overline{u'} = 1$. We have

$$T_{v_\infty}\langle f, g\rangle = T_{v_\infty}\langle X^m, X^{m'}\rangle \cdot T_{v_\infty}\langle X^m, u'\rangle T_{v_\infty}\langle u, X^{m'}\rangle \cdot T_v\langle u, u'\rangle = (-1)^{mm'} \in K^*.$$

Let $K[X]/(f) = K(\alpha),\ K[X]/(g) = K(\beta),\ \alpha, \beta$ denoting the images of X. Let $f(X) = \prod_{1\le i\le m}(X-\alpha_i),\ \alpha_1 = \alpha,\ g(X) = \prod_{1\le j\le m'}(x-\beta_j),\ \beta_1 = \beta, \alpha_i, \beta_j \in \overline{K}$, the algebraic closure of K. Since f and g are distinct irreducible polynomials. f and g have no common roots. We have

$$\begin{aligned} N_{K(\alpha)/K}(\overline{g}) = N_{K(\alpha)/K}\prod_j(\alpha-\beta_j) &= \prod_{i,j}(\alpha_i-\beta_j). \\ N_{K(\beta)/K}(\overline{f}) = N_{K(\beta)/K}\prod_i(\beta-\alpha_j) &= \prod_{i,j}(\beta_j-\alpha_i) \ = \\ &= (-1)^{\deg f\cdot\deg g}\prod_{i,j}(\alpha_i-\beta_j). \end{aligned}$$

We therefore have $\prod_{v\in\mathfrak{P}} N_{N(X)_v/K}T_v\langle f,g\rangle = 1$. □

Corollary 14. *(Bass–Tate) The sequence*

$$0 \longrightarrow K_n(K) \xrightarrow{\text{ext}} K_2(K(X)) \xrightarrow{T=(T_v)} \coprod_{v\in\mathfrak{P}} K_1(K(X)_v) \xrightarrow{N} K_1(K) \longrightarrow 0$$

is split exact, where $N = (N_v),\ N_v : K(X)_v^* \to K^*$ being the norm.

Appendix III: Transfer on K–groups

§ 1. Statement of the theorem

The aim of this Appendix is to prove the following theorem.

Theorem 1.1. *Let K/L be a finite extension of fields. Then there exists a homomorphism $N_{L/K} : K_*(K)$ of degree 0, called the norm or transfer homomorphism, satisfying the following conditions.*

1) *(Projection formula) For $x \in K_*(K)$, $y \in K_*(L)$,*

$$N_{L/K}(\text{ext}\, x \cdot y) = x \cdot N_{L/K} y\,,$$

where ext *is the extension homomorphism $K_*(K) \to K_*(L)$, i.e., $N_{L/K}$ is $K_*(K)$–linear if we regard $K_*(L)$ as $K_*(K)$–module through extension.*

2) *(Functoriality) $N_{K/K} =$ Identity and for finite extensions $E \supset L \supset K$, $N_{L/K} \circ N_{E/L} = N_{E/K}$.*

3) *(Reciprocity) $\sum_v N_{K(X)_v/K} \circ T_v(x) = 0$ for all $x \in K_*(K(X))$, v running over all the discrete valuations v of $K(X)$ trivial on K.*

By the uniqueness of the N_v proved in (App. II, **(10)**), since $N_{K(X)_{v_\infty}/K} = N_{K/K} =$ identity, it follows from 3) that $N_{K(X)_v/K} = N_v$ and this suggests, in fact, a method of defining $N_{L/K}$ in general. Let $L = K(\alpha)$ be a finite simple extension of K and π the minimal (monic) polynomial of α over K. We then have an isomorphism $\varphi_\alpha : K(\alpha) \xrightarrow{\sim} K[X]/(\pi) = K(X)_{v_\pi}$, sending α to the class of X modulo π. We define $N_{\alpha/K} = N_{v_\pi} \circ K_*(\varphi_\alpha) : K_*(K(\alpha)) \to K_*(K(X)_{v_\pi}) \to K_*(K)$. Since N_{v_π} and $K_*(\varphi_\alpha)$ are $K_*(K)$–linear, $N_{\alpha/K}$ is $K_*(K)$–linear; i.e., $N_{\alpha/K}$ satisfies the projection formula.

Let L/K be a finite extension and $(\alpha_1, \ldots, \alpha_n)$ a set of generators of L over K. We define $N_{(\alpha_1,\ldots,\alpha_n)/K}$ to be

$$K_*(L) \overset{N_{\alpha_n/K_{n-1}}}{\longrightarrow} K_*(K_{n-1}) \longrightarrow \ldots \overset{N_{\alpha_2/K_1}}{\longrightarrow} K_*(K_1) \overset{N_{\alpha_1/K}}{\longrightarrow} K_*(K)$$

where K_i denotes $K(\alpha_1, \ldots, \alpha_i)$, $1 \le i \le n-1$. Obviously $N_{(\alpha_1,\ldots,\alpha_n)/K}$ satisfies the projection formula, since each $N_{\alpha_i/K_{i-1}}$ is $K_*(K)$–linear. For $\alpha \in K$, clearly $N_{\alpha/K} =$ identity, since $N_{v_{(X-\alpha)}} =$ identity. The crucial point in order to define a functorial transfer is the following

Proposition 1.2. *The map $N_{(\alpha_1,\ldots,\alpha_n)/K}$ is independent of the chosen ordered set $(\alpha_1, \ldots, \alpha_n)$ of generators of L over K.*

Granting Proposition **1.2.**, we may write $N_{L/K} = N_{(\alpha_1,\ldots,\alpha_n)/K}$. Then, by our earlier remark, $N_{K/K}$ = identity and **1.2.** implies that $N_{E/K} = N_{L/K} \circ N_{E/L}$ for $E \supset L \supset K$, E, L finite extensions of K. Further, taking for α the image of X in $K[X]/(\pi) = K(X)_{v_\pi}$, we have $N_{K(X)_v/K} = N_{\alpha/K} = N_v$, so that reciprocity follows from (App. II, (10)). Thus Theorem **1.1.** would be proved, provided, we prove **1.2.**. In Sections 3 and 4, we give a proof, due to Kato of **1.2.** (K. Kato, 'A generalization of local class field theory using K–groups', Ch. II, § 1.7, J. Fac. Sci, Univ. Tokyo, 1A 27 1980). Section 2 contains some preliminary results, taken from Bass–Tate, "The Milnor ring of a global field", Springer Notes 342.

§ 2. Some preliminary results

Lemma 2.1. *For any discrete valuation v of $K(X)$ over K, the composite $K_*(K) \xrightarrow{ext} K_*(K(X)_v) \xrightarrow{N_v} K_*(K)$ is multiplication by* $\deg v = [K(X)_v : K]$.

Proof. For $x \in K_*(K)$, $N_v(\text{ext } x) = N_v(\text{ext } x \cdot 1) = x \cdot N_v(1) = x \cdot \deg v$ by (App. II, **(12)**). □

Corollary 2.2. *Let L/K be an algebraic extension. Then, the kernel of the map* $\text{ext}_{L/K} : K_*(L)$ *is torsion. If L/K is finite,* $\ker \text{ext}_{L/K}$ *is $[L : K]$–torsion. If L/K is an algebraic extension such that every finite subextension L_0/K has degree coprime to a prime p, then* $\text{ext}_{L/K}$ *is injective on the p–torsion of $K_*(K)$.*

Proof. For a simple extension $K(\alpha)/K$, $N_{\alpha/K} \circ \text{ext}_{K(\alpha)/K}$ is multiplication by $[K(\alpha) : K]$, by **2.1.**. For any finite extension $L = K(\alpha_1, \ldots, \alpha_n)$, we have $N_{(\alpha_1,\ldots,\alpha_n)/K} \circ \text{ext}_{L/K}$ is multiplication by $[L : K]$ so that $\ker \text{ext}_{L/K}$ is $[L : K]$–torsion. If L/K is any algebraic extension, and $\eta \in \ker \text{ext}_{L/K}$, $\eta \in \ker \text{ext}_{\widetilde{L}/K}$ for some finite extension $\widetilde{L}$ of K, contained in L so that η is torsion. If each finite subextension $\widetilde{L}/K$ of L/K has degree coprime to p, $\eta \in \ker \text{ext}_{\widetilde{L}/K}$ has m torsion where $(m, p) = 1$ so that $\text{ext}_{L/K}$ is injective on the p–torsion of $K_*(K)$. □

Lemma 2.3. *Let K be a discrete valuated field with valuation v. Let L/K be an algebraic extension and w an extension of v to L with $e = e(w/v)$ the ramification index. Then the diagram*

$$\begin{array}{ccc} K_n(K) & \xrightarrow{\text{ext}} & K_n(L) \\ {\scriptstyle T_v}\downarrow & & \downarrow{\scriptstyle T_w} \\ K_{n-1}(K_v) & \xrightarrow{e\cdot\text{ext}} & K_{n-1}(L_w) \end{array}$$

is commutative.

Proof. In view of **(2)** of Appendix II, $K_n(K)$ is generated by $\langle \pi, u_2, \ldots, u_n \rangle$ and $\langle u_1, \ldots, u_n \rangle$, where $v(\pi) = 1$ and $v(u_1) = 0$. Let π_w be a parameter of w and

$\pi = u_0 \cdot \pi_w^e$ with $w(u_0) = 0$. Then, $T_w \circ \text{ext}\,\langle \pi, u_2, \ldots, u_n\rangle = T_w\langle \pi, u_2, \ldots, u_n\rangle_L = e\langle \overline{u}_2, \ldots, \overline{u}_n\rangle = e \cdot \text{ext} \circ T_v\langle \pi, u_2, \ldots, u_n\rangle$ and, $T_w \circ \text{ext}\,\langle u_1, \ldots, u_n\rangle = 0 = e \cdot \text{ext} \circ T_v\langle u_1, \ldots, u_n\rangle$. □

Lemma 2.4. *Let K be a field such that every finite extension of K has degree equal to a power of a fixed prime p. Let L/K be an extension of degree p. Then $K_n(L)$ is generated by elements of the form $\langle \lambda, a_2, \ldots, a_n\rangle$, $\lambda \in L^*,\ a_1 \in K^*,\ 2 \leq i \leq n,\ n \geq 1$.*

Proof. We have $L = K(\alpha) = K[X]/(\pi)$ where π is the monic irreducible polynomial of α over K. By (App. II, **(9)**), $K_n(K[X]/(\pi))$ is generated by elements of the form $\langle \overline{g}_1, \ldots, \overline{g}_n\rangle$ where $g_i \in K[X],\ p > \deg g_1 > \cdots > \deg g_m = 0 = \deg g_{m+1} = \cdots = \deg g_n$ and g_i are monic irreducible over K for $1 \leq i \leq m-1$. By hypothesis, since $\deg g_1 < p,\ g_1$ is either linear or constant and $g_i,\ i \geq 2$ are constants in K^*. Thus $K_n(K(\alpha))$ is generated by $\langle \alpha - a_1, a_2, \ldots, a_n\rangle,\ a_i \in K^*$. □

Lemma 2.5. *Let K be a field and p a prime. There exists an algebraic extension ${}^pK$ of K such that every finite extension of ${}^pK$ has degree equal to a power of p and every finite subextension K'/K, contained in ${}^pK$ has degree coprime to p.*

Proof. If char $K = p$, let ${}^pK$ be the fixed field of a p–Sylow subgroup of the profinite group $G(K_s/K)$ and if char $K \neq p$, let ${}^pK$ be the fixed field of a p–Sylow subgroup of the profinite group $G(\overline{K}/K)$, where K_s and $\overline{K}$ denote, respectively, the separable and algebraic closures of K. The field ${}^pK$ is the required extension of K. □

Let L/K be an algebraic extension. Let $\mathfrak{P}(L)$ and $\mathfrak{P}(K)$ denote the set of valuations of $L(X)$ and $K(X)$, trivial on L and K, respectively. We denote by w a typical element of $\mathfrak{P}(L)$ and by v a typical element of $\mathfrak{P}(K)$: Let π be an irreducible polynomial in $K[X]$ and let $\pi = \prod_i \pi_i^{e_i}$ be a factorization of π over L, π_i irreducible in $L[X]$. Let v_π, w_{π_i} be elements of $\mathfrak{P}(K)$ and $\mathfrak{P}(L)$, respectively, corresponding to π and π_i. Then w_{π_i} are precisely the valuations of $L(X)$ extending v_π with ramifications e_i and w_∞ is the unique extension of v_∞, with ramification 1. We have embeddings $K(X)_{v_\pi} = K[X]/(\pi) \hookrightarrow L[X]/(\pi_1) = L(X)_{w_{\pi_i}}$ for each i.

Proposition 2.6. *The following diagram is commutative*

$$\begin{array}{ccccccc}
0 \to K_*(L) & \xrightarrow{\text{ext}} & K_*(L(X)) & \xrightarrow{T=(T_w)} & \coprod_v \coprod_{w/v} L(X)_w & \xrightarrow{N=(N_w)} & K_*(L) \to 0 \\
\uparrow{\scriptstyle \text{ext}} & & \uparrow{\scriptstyle \text{ext}} & & \uparrow{\scriptstyle (e(w/v)\text{ext})} & & \uparrow{\scriptstyle \text{ext}} \\
0 \to K_*(K) & \xrightarrow{\text{ext}} & K_*(K(X)) & \xrightarrow{T=(T_w)} & \coprod_v K(X)_v & \xrightarrow{N=(N_v)} & K_*(K) \to 0
\end{array}$$

where in the third vertical arrow from the left $\text{ext} = \text{ext}_{L(X)_w/K(X)_v}$.

Proof. The commutativity of the square on the left follows from the functoriality of K_*. The commutativity of the middle square is a consequence of **2.3.**. Since the top and the bottom rows are exact (Corollary **(14)** of App. II), there exists a unique homomorphism $h : K_*(K) \to K_*(L)$ which makes the square on the right hand side commutative. In particular, the diagram

$$\begin{array}{ccc}
K_*(L) = K_*(L(X)_{w_\infty}) & \xrightarrow{N_{w_\infty}} & K_*(L) \\
\uparrow{\scriptstyle \text{ext}} & & \uparrow{\scriptstyle h} \\
K_*(K) = K_*(K(X)_{v_\infty}) & \xrightarrow{N_{v_\infty}} & K_*(K)
\end{array}$$

is commutative. Since $N_{w_\infty} = \text{identity}$, $N_{v_\infty} = \text{identity}$, $h = \text{ext}_{L/K}$ and the proposition is proved. □

Corollary 2.7. *Let K'/K be an algebraic extension and π an irreducible (monic) polynomial over K which splits as $\prod_i \pi_i^{e_i}$ over K, π_i irreducible over K'. Let $L = K[X]/(\pi)$, $L_i = K'[X]/(\pi_i)$, α and α_i denoting the images of X in L and L_i, respectively. If $L \hookrightarrow L_i$ is the inclusion induced by $K \to K'$, $X \mapsto X$, the following diagram is commutative.*

$$\begin{array}{ccc}
K_*(L) & \xrightarrow{(e_i \text{ext}_{L_i/L})} & \coprod_i K_*(L_i) \\
\downarrow{\scriptstyle N_{\alpha/K}} & & \downarrow{\scriptstyle (N_{\alpha/K'})} \\
K_*(K) & \longrightarrow & K_*(K')
\end{array}$$

Proof. The corollary is a consequence of the commutativity of the right hand square of **2.6.** if we identify L with $K(X)_{v_\pi}$, L_i with $K'(X)_{w_{\pi_i}}$ and $N_{\alpha/K}$ and $N_{\alpha_i/K'}$ with N_{v_π} and $N_{w_{\pi_i}}$, respectively. □

Let L/K be a finite extension and K'/K any extension. Then $K' \otimes_K L$ is artinian and if $\{m_i\}$ $1 \le i \le r$ are the distinct maximal ideals of $K' \otimes_K L$, $(K' \otimes_K L)/\cap \mathfrak{m}_i \simeq \prod_{1 \le i \le r} (K' \otimes_K L)/\mathfrak{m}_i = \prod_{1 \le i \le r} L_i$ where $L_i = (K' \otimes_K L)/\mathfrak{m}_i$.
If e_i is the index of nilpotence of $\mathfrak{m}_i$ in $(K' \otimes_K L)\mathfrak{m}_i$, we call e_i the **ramification of $K' \otimes_K L$ in L_i**. With this notation, the above corollary may be reformulated as follows.

Corollary '2.7. *Let K'/K be an algebraic extension and L/K a finite simple extension. Let $(K'\otimes_K L)/\operatorname{rad} \cong \prod\ L_i$ and e_i the ramification of $K'\otimes_K L$ in L_i. If $L = K(\alpha)$ and $\alpha_i \in L_i$ are the images of α under the canonical injection $L \hookrightarrow K'\otimes_K L \to (K'\otimes_K L)/\operatorname{rad} \xrightarrow{\sim} \prod_i\ L_i \xrightarrow{p_i} L_i$, the following diagram is commutative:*

$$\begin{array}{ccc} K_*(L) & \xrightarrow{(e_i \mathrm{ext}_{L_i/L})} & \prod_i K_*(L_i) \\ {\scriptstyle N_{\alpha/K}}\downarrow & & \downarrow{\scriptstyle (N_{\alpha/K'})} \\ K_*(K) & \xrightarrow{\mathrm{ext}_{K'/K}} & K_*(K') \end{array}$$

Corollary 2.8. *Let $L = L(\alpha_1, \ldots, \alpha_n)$ be a finite extension of K and K'/K any algebraic extension. Let $(K'\otimes_K L)/\operatorname{rad} \xrightarrow{\sim} \prod_{1\le i\le r}\ L_i$ and let $(\alpha_1^i, \ldots, \alpha_n^i)$ denote the images of $(\alpha_1, \ldots, \alpha_n)$ under the embedding $L \to L_i$ and e_i the ramifications of $K'\otimes_K L$ in L_i. Then the following diagram is commutative*

$$\begin{array}{ccc} K_*(L) & \xrightarrow{(e_i \mathrm{ext}_{L_i/L})} & \prod_i K_*(L_i) \\ \downarrow{\scriptstyle N_{(\alpha-1,\ldots,\alpha_n)/K}} & & \downarrow{\scriptstyle \prod(N_{\alpha_1^i,\ldots,\alpha_n^i)/K'}} \\ K_*(K) & \xrightarrow{\mathrm{ext}_{K'/K}} & K_*(K') \end{array}$$

Proof. The corollary follows from Corollary **'2.7.** by an easy induction on n. □

§ 3. A crucial lemma

Lemma 3.1. *Let E/K be a normal extension of degree p. Then* **1.2.** *is true for the extension E/K.*

Proof. ,We prove the lemma in two steps.

Step 1. The lemma is true if $K = {}^pK$ for some prime p and ${}^pK$ is as in **2.5.**.

Step 2. It is enough to prove the lemma when $K = {}^pK$ for some prime p.

Proof of Step 1. In view of **2.4.**, $K_n(E)$ is generated by $\langle x, y_1, \ldots, y_{n-1}\rangle$ where $x \in E'$, $y_i \in K^*$, $1 \le i \le n-1$. It is enough to verify $N_{a/K}\langle x, y_1, \ldots, y_{n-1}\rangle = N_{b/K}\langle x, y_1, \ldots, y_{n-1}\rangle$ for two generators a, b of E over K. By the projection formula, we have $N_{a/K}\langle x, y_1, \ldots, y_{n-1}\rangle = \langle N_{E/K}x, y_1, \ldots, y_{n-1}\rangle =$
$N_{b/K}\langle x, y_1, \ldots, y_{n-1}\rangle$. □

Proof of Step 2. Since $[E : K] = p$, ${}^pK$ and E are linearly disjoint over K, so that

$E \otimes_K {}^pK \simeq E^pK$, the composite of E and ${}^pK$. Let a, b be two generators of E over K. By Corollary **'2.7.**, the following diagrams are commutative:

$$\begin{array}{ccc} K_*(E) & \xrightarrow{\text{ext}} & K_*(E^pK) \\ {\scriptstyle N_{a/K}}\downarrow\downarrow{\scriptstyle N_{b/K}} & & {\scriptstyle N_{a/{}^pK}}\downarrow\downarrow{\scriptstyle N_{b/{}^pK}} \\ K_*(K) & \xrightarrow{\text{ext}} & K_*({}^pK) \end{array}$$

Since the lemma is true for ${}^pK$, we have $N_{a/{}^pK} = N_{b/{}^pK}$. Thus $\text{ext} \circ (N_{a/k} - N_{b/K}) = 0$. By **2.2.**, for $x \in K_*(E)$, there exists an integer m coprime with p such that $m \cdot (N_{a/K} - N_{b/K})(x) = 0$. Since E/K is normal of degree p, $(E \otimes_K E)/\operatorname{rad} \xrightarrow{\sim} \prod_i E_i$ with $E_i = E$ and e_i the ramification of $E \otimes E$ in E_i. (In fact, if π is the irreducible polynomial of any generator of E over K, π splits completely over E.) If a_i, b_i denote the images of a, b in E_i, then the following diagrams are commutative.

$$\begin{array}{ccc} K_*(E) & \xrightarrow{e_i\text{ext}} & \prod_*(E_i) \\ {\scriptstyle N_{a/K}}\downarrow\downarrow{\scriptstyle N_{b/K}} & & (N_{a_i/E}\downarrow\downarrow N_{b_i/E}) \\ K_*(K) & \xrightarrow{\text{ext}} & K_*(E) \end{array}$$

Since $E \xrightarrow{\sim} E_i$ for each i, $N_{a_i/E} = N_{b_i/E} =$ identity so that

$$\text{ext}_{E/K}\ (N_{a/K} - N_{b/K})(x) = 0.$$

Thus by **2.2.** $p(N_{a/k} - N_{b/K})(x) = 0$. Since $(p, m) = 1$, $N_{a/K}(x) = N_{b/K}(x)$. This is true for every $x \in K_*(E)$ so that $N_{a/K} = N_{b/K}$. □

□

Definition *Let E/K be a normal extension of degree p, a prime. We denote by $N_{E/K} : K_*(E) \to K_*(K)$, the homomorphism $N_{a/K}$ for any generator a of E over K, which is independent of the choice of a.*

Lemma 3.2. *Let K be a field, complete with respect to a discrete valuation v and L a normal extension of K of degree p. Let H be the subgroup of $K_{n+1}(L)$ generated by $\langle x, y_1, \ldots, y_n \rangle$, $x \in L^*$, $y_i \in K^*$, $1 \leq i \leq n$. Then, for every $x \in H$, $T_v \circ N_{L/K}(x) = N_{L_w/K_v} \circ T_w(x)$ where w is the extension of v to L (noting that N_{L_w/K_v} makes sense since $[L_w : K_v]$ is 1 or p (App. I (2.3))).*

Proof. Since H is generated by $\langle x, y_1, \ldots, y_n \rangle$, $x \in L^*$, $y_i \in K^*$, $1 \leq i \leq n$ and since $K_n(K)$ is generated by $\langle \pi, u_2, \ldots, u_n \rangle$ and $\langle u_1, u_2, \ldots, u_n \rangle$ where $v(\pi) = 1$, $v(u_i) = 0$, using the additivity of $\langle , \ldots, \rangle$ in each component, it is enough to check that $T_v \circ N_{L/K} = N_{L_w/K_v} \circ T_w$ on elements of $K_{n+1}(L)$ of the form $\langle u_0, \pi_v, u_2, \ldots, u_n \rangle$, $\langle u_0, u_1, \ldots, u_n \rangle$, $\langle \pi_w, u_1, u_2, \ldots, u_n \rangle$, $\langle \pi_w, \pi_v, u_2, \ldots, u_n \rangle$ where u_i, $0 \leq i \leq n$ are units of v in K, and π_v, π_w *some* parameters for v and w, respectively. If $e = e(w/v) = 1$, we take some parameter π_v for v and set $\pi_w = \pi_v$. If

$e = p$, we take some parameter π_w for w. Since $\mathfrak{O}_w$ is integral over $\mathfrak{O}_v$ (App. I, **2.3.**), π_w satisfies a monic polynomial $\pi_w^p + a_1\pi_w^{p-1} + \cdots + a_p = 0$ with $a_1 \in \mathfrak{O}_v$. It is easy to verify that $a_i \in \mathfrak{p}_v$ and $a_p \in \mathfrak{p}_v - \mathfrak{p}_v^2$. We take $\pi_v = a_p$. Then $N_{L/K}\pi_w = (-1)^p\pi_v$ and $\pi_v = -\pi_w^p \cdot u$ where $w(u) = 0$ and $\overline{u} = 1$ modulo $\mathfrak{p}_w$. Let $f = [L_w : K_v]$.

$$\begin{aligned}
T_v \circ N_{L/K}\langle u_0.\pi_v, u_2, \ldots, u_n\rangle &= T_v\langle N_{L/K}u_0, \pi_v, u_2, \ldots, u_n\rangle \\
&= -\langle\overline{N_{L/K}u_0}, \overline{u}_2, \ldots, \overline{u}_n\rangle \\
N_{L_w/K_v} \circ T_w\langle u_0, \pi_v, u_2, \ldots, u_n\rangle &= N_{L_w/K_v} \circ T_w\langle u_0, -u\pi_w^{e(w)}, u_2, \ldots, u_n\rangle \\
&= N_{L_w/K_v}\{-e(w)\langle\overline{u}_0, \overline{u}_2, \ldots, \overline{u}_n\rangle\} \\
&= -e(w)\langle N_{L_w/K_v}\overline{u}_0, \overline{u}_2, \ldots, \overline{u}_n\rangle \\
&= -\langle\overline{N_{L/K}u_0}, \overline{u}_2, \ldots, \overline{u}_n\rangle \qquad \text{(App. I, \textbf{1.10.})} \\
T_v \circ N_{L/K}\langle u_0, u_1, \ldots, u_n\rangle &= N_{L_w/K_v} \circ T_w\langle u_0, \ldots, u_n\rangle = 0 \\
T_v \circ N_{L/K}\langle \pi_w, u_1, \ldots, u_n\rangle &= T_v\langle N_{L/K}\pi_w, u_1, \ldots, u_n\rangle \\
&= vN_{L/K}\pi_w\langle\overline{u}_1, \ldots, \overline{u}_n\rangle \\
&= f\langle\overline{u}_1, \ldots, \overline{u}_n\rangle \qquad \text{(App. I, \textbf{2.4.})} \\
N_{L_w/K_v} \circ T_w\langle \pi_w, u_1, \ldots, u_n\rangle &= N_{L_w/K_v}\langle\overline{u}_1, \ldots, \overline{u}_n\rangle \\
&= f\langle\overline{u}_1, \ldots, \overline{u}_n\rangle \qquad \text{since } \overline{u}_i \in K_v.
\end{aligned}$$

Suppose $e(w/v) = 1$ and $\pi_w = \pi_v$, $f = p$.

$$\begin{aligned}
T_v \circ N_{L/K}\langle \pi_v, \pi_v, u_2, \ldots, u_n\rangle &= T_v\{p\langle\pi_v, \pi_v, u_2, \ldots, u_n\rangle\} \\
&= p\langle\overline{-1}, \overline{u}_2, \ldots, \overline{u}_n\rangle \\
N_{L_w/K_v} \circ T_w\langle \pi_v, \pi_v, u_2, \ldots, u_n\rangle &= N_{L_w/K_v}\langle\overline{-1}, \overline{u}_2, \ldots, \overline{u}_n\rangle \\
&= f\langle\overline{-1}, \overline{u}_2, \ldots, \overline{u}_n\rangle = p\langle\overline{-1}, \overline{u}_2, \ldots, \overline{u}_n\rangle.
\end{aligned}$$

Suppose $e(w/v) = p$, $f = 1$ and $\pi_v = -u\pi_w^p$ with $\overline{u} = 1$ and $N_{L/K}\pi_w = (-1)^p\pi_v$.

$$\begin{aligned}
T_v \circ N_{L/K}\langle \pi_w, \pi_v, u_2, \ldots, u_n\rangle &= T_v\langle(-1)^p\pi_v, \pi_v, u_2, \ldots, u_n\rangle \\
&= \langle\overline{(-1)}^{p+1}, \overline{u}_2, \ldots, \overline{u}_n\rangle \\
N_{L_w/K_v} \circ T_w\langle \pi_w, \pi_v, u_2, \ldots, u_n\rangle &= N_{L_w/K_v} \circ T_w\langle \pi_w, -u\pi_w^p, u_2, \ldots, u_n\rangle \\
&= N_{L_w/K_v}\langle -\overline{u}, \overline{u}_2, \ldots, \overline{u}_n\rangle \\
&\quad + N_{L_w/K_v}\{p\langle\overline{-1}, \overline{u}_2, \ldots, \overline{u}_n\rangle\} \\
&= \langle(\overline{-1})^{p+1}, \overline{u}_2, \ldots, \overline{u}_n\rangle.
\end{aligned}$$

□

Proposition 3.3 *Let K be complete, w.r.t a discrete valuation v and L a normal*

extension of K of degree a prime p. Then the following diagram is commutative:

$$\begin{array}{ccc} K_{n+1}(L) & \xrightarrow{N_{L/K}} & K_{n+1}(K) \\ {\scriptstyle T_w}\downarrow & & \downarrow{\scriptstyle T_v} \\ K_n(L_w) & \xrightarrow{N_{L_w/K_v}} & K_n(K_v) \end{array}$$

where w is the extension of v to L.

Proof. Let $u \in K_{n+1}(L)$. By **2.4.**, $\mathrm{ext}_{L^pK/L}\, u \in K_{n+1}(L^pK)$ is a sum of elements of the form $\langle x, y_1, \ldots, y_n\rangle$ with $x \in (L^pK)^*$, $y_i \in {}^pK^*$, $1 \le i \le n$. Clearly, there is a finite subextension K'/K of ${}^pK/K$ such that $\mathrm{ext}_{LK'/L}(u) = \sum \langle x, y_1, \ldots, y_n\rangle$, $x \in (LK')^*$, $y_i \in K'^*$, $1 \le i \le n$. Since $K \subset K' \subset {}^pK$, $[K' : K] = m$ is coprime with p. Since L and K' have coprime degree over K, $L \otimes K' \simeq LK'$ and the following diagram

$$\begin{array}{ccc} K_{n+1}(L) & \xrightarrow{\mathrm{ext}} & K_{n+1}(LK') \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{LK'/K'}} \\ K_{n+1}(K) & \xrightarrow{\mathrm{ext}} & K_{n+1}(K') \end{array}$$

is commutative. Denoting by bar, the corresponding residue fields, since $[\overline{L} : \overline{K}]$ divides $[L : K]$ and $[\overline{K}' : \overline{K}]$ divides $[K' : K]$, $\overline{L} \otimes \overline{K}'$ is a field and $\overline{L}\,\overline{K}' \simeq \overline{LK}'$ (noting that $f(LK'/K) = f(LK'/L)f(L/K) = f'(K'/K)f(L/K)$, and $\overline{L}\,\overline{K}' \hookrightarrow \overline{LK}'$). We have the following commutative diagram

$$\begin{array}{ccc} K_{n+1}(\overline{L}) & \xrightarrow{\mathrm{ext}} & K_{n+1}(\overline{LK'}) \\ \downarrow{\scriptstyle N_{\overline{L}/\overline{K}}} & & \downarrow{\scriptstyle N_{\overline{LK'}/\overline{K'}}} \\ K_{n+1}(\overline{K}) & \xrightarrow{\mathrm{ext}} & K_{n+1}(\overline{K'}) \end{array}$$

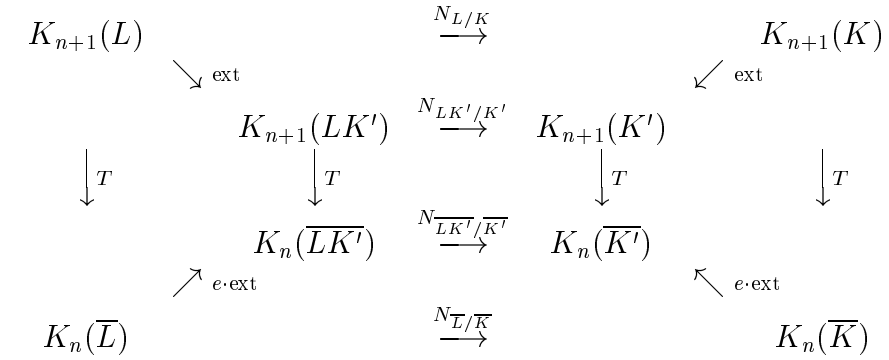
Since $[\overline{K'} : \overline{K}] = [\overline{LK}' : \overline{L}]$, $e(LK'/L) = e$. By Lemma **2.3.**, the following diagrams are commutative

$$\begin{array}{ccc} K_{n+1}(L) & \xrightarrow{\mathrm{ext}} & K_{n+1}(LK') \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} \\ K_n(\overline{L}) & \xrightarrow{e\cdot\mathrm{ext}} & K_n(\overline{LK'}) \end{array} \qquad \begin{array}{ccc} K_{n+1}(K) & \xrightarrow{\mathrm{ext}} & K_{n+1}(K') \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} \\ K_n(\overline{K}) & \xrightarrow{e\cdot\mathrm{ext}} & K_n(\overline{K'}) \end{array}$$

(T denotes the corresponding tame symbols.)

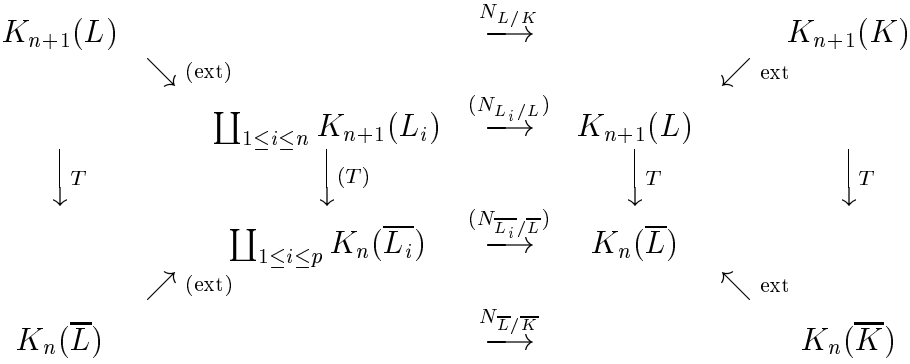
Thus, in the following cube (in projection), all "vertical" faces (= outer squares) are

commutative.



By **3.2.**, $T \circ N_{LK'/K'} \operatorname{ext}_{LK'/L}(u) = N_{\overline{LK'}/\overline{L}} \circ T \operatorname{ext}_{LK'/L}(u)$. Thus, it follows that $\operatorname{ext}_{K'/\overline{K}}(T \circ N_{L/K} - N_{\overline{L}/\overline{K}} \circ T)(u) = 0$. By **2.2.**, $m \cdot (T \circ N_{L/K} - N_{\overline{L}/\overline{K}} \circ T)(u) = 0$ where $m = [\overline{K}' : \overline{K}]$. We next show that $p^2(T \circ N_{L/K} - N_{\overline{L}/\overline{K}} \circ T)(u) = 0$.

Case 1. Suppose L/K is unramified: Since L/K is normal, L/K is Galois and $G(L/K) \xrightarrow{\sim} G(\overline{L}/\overline{K})$ (**3.6.** of App. I). Thus $L \otimes_K L \xrightarrow{\sim} \prod_{1 \le i \le p} L_i$, each $L_i \simeq L$ and $\overline{L} \otimes_{\overline{K}} \overline{L} \xrightarrow{\sim} \prod_{1 \le i \le p} \overline{L}_i$, $\overline{L}_i \xrightarrow{\sim} \overline{L}$, the ramifications of $L \otimes_K L$, $(\overline{L} \otimes_{\overline{K}} \overline{L})$ in L_i, $(\overline{L}_i)$ being 1. We have the following cube with all the vertical faces commutative.



Since $L_i \xrightarrow{\sim} L$ and $\overline{L}_i \xrightarrow{\sim} \overline{L}$, $N_{L_i/L} =$ identity, $N_{\overline{L}_i/\overline{L}} =$ identity. Thus the top of the cube (= central square) is commutative. Hence $\operatorname{ext}_{\overline{L}/\overline{K}}(T \circ N_{L/K} - N_{\overline{L}/\overline{K}} \circ T)(u) = 0$. Hence by **2.2.** $p(T \circ N_{L/K} - N_{\overline{L}/\overline{K}} \circ T)(u) = 0$.

Case 2. Suppose L/K is totally ramified; $e(L/K) = p$, $f(L/K) = 1$.

a) Let L/K be separable. Then $L \otimes_K L \xrightarrow{\sim} \prod_{1 \le i \le p} L_i$, $L_i \xrightarrow{\sim} L$, $1 \le i \le p$. In the

following diagram, all the vertical faces are commutative.

$$\begin{array}{ccccc}
K_{n+1}(L) & & \xrightarrow{N_{L/K}} & & K_{n+1}(K) \\
& \searrow^{(\mathrm{ext})} & & \swarrow^{\mathrm{ext}} & \\
& \coprod_{1\le i\le n} K_{n+1}(L_i) & \xrightarrow{(N_{L_i/L})} & K_{n+1}(L) & \\
\downarrow T & \downarrow (T) & & \downarrow T & \downarrow T \\
& \coprod_{1\le i\le p} K_n(\overline{L_i}) & \xrightarrow{(N_{\overline{L_i}/\overline{L}})} & K_n(\overline{L}) & \\
& \nearrow^{(\mathrm{ext})} & & \nwarrow^{p\cdot\mathrm{ext}} & \\
K_n(\overline{L}) & & \xrightarrow{N_{\overline{L}/\overline{K}}} & & K_n(\overline{K})
\end{array}$$

Since $L_i \simeq L$, $\overline{L_i} \simeq \overline{L}$, $N_{L_i/L} = \text{identity}$, $N_{\overline{L_i}/\overline{L}} = \text{identity}$, so that the top of the cube (in projection) is commutative. Thus $p\cdot\mathrm{ext}(T\circ N_{L/K} - N_{\overline{L}/\overline{K}}\circ T)(u) = 0$. Hence $p^2(T\circ N_{L/K} - N_{\overline{L}/\overline{K}}\circ T)(u) = 0$.

b) Let L/K be purely inseparable. We have $L\otimes_K L/\operatorname{rad} \simeq L$ with p as the ramification of $L\otimes L$ in L, and $\overline{L} = \overline{K}$. We have the following cube with all vertical faces commutative.

$$\begin{array}{ccccc}
K_{n+1}(L) & & \xrightarrow{N_{L/K}} & & K_{n+1}(K) \\
& \searrow^{p\cdot\mathrm{ext}} & & \swarrow^{\mathrm{ext}} & \\
& K_{n+1}(L) & \xrightarrow{=} & K_{n+1}(L) & \\
\downarrow T & \downarrow (T) & & \downarrow T & \downarrow T \\
& K_n(\overline{L}) & \xrightarrow{=} & K_n(\overline{L}) & \\
& \nearrow^{p\cdot\mathrm{ext}} & & \nwarrow^{p\cdot\mathrm{ext}} & \\
K_n(\overline{L}) & & \xrightarrow{N_{\overline{L}/\overline{K}}} & & K_n(\overline{K})
\end{array}$$

Since the top square is clearly commutative, $p\ \mathrm{ext}(T\circ N_{L/K} - N_{\overline{L}/\overline{K}}\circ T)(u) = 0$. Thus $p^2(T\circ N_{L/K} - N_{\overline{L}/\overline{K}}\circ T)(u) = 0$. We also have $m(T\circ N_{L/K} - N_{\overline{L}/\overline{K}}\circ T)(u) = 0$ so that, since $(p,m) = 1$, $(T\circ N_{L/K} - N_{\overline{L}/\overline{K}}\circ T)(u) = 0$. Since this is true for any $u \in K_{n+1}(L)$, the proposition is proved. □

Corollary 3.4. *Let E/K be a normal extension of degree p where p is a prime. Then for each valuation v of $K(X)$ over K, the following diagram is commutative*

$$\begin{array}{ccc}
K_{n+1}(E(X)) & \xrightarrow{(T_w)} & \coprod_{w/v} K_n(E(X)_w) \\
{\scriptstyle N_{E(X)/K(X)}}\downarrow & & \downarrow{\scriptstyle (N_{E(X)_w/K(X)_v})} \\
K_{n+1}(K(X)) & \xrightarrow{T_v} & K_n(K(X)_v)
\end{array}$$

Proof. Let $\widehat{E(X)}_w$ and $\widehat{K(X)}_v$ denote the completions of $E(X)$ and $K(X)$ at w and v, respectively. Let π be the irreducible polynomial of a generator α of E over K. We

claim that π remains irreducible over $K(X)_v$ if E/K is purely inseparable. Suppose π splits over $K(X)_v$. Then π would become a power of a linear polynomial over $\widehat{K(X)}_v$ and $E(X)\otimes_{K(X)}\widehat{K(X)}_v/\mathrm{rad} \xrightarrow{\sim} \widehat{K(X)}_v$. Since $E(X)\otimes_{K(X)}\widehat{K(X)}_v/\mathrm{rad} \simeq \prod_{w/v}\widehat{E(X)}_w$, it follows that there is a unique extension w of v to $E(X)$ whose completion is isomorphic to $\widehat{K(X)}_v$. We have $e(w/v) = e(\widehat{E(X)}_w/\widehat{K(X)}_v) = 1$ and since $E(X)_w =$ residue field of $\widehat{E(X)}_w =$ residue field of $\widehat{K(X)}_v = K(X)_v$, $f(w/v) = 1$. Since w is the unique extension of v to $E(X)$, we have $p = e(w/v)\cdot f(w/v) = 1$, a contradiction. Thus π is irreducible over $K(X)_v$. On the other hand, if E/K is separable, then E/K is Galois and $E(X)\otimes_{K(X)}\widehat{K(X)}_v = \coprod_{w/v}\widehat{E(X)}_v$ where either there is a unique extension w of v to $E(X)$ in which case π is irreducible over $\widehat{K(X)}_v$ or there are p distinct extensions w of v to $E(X)$ in which case π splits into distinct irreducible factors over $\widehat{K(X)}_v$. We therefore have the commutativity of the left hand square of the following diagram.

$$\begin{array}{ccccc} K_{n+1}(E(X)) & \xrightarrow{\text{ext}} & \coprod_{w/v} K_{n+1}(\widehat{E(X)}_w) & \xrightarrow{(T_w)} & \coprod_{w/v} K_n(E(X)_w) \\ \downarrow{\scriptstyle N_{E(X)/K(X)}} & & \downarrow{\scriptstyle N_{\widehat{E(X)}_w/\widehat{K(X)}_v}} & & \downarrow{\scriptstyle (N_{E(X)_w/K(X)_v})} \\ K_{n+1}(K(X)) & \xrightarrow{\text{ext}} & K_{n+1}(\widehat{K(X)}_v) & \xrightarrow{T_v} & \coprod_{w/v} K_n(K(X)_v) \end{array}$$

The commutativity of the right hand square follows from **3.4.**. We note that $T_w \circ \mathrm{ext} = T_w : K_{n+1}(E(X)) \to K_n(E(X)_w)$, since a parameter or a unit of w remains a parameter or a unit of w, respectively, in the completion $\widehat{E(X)}_w$. Similarly, $T_v \circ \mathrm{ext}$ is the tame symbol $T_v : K_{n+1}(K(X)) \to K_n(K(X)_v)$ and the lemma is proved. $\square$

(Crucial) Lemma 3.5. *Let K be a field and E a normal extension of degree p over K. Let $K' = K(a)$ be a simple extension. Let $E' = E(a)$ be the composite of E and K' over K. Then, the following diagram is commutative.*

$$\begin{array}{ccc} K_n(E') & \xrightarrow{N_{a/E}} & K_n(E) \\ \downarrow{\scriptstyle N_{E'/K'}} & & \downarrow{\scriptstyle N_{E/K}} \\ K_n(K') & \xrightarrow{N_{a/K}} & K_n(K) \end{array}$$

Proof. Let $\pi_{a,K}$ and $\pi_{a,E}$ denote the minimal polynomials of a over K and E, respectively. Let $v_{a,K}$ and $w_{a,E}$ denote the valuations of $K(X)$ and $E(X)$ corresponding to $\pi_{a,K}$ and $\pi_{a,E}$, respectively. We identify E' with $K(X)_{v_{a,E}}$ and K' with $K(X)_{v_{a,K}}$. Since the sequence

$$K_{n+1}(E(X)) \xrightarrow{(T_w)} \coprod_v \coprod_{w/v} K_n(E(X)_w) \xrightarrow{(N_w)} K_n(E) \longrightarrow 0$$

is exact (Theorem **11** of App. II), there exists $y \in K_{n+1}(E(X))$ such that

$$T_w(y) = \begin{cases} x & \text{if } w = w_{a,E} \\ -N_{a/E}x & \text{if } w = w_\infty \\ 0 & \text{otherwise,} \end{cases}$$

noting that $N \circ (T_w)(y) = 0$. By **3.4.**, we have

$$T_v \circ N_{E(X)/K(X)}(y) = \sum_{w/v} N_{E(X)_w/K(X)_v} \circ T_w(y),$$

so that we have

$$T_v \circ N_{E(X)/K(X)}(y) = \begin{cases} N_{E'/K'}(x) & \text{if } v = v_{a,K} \\ -N_{E/K} \circ N_{a/E}(x) & \text{if } v = v_\infty \\ 0 & \text{otherwise.} \end{cases}$$

Since $K_{n+1}(K(X)) \xrightarrow{(T_v)} \coprod_v K_n(K(X)_v) \xrightarrow{(N_v)} K_n(K)$ is a complex,

$$N \circ T(N_{E(X)/K(X)}(y)) = 0$$

i.e.
$$N \circ \sum_{w/v} N_{E(X)_w/K(X)_v} \circ T_w(y) = 0,$$

i.e.
$$N_{a/K} \circ N_{E'/K'}(x) - N_{E/K} \circ N_{a/E}(x) = 0.$$

This proves the lemma. □

§ 4. Proof of Proposition 1.2

Proposition 4.1. *Let p be a prime and K a field such that $K = {}^pK$. Let E/K be a finite extension of degree p^n. Then there exists a tower of fields $K = K_0 \subset K_1 \subset \cdots \subset K_n = E$ such that $[K_i : K_{i-1}] = p$ for each i, and K_i/K_{i-1} is normal. Further the composite*

$$K_*(E) = K_*(K_n) \overset{N_{K_n/K_{n-1}}}{\longrightarrow} K_*(K_{n-1}) \to \ldots \overset{N_{K_1/K_0}}{\longrightarrow} K_*(K_0) = K_*(K)$$

is independent of the family $\{K_i\}$ chosen.

Proof. We claim that for any field L with $L = {}^pL$, every finite extension L'/L of degree p is normal. If L'/L is purely inseparable, it is normal. If L'/L is separable,

if $\overline{L}'$ denotes the Galois closure of $\overline{L}'/L$, $G(\overline{L}'/L)$ is a p–group and $G(\overline{L}'/L')$ is a subgroup of index p in $G(\overline{L}'/L)$ so that it is normal. Hence L'/L is normal. Further, for any field L with $L = {}^pL$, and any finite extension L' of L, ${}^pL' = L'$. thus if such a tower $K_0 = K \subset K_1 \subset \cdots \subset K_n = K$ exists with $[K_i : K_{i-1}] = p$, then each K_i/K_{i-1} is normal since $K = {}^pK$.

Let $[E : K] = p^n$. If E/K is purely inseparable, the existence of a tower is clear. Let $K \subset K_s \subset E$ be such that K_s is the separable closure of K in E. Replacing E by K_s we may assume E/K separable. Let $\overline{E}/K$ be the Galois closure of $E/K$with Galois group $G(\overline{E}/K)$. Let H be a maximal subgroup of $G(\overline{E}/K$ containing $G(\overline{E}/E)$. Since $G(\overline{E}/E)$ is a p–group such an H exists. Let K_1 be the fixed field of H. Then $K \subset K_1 \subset E$ with $[K_1 : K] = p$. Since $[E : K_1] = p^{n-1}$, inductively, one gets a tower $K_1 \subset K_2 \subset \cdots \subset K_n = E$ with $[K_i : K_{i-1}] = p,\ 1 \leq i \leq n$.

We now show that $N_{K_1/K} \circ N_{K_2/K_1} \circ \cdots \circ N_{K_n/K_{n-1}}$ is independent of the family $\{K_i\}$ The proof is by induction on n. For $n = 1$, this is precisely **3.1.**. Suppose that the result is true for $n = 2$. Let $K \subset K_1 \subset \cdots \subset K_n = E,\ K \subset K_1' \subset \cdots \subset K_n' = E$ be two such towers. If $K_1 = K_1'$, by induction, $N_{K_2/K_1} \circ \cdots \circ N_{E/K_{n-1}} = N_{K_2'/K_1} \circ \cdots \circ N_{E/K_{n-1}'}$ and hence $N_{K_1/K} \circ \cdots \circ N_{E/K_{n-1}} = N_{K_1'/K} \circ \cdots \circ N_{E/K_{n-1}'}$. Suppose $K_1 \neq K_1'$. We have the following towers

$$
\begin{aligned}
&K \subset K_1 \subset K_2 \subset \cdots \subset K_n = E \ldots && ① \\
&K \subset K_1 \subset K_1K_1' \subset K_2K_1' \subset \cdots \subset K_nK_1' = E \ldots && ② \\
&K \subset K_1' \subset K_1K_1' \subset K_1K_2' \subset \cdots \subset K_1K_n' = E \ldots && ③ \\
&K \subset K_1' \subset K_2' \subset \cdots \subset K_n' = E \ldots && ④
\end{aligned}
$$

Since the first extension in ①and ②is the same, ①and ②yield the same composite of norms. Similarly, ③and ④yield the same composite of norms. Since we have assumed the result for $n = 2$, $N_{K_1/K} \circ N_{K_1/K_1'/K} = N_{K_1'/K} \circ N_{K_1/K_1'/K}$ and by induction it follows that ②and ③yield the same composite of norms.

Let $n = 2$ and $K \subset K_1 \subset E,\ K \subset K_1' \subset E$ be two distinct towers. Let $K_1' = K(a)$. By the Crucial Lemma **3.5.**, $N_{K_1/K} \circ N_{a/K_1} = N_{a/K} \circ N_{E/K_1'}$. Since $[K(a) : K] = p,\ [K_1(a) : K_1] = p,\ N_{a/K_1} = N_{E/K_1}$ and $N_{a/K} = N_{K_1'/K}$ so that $N_{K_1/K} \circ N_{E/K_1} = N_{K_1'/K} \circ N_{E/K_1} = N_{K_1'/K} \circ N_{E/K_1'}$. □

Definition. *Let E and K be as in Proposition 4.1. We denote by $N_{E/K}$ the composite homomorphism given in Proposition 4.1.*

Proof of of Proposition 1.2. To prove **1.2.**, we show first that we may assume $K = {}^pK$ for some prime p. For each prime q, let $E \otimes_K {}^qK/\operatorname{rad} \xrightarrow{\sim} \coprod_i E_i$ with e_i the ramifications of $E \otimes_K {}^qK$ in E_i. Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_m\}$ be two sets of generators of E over K and let $\{\alpha_1^i, \ldots, \alpha_n^i\}$ and $\{\beta_1^i, \ldots, \beta_m^i\}$ denote their images

in E_i under the map

$$E \longrightarrow E \otimes_K {}^qK \longrightarrow E \otimes_K {}^qK/\operatorname{rad} \longrightarrow \coprod_i E_i \xrightarrow{p_i} E_i.$$

We have, in view of **2.8.**, the following commutative diagrams

$$\begin{array}{ccc} \coprod_i K_n(E_i) & \xrightarrow{(N_{(\alpha_1^i,\ldots,\alpha_n^i)/{}^pK})} & K_n({}^pK) \\ \uparrow{\scriptstyle (e_i\cdot \mathrm{ext})} & & \uparrow{\scriptstyle \mathrm{ext}} \\ K_n(L) & \xrightarrow{(N_{(\alpha_1,\ldots,\alpha_n)/{}^pK})} & K_n(K) \end{array} \qquad \begin{array}{ccc} \coprod_i K_n(E_i) & \xrightarrow{(N_{(\beta_1^i,\ldots,\beta_m^i)/{}^pK})} & K_n({}^pK) \\ \uparrow{\scriptstyle (e_i\cdot \mathrm{ext})} & & \uparrow{\scriptstyle \mathrm{ext}} \\ K_n(L) & \xrightarrow{(N_{(\beta_1,\ldots,\beta_m)/{}^pK})} & K_n(K) \end{array}$$

If we assume **1.2.** true for ${}^pK$, then $N_{(\alpha_1^i,\ldots,\alpha_n^i)/{}^pK} = N_{(\beta_1^i,\ldots,\beta_m^i)/{}^pK}$. Thus $\mathrm{ext}_{{}^pK/K}(N_{(\alpha_1,\ldots,\alpha_n)/K} - N_{(\beta_1,\ldots,\beta_m)/K}) = 0$. Thus for each $u \in K_n(L)$, there exists an integer m_p coprime with p such that

$$m_p(N_{(\alpha_1,\ldots,\alpha_n)/K} - N_{(\beta_1,\ldots,\beta_m)/K})(u) = 0.$$

Hence $N_{(\alpha_1,\ldots,\alpha_n)/K} = N_{(\beta_1,\ldots,\beta_m)/K}$. Suppose then that $K = {}^pK$ for a prime p. It is enough to show that if $E = K(\alpha)$ a finite simple extension, $N_{\alpha/K} = N_{E/K}$, $N_{E/K}$ as in the definition after Proposition **4.1.** In fact,

$$\begin{aligned} N_{\alpha_1,\ldots,\alpha_n)/K} &= N_{\alpha_1/K} \circ N_{\alpha_2/K_1} \cdots \circ N_{\alpha_n/K_{n-1}} \quad \text{where } K_i = K(\alpha_1,\ldots,\alpha_i) \\ &= N_{K_1/K} \circ N_{K_2/K_1} \circ \cdots \circ N_{K_n/K_{n-1}} \\ &= N_{F_1/K} \circ N_{F_2/F_1} \circ \cdots \circ N_{F_m/F_{m-1}} \text{ where } F_i = K(\beta_1,\ldots,\beta_i), \text{ by } \mathbf{4.1.} \\ &= N_{\beta_1/K} \circ N_{\beta_2/F_1} \circ \cdots \circ N_{\beta_m/F_{m-1}} = N_{\beta_1,\ldots,\beta_m)/K}. \end{aligned}$$

Let $E = K(\alpha)$. Let $K = K_0 \subset K_1 \subset \cdots \subset K_n = E$ with $[K_i : K_{i-1}] = p$. If $E = K_1$, by **3.1**, $N_{\alpha_1/K} = N_{E/K}$. Suppose $n \geq 2$. By induction on n, $N_{a/K_1} = N_{E/K_i}$. By the "Crucial Lemma",

$$\begin{array}{ccc} K_n(E) & \xrightarrow{N_{a/K_1}} & K_n(K_1) \\ & = & \downarrow{\scriptstyle N_{K_1/K}} \\ K_n(E) & \xrightarrow{N_{a/K}} & K)n(K) \end{array}$$

commutes, i.e. $N_{K_1/K} \circ N_{a/K_1} = N_{a/K}$. Thus $N_{K_1/K} \circ N_{E/K_1} = N_{a/K}$; i.e. $N_{E/K} = N_{a/K}$ and **1.2.** is proved. □

Appendix IV: A theorem of Rosset–Tate

Let k be a field and let $\underline{\underline{C}}_k$ denote the category of finite field extensions of k. A *Milnor functor* $M : \underline{\underline{C}}_k \to \underline{\underline{Ab}}$ is a covariant functor together with maps $\varphi_K : K^* \times K^* \to M(K)$, $\forall K \in \text{Obj } \underline{\underline{C}}_k$ which are biadditive and for each k–injection $K \to L$, $K, L \in \text{Obj } C_k$, a homomorphism , $\text{tr}_{L/K} : M(L) \to M(K)$, called the *transfer*, satisfying the following properties.

1) The maps φ are functorial; i.e., given an injection $i : K \to L$ in $\underline{\underline{C}}_k$, the diagram

$$\begin{array}{ccc} K^* \times K^* & \xrightarrow{\varphi_K} & M(K) \\ {\scriptstyle i\times i}\downarrow & & \downarrow{\scriptstyle M(i)} \\ L^* \times L^* & \xrightarrow{\varphi_L} & M(L) \end{array}$$

is commutative.

2) $\varphi_k(a, 1-a) = 0$ if a , $1-a \in K^*$.

3) If $K \to L \to N$ are injections in $\underline{\underline{C}}_k$, then,

$$\text{tr}_{N/K} = \text{tr}_{L/K} \circ \text{tr}_{N/L} \ .$$

4) If $K \to L$ is an injection in $\underline{\underline{C}}_k$ and if $x \in K^*$, $y \in L^*$, we have the "projection formula"

$$\text{tr}_{L/K}\varphi_L(x, y) = \varphi_K(x, N_{L/K}y) \ ,$$

$N_{L/K} : L \to K$ denoting the norm in the extension L/K.

Example 1. For any field K, let $K_2(K)$ denote the Milnor K_2 defined in Chapter III. The functor K_2 is a Milnor functor with $\varphi = \varphi_K : K^* \times K^* \to K_2(K)$ being the map $\varphi(a, b) = \langle a, b\rangle$ and for any finite extension L/K, $\text{tr}_{L/K} : K_2(L) \to K_2(K)$ being the transfer defined in Appendix II. The functor K_2 is in fact a Universal Milnor functor in the sense that given any Milnor functor M, there is a natural transformation $T : K_2 \to M$ such that the diagram

$$\begin{array}{ccc} K^* \times K^* & \xrightarrow{\varphi} & K_2(K) \\ & {\scriptstyle \varphi_K}\searrow & \downarrow{\scriptstyle T_K} \\ & & M(K) \end{array}$$

is commutative.

Example 2. Let K be any field of characteristic $\neq 2$. The functor $K \to H^2(K) = H^2_c(G(K_s/K), \mu_2)$ is a Milnor functor with $\text{tr}_{L/K} = \text{cores}_{L/K}$ and $\varphi_K : K^* \times K^* \to H^2(K)$ being given by $(a, b) \mapsto \chi_a \cup \chi_b$. The norm residue homomorphism $\beta_K : K_2(K) \to H^2(K)$ is a natural transformation which commutes with φ.

If M is a Milnor functor, M can be extended to the category $\widetilde{\underline{\underline{C}}}_k$ of finite dimensional semisimple (commutative) k–algebras by defining $M(\prod_{1\le i\le \ell} K_i) = \prod_{1\le i\le \ell} M(K_i)$. We have

$$\varphi_{\prod K_i} = (\varphi_{K_i}) : (\prod K_i)^* \times (\prod K_i)^* \to M(\prod K_i) = \prod M(K_i).$$

Further, if $\prod K_i \to A$ is an injection of semi–simple k–algebras, $\mathrm{tr}_{A/\prod K_i}$ is defined to be (tr_{A_i/K_i}) where $A = \prod A_i,\ A_i$ semisimple K_i–algebras and if $A_i = \prod K_{ij},\ K_{ij}$ finite field extensions of $K_i,\ \mathrm{tr}_{A_i/K_i} = \prod \mathrm{tr}_{K_{ij}/K_i}$. The map φ_K satisfies $\varphi_K(a, 1-a) = 0$ for $a,\ 1-a \in A^*$ (A^* denoting the group of units of A) and $\varphi_K(a,-a) = 0$ if $a \in A^*$. The transitivity $\mathrm{tr}_{C/A} = \mathrm{tr}_{B/A} \circ \mathrm{tr}_{C/B}$ for $A \to B \to C,\ A, B, C$ in Obj $\widetilde{\underline{\underline{C}}}_k$ and the projection formula

$$\mathrm{tr}_{B/A}\varphi_B(x, y) \ = \ \varphi_A(x, N_{B/A}y) \quad \text{for} \ \ x \in A^*,\ y \in B^* \ ,$$

$N : B \to A$ being the norm of the finite dimensional A–algebra B are easily verified.

Let k be a fixed base field and M a Milnor functor. For any $K \in$ Obj $\widetilde{\underline{\underline{C}}}_k$ and $x, y \in E^*$, we shall abbreviate $\varphi_E(x, y) = (x, y)_E$, or simply (x, y) if E is clear from the context. Let K/k be a finite field extension. Let $f, g \in K[T]$ be relatively prime (non–zero) polynomials. We define a symbol (f/g) with values in $M(K)$ by the following requirements.

(1) $(f/g_1g_2) = (f/g_1) + (f/g_2)$

(2) If g is a constant or T, $(f/g) = 0$.

(3) If g is a monic irreducible polynomial, not a constant or T, and x a root of $g(T)$ in an algebraic closure, then,

$$(f/g) = \mathrm{tr}_{K(x)/K}(x, f(x))_{K(x)} \ .$$

The symbol (f/g) is 'additive' in both f and g and depends only on the residue of f modulo (g). As a function of g, it depends only on the ideal generated by g in $K[T, T^{-1}]$. For $p(T) \in K[T],\ p(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_mT^m,\ a_n{\cdot}a_m \neq 0$, we define

$$p^*(T) \ = \ (a_mT^m)^{-1}p(T)$$

$$c(p) \ = \ (-1)^n a_n.$$

We note that for $p,\ p' \in K[T],\ (pp')^* = p^*{\cdot}p'^*$ and $c(pp') = c(p){\cdot}c(p')$.

Theorem 1. (Reciprocity Law) *For relatively prime polynomials, $f, g \in K[T]$, we have*

$$(f/g) \ = \ (g^*/f) \ - \ (c(g^*), c(f)). \qquad (*)$$

Proof. Suppose $g = a \in K^*$ or $g = T$. Then $g^* = 1$, and $c(g^*) = 1$. We have, if $f = \prod f_i^{e_i}$, f_i irreducible over K,

$$\begin{aligned}(g^*/f) &= \sum e_i(1/f_i) \\ &= \sum e_i \mathrm{tr}_{K/x_i)/K}(x_i, 1)_{K(x_i)}, \quad x_i \text{ being a root of } f_i, \\ &= \sum e_i(N_{K(x_i)/K}(x_i), 1)_K \\ &= 0.\end{aligned}$$

(We note that $(x,1)_K = (x,1)_K + (x,1)_K$ so that $(x,1)_K = 0$.) Thus both sides of $(*)$ are zero. Since both sides of $(*)$ are 'additive' in f and g, we assume that f and g are monic, irreducible and g is not a constant or T. Suppose $f = a \in K^*$. Let x be a root of $g(T)$. Then,

$$\begin{aligned}(a/g) &= \mathrm{tr}_{K(x)/K}(x, a)_{K(x)} \\ &= (N_{K(x)/K}(x), a)_K \\ &= (c(g^*)^{-1}, a)_K \\ &= -(c(g^*), c(f))_K,\end{aligned}$$

and $(g^*/a) = 0$. If $f = T$,

$$\begin{aligned}(T/g) &= \mathrm{tr}_{K(x)/K}(x, x)_{K(x)} \\ &= \mathrm{tr}_{K(x)/K}(x, -1)_{K,(x)} \quad (\text{since } (x, -x)_{K(x)} = 0) \\ &= (c(g^*)^{-1}, -1)_K \\ &= -(c(g^*), c(f)),\end{aligned}$$

and $(g^*/T) = 0$. We assume that both f and g are monic irreducible and different from T. Let x be a root of g and y a root of f. We write $f = \prod_{1 \le i \le \ell} f_i^{e_i}$, f_i irreducible over $K(x)$. The integers ℓ and $\{e_i\}$, $1 \le i \le \ell$, can be described as follows. The integer ℓ is the number of distinct maximal ideals $\{\mathfrak{m}_i\}$ of $K(x) \otimes_K K(y) = A$ and e_i = index of nilpotence of $\mathfrak{m}_i$ in $A_{\mathfrak{m}_i}$. Thus, g also decomposes over $K(y)$ as $g = \prod_{1 \le i \le \ell} g_i^{e_i}$, g_i being irreducible over $K(y)$. Let $A/\operatorname{rad} A = \prod L_i$. Then $L_i \simeq K(x)[Y]/(f_i) \simeq K(y)[X]/(g_i)$. Let $\overline{x}, \overline{y} \in L_i$ denote the images of $x \otimes 1$ and $1 \otimes y$ in A. Since $f_i(\overline{y}) = 0$ and $g_i(\overline{x}) = 0$, f_i a divisor of f, g_i a divisor of g and f, g distinct irreducible polynomials over K, $\overline{x} \neq \overline{y}$. We have $\overline{x} \neq 0$, $\overline{y} \neq 0$ since f and g are distinct from T. Further,

$$\begin{aligned}(\overline{x}, \overline{x} - \overline{y})_{L_i} &= (\overline{x}, \frac{\overline{y} - \overline{x}}{-\overline{x}}) + (\overline{x}, \overline{x}) \\ &= (\overline{y} \cdot \frac{\overline{x}}{\overline{y}}, \frac{\overline{y} - \overline{x}}{-\overline{x}} + (\overline{x}, -1) \\ &= (\overline{y}, \frac{\overline{y} - \overline{x}}{-\overline{x}}) + (\overline{x}, -1) + (\frac{\overline{x}}{\overline{y}}, 1 - \frac{\overline{y}}{\overline{x}}) \\ &= (\overline{y}, \frac{\overline{y} - \overline{x}}{-\overline{x}})_{L_i} + (\overline{x}, -1)_{L_i} \ . \qquad (**)\end{aligned}$$

Let $\theta = (\theta_i)$, $\theta' = (\theta'_i)$, $\eta = (\eta_i)$, $\eta' = (\eta'_i)$ be elements of $\overline{A} = \prod L_i$ where $\theta_i = (\overline{x} - \overline{y})^{e_i}$, $\theta'_i = (-1)^i \theta_i$, $\eta_i = \overline{x}^{e_i}$, $\eta'_i = (-1)^{e_i} \cdot \eta_i$. Then

$$\begin{aligned}
N_{\overline{A}/K(x)}(\theta) &= \prod_i N_{L_i/K(x)}(\overline{x} - \overline{y})^{e_i} \\
&= \prod_i f_i(x)^{e_i} = f(x) \ . \\
N_{\overline{A}/K(y)}(\theta') &= g(y) \\
N_{\overline{A}/K(x)}(\eta) &= \prod_i N_{L_i/K(x)}(\overline{x}^{e_i}) \\
&= x^{\deg f} \\
N_{\overline{A}/K(y)}(\eta') &= \prod_i N_{L_i/K(y)}(-\overline{x})^{e_i} \\
&= \prod_i g_i(0)^{e_i} = g(0) \ .
\end{aligned}$$

We have the identity

$$(\overline{x}, \theta)_{\overline{A}} = (\overline{y}, \theta'/\eta')_{\overline{A}} + (\eta, -1)_{\overline{A}}$$

in $M(\overline{A})$, in view of $(**)$. Computing $\mathrm{tr}_{\overline{A}/K}(\overline{x}, \theta)_{\overline{A}}$ in two different ways, we have,

$$\begin{aligned}
\mathrm{tr}_{\overline{A}/K}(\overline{x}, \theta)_{\overline{A}} &= \mathrm{tr}_{K(x)/K} \circ \mathrm{tr}_{\overline{A}/K(x)}(\overline{x}, \theta)_{\overline{A}} \\
&= \mathrm{tr}_{K(x)/K}(x, N_{\overline{A}/K(x)}\theta)_{K(x)} \\
&= \mathrm{tr}_{K(x)/K}(x, f(x))_{K(x)} \\
&= (f/g) \ . \\
\mathrm{tr}_{\overline{A}/K}(\overline{y}, \theta'/\eta')_{\overline{A}} &= \mathrm{tr}_{K(y)/K} \circ \mathrm{tr}_{\overline{A}/K(y)}(\overline{y}, \theta'/\eta')_{\overline{A}} \\
&= \mathrm{tr}_{K(y)/K}(y, N_{\overline{A}/K(y)}(\theta'/\eta'))_{K(y)} \\
&= \mathrm{tr}_{K(y)/K}(y, g(y)/g(0))_{K(y)} \\
&= \mathrm{tr}_{K(y)/K}(y, g^*(y))_{K(y)} \\
&= (g^*/f) \\
\mathrm{tr}_{\overline{A}/K}(\eta, -1)_{\overline{A}} &= \mathrm{tr}_{K(x)/K}(N_{\overline{A}/K(x)}(\eta), -1)_{K(x)} \\
&= \mathrm{tr}_{K(x)/K}(x^{\deg f}, -1)_{K(x)} \\
&= \mathrm{tr}_{K(x)/K}(x, c(f))_{K(x)} \\
&= (c, g^*)^{-1}, c(f))_K \\
&= -(c, g^*), c(f))_K \ .
\end{aligned}$$

We thus obtain the formula

$$(f/g) = (g^*/f) - (c(g^*), c(f))_K \ .$$

□

Let $E \hookrightarrow F$ be a finite extension of fields, finite over k. Let $x, y \in F^*$. Let $N_{F/E(x)}(y) = f(x)$ with $f \in E[T]$ and $\deg f < [E(x) : E]$. Then

$$\begin{aligned} \mathrm{tr}_{F/E}(x,y)_F &= \mathrm{tr}_{E(x)/E} \circ \mathrm{tr}_{F/E(x)}(x,y)_F \\ &= \mathrm{tr}_{E(x)/E}(x, N_{F/E(x)}(y))_{E(x)} \\ &= \mathrm{tr}_{E(x)/E}(x, f(x))_{E(x)} \\ &= (f/g) \ . \end{aligned}$$

Proposition 2. *Let $\{g_0, g_1, \ldots, g_m\}$ be the sequence of polynomials in $E[T]$ defined by $g_0 = g$, $g_1 = f$, $g_{i+1} =$ remainder of division of g_{i-1}^* by g_i, $i \geq 1$ and $g_m \neq 0$, $g_{m+1} = 0$. Then $m \leq \deg g$ and*

$$\mathrm{tr}_{F/E}(x,y)_F = -\sum_{1 \leq i \leq m} (c(g_i^*), c(f))_E \ .$$

Proof. Since $\deg g_{i+1}^* \leq \deg g_{i+1} < \deg g_i$, it follows that $m \leq \deg g$. Further, since $g_{m+1} = 0$, g_m divides $g_0 = g$ and $g_1 = f$ which are relatively prime so that g_m is a constant. Thus $(g_{m-1}^*/g_m) = 0$. Using reciprocity, we have

$$\begin{aligned} (f/g) = (g_1/g_0) &= -\textstyle\sum_{1 \leq i \leq m} (c(g_{i-1}^*), c(g_i)) + (g_{m-1}^*/g_m) \\ &= -\textstyle\sum_{1 \leq i \leq m} (c(g_{i-1}^*), c(g_i)) \ . \end{aligned}$$

This proves the proposition. □

The sequence $\{g_i\}$, $0 \leq i \leq m$ of polynomial depends only on E, F, x and y and not on the Milnor functor M. Thus $\mathrm{tr}_{E/F}(x,y)_F$ can be expressed as a sum of 'symbols' independent of M. Thus, if $T : M_1 \to M_2$ is a morphism of Milnor functors such that the diagram

$$\begin{array}{ccc} A^* \times A^* & \xrightarrow{\varphi_A} & M_1(A) \\ & \searrow^{\varphi_A} & \downarrow{\scriptstyle T_A} \\ & & M(A) \end{array}$$

commutes, then T must commute with transfer. In particular, $\beta_K : K_2(K) \to H^2(K)$ is such a morphism so that we have the following

Corollary 3. *Let F/E be a finite extension. Then the following diagram is commutative*

$$\begin{array}{ccc} K_2(F) & \xrightarrow{\beta_F} & H^2(F) \\ \downarrow{\scriptstyle \mathrm{tr}} & & \downarrow{\scriptstyle \mathrm{cores}_{F/E}} \\ K_2(E) & \xrightarrow{\beta_E} & H^2(E) \end{array}$$

Remark. The contents of this section are taken from the paper "A reciprocity law for K_2–traces" (Comment. Math. Helvetici 58 (1983)) by Rosset–Tate, with obvious modifications to avoid the use of the transfer from Quillen's theory. We only use transfer for K_2 of fields (and their finite products) whose existence is proved in Appendix II.