pp. 69-73 in: Algebraic K-theory, Evanston 1976, edited by Michael R. Stein, Lecture Notes in Mathematics 551, Springer-Verlag, Berlin 1976.

K_2 OF A GLOBAL FIELD CONSISTS OF SYMBOLS

H.W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Amsterdam, The Netherlands

Introduction. It is well known that K_2 of an arbitrary field is generated by symbols $\{a, b\}$. In this note we prove the curious fact that every element of K_2 of a global field is not just a product of symbols, but actually a symbol. More precisely, we have:

Theorem. Let F be a global field, and let $G \subset K_2(F)$ be a finite subgroup. Then $G \subset \{a, F^*\} = \{\{a, b\} \mid b \in F^*\}$ for some $a \in F^*$.

The proof is given in two sections. In section 1 we prove the analogous assertion for a certain homomorphic image of $K_2(F)$, by a rearrangement of the proof of Moore's theorem given by Chase and Waterhouse [3]. In section 2 we lift the property to $K_2(F)$, using results of Garland and Tate.

1. A sharpening of Moore's theorem. Let F be a global field, i. e., a finite extension of $\mathbf{Q}$ or a function field in one variable over a finite field. The multiplicative group of F is denoted by F^*, the group of roots of unity in F by μ, and its finite order by m. By a prime v of F we shall always mean a prime divisor of F which is not complex archimedean. If v is non-archimedean, then we also use the symbol v to denote the associated normalized exponential valuation. For a prime v of F, let F_v be the completion of F at v. The group of roots of unity in F_v is called μ_v, and its finite order $m(v)$. The $m(v)$-th power norm residue symbol $F_v^* \times F_v^* \to \mu_v$ is denoted by $(\ ,\ )_v$. For all but finitely many v this map is given by the so-called "tame formula", cf. [1, sec. 1]. This formula implies that, for those v, and for all $a, b \in F_v^*$ with $v(a) = 0$, the symbol $(a, b)_v$ is the unique root of unity in F_v^* which modulo the maximal ideal is congruent to $a^{v(b)}$. It follows that, for any $a, b \in F^*$, we have $(a, b)_v = 1$ for almost all v. Thus a bimultiplicative map

$$\phi: F^* \times F^* \longrightarrow \bigoplus_v \mu_v, \qquad \phi(a, b) = ((a, b)_v)$$

is induced; here v ranges over the primes of F. The image of ϕ is, by the m-th power reciprocity law, contained in the kernel of the homomorphism

$$\psi: \bigoplus_v \mu_v \longrightarrow \mu$$

defined by

$$\psi(\zeta) = \prod_v \zeta_v^{m(v)/m}, \qquad \zeta = (\zeta_v).$$

We need the following converse, which is a sharpening of Moore's theorem [3].

Proposition. Let H be a finite subgroup of the kernel of ψ. Then $H \subset \phi(a, F^*) = \{\phi(a, b) \mid b \in F^*\}$ for some $a \in F^*$.

The proof is a bit technical. The ingredients are taken from [3], but the strengthened conclusion requires a reorganization of the argument which does not add to its transparency. The reader may find the table at the end of this section of some help.

Proof of the proposition. We begin by selecting four finite sets S, T, U, V of primes of F.

For S we take the set of real archimedean primes of F. It can be identified with the set of field orderings of F. If F is a function field it is empty.

For T we take a finite set of non-archimedean primes of F containing those v for which at least one of (1), (2), (3), (4) holds:

(1) $\zeta_v \neq 1$ for some $\zeta = (\zeta_v) \in H$;

(2) $v(h) > 0$, where h is the order of H;

(3) $v(m) > 0$;

(4) $(\ ,\ )_v$ is not tame.

Note that in the function field case (2), (3) and (4) do not occur.

If F is a function field, then choose an arbitrary prime v_∞ of F which is not in T, and put $U = \{v_\infty\}$. In the number field case let $U = \emptyset$.

The selection of V requires some preparation. Let $R \subset F$ be the Dedekind domain $R = \{x \in F \mid v(x) \geq 0$ for all primes $v \notin S \cup U\}$. Every prime $v \notin S \cup U$ corresponds to a prime ideal of R, denoted by P_v. For any rational prime number ℓ dividing the order h of H, consider the abelian extension $F \subset F(\eta_\ell)$, where η_ℓ denotes a primitive ℓm-th root of unity. Clearly, $F \neq F(\eta_\ell)$, and the extension $F \subset F(\eta_\ell)$ is unramified at every $v \notin S \cup T$. So for every $v \notin S \cup T \cup U$ the Artin symbol $(P_v, F(\eta_\ell)/F) \in \mathrm{Gal}(F(\eta_\ell)/F)$ is defined. By Čebotarev's density theorem, cf. [2, p.82], it assumes every value infinitely often. Hence we can choose a finite set V of primes, disjoint from $S \cup T \cup U$, such that

(5) for every rational prime ℓ dividing h there exists $u \in V$ with $(P_u, F(\eta_\ell)/F) \neq 1$.

Next, using the approximation theorem, we choose $a \in F^*$ such that

(6) $a < 0$ for every ordering of F,

(7) $v(a) = 1$ for all $v \in T$,

$v(a) = 0$ for all $v \in U$,

$a \sim 1$ at all $v \in V$

(here "$\sim$" means "close to"). We claim that this element a has the required property. Before proving this, we split the remaining primes of F in two parts:

$W = \{v \mid v \notin S \cup T \cup U \cup V,\ \ v(a) \neq 0\}$

$X = \{v \mid v \notin S \cup T \cup U \cup V,\ \ v(a) = 0\}.$

Thus, we are in the situation described by the first two columns of the table. Notice that W is finite.

Now let $\zeta = (\zeta_v) \in H$ be an arbitrary element. To prove the proposition, we must find an element $b \in F^*$ such that $\zeta = \phi(a, b)$, i. e., $\zeta_v = (a, b)_v$ for all v.

By (6) and (7) we can find, for each $v \in S \cup T$, an element $c_v \in F_v^*$ with $(a, c_v)_v = \zeta_v$, cf. [4, lemma 15.8]. Choose $c \in F^*$ close to c_v at all $v \in S \cup T$ and close to 1 at all $v \in W \cup U$. Then for $v \in X$ the tame formula tells us that $(a, c)_v$ is the unique root of unity which modulo the maximal ideal is congruent to $a^{v(c)}$. For the value of $(a, c)_v$ if $v \notin X$, see the table.

We fix, temporarily, a rational prime number ℓ dividing h. We make some choices depending on ℓ. First, using (5), choose $u \in V$ such that $(P_u, F(\eta_\ell)/F) \neq 1$. Next, choose $k \in \{0, 1\}$ such that the fractional R-ideal

$$Q = P_u^k \cdot \prod_{v \in X} P_v^{v(c)}$$

satisfies $(Q, F(\eta_\ell)/F) \neq 1$. Finally, using a generalized version of Dirichlet's theorem on primes in arithmetic progressions [2, pp. 83-84], we select a prime $w \in X$ such that

(8) $\quad P_w \cdot Q = (d)$ (as fractional R-ideals)

where d satisfies the following conditions:

(9) $\quad d > 0$ for every ordering of F,

(10) $\quad d \sim 1$ at all $v \in T$,

(11) $\quad v(d) \equiv 0 \bmod N$, where $N = m(v) \cdot [F(\eta_\ell):F]$, for all $v \in U$,

$\quad d \sim 1$ at all $v \in W$.

Then d has the properties indicated in the sixth column of the table, and $(a, d)_v$ is given by the seventh column. Also, (9), (10) and (11) imply that $((d), F(\eta_\ell)/F) = 1$, so (8) and the choice of Q give

$$(P_w, F(\eta_\ell)/F) = (Q, F(\eta_\ell)/F)^{-1} \neq 1.$$

Therefore, P_w does not split completely in the extension $F \subset F(\eta_\ell)$, which is easily seen to be equivalent to

$$m(w)/m \not\equiv 0 \bmod \ell.$$

The table tells us that $(a, c/d)_v = \zeta_v$ for all $v \neq w$, so

$$\phi(a, c/d) = \zeta \cdot \theta$$

where $\theta = (\theta_v)$ is such that $\theta_v = 1$ for all $v \neq w$. Since ζ and $\phi(a, c/d)$ are in the kernel of ψ, the same must hold for θ. That means $\theta^{m(w)/m} = 1$, so

$$\phi(a, (c/d)^{m(w)/m}) = \zeta^{m(w)/m}.$$

We conclude that for every rational prime ℓ dividing h we can find a positive integer $n(\ell) = m(w)/m$ and an element $b(\ell) = (c/d)^{n(\ell)}$ of F^* such that

$$\phi(a, b(\ell)) = \zeta^{n(\ell)}, \qquad n(\ell) \not\equiv 0 \bmod \ell.$$

Clearly, if ℓ ranges over the rational primes dividing h, the numbers $n(\ell)$ have a greatest common divisor which is relatively prime to h. Hence we can choose integers $k(\ell)$ with $\Sigma_\ell\, k(\ell)n(\ell) \equiv 1 \bmod h$, and putting $b = \Pi_\ell\, b(\ell)^{k(\ell)}$ we find

$$\phi(a, b) = \prod_\ell \phi(a, b(\ell))^{k(\ell)} = \zeta^{\Sigma\, k(\ell)n(\ell)} = \zeta.$$

This proves the proposition.

The table:

$v\in$	a	ζ_v	c	$(a,c)_v$	d	$(a,d)_v$	$(a,c/d)_v$
S	<0	$(a,c_v)_v$	$\sim c_v$	$(a,c_v)_v$	>0	1	$(a,c_v)_v$
T	$v(a)=1$	$(a,c_v)_v$	$\sim c_v$	$(a,c_v)_v$	~ 1	1	$(a,c_v)_v$
U	$v(a)=0$	1	~ 1	1	$N \mid v(d)$	1	1
V	~ 1	1	–	1	–	1	1
W	$v(a)\neq 0$	1	~ 1	1	~ 1	1	1
X	$v(a)=0$	1	–	$\equiv a^{v(c)}$	$v(d)=v(c)$ $(v\neq w)$	$\equiv a^{v(d)}$	1 $(v\neq w)$

2. <u>Proof of the theorem</u>. We preserve the notations of section 1. There is a group homomorphism

$$\lambda\colon K_2(F) \longrightarrow \bigoplus_v \mu_v$$

sending $\{a, b\}$ to $\phi(a, b)$, for $a, b \in F^*$. A theorem of Bass, Tate and Garland [1, sections 6 and 7] asserts that

(12) $\quad \mathrm{Ker}(\lambda)$ is finite.

Further, Tate [1, sec. 9, cor. to th. 9] has proved that

(13) $\quad \mathrm{Ker}(\lambda) \subset (K_2(F))^p$ for every prime number p.

From (12) and (13) it is easy to see that there exists a <u>finite</u> subgroup $A \subset K_2(F)$ such that $\mathrm{Ker}(\lambda) \subset A^p$ for each prime number p.

We turn to the proof of the theorem. Let $G \subset K_2(F)$ be a finite subgroup. Replacing G by $G\cdot A$ we may assume that

(14) $\quad \mathrm{Ker}(\lambda) \subset G^p$ for every prime number p.

By the proposition of section 1, applied to $H = \lambda(G)$, there exists $a \in F^*$ such that $\lambda(G) \subset \lambda(\{a, F^*\})$. We claim that $G \subset \{a, F^*\}$.

To prove this, let $N = \{a, F^*\} \cap G$. Then $\lambda(G) = \lambda(N)$ so $G = N\cdot\mathrm{Ker}(\lambda)$, and using (14) we find

$$(G/N) = (N\cdot\mathrm{Ker}(\lambda))/N \subset (N\cdot G^p)/N = (G/N)^p$$

for every prime number p. Thus, the finite group G/N is divisible, and consequently $G/N = \{1\}$. It follows that $G = N$, so $G \subset \{a, F^*\}$.

This concludes the proof of the theorem.

References.

1. H. BASS, K_2 des corps globaux, Sém. Bourbaki 23 (1970/71), exp. 394; Lecture Notes in Math. 244, Berlin 1971.
2. H. BASS, J. MILNOR, J.-P. SERRE, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), Pub. Math. I. H. E. S. 33 (1967), 59-137.
3. S.U. CHASE, W.C. WATERHOUSE, Moore's theorem on uniqueness of reciprocity laws, Invent. Math. 16 (1972), 267-270.
4. J. MILNOR, Introduction to algebraic K-theory, Ann. of Math. Studies 72, Princeton 1971.