Comment. Math. Helvetici 58 (1983) 038–047 0010–2571/83/001038–10$01.50 + 0.20/0

A reciprocity law for K_2-traces

SHMUEL ROSSET and JOHN TATE

Suppose $E \subset F$ is a finite field extension and let

$$\mathrm{Tr}: K_2(F) \to K_2(E)$$

be the trace map (also called transfer, see [5, §14]). If $x, y \in F^*$ and $\{x, y\}$ is the corresponding symbol in $K_2(F)$ then we know, since $K_2(E)$ is generated by symbols, that $\mathrm{Tr}_{F/E}(\{x, y\})$ can be expressed as a sum of symbols. In this paper we give an algorithm for computing such an expression explicitly (cf. the proposition in §3). The algorithm is based on a reciprocity law (§2) and involves repeated polynomial division with remainder, like the Euclidean algorithm. The proof works not only for Milnor's K_2, but for functors sufficiently like K_2, which we define in §1 and call Milnor functors. This abstraction is useful for it yields as a corollary (§3) the fact that the canonical map from K_2 to any Milnor functor commutes with traces. Another corollary is that, if $(F:E) = n$, then $\mathrm{Tr}_{F/E}(\{x, y\})$ can be written as a sum of n symbols (or less). On the other hand this is also the best bound: in §4 we give an example, using division algebras, of a symbol whose trace is not a sum of less than n symbols.

One of us (S.R) would like to thank David Saltman for a conversation which helped realize the example in section 4.

1. Milnor functors

Let K be a fixed base field and let $\mathfrak{C}$ be the category of commutative finite dimensional k-algebras.

DEFINITION. A *Milnor functor over k* is a functor $M: \mathfrak{C} \to$ (Abelian groups) together with

(i) For each $A \in \mathfrak{C}$ a bilinear map $\varphi = \varphi_A : A^* \times A^* \to M(A)$;

(ii) For each extension $A \to B$ in $\mathfrak{C}$ such that B is a projective A-module, a homomorphism $\mathrm{Tr}_{B/A}: M(B) \to M(A)$; such that the following properties hold.

(φ) The maps φ are functorial, i.e., induce a morphism of functors from the functor $A \mapsto A^* \times A^*$ to the functor $A \mapsto M(A)$, and satisfy

$$\varphi_A(a, 1-a) = 0, \quad \text{if} \quad a \in A^* \quad \text{and} \quad 1-a \in A^*,$$
$$\varphi_A(a, -a) = 0, \quad \text{if} \quad a \in A^*.$$

(Tr) if $A \to B \to C$ are $\mathfrak{C}$-morphisms such that C is projective over B and B over A, then

$$\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$$

(Tr$-\varphi$) If $A \to B$ is a $\mathfrak{C}$-morphism with B projective as A-module, and if $x \in A^*$, $y \in B^*$ then

$$\mathrm{Tr}_{B/A}\varphi_B(x, y) = \varphi_A(x, N_{B/A}y),$$

where $N_{B/A} : B^* \to A^*$ is the usual norm:

$$N_{B/A}(y) = \det \quad (\text{multiplication by } y).$$

EXAMPLE 1. Milnor's K_2; see [5] and [6].

EXAMPLE 2. Assume that the characteristic of k does not divide a given integer n and let μ_n denote the sheaf on n-th roots of 1 on the étale site over Spec A; here A is a given element in Ob ($\mathfrak{C}$). By Kummer theory

$$H^1(\operatorname{Spec} A, \mu_n) = A^*/(A^*)^n.$$

The cup product

$$H^1(\operatorname{Spec} A, \mu_n) \times H^1(\operatorname{Spec} A, \mu_n) \to H^2(\operatorname{Spec} A, \mu_n^{\otimes 2}) = M(A)$$

provides us with a context satisfying (i) and (ii). We refer to Milne's book [4] for details. The existence of a trace can probably be extracted from [7, exp. XVII]. However, this Milnor functor can be expressed entirely in terms of Galois cohomology and the trace in terms of corestriction, as follows. For $A \in \mathfrak{C}$, $\alpha \in M(A)$, and $x \in \operatorname{Spec} A$, let $\alpha(x) \in M(A/x)$ be the image of α under the residue class map $A \to A/x$. then the map

$$\alpha \mapsto (\alpha(x))_{x \in \operatorname{Spec} A}$$

gives an isomorphism

$$M(A) \xrightarrow{\sim} \prod_{x \in \operatorname{Spec} A} M(A/x). \tag{*}$$

For each $x \in \operatorname{Spec} A$, A/x is a finite extension field of k. If E is a finite extension field of k, then

$$M(E) = H^2(\operatorname{Gal}(E_s/E), \mu_n(E_s) \otimes \mu_n(E_s)),$$

where E_s is a separable algebraic closure of E. The map φ_A is characterized in terms of the isomorphism (*) by

$$(\varphi_A(a, b))(x) = \varphi_{A/x}(a(x), b(x))$$

for each $x \in \operatorname{Spec} A$, where $a(x)$ (resp. $b(x)$) is the residue mod x of a (resp. b), and for a field E the map

$$\varphi_E : E^* \times E^* \to M(E)$$

is the Galois cohomology symbol (cf. [8]) characterized by $\varphi(a, b) = da \cup db$, where $d : E^* \to H^1(\operatorname{Gal}(E_s/E), \mu_n(E_s))$ is the connecting homomorphism in the exact cohomology sequence associated with

$$0 \to \mu_n(E_s) \to E_s^* \xrightarrow{n} E_s^* \to 0.$$

Let $A \to B$ be an extension in $\mathfrak{C}$ such that B is a projective A-module. Then for each $x \in \operatorname{Spec} A$ and each $y \in \operatorname{Spec} B$ lying over x, the local ring B_y is a free A_x-module; let $r(y/x)$ denote its rank. Let $E_x = A/x$ and let F_y be the field between E_x and B/y such that F_y/E_x is separable and $(B/y)/F_y$ purely inseparable. Then the ratio

$$q(y/x) \overset{\text{defn}}{=} \frac{r(y/x)}{[F_y : E_x]}$$

is an integer, and the M-trace from B to A is characterized in terms of the isomorphism (*) by

$$(\operatorname{Tr}_{B/A}\beta)(x) = \sum_{y \mid x} q(y/x) \operatorname{cor}_{F_y/E_x}(\beta(y)),$$

where cor is the corestriction in Galois cohomology, and we identify $M(B/y)$ with $M(F_y)$ via the isomorphism induced by the inclusion $F_y \hookrightarrow B/y$.

In case $E \in \mathfrak{C}$ is a field containing a primitive n-th root of unity ζ, we can identify $M(E)$ with the group $\mathrm{Br}_n(E)$ of elements of order n in the Brauer group of E in such a way that

$$(a, b)_M = \text{the Brauer class of } A_\zeta(a, b)$$

where $A_\zeta(a, b)$ denote the cyclic algebra generated over E by elements X and Y subject to the relations

$$X^N = a, \qquad Y^n = b, \qquad XY = \zeta YX;$$

(cf. [5], p. 143).

EXAMPLE 3. The dlog symbol, see [1]. If A is a k algebra in $\mathfrak{C}$ let $\Omega^1_{A/k}$ be the A-module of Kähler differentials of A over k, and let $\Omega^2_{A/k}$ be its second exterior power. Define

$$\mathrm{dlog}: A^* \to \Omega^1_{A/k}$$

by $\mathrm{dlog}(f) = f^{-1} \cdot df$. It is simple to verify that Ω^2 and $\mathrm{dlog} \wedge \mathrm{dlog}$ satisfy axioms (i), (ii) above. The existence of a good trace is a non-trivial fact [2].

2. Reciprocity

Let M be a Milnor functor over k. In this section we shall write the M-symbol $\varphi_E(x, y)$ by

$$(x, y)_E, \quad \text{or} \quad (x, y)$$

if E is evident.

Let K be a field of finite degree over k. For relatively prime non-zero polynomials $f(T)$, $g(T)$ in $K[T]$ we define a new kind of symbol (f/g). Its values are in the group $M(K)$ and it is defined by the following requirements.

1) It is additive in g, i.e. if g_1, g_2 are both prime to f then

$$\left(\frac{f}{g_1 g_2}\right) = \left(\frac{f}{g_1}\right) + \left(\frac{f}{g_2}\right)$$

2) It is 0 if g is a constant or $g = T$.

3) If g is *monic irreducible* $\neq T$ and x is a root of $g(T)$ then

$$\left(\frac{f}{g}\right)=\mathrm{Tr}_{K(x)/K}\,(x, f(x))_{K(x)}.$$

It is clear that, thus defined, the symbol (f/g) is additive in f, as well as in g, and it depends only on the residue class of f modulo (g). As function of g it depends only on the ideal generated by g in the ring $K[T, T^{-1}]$.

To formulate the reciprocity law satisfied by (f/g) we introduce some notation: if

$$p(T)=a_nT^n+a_{n-1}T^{n-1}+\cdots+a_mT^m$$

with $a_m a_n \neq 0$. let

$$p^*(T)=(a_mT^m)^{-1}p(T)$$
$$c(p)=(-1)^n a_n.$$

Reciprocity law

$$\left(\frac{f}{g}\right)=\left(\frac{g^*}{f}\right)-(c(g^*), c(f)). \tag{**}$$

Proof. We first dispose of a few trivial cases. If g is a constant or T it is easily checked that both sides are 0, so we assume henceforth that $g(T)$ is monic irreducible $\neq T$. let x be a root of $g(T)$. If $f(T)$ is a constant c then the left side of (**) is

$$\begin{aligned}\mathrm{Tr}_{K(x)/K}\,(x, c)_{K(x)} &= (N_{K(x)/K}x, c)_k\\ &=((-1)^{\deg(g)}\cdot g(0), c)=-((-1)^{\deg(g)}\cdot g(0)^{-1}, c)\\ &=-(c(g^*), c(f))\end{aligned}$$

which is equal to the right hand side since $(g^*/f)=0$, by definition.

A similar computation using $(x, -x)=0$ works when $f(T)=T$ so we now assume that both f and g are monic irreducible, and not T.

Let x be a root of g and y a root of f. Let

$$A=K(x)\otimes_K K(y).$$

$K(x)$ and $K(y)$ are naturally imbedded in A and we identify them as such. Then the elements x, y, $x-y$ are invertible in A, indeed the norm

$$N_{A/K(x)}(x-y)=f(x)$$

is invertible, so $x-y$ is.

The identity

$$(x, x-y)=\left(y, \frac{y-x}{-x}\right)+(x, -1)$$

follows from a little computation with the relations $(u, 1-u)=(u, -u)=0$. We use it to compute the same thing in two ways

$$\begin{aligned}\mathrm{Tr}_{A/K}\,(x, x-y)&=\mathrm{Tr}_{K(x)/K}\,\mathrm{Tr}_{A/K(x)}\,(x, x-y)\\&=\mathrm{Tr}_{K(x)/K}\,(x, N_{A/K(x)}(x-y))\\&=\mathrm{Tr}_{K(x)/K}\,(x, f(x))=\left(\frac{f}{g}\right).\end{aligned}$$

$$\begin{aligned}\mathrm{Tr}_{A/K}\left(y, \frac{y-x}{-x}\right)&=\mathrm{Tr}_{K(y)/K}\,\mathrm{Tr}_{A/K(y)}\left(y, \frac{y-x}{-x}\right)\\&=\mathrm{Tr}_{K(y)/K}\left(y, \frac{N_{A/K(y)}(y-x)}{N_{A/K(y)}(-x)}\right)\\&=\mathrm{Tr}_{K(y)/K}\left(y, \frac{g(y)}{g(0)}\right)\\&=\mathrm{Tr}_{K(y)/K}\,(y, g^*(y))=\left(\frac{g^*}{f}\right).\end{aligned}$$

Finally

$$\begin{aligned}\mathrm{Tr}_{A/K}\,(x, -1)&=\mathrm{Tr}_{K(y)/K}\,\mathrm{Tr}_{A/K(y)}\,(x, -1)_A\\&=\mathrm{Tr}_{K(y)/K}\,(N_{A/K(y)}x, -1)_{K(y)}\\&=\mathrm{Tr}_{K(y)/K}\,(N_{K(x)/K}x, -1)_{K(y)}\\&=(c(g^*)^{-1}, (-1)^{\deg(f)})=-(c(g^*), c(f)).\end{aligned}$$

Here we used the obvious fact that

$$N_{A/K(y)}(x)=N_{K(x)/K}(x).$$

This completes the proof of the reciprocity law.

3. Consequences

Let $E \subset F$ be a finite extension of fields finite over k, and let $x, y \in F^*$. Then

$$\mathrm{Tr}_{F/E}\,(x, y) = \left(\frac{f}{g}\right)$$

where $g(T) \in E[T]$ is the monic irreducible polynomial with root x and $f(T) \in E[T]$ is the polynomial of smallest degree such that $N_{F/E(x)}y = f(x)$.

PROPOSITION. *Let $g_0, g_1, \ldots, g_m \neq 0$, $g_{m+1} = 0$ be the sequence of polynomials defined by:*

$$g_0 = g, \qquad g_1 = f,$$

and for $i \geq 1$

$$g_{i+1} = \textit{the remainder of the division of } g^*_{i-1} \textit{ by } g_i,$$

as long as $g_i \neq 0$. We have then

$$1 \leq m \leq \deg g = [E(x):E] \leq [F:E]$$

and

$$\mathrm{Tr}_{F/E}\,(x, y) = -\sum_{i=1}^{m} (c(g^*_{i-1}), c(g_i)).$$

By the reciprocity law, we find by induction on j, using $(g^*_{i-1}/g_i) = (g_{i+1}/g_i)$:

$$\left(\frac{g_1}{g_0}\right) = -\sum_{i=1}^{j} (c(g^*_{i-1}), c(g_i)) + \left(\frac{g^*_{j-1}}{g_j}\right)$$

for $1 \leq j \leq m$. But the last non-zero polynomial g_m is a constant because it divides the relatively prime polynomials g_0 and g_1. Hence $(g^*_{m-1}/g_m) = 0$, and the proposition follows on putting $j = m$; We have $m \leq \deg g$ because the degrees of the polynomials in the sequence are strictly decreasing, and $m \geq 1$ because $f \neq 0$.

COROLLARY 1. *If $[F:E] = r$ and $x, y \in F^*$, then* $\mathrm{Tr}_{F/E}\,(x, y)$ *is a sum of at most r symbols.*

The sequence of polynomials in the proposition depends only on F, E, x, and y, not on the Milnor functor M. Thus the trace of a symbol $(x, y)_M$ has an expression as a sum of symbols which is *independent of the Milnor functor M;* on symbols, the trace is uniquely determined. Any morphism $M_1 \to M_2$ of Milnor functors which carries each symbol $(a, b) \in M_1(A)$ to the "same" symbol $(a, b) \in M_2(A)$ must therefore commute with $\mathrm{Tr}_{F/E}$ on symbols. In particular, letting $R_F : K_2(F) \to M(F)$ be the homomorphism (whose existence and unicity are guaranteed by Matsumoto's theorem) such that $R_F(\{a, b\}) = (a, b)_M$ for $a, b \in F^*$, and similarly R_E, we have

COROLLARY 2. *The diagram*

$$\begin{tikzcd} K_2 \arrow[r, "R_F"] \arrow[d, "\mathrm{Tr}_{F/E}"'] & M(F) \arrow[d, "\mathrm{Tr}_{F/E}"] \\ K_2(E) \arrow[r, "R_E"'] & M(E) \end{tikzcd}$$

is commutative.

4. An example

We have just proved that if $[F:E] = r$ and $x, y \in F^*$ then $\mathrm{Tr}_{F/E}\,(x, y)$ is a sum of r symbols. Yet it is known that in some cases, e.g. global or local fields, every element of K_2 (say) is a symbol [8, 3], so it is well to give an example where $\mathrm{Tr}\,(x, y)$ cannot be written as a sum of fewer than r symbols. For this it will suffice to work with the functor of Example of Section 1.

Let $n \geq 2$ and $r \geq 1$ be integers. Let k_0 be a field containing a primitive n-th root of unity, ζ. Let $u_1, v_1, \ldots, u_r, v_r$ be $2r$ independent variable over k_0 and let

$$F = k_0(u_1, v_1; u_2, v_2; \ldots ; u_r, v_r)$$

be the field they generate. Let M be the Milnor functor of Example 2.

LEMMA. *The element $\beta = \sum_{i=1}^{r} (u_i, v_i)$ in $M(F)$ is not a sum of fewer than r symbols.*

Proof. We use the identification $M(F) \xrightarrow{\sim} \mathrm{Br}_n\,(F)$ discussed at the end of

Example 2. For $1 \leq i \leq r$ let B_i by the cyclic algebra over F generated by elements X_i and Y_i subject to the relations

$$X_i^n = u_i, \qquad Y_i^n = v_i, \qquad X_i Y_i = \zeta Y_i X_i,$$

so that (u_i, v_i) is the Brauer class of B_i. Then β is the Brauer class of $B = \otimes_{i=1}^r B_i$, an algebra of dimension n^{2r} over F. We will show B is a division algebra. This will prove the lemma, for it shows that β cannot be the Brauer class of an algebra of dimension less than n^{2r}, and consequently cannot be a sum of fewer than r symbols.

If B were not a division algebra it would have zero divisors, and multiplying these zero divisors by a common denominator of their coefficients in F relative to the basis

$$\{X_1^{l_1} Y_1^{m_1} \cdots X_r^{l_r} Y_r^{m_r}\} \quad (0 \leq l_i, m_i < n)$$

for B over F, we would find zero divisors in the ring

$$R = k_0[u_1, v_1, \ldots, u_r, v_r][X_1, Y_1, \ldots, X_r, Y_r] = k_0[X_1, y_1, \ldots, X_r, Y_r].$$

But this ring has no zero divisors, for it has a basis over k_0 consisting of the monomials

$$X_1^{l_1} Y_1^{m_1} \cdots X_r^{l_r} Y_r^{m_r}$$

with l_i, m_i integers ≥ 0, and the product of two such monomials is a power of ζ times the monomial obtained by adding exponents. Hence, if we order the monomials by the lexicographical order of their exponent sequences, the product of two non-zero polynomials will contain the product of the highest terms in the two factors with a non-zero coefficient, so will not be 0. This proves the lemma.

Let σ be the automorphism of F which is identity on k_0 and acts on the variables by

$$\begin{aligned} \sigma u_i &= u_{i+1}, \qquad 1 \leq i \leq r; \qquad u_{r+1} = u_1, \\ \sigma v_i &= v_{i+1}, \qquad 1 \leq i \leq r; \qquad v_{r+1} = v_1. \end{aligned}$$

Let G be the cyclic group of order r generated by σ, and let $E = F^G$.

PROPOSITION. *The image of* $\{u_1, v_1\}$ *under* $\mathrm{Tr}_{F/E} : K_2F \to K_2E$ *is not a sum of fewer than r symbols.*

Proof. We use the commutativity of

$$\begin{tikzcd} K_2(F)/nK_2(F) \arrow[r, "R_F"] \arrow[d, "\mathrm{Tr}"'] & \mathrm{Br}_n\,(F) \arrow[d, "\mathrm{Tr}"] \\ K_2(E)/nK_2(E) \arrow[r, "R_E"'] & \mathrm{Br}_n\,(E). \end{tikzcd}$$

and the rule

$$\mathrm{res}_{E/F}\,\mathrm{Tr}_{F/E}\,\alpha = \sum_{\tau\in G} \tau\alpha$$

for $\alpha \in \mathrm{Br}\,F$. If $\mathrm{Tr}\,\{u_1, v_1\}$ were a sum of $s<r$ symbols so also would be

$$\begin{aligned}\mathrm{res}\,R_E\,\mathrm{Tr}\,\{u_1, v_1\} &= \mathrm{res}\,\mathrm{Tr}\,R_F\{u_1, v_1\} = \mathrm{res}\,\mathrm{Tr}\,(u_1, v_1)\\ &= \sum_{\tau\in G} \tau(u_1, v_1) = \sum_{i=1}^{r} (u_i, v_i) = \beta,\end{aligned}$$

contradicting the lemma.

REFERENCES

[1] BLOCH, S., *K_2 and algebraic cycles.* Ann. Math. *99* (1974), 349–379.
[2] HARTSHORNE, R., *Residues and Duality*, Springer Lecture notes #20 (1966).
[3] LENSTRA, H. W., *K_2 of global fields consists of symbols*, in *Algebraic K-theory* Evanston 1976, Springer Lecture notes #551, pp. 69–73.
[4] MILNE, J. S., *Etale Cohomology*, Princeton Univ. Press, 1980.
[5] MILNOR, J., *Introduction to algebraic K-theory*, Ann. Math. Studies #72, Princeton, 1971.
[6] QUILLEN, D., *Higher algebraic K-theory I*, in *Algebraic K-theory I*, Springer Lecture notes #341, 1973.
[7] SGA 4, Tome 3, Springer Lecture notes #305, 1972.
[8] TATE, J., *Relations between K_2 and Galois cohomology*, Inv. Math. *36* (1976), 257–274.

Dept. of Mathematical Sciences
Tel-Aviv University
Tel-Aviv, Israel
and
Dept. of Mathematics
Harvard University
Cambridge, MA 02138, USA

Received August 18, 1982