PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 128, Number 1, Pages 27–29
S 0002-9939(99)05101-1
Article electronically published on June 30, 1999

ON A THEOREM BY SERRE

ARNE LEDET

(Communicated by Ronald M. Solomon)

ABSTRACT. We present a short proof of a theorem by Serre on the trace form of a finite separable field extension.

Let M/K be a finite Galois extension in characteristic $\neq 2$, and assume that M is the splitting field over K of an irreducible polynomial $f(X) \in K[X]$ of degree n. We embed the Galois group $G = \mathrm{Gal}(M/K)$ transitively into S_n by considering the elements of G as permutations of the roots of $f(X)$. From the 'positive' double cover

$$1 \to \mu_2 \to \widetilde{S}_n^+ \to S_n \to 1$$

of S_n (i.e., the double cover in which transpositions lift to elements of order 2) we then get an extension

$$(*) \qquad 1 \to \mu_2 \to \widetilde{G}^+ \to G \to 1$$

of G with the cyclic group $\mu_2 = \{\pm 1\}$. Let $\gamma^+ \in H^2(G, \mu_2)$ be the characteristic class of $(*)$.

We embed S_n into the orthogonal group $O_n(\bar{K}_{\mathrm{sep}})$ as permutations of the standard basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_n \in \bar{K}_{\mathrm{sep}}^n$. ($\bar{K}_{\mathrm{sep}}$ being the separable closure of K.) As the pre-image in the Clifford group $C_n^*(\bar{K}_{\mathrm{sep}})$ of a transposition $(i\,j)$, $i < j$, we can then take the element $x_{ij} = (\mathbf{e}_i - \mathbf{e}_j)/\sqrt{2}$. The subgroup of $C_n^*(\bar{K}_{\mathrm{sep}})$ generated by these is exactly the double cover $\widetilde{S}_n^+$ of S_n, and we get a diagram

$$\begin{array}{ccccccccc}
 & & & & & & \mathrm{Gal}(K) & & \\
 & & & & & & \big\downarrow \mathrm{res} & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{G}^+ & \longrightarrow & G & \longrightarrow & 1 \\
 & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{S}_n^+ & \longrightarrow & S_n & \longrightarrow & 1 \\
 & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\
1 & \longrightarrow & \bar{K}_{\mathrm{sep}}^* & \longrightarrow & C_n^*(\bar{K}_{\mathrm{sep}}) & \longrightarrow & O_n(\bar{K}_{\mathrm{sep}}) & \longrightarrow & 1,
\end{array}$$

Received by the editors March 7, 1998.
1991 *Mathematics Subject Classification.* Primary 12G05.
This work was supported by a Queen's University Advisory Research Committee Postdoctoral Fellowship.

where $\mathrm{Gal}(K) = \mathrm{Gal}(\bar{K}_{\mathrm{sep}}/K)$ is the absolute Galois group of K. The last row of this diagram is a short-exact sequence of G-groups, inducing a connecting map $\delta : H^1(\mathrm{Gal}(K), O_n(\bar{K}_{\mathrm{sep}})) \to H^2(\mathrm{Gal}(K), \bar{K}^*_{\mathrm{sep}})$, cf. [Se1], and we know from [Sp] that the image of the crossed homomorphism $e : \mathrm{Gal}(K) \to O_n(\bar{K}_{\mathrm{sep}})$ in the last column of the diagram is the Hasse-Witt invariant of the quadratic form obtained from $\langle 1, \dots, 1\rangle$ by Galois twist with e. The *Hasse-Witt invariant* of a regular quadratic form $q \sim \langle a_1, \dots, a_n\rangle$ is

$$\mathrm{hw}(q) = \prod_{i<j} (a_i, a_j) \in H^2(\mathrm{Gal}(K), \bar{K}^*_{\mathrm{sep}}),$$

where the elements $(a_i, a_j) \in H^2(\mathrm{Gal}(K), \bar{K}^*_{\mathrm{sep}})$ are *quaternion symbols*: For $a, b \in K^*$ the quaternion symbol (a, b) is represented by the factor system $(\sigma, \tau) \mapsto (-1)^{\chi_a(\sigma)\chi_b(\tau)}$, where $\chi_a, \chi_b : \mathrm{Gal}(K) \to \mathbb{F}_2$ are the homomorphisms with kernels $\mathrm{Gal}(K(\sqrt{a}))$ and $\mathrm{Gal}(K(\sqrt{b}))$, resp.

Now, let $L = K(\theta)$, where θ is a root of $f(X)$, and let $\theta_1 = \theta, \theta_2, \dots, \theta_n \in M$ be the conjugates. This numbering fixes our embedding of G into S_n. The Galois twist corresponding to e above is obtained by restricting $\langle 1, \dots, 1\rangle$ from $\bar{K}^n_{\mathrm{sep}}$ to the space of fixed points under the G-action ${}^\sigma\mathbf{x} = e_\sigma(\sigma\mathbf{x})$. It is easy to see that the fixed points are exactly the points

$$(g(\theta_1), \dots, g(\theta_n)), \quad g(X) \in K[X],$$

meaning that the twisted quadratic space is L equipped with the *trace form* $q_L : x \mapsto \mathrm{Tr}_{L/K}(x^2)$.

We compute $\delta(e)$ directly as follows: Let $s_\sigma \in \widetilde{G}^+$ be a pre-image of $\sigma \in G$. Then $s_{\mathrm{res}\,\sigma} \in C_n^*(\bar{K}_{\mathrm{sep}})$ is a pre-image of $e_\sigma \in O_n(\bar{K}_{\mathrm{sep}})$ for $\sigma \in \mathrm{Gal}(K)$, and $\delta(e)$ is given by the factor system

$$(\sigma, \tau) \mapsto s_{\mathrm{res}\,\sigma}\, \sigma s_{\mathrm{res}\,\tau}\, s^{-1}_{\mathrm{res}\,\sigma\,\tau} = (-1)^{\chi_2(\sigma)\chi_d(\tau)} s_{\mathrm{res}\,\sigma}\, s_{\mathrm{res}\,\tau}\, s^{-1}_{\mathrm{res}\,\sigma\,\tau}, \quad \sigma, \tau \in \mathrm{Gal}(K),$$

where $d = d_{L/K}$ is the discriminant of L/K, since σ operates on $s_{\mathrm{res}\,\tau}$ through the factor $1/\sqrt{2}$ contributed by each transposition. Here, $(\sigma, \tau) \mapsto s_{\mathrm{res}\,\sigma}\, s_{\mathrm{res}\,\tau}\, s^{-1}_{\mathrm{res}\,\sigma\tau}$ is the inflation of γ^+ to $H^2(\mathrm{Gal}(K), \bar{K}^*_{\mathrm{sep}})$, and $(\sigma, \tau) \mapsto (-1)^{\chi_2(\sigma)\chi_d(\tau)}$ is the quaternion symbol $(2, d)$. Hence, we have

Theorem (Serre, [Se2])**.** *With notation as above,*

$$\inf_{G \to \mathrm{Gal}(K)}(\gamma^+) = \mathrm{hw}(q_L) \cdot (2, d_{L/K}) \in H^2(\mathrm{Gal}(K), \bar{K}^*_{\mathrm{sep}}).$$

If we look instead at the 'negative' double cover

$$1 \to \mu_2 \to \widetilde{S}_n^- \to S_n \to 1$$

of S_n, where transpositions lift to elements of order 4, we get an extension

$$(**) \qquad 1 \to \mu_2 \to \widetilde{G}^- \to G \to 1$$

of G with μ_2. Let $\gamma^- \in H^2(G, \mu_2)$ be the characteristic class of $(**)$. The elements $y_{ij} = (\mathbf{e}_i - \mathbf{e}_j)/\sqrt{-2} \in C_n(\bar{K}^*_{\mathrm{sep}})$, $i < j$, generate a copy of $\widetilde{S}_n^-$ mapping onto $S_n \subseteq O_n(\bar{K}_{\mathrm{sep}})$, and we can repeat the entire argument above with -2 instead of 2,[1] getting

[1]The author would like to thank the referee for suggesting this modified argument.

Theorem. *With notation as above,*

$$\inf_{G\to \mathrm{Gal}(K)}(\gamma^-) = \mathrm{hw}(q_L)\cdot(-2, d_{L/K}) \in H^2(\mathrm{Gal}(K), \bar{K}^*_{sep}).$$

References

[Se1] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics 5, Springer-Verlag, 1973. MR **53:**8030

[Se2] ———, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comm. Math. Helv. **59** (1984), 651–676. MR **86k:**11067

[Sp] T. A. Springer, *On the Equivalence of Quadratic Forms*, Proc. Neder. Acad. Sci. **62** (1959), 241–253. MR **21:**7184

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

E-mail address: ledet@mast.queensu.ca