Remarks

REMARKS

There are several proofs and several formulations of this result ($S(K)$ when K is dyadic) in the literature. We shall briefly indicate why these formulations are, with one exception, equivalent to the above one.

1. *T. Yamada*, [*Y*], *p. 88*. One formulation of Yamada's theorem is that *$S(K)$ is non-trivial iff there is a root of unity ζ such that the inertia group of the extension $\mathbf{Q}_2(\zeta)/K$ is non-cyclic.* The inertia group of $\mathbf{Q}_2(\zeta)/K$ is the image of the inertia group of $\mathcal{G}(\mathbf{Q}_2^c/K)$, namely $\mathcal{G}(\mathbf{Q}_2^c/K_{nr})$. The latter group is of the form $\hat{\mathbf{Z}}_2 \times (\mathbf{Z}/2)$ or $\hat{\mathbf{Z}}_2$, depending on whether or not $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$. If $\sigma_{-1} \notin \mathcal{G}(\mathbf{Q}_2^c/K)$, then it follows that the inertia group of $\mathbf{Q}_2(\zeta)/K$ is always cyclic. Suppose $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$. Then $\mathcal{G}(\mathbf{Q}_2^c/K_{nr}) = \hat{\mathbf{Z}}_2 \times \mathbf{Z}/2$ where the first factor is topologically generated by $\sigma_5^{2^k}$ for some $k \geqslant 0$ and $\mathbf{Z}/2$ is generated by σ_{-1}. If we choose ζ to have order divisible by a power of 2 large enough so that $\sigma_5^{2^k}(\zeta) \neq \zeta$, then it is clear that the inertia subgroup of $\mathbf{Q}_2(\zeta)/K$ is not cyclic. Thus the inertia group of $\mathbf{Q}_2(\zeta)/K$ is non-cyclic iff $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$, and so Yamada's criterion is equivalent to mine.

2. *U. Fontaine*, [*F*], *Cor. 2′, p. 138.* The result is: *$S(K)$ is non-trivial iff $\varepsilon_4 \notin K$.* This is easily seen to be inequivalent to the other formulations. As an example, let K be the subfield of $\mathbf{Q}_2(\varepsilon_{16})$ fixed by the automorphism $\sigma_{-1}\sigma_5^2$. Then $\varepsilon_4 \notin K$ and $\sigma_{-1} \notin \mathcal{G}(\mathbf{Q}_2^c/K)$.

3. *G. J. Janusz*, [*J*], *p. 543.* Let h be the smallest integer $\geqslant 2$ such that there is an odd integer $c \geqslant 1$ with the property that $\mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_c)$ contains K. Then Janusz' theorem is the following:

$S(K)$ is non-trivial iff there is an odd integer n with the following properties:

(i) *$K(\varepsilon_4)/K$ is ramified.*

(ii) $K(\varepsilon_{4n}) = \mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_n)$.

(iii) $(K(\varepsilon_n): K) = 2^r w$, *where w is odd and $r \geqslant 1$.*

(iv) *The automorphism of order 2 in $\mathcal{G}(K(\varepsilon_{4n})/K(\varepsilon_n))$ carries ε_{2^h} to $\varepsilon_{2^h}^{-1}$.*

(v) *If $r \leqslant h-1$, then any root of unity in $K(\varepsilon_{4n})$ whose order divides 2^{h-r+1} already lies in $K(\varepsilon_4)$.*

It can be shown that the conditions (iii) and (v) can be omitted. Indeed suppose that we are given an odd integer n such that (i), (ii), and (iv) are satisfied. Let the the residue class field of $K(\varepsilon_n)$ have 2^k elements. Set $n' = (2^k)^{2^h} - 1$. Then $n \mid n'$, n' is odd, and $K(\varepsilon_{n'})/K(\varepsilon_n)$ is unramified of degree 2^h. Consider the conditions (i)-(v) with n' instead of n. Then (i) is unchanged, (ii) holds because $n \mid n'$, (iii) holds trivially and (v) holds vacuously because $2^h \mid (K(\varepsilon_{n'}) \colon K)$. Finally $K(\varepsilon_{n'}) \cap K(\varepsilon_4) = K$ since one is ramified and the other is not, so the non-trivial automorphism of $K(\varepsilon_{4n})/K(\varepsilon_n)$ is the restriction of that of $K(\varepsilon_{4n'})/K(\varepsilon_{n'})$, so (iv) holds also for n'.

We can deduce from this abbreviated form of Janusz' theorem that it is equivalent to Yamada's. Suppose that Janusz' conditions are satisfied, and consider the extension $\mathbf{Q}_2(\varepsilon_{2^{h+1}}, \varepsilon_n)/K$. The inertia subgroup of its Galois group is $\mathscr{g} = \mathscr{G}(\mathbf{Q}_2(\varepsilon_{2^{h+1}}, \varepsilon_n)/K(\varepsilon_n))$, a group of order 4. Suppose that ρ is an extension of the non-trivial automorphism of $\mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_n)/K(\varepsilon_n)$ to $\mathbf{Q}_2(\varepsilon_{2^{h+1}}, \varepsilon_n)$, so $\rho \in \mathscr{g}$. By condition (iv), there is an integer $a \equiv -1 \pmod{2^h}$ such that $\rho(\varepsilon_{2^{h+1}}) = \varepsilon_{2^{h+1}}^a$. It follows that ρ^2 is the identity. Thus $\mathscr{g}$ is non-cyclic. Conversely suppose that there is an extension $\mathbf{Q}_2(\zeta)/K$ whose inertia subgroup $\mathscr{g}$ is non-cyclic. As we saw in 1., this means that σ_{-1} is in the Galois group of $\mathbf{Q}_2^c/K$ and so its restriction (which we also call σ_{-1}) is in $\mathscr{G}(\mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_c)/K)$ and is non-trivial. Its fixed field contains $K(\varepsilon_c)$; by Lemma 3.3 of [J], $K(\varepsilon_c, \varepsilon_4) = \mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_c)$ and so the fixed field is *exactly* $K(\varepsilon_c)$. Thus both (iv) and (ii) are also fulfilled. (i) holds by Lemma 1.

4. *F. Lorenz*, [*L*], *p. 463*. His condition for *non-triviality of* $S(K)$ is that -1 *is a norm in the extension* $K/\mathbf{Q}_2$. The norm residue symbol in the extension $\mathbf{Q}_2^c/\mathbf{Q}_2$ sends -1 to $\sigma_{-1} \in \mathscr{G}(\mathbf{Q}_2^c/\mathbf{Q}_2)$. Thus it follows from [S], pp. 204-205, that -1 is a norm in $K/\mathbf{Q}_2$ iff $\sigma_{-1} \in \mathscr{G}(\mathbf{Q}_2^c/K)$.

REFERENCES

[C-F] Cassels, J. W. S. and A. Frohlich. *Algebraic Number Theory*. Thompson Book Co. Inc., Washington (1967).

[F] Fontaine, J.-M. Sur la décomposition des algèbres de groupes. *Ann. Sc. Ec. Norm. Sup. 49* (1971), 121-180.

[H] Hasse, H. *Zahlentheorie*, 2nd ed. Akademie-Verlag, Berlin, 1963.

[I] Isaacs, I. M. *Character Theory of Finite Groups*. Academic Press, New York (1976).