96. Cyclotomic Algebras over a 2-adic Field

By Toshihiko YAMADA
Department of Mathematics, Tokyo Metropolitan University

(Comm. by Kenjiro SHODA, M. J. A., June 12, 1973)

1. Let K be a finite extension of Q_2, the rational 2-adic numbers. E. Witt [5] proved that the order of the Schur subgroup $S(K)$ of the Brauer group $Br(K)$ is 1 or 2. So, given any finite extension K of Q_2, we must tell whether $S(K)=1$ or $S(K)$ is the subgroup of $Br(K)$ of order 2. This problem was completely settled by the author [3]. The purpose of the present paper is to outline another proof of the result. (The details will appear in the lecture note [4].) The idea of the new proof is the same as the one devised by the author in [1], where for any finite extension K of the rational p-adic numbers Q_p, p being any odd prime, the Schur subgroup $S(K)$ was determined.

Notation. For a positive integer n, ζ_n is a primitive nth root of unity. Let $L \supset k$ be extensions of Q_p such that L/k is normal. Then $G(L/k)$ is the Galois group of L over k. $e_{L/k}$ (resp. $f_{L/k}$) denotes the ramification index (resp. the residue class degree) of L/k.

2. Throughout this paper, k denotes a cyclotomic extension of Q_2. Let B be a *cyclotomic algebra* over k:

$$B=(\beta, k(\zeta)/k)=\sum_{\sigma \in G} k(\zeta)u_\sigma \text{ (direct sum)}, \qquad (u_1=1),$$
$$u_\sigma u_\tau=\beta(\sigma,\tau)u_{\sigma\tau}, \quad u_\sigma x = x^\sigma u_\sigma \qquad (x \in k(\zeta)),$$

where ζ is a root of unity, $G=G(k(\zeta)/k)$, and β is a factor set of $k(\zeta)/k$ such that the values of β are roots of unity in $k(\zeta)$. Let $L=Q_2(\zeta')$ be a cyclotomic field containing $k(\zeta)$, ζ' being some root of unity. Let Inf denote the inflation map from $H^2(k(\zeta)/k)$ into $H^2(L/k)$. Then $B \sim (\mathrm{Inf}\,(\beta), L/k)$. Thus we always assume that any cyclotomic algebra B over k is of the form: $B=(\beta, L/k)$, L being a cyclotomic field over Q_2. We can write $L=Q_2(\zeta_{2^n}, \zeta_r)$, $r=2^a-1$, where $a=f_{L/Q_2}$ and n is some non-negative integer. If $n \leq 1$, then $B \sim 1$, because the extension L/k is unramified and the factor set β consists of roots of unity. So we assume $n \geq 2$. We have $\beta(\sigma,\tau)=\alpha(\sigma,\tau)\gamma(\sigma,\tau)$, $\alpha(\sigma,\tau) \in \langle \zeta_{2^n} \rangle$, $\gamma(\sigma,\tau) \in \langle \zeta_r \rangle$, for any σ, τ of $G(L/k)$, whence $(\beta, L/k) \sim (\alpha, L/k) \otimes_k (\gamma, L/k)$.

Proposition 1 (Witt [5, pp. 242–243]). $(\gamma, L/k) \sim 1$.

Remark. The result can also be proved by the techniques that will be developed in this paper. (See [4].) Another proof was already given in [3].

Thus we only need to study the following type of cyclotomic algebra:

$$B=(\beta, L/k), \quad L=Q_2(\zeta_{2^n}, \zeta_r), \quad n\geq 2, \quad r=2^a-1, \qquad (1)$$
$$\beta(\sigma, \tau)\in\langle\zeta_{2^n}\rangle \qquad (\sigma, \tau\in G(L/k)).$$

For the remainder of this section, we assume $n\geq 3$. Let $\mathfrak{H}_0$ denote the inertia group of L/Q_2. Then, $\mathfrak{H}_0=\langle\theta\rangle\times\langle\iota\rangle$, $\theta^{2^{n-2}}=\iota^2=1$, where

$$\zeta_{2^n}^{\theta}=\zeta_{2^n}^{5}, \qquad \zeta_{2^n}^{\iota}=\zeta_{2^n}^{-1}, \qquad (2)$$

$\zeta_r^{\theta}=\zeta_r^{\iota}=\zeta_r$. A Frobenius automorphism ξ of L/Q_2 is given by $\zeta_r^{\xi}=\zeta_r^2$, $\zeta_{2^n}^{\xi}=\zeta_{2^n}$. The subgroups of $\mathfrak{H}_0$ are classified into three types: (i) $\langle\theta^{2^\lambda}\rangle\times\langle\iota\rangle$, (ii) $\langle\theta^{2^\lambda}\rangle$, $(\lambda=0, 1, \cdots, n-2)$, (iii) $\langle\iota\theta^{2^\nu}\rangle$, $(\nu=0, 1, \cdots, n-3)$. Let $\mathfrak{H}$ denote the inertia group of L/k. Then $\mathfrak{H}=\mathfrak{H}_0\cap G(L/k)$, so $\mathfrak{H}$ is in one of the above three types.

Theorem 1. *Notation being as above, if $\mathfrak{H}=\langle\theta^{2^\lambda}\rangle$ $(0\leq\lambda\leq n-2)$, or if $\mathfrak{H}=\langle\theta^{2^\nu}\iota\rangle$ $(0\leq\nu\leq n-3)$, then $B=(\beta, L/k)\sim 1$.*

Before proving the theorem, we will represent a lemma which was one of the ideas in [1].

Lemma 1 (Yamada [1]). *Let p be a prime number and Q_p the field of rational p-adic numbers. Let $\Lambda\supset K$ be finite extensions of Q_p such that Λ/K is normal. Set $e=e_{\Lambda/K}$, $f=f_{\Lambda/K}$. Let z be a natural number divisible by $ef=[\Lambda: K]$ and let Ω be the unramified extension of K of degree z. Set $\Lambda'=\Lambda\cdot\Omega$. Then $e_{\Lambda'/K}=e$ and $f_{\Lambda'/K}=z$. Furthermore, there is a totally ramified extension F of K in Λ' of degree e so that $F\cdot\Omega=\Lambda'$ and $F\cap\Omega=K$. That is, there exists a Frobenius automorphism φ of Λ'/K of order z. The inertia group of Λ'/K is canonically isomorphic to that of Λ/K.*

Proof (The reader should refer [1, p. 302]). Since an unramified extension is uniquely determined by its degree, it follows that $[\Omega\cap\Lambda: K]=f$. Hence $\Lambda'=\Lambda\cdot\Omega$ is normal over K of degree ze, Λ'/Ω is totally ramified of degree e, and Λ'/Λ is unramified of degree z/f. Set $G(\Lambda'/K)=G$, $G(\Lambda'/\Lambda)=H$, and $G(\Lambda'/\Omega)=H_1$. Then $H\cap H_1=1$, $|G/H|=ef$, and $|G/H_1|=z$. This implies that for any element σ of G, σ^z belongs to $H\cap H_1=1$, i.e. $\sigma^z=1$. The assertions of the lemma easily follow.

Proof of Theorem 1. Keeping the notation of Theorem 1, we apply Lemma 1 to the extension L/k. Recall that $L=Q(\zeta_{2^n}, \zeta_r)$, $r=2^a-1$, $G(L/Q_2)=\langle\theta\rangle\times\langle\iota\rangle\times\langle\xi\rangle$. Put $e=e_{L/k}$, $f=f_{L/k}$. Denote by Ω the unramified extension of k of degree ef and set $L'=L\cdot\Omega=Q_2(\zeta_{2^n}, \zeta_{r'})$, $r'=2^{ae}-1$. Then Lemma 1 implies that there exists a totally ramified extension F of k of degree e such that $F\cdot\Omega=L'$, $F\cap\Omega=k$, and $G(L'/\Omega)$ is canonically isomorphic to $\mathfrak{H}$, the inertia group of L/k. We can describe the circumstances more explicitly. We may obviously write $G(L'/Q_2)=\langle\theta\rangle\times\langle\iota\rangle\times\langle\xi'\rangle$, where θ and ι are defined by (2) with $\zeta_{r'}^{\theta}=\zeta_{r'}^{\iota}=\zeta_{r'}$, and $\zeta_{r'}^{\xi'}=\zeta_{r'}^2$, $\zeta_{2^n}^{\xi'}=\zeta_{2^n}$. Let $\mathfrak{H}'$ denote the inertia group of L'/k. If $\mathfrak{H}=\langle\theta^{2^\lambda}\rangle\subset G(L/k)$ then $\mathfrak{H}'=\langle\theta^{2^\lambda}\rangle\subset G(L'/k)$. Also, if $\mathfrak{H}=\langle\theta^{2^\nu}\iota\rangle$ then

$\mathfrak{H}'=\langle\theta^{2^\lambda}\iota\rangle$. Put $f'=f_{k/Q_2}$. $(f'f=a)$. Let η be a Frobenius automorphism of L/k. Regarding η as an automorphism of L/Q_2, we write $\eta=\xi^{f'}\theta^x\iota^y$, for some integers x, y. Then, $\eta'=(\xi')^{f'}\theta^x\iota^y$ is a Frobenius automorphism of L'/k and $(\eta')^{ef}=1$, $(ef=f_{L'/k})$. Hence $G(L'/k)=\mathfrak{H}'\times\langle\eta'\rangle$. Note that $B=(\beta, L/k)\sim(\mathrm{Inf}\,(\beta), L'/k)$, where Inf denotes the inflation map of $H^2(L/k)$ into $H^2(L'/k)$. Therefore, in order to prove Theorem 1 we may assume that the extension L/k has a Frobenius automorphism η of order f, $f=f_{L/k}$, so that $G(L/k)=\mathfrak{H}\times\langle\eta\rangle$. As is remarked above, we write $\eta=\xi^{f'}\theta^x\iota^y$, $(y=0,1)$.

(i) The case $\mathfrak{H}=\langle\theta^{2^\lambda}\rangle$, $(0\leq\lambda\leq n-2)$. Suppose first that $y=1$, so $\eta=\xi^{f'}\theta^x\iota$. Set $\tau=\theta^{2^\lambda}$. We have $B=(\beta, L/k)=\sum Lu_\sigma=\sum_{i=0}^{e-1}\sum_{j=0}^{f-1}Lu_\tau^i u_\eta^j$, $e=2^{n-2-\lambda}$. Let $\beta(\tau,\eta)/\beta(\eta,\tau)=\zeta_{2^n}^b$, so $u_\tau u_\eta=\zeta_{2^n}^b u_\eta u_\tau$. Since $u_\tau u_\tau^e u_\tau^{-1}=u_\tau^e$, we have $u_\tau^e=\zeta_{2^{\lambda+2}}^c$ for some integer c. It follows from the relation [2, (1.11)] that

$$\zeta_{2^{\lambda+2}}^{cA}=(\zeta_{2^{\lambda+2}}^c)^{\eta-1}=(\zeta_{2^n}^{-b})^{1+\tau+\cdots+\tau^{e-1}}=\zeta_{2^n}^{-bS}, \tag{3}$$

where $A=-5^x-1$ and $S=1+5^{2^\lambda}+\cdots+(5^{2^\lambda})^{e-1}=(1-5^{2^{n-2}})/(1-5^{2^\lambda})$. S (resp. A) is exactly divisible by $2^{n-2-\lambda}$ (resp. 2). By (3) we conclude that $2|b$. Let Y be an integer satisfying $AY\equiv b\pmod{2^n}$. (Since $(2, A/2)=1$ and $2|b$, such an integer Y does exist.) Then $u_\eta(\zeta_{2^n}^Y u_\tau)=\zeta_{2^n}^{-5^xY-b}u_\tau u_\eta=(\zeta_{2^n}^Y u_\tau)u_\eta$. Let E (resp. F) be the subfield of L over k corresponding to $\langle\tau\rangle$ (resp. $\langle\eta\rangle$) in the sense of Galois theory. We have $B=\sum_i\sum_j E\cdot F(\zeta_{2^n}^Y u_\tau)^i u_\eta^j\simeq(u_\eta^f, E/k, \eta)\otimes_k((\zeta_{2^n}^Y u_\tau)^e,\ F/k, \tau)\sim(\pm 1, F/k, \tau)$, because $u_\eta^f=\pm 1$, $(\zeta_{2^n}^Y u_\tau)^e=\zeta_{2^n}^{Y(1+\tau+\cdots+\tau^{e-1})}\beta(\tau,\tau)\beta(\tau^2,\tau)\cdots\beta(\tau^{e-1},\tau)=\pm 1$, and E/k is unramified $(\zeta_4\notin k)$. Since $e_{k/Q_2}=2^{n-1}/e=2^{1+\lambda}$, it follows that $N_{k/Q_2}(-1)=1$, and so the order of the norm residue symbol $(-1, F/k)=(N_{k/Q_2}(-1), F/Q_2)=(1, F/Q_2)$ is equal to 1. Thus, $B\sim 1$, as required.

Suppose next that $y=0$. Then, $\zeta_4^\sigma=\zeta_4$ for every $\sigma\in G(L/k)$, so $\zeta_4\in k$. It follows from the Witt's result [5, Satz 12, p. 245] that $B=(\beta, L/k)\sim 1$. (This can be also proved by the same techniques as above. The details will appear in [4].)

(ii) The case $\mathfrak{H}=\langle\theta^{2^\nu}\iota\rangle$, $(0\leq\nu\leq n-3)$. Set $\tau=\theta^{2^\nu}\iota$. Since $u_\tau u_\tau^e u_\tau^{-1}=u_\tau^e$, it follows that $u_\tau^e=\pm 1$, $e=2^{n-2-\nu}$. Let $u_\tau u_\eta=\zeta_{2^n}^b u_\eta u_\tau$. By the relation [2, (1.11)] we conclude that $1=(\pm 1)^{\eta-1}=(\zeta_{2^n}^{-b})^{1+\tau+\cdots+\tau^{e-1}}=\zeta_{2^n}^{-bT}$, $T=1+(-5^{2^\nu})+\cdots+(-5^{2^\nu})^{e-1}=(1-5^{2^{n-2}})/(1+5^{2^\nu})$. T is exactly divisible by 2^{n-1}, so $2|b$. Let X be an integer satisfying $(1+5^{2^\nu})X\equiv b\pmod{2^n}$. Then $u_\tau(\zeta_{2^n}^X u_\eta)=\zeta_{2^n}^{-5^{2^\nu}X+b}u_\eta u_\tau=(\zeta_{2^n}^X u_\eta)u_\tau$. Let E (resp. F) be the subfield of L over k corresponding to $\langle\tau\rangle$ (resp. $\langle\eta\rangle$) in the sense of Galois theory. Then we have $B=\sum\sum E\cdot Fu_\tau^i(\zeta_{2^n}^X u_\eta)^j\simeq((\zeta_{2^n}^X u_\eta)^f, E/k, \eta)\otimes_k(u_\tau^e, F/k, \tau)\sim(\pm 1, F/k, \tau)$. Since $2|e_{k/Q_2}$, the same argument as in the case (i) yields that $B\sim 1$. This completes the proof of Theorem 1.

Remark. If $\mathfrak{H}=\langle\theta^{2^\lambda}\rangle\times\langle\iota\rangle$ $(0\leq\lambda\leq n-2)$, then the computation of invariant of the cyclotomic algebra $B=(\beta, L/k)$ is a bit complicated (in particular, for the case that $\langle\theta^{2^\lambda}\rangle\neq 1$, $x\neq 0$, where $\eta=\xi^{f'}\theta^x\iota^y$). So, it will be dealt with in the subsequent paper.

3. Let h be the smallest non-negative integer such that k is contained in $Q_2(\zeta_{2^h m})$ for some odd integer m. $h=0$ if and only if k/Q_2 is unramified. Set $M=k(\zeta_{2^h})$, $f=f_{M/Q_2}$. Then $M=Q_2(\zeta_{2^h},\zeta_{2^f-1})$ and M is the *minimal* cyclotomic field containing k. If E is the maximal unramified extension of k in M, then $M=E(\zeta_4)$ $(h\neq 0)$. Suppose that $h\neq 0$ and $k(\zeta_4)/k$ is ramified. Then M/E is also ramified and $h\geq 3$. Let ω be the generator of $G(M/E)$ $(\omega^2=1)$. Let $\zeta_{2^h}^{\omega}=\zeta_{2^h}^{z}$. Then either $z\equiv -1$ or $z\equiv -1+2^{h-1}$ (mod 2^h). (These results follow from elementary properties of local fields and have been proved in [3].)

Theorem 2 (Yamada [3]). *Notation is the same as above.*
(I) *If* $k(\zeta_4)/k$ *is ramified, then only three cases arise*: i) $h=0$, ii) $h\geq 3$, $z\equiv -1$ (mod 2^h), iii) $h\geq 3$, $z\equiv -1+2^{h-1}$ (mod 2^h). *For the cases* i) *and* ii), $S(k)$ *is the subgroup of order* 2 *of* $Br(k)$. *For the case* iii), $S(k)=1$.
(II) *If* $k(\zeta_4)/k$ *is unramified, then* $S(k)=1$.

Proof. Let $B=(\beta, L/k)$ be a cyclotomic algebra over k given by (1). Then, $L\supset M$, so $n\geq h$. We also keep the notation of Theorem 1. $\mathfrak{H}$ is the inertia group of L/k. If $k(\zeta_4)/k$ is unramified, then either $n=2$, $\mathfrak{H}=1$ or $n\geq 3$, $\mathfrak{H}=\langle\theta^{2^\lambda}\rangle$ for some λ. Hence, Theorem 1 yields that $B\sim 1$, whence $S(k)=1$. If $k(\zeta_4)/k$ is ramified, $h\geq 3$, and $z\equiv -1+2^{h-1}$ (mod 2^h), then $\mathfrak{H}=\langle\theta^{2^\nu}\iota\rangle$ for some ν $(0\leq\nu\leq n-3)$. It follows from Theorem 1 that $B\sim 1$, whence $S(k)=1$.

Finally suppose that $k(\zeta_4)/k$ is ramified and that either $h=0$, or $h\geq 3$, $z\equiv -1$ (mod 2^h). Put $l=2$ for $h=0$ and $l=h$ for $h\geq 3$. Let L be the unramified extension of $k(\zeta_{2^l})$ of degree 2. Then $L=Q_2(\zeta_{2^l},\zeta_{2^{f'}-1})$, $f'=f_{L/Q_2}$. It turns out that $e_{L/k}=2$ and that there is a Frobenius automorphism φ of order $f=f_{L/k}$, whence $G(L/k)=\langle\omega\rangle\times\langle\varphi\rangle$, $\omega^2=\varphi^f=1$, $\zeta_{2^l}^{\omega}=\zeta_{2^l}^{-1}$. Let $\zeta_{2^l}^{\varphi}=\zeta_{2^l}^{t}$, $3\leq t\leq 2^l+1$. Set $t=1+2^a m$, $(2,m)=1$. It can be shown that t^f-1 is divisible by $2^{l+1}m$. Set $y=(t^f-1)/2^{l+1}m$. Then the following cyclotomic algebra B over k has Hasse invariant $1/2$:

$$B=\sum_{i=0}^{1}\sum_{j=0}^{f-1} Lu_\omega^i u_\varphi^j \qquad \text{(direct sum)}$$

$$u_\omega u_\varphi=\zeta_{2^l}u_\varphi u_\omega, \quad u_\omega^2=1, \quad u_\varphi^f=\zeta_{2^a}^{-y}.$$

(For the proof, see [3].) This completes the proof of Theorem 2.

Remark. For any finite extension K of Q_2, $S(K)$ is readily determined from Theorem 2 (cf. [3, Theorem 3]).

References

[1] T. Yamada: Characterization of the simple components of the group algebras over the p-adic number field. J. Math. Soc. Japan, **23**, 295–310 (1971).
[2] ——: The Schur subgroup of the Brauer group. I (to appear in J. Algebra).
[3] ——: The Schur subgroup of a 2-adic field (to appear).
[4] ——: The Schur Subgroup. Queen's Papers (to appear).
[5] E. Witt: Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper. J. reine angew. Math., **190**, 231–245 (1952).