Hokkaido Mathematical Journal Vol. 39 (2010) p. 173–209

On a theorem of Benard

Joujuu Ohmori

(Received February 16, 2009; Revised October 14, 2009)

Abstract. We shall give some remarks on a theorem of Benard.

Key words: Brauer group, cyclotomic algebra, Schur index.

Introduction

To state the theorem in the title, we need some notations.

Let k be a field of characterictic 0 and let $\bar{k}$ be an algebraic closure of k. Let χ be an irreducible character of a finite group G over $\bar{k}$ such that $\chi(g) \in k$ for all $g \in G$. Let $A = A(\chi, k)$ be the simple component of the group algebra $k[G]$ of G over k corresponding to χ, i.e. $\chi(A) \neq \{0\}$, where χ is extended by linearlity to a character of $k[G]$. When k is a finite algebraic extension of the field $\boldsymbol{Q}$ of rational numbers, for a place v of k (or, equivalently, a valuation of k), k_v denotes the completion of k at v (see (1.4) below). Then the theorem in the title is the following:

Theorem 1 (M. Benard [Be, Theorem 1]) *Assume that k is a finite abelian extension of $\boldsymbol{Q}$, i.e., a subfield of a finite cyclotomic extension of $\boldsymbol{Q}$. Let p be a place of $\boldsymbol{Q}$ (possibly p is infinite), and let v, w be any two places of k lying above p. Then $k_v \otimes_k A$ and $k_w \otimes_k A$ have the same index.*

By the following theorem, we see that the conclusion of Theorem 1 also holds when k is a finite Galois extension of $\boldsymbol{Q}$.

Theorem 2 (Benard-Schacher Theorem [BS]; see Curtis and Reiner [CR II, (74.20), pp. 746–747]) *Assume that k is a finite algebraic extension of $\boldsymbol{Q}$. Let m be the index of A, and let $\varepsilon_m \in \bar{k}$ be a primitive m-th root of* 1. *Then*

(i) *k contains ε_m.*
(ii) *For each place v of k and each $\sigma \in \mathrm{Aut}_{\boldsymbol{Q}}\, k$, we have:*

2000 Mathematics Subject Classification : 20C05, 16G10.

$$\mathrm{inv}_{k_v}[k_v \otimes_k A] = r \cdot \mathrm{inv}_{k_{v^\sigma}} \left[k_{v^\sigma} \otimes_k A\right],$$

where $\sigma(\varepsilon_m) = \varepsilon_m^r$ *and* v^σ *is the conjugate place of* v *under* σ *(see below). Consequently,* $k_v \otimes_k A$ *and* $k_{v^\sigma} \otimes_k A$ *have the same index.*

Here, if the place v is determined by a completion (λ, K) of k, where K is a local field and λ is an embedding (an injective homomorophism) of k into K such that $\lambda(k)$ is dense in K, v^σ is the place of k determined by the completion $(\lambda \circ \sigma^{-1}, K)$ of k (see (1.4) below), $[k_v \otimes_k A]$ (resp. $[k_{v^\sigma} \otimes_k A]$) denotes the class of $k_v \otimes_k A$ (resp. $k_{v^\sigma} \otimes_k A$) in the Brauer group $B(k_v)$ of k_v (resp. $B(k_{v^\sigma})$ of k_{v^σ}), and $\mathrm{inv}_{k_v}[k_v \otimes_k A]$ (resp. $\mathrm{inv}_{k_{v^\sigma}}[k_{v^\sigma} \otimes A]$ denotes the Hasse invariant of $[k_v \otimes_k A]$ (resp. $[k_{v^\sigma} \otimes_k A]$) (see (1.5) below).

Let us consider the folowing problem:

(P) Assume that k is a finite albegraic extension of $\boldsymbol{Q}$. Then, does the conclusion of Theorem 1 hold for k?

The first purpose of this paper is to show that generally the problem (P) has a negative answer.

The problem (P) is the one in algebraic number-theory and in the theory of compositions of fields.

The motivation for considering the problem (P) is as follows.

On page 377 of [Be], after proving Theorem 1, M. Benard is stating as follows:

"Let K be an algebraic number field. Then, for some prime $\mathfrak{p}$ of K dividing p, $K_\mathfrak{p} = K\boldsymbol{Q}_p$. Thus we have also proved the follwing theorem.

Theorem 1′ *Let* K *be an algebraic number field and let* χ *be an irreducible character. Then for a rational prime* p, $m_{K_\mathfrak{p}}(\chi) = m_{K\boldsymbol{Q}_p}(\chi)$ *for all primes* $\mathfrak{p}$ *of* K *dividing* p."

Here $m_{K_\mathfrak{p}}(\chi)$ denotes "the Schur index of χ with respect to $K_\mathfrak{p}$".

By our result, we see that Benard's "Theorem 1′" does not hold generally. But after the publication of [Be], it seems that some people (including myself) had been believing that Benard's "Theorem 1′" holds. For example, on page 113 of [Sch], the author is stating as follows:

"**Application 5** (Benard) Suppose v, w are non-archimedean valuations of K lying over the same prime. Then $m_{K_v}(\chi) = m_{K_w}(\chi)$," Here K is an algebraic number field and χ is a complex irreducible character of a finite group.

The error in the "proof" of Benard's "Theorem 1′" lies in the fact that "the composition $K\boldsymbol{Q}_p$" cannot be defined canonically. Thus, since there may still exist some people who are believing that "Theorem 1′" holds, it will have some meaning to publish such a paper.

The second theme of this paper is related to the previous paper [Oh] where we justified W. Feit's definition of the Schur index in his book, Characters of finite groups, Benjamin, 1967.

Let the notation be as in the beginning of this introduction. Let r be an integer such that $(r, |G|) = 1$. Let $\Psi^r(\chi)$ be the irreducible character of G over $\bar{k}$ defined by $\Psi^r(\chi)(g) = \chi(g^r)$, $g \in G$. Let $A(\Psi^r(\chi), k)$ be the simple component of $k[G]$ corresponding to $\Psi(\chi)$. In [Oh], we quoted from [De] the following result as a theorem of Deligne:

Theorem 3 *In the Brauer group $B(k)$ of k, we have*

$$\big[A(\Psi^r(\chi), k)\big] = [A(\chi, k)]^r.$$

After publishing [Oh], the author found that in [Sch], P. Schmid had already stated Theorem 3 at least when k is a finite algebraic extension of its prime field $\boldsymbol{Q}^{(k)}$. It should be remarked that the general case of Theorem 3 follows from the case where $[k : \boldsymbol{Q}^{(k)}] < \infty$ by using the restriction morphism $B(\boldsymbol{Q}^{(k)}(\chi)) \to B(k)$, where $\boldsymbol{Q}^{(k)}(\chi) = \boldsymbol{Q}^{(k)}(\{\chi(g) \mid g \in G\})$.

Deligne's proof of Theorem 3 in [De] is the one by using properties of Adam's operators and Schur functions. But it is difficult to understand it. It is also difficult to understand the arguments in [Sch]. Instead we present a proof of Theorem 3 by using T. Yamada's version of the Brauer-Witt theorem in [Y, pp. 31–32].

The following fact follows from Theorem 3:

Theorem 4 (see [Oh, Propositiln 1]) *$A(\Psi^r(\chi), k)$ and $A(\chi, k)$ have the same index.*

As we have remarked in [Oh, Section 1], in a special case, Theorem 4 (or its corollary [Oh, Theorem 1]) is equivalent to Theorem 1 in this introduction.

1. Preliminaries

1.1.

Let K be a (commutative) field. By a central simple algebra over K, we mean a finite-dimentional simple algebra over K with cntre K. If A is a central simple algebra over K, then there exists a division algebra D over K with centre K and $n \in \boldsymbol{N}$ such that A is isomorphic over K to the full matrix algebra $M_n(D)$ of degree n over D (see [Bour I, Chap. 10, Section 5, $n^0 4$, Corollary 2 to Proposition 12] or [W, Chap. IX, Section 1, Proposition 2, p. 163]); D is uniquely determined by A up to isomorphisms over K and n is also uniquely determined (see [W, Chap. IX, Section 1, Theorem 1, p. 164]).

For two central simple algebras A, A' over K, if A (resp. A') is isomorphic to $M_n(D)$ (resp. $M_{n'}(D')$) where D (resp. D') is a division algebra over K with centre K and $n \in \boldsymbol{N}$ (resp. $n' \in \boldsymbol{N}$), then we say that A and A' are similar if D and D' are isomorphic over K. For a central simple algebra A over K, we denote by $[A]$ the class of all central simple algebras over K that are similar to A. The class $B(K)$ of all such classes $[A]$ becomes a set and with respect to the multiplication $[A][B] = [A \otimes_K B]$ $B(K)$ is an abelian group, which is called the Brauer group of K.

Let L be a finite Galois extension of K with the Galois group G over K. Let $f : G \times G \to L^\times$ be a 2-cocycle of G with values in the multiplicative group $L^\times$ of L, i.e.

$$f(\sigma,\tau)f(\sigma\tau,\rho) = \sigma(f(\tau,\rho))f(\sigma,\tau\rho) \quad (\sigma,\tau,\rho \in G).$$

Let $(L/K, f)$ be the left vector space over L with a basis $\{u_\sigma, \sigma \in G\}$ and with the multiplication given by

$$\Big(\sum_{\sigma\in G} x_\sigma u_\sigma\Big)\Big(\sum_{\tau\in G} y_\tau u_\tau\Big) = \sum_{\sigma,\tau\in G} x_\sigma \sigma(y_\tau) f(\sigma,\tau) u_{\sigma\tau} \quad (x_\sigma, y_\tau \in L).$$

Then $(L/K, f)$ is a central simple algebra over K (see [R, (29.6), p. 243]). Let K^{sep} be the separable closure of K in an algebraic closure $\bar{K}$ of K. When L ranges over all subfields of K^{sep} that are finite Galois extensions of K, $f \mapsto (L/K, f)$ induces an isomorphism

$$H^2\big(\operatorname{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times\big) \xrightarrow{\sim} B(K)$$

(see [R, (29.12), p. 246]).

Assume that K is of characteristic 0. Let ε be a root of 1 in $\bar{K}$, and let $f : \mathrm{Gal}(K(\varepsilon)/K) \times \mathrm{Gal}(K(\varepsilon)/K) \to \langle\varepsilon\rangle$ be a 2-cocycle of the Galois group $\mathrm{Gal}(K(\varepsilon)/K)$ of $K(\varepsilon)$ over K with values in the multiplicative subgroup $\langle\varepsilon\rangle$ of $K(\varepsilon)^\times$. Then $(K(\varepsilon)/K, f)$ will be called a cyclotomic algebra over K (see [Y]). Such an algebra is similar to a simple component of the group algebra $K[H]$ for some finite group H, and conversely (see [Y, Proposition 2.1, p. 15, and Corollary 3.10, pp. 32–33]).

1.2.

Let $\boldsymbol{Q}$ be the field of rational numbers. For $x \in \boldsymbol{Q}$, let $|x| = |x|_\infty$ be the ordinary absolute value of $x : |x| = x$ (resp. $-x$) if $x \geq 0$ (resp. $x < 0$). Then the mapping $(x, y) \mapsto |x - y|$ $(x, y \in \boldsymbol{Q})$ is a distance function on $\boldsymbol{Q}$. We denote by $\boldsymbol{R}$ or $\boldsymbol{Q}_\infty$ the completion of $\boldsymbol{Q}$ with respect to this distance function.

We denote by $\boldsymbol{C}$ the filed $\boldsymbol{R}[X]/(X^2+1)\boldsymbol{R}[X]$, where X is a variable.

Let p be a prime number. Let $x \in \boldsymbol{Q}^\times$. Then there exist n, a, $b \in \boldsymbol{Z}$ with $ab \neq 0$ and $(p, ab) = 1$ such that $x = p^n(b/a)$. We put $|x|_p = p^{-n}$. And we put $|0|_p = 0$. Then the mapping $(x, y) \mapsto |x-y|_p$ $(x, y \in \boldsymbol{Q})$ is a distance function on $\boldsymbol{Q}$. We denote by $\boldsymbol{Q}_p$ the completion of $\boldsymbol{Q}$ with respect to this distance function.

$\boldsymbol{R}$, $\boldsymbol{C}$ and any finite algebraic extension of $\boldsymbol{Q}_p$ are locally compact topological fields. In this paper, by a local field, we mean a locally compact topological field which is isomorphic (as topological fields) to $\boldsymbol{R}$ or $\boldsymbol{C}$ or a finite algebraic extension of $\boldsymbol{Q}_p$ for some prime number p. (We need not a local field of positive characteristic; cf. [W].)

Let K be a local field. Let α be a Haar measure on K (see [Bour II, Chap. 7, Section 1, $n^0 2$]). For $a \in K$, we define

$$\mathrm{mod}_K(a) = \frac{\alpha(aX)}{\alpha(X)},$$

where X is a measurable subset of K such that $\alpha(X) > 0$ (see [Bour II, Chap. 7, Section 1, $n^0 4$, (32)]). As to properties of mod_K, see [W, Chap. I, Sections 2, 3].

1.3.

Let p be a prime number. Let $\boldsymbol{Z}_p = \varprojlim \boldsymbol{Z}/p^n\boldsymbol{Z}$, and let K be the quotient field of $\boldsymbol{Z}_p$. Let $x \in K^\times$. Then we have $x = p^n u$ with $n \in \boldsymbol{Z}$ and $u \in \boldsymbol{Z}_p^\times = \{\text{invertible elements in } \boldsymbol{Z}_p\}$. We put $|x|_p = p^{-n}$. And we put $|0|_p = 0$. Then $(x, y) \mapsto |x - y|_p$ is a distance function on K, K is complete with respect to this distance function and $\boldsymbol{Q}$ is dense in K. Therefore the natural embedding $\boldsymbol{Q} \hookrightarrow K$ induces an isomorpsm (as topological fields) of $\boldsymbol{Q}_p$ onto K. (see [Serre III, Chap. 2, Section 1].) We shall identify $\boldsymbol{Q}_p$ with K.

$\boldsymbol{Z}_p$ is a compact subset of $\boldsymbol{Q}_p$ and $\boldsymbol{Z}_p/p\boldsymbol{Z}_p \cong \boldsymbol{Z}/p\boldsymbol{Z}$, so that $(\boldsymbol{Z}_p : p\boldsymbol{Z}_p) = p$. Thus, if α is a Haar measure on $\boldsymbol{Q}_p$, we have

$$\mathrm{mod}_{\boldsymbol{Q}_p}(p) = \frac{\alpha(p\boldsymbol{Z}_p)}{\alpha(\boldsymbol{Z}_p)} = \frac{1}{p}.$$

As $\mathrm{mod}_{\boldsymbol{Q}_p}(ab) = \mathrm{mod}_{\boldsymbol{Q}_p}(a)\mathrm{mod}_{\boldsymbol{Q}_p}(b)$ (see [W, Chap. I, Section 2, Proposition 1, p. 4]), we see that

$$\mathrm{mod}_{\boldsymbol{Q}_p}(a) = |a|_p, \quad a \in \boldsymbol{Q}_p.$$

And we have

$$\boldsymbol{Z}_p = \big\{x \in \boldsymbol{Q}_p \mid \mathrm{mod}_{\boldsymbol{Q}_p}(x) \leq 1\big\},$$
$$\boldsymbol{Z}_p^\times = \big\{x \in \boldsymbol{Q}_p \mid \mathrm{mod}_{\boldsymbol{Q}_p}(x) = 1\big\}$$

and

$$p\boldsymbol{Z}_p = \big\{x \in \boldsymbol{Q}_p \mid \mathrm{mod}_{\boldsymbol{Q}_p}(x) < 1\big\}.$$

Let $M^\times$ be the multiplicative subgroup of $\boldsymbol{Q}_p^\times$ of roots of 1 in $\boldsymbol{Q}_p$ of order prime to p. Then $M^\times$ is a cyclic group of order $p-1$ and $M^\times \cup \{0\}$ is a full set of representatives of $\boldsymbol{Z}_p$ modulo $p\boldsymbol{Z}_p$ (see [W, Chap. I, Section 4, Theorem 7, p. 16]). Therefore we see that

$$\boldsymbol{Z}_p^\times = M^\times \times (1 + p\boldsymbol{Z}_p).$$

Lemma 1 (see [W, Chap. II, Section 3, Proposition 8, p. 32]) *Let $n \in \boldsymbol{Z}$ be such that $(p, n) = 1$. Then $x \mapsto x^n$ induces an automorphism of the group $1 + p\boldsymbol{Z}_p$. Thus, if $(p(p-1), n) = 1$, then $x \mapsto x^n$ induces an automorpism of $\boldsymbol{Z}_p^\times$.*

1.4.

Let K be a finite algebraic extension of $\boldsymbol{Q}$, i.e. an algebraic number field. We recall about the plaes of k (see [W, Chap. III]).

By a completion of k, we mean a pair (λ, K) where K is a local field and λ is an embedding (an injective homomorphism) of k into K such that $\lambda(k)$ is dense in K. Two completions (λ, K), (λ', K') of k are said to be equivalent if there exists an isomorphism ρ of K onto K' (as topological fields) such that $\lambda' = \rho \circ \lambda$. For a completion (λ, K) of k, the class of completions of k that are equivalent to (λ, K) will be called the place of k determined by (λ, K). A place of k is the place of k determined by some completion of k.

Let v be a place of K. Let $(\lambda, K) \in v$. We define a function $|\ \ |_v$ on k by $|x|_v = \mathrm{mod}_K(\lambda(x))$, $x \in k$. Then $|\ \ |_v$ is independent of the choice of (λ, K), and $(x, y) \mapsto |x-y|_v^d$ ($x,\ y \in k$, $d = 1/2$ or 1 according as $K \cong \boldsymbol{C}$ or not) is a distance function on k. We denote by k_v the completion of k with respect to this distance function, and we call k_v the completion of k at v. For $(\lambda, K) \in v$, λ induces a canonical isomorphism of k_v onto K (as topological fields).

The natural embedding $\boldsymbol{Q} \hookrightarrow \boldsymbol{R}$ determines the infinite place ∞ of $\boldsymbol{Q}$ and, for a prime number p, the natural embedding $\boldsymbol{Q} \hookrightarrow \boldsymbol{Q}_p$ determines a place of $\boldsymbol{Q}$ which will be denoted as p again. The place of $\boldsymbol{Q}$ are in one-to-one correspondence with ∞ and the prime numbers (see [W, p. 44]).

Let k' be a finite algebraic extension of k. Let w' be a place of k'. Then the pair $(\lambda', k'_{w'})$ where λ' is the nutural embedding $k' \hookrightarrow k'_{w'}$ is a completion of k' which determines w'. Let K be the closure of $\lambda'(k)$ in $k'_{w'}$ and let λ be the restriction of λ' to k. Then (λ, K) is a completion of k. Let w be the place of k determined by (λ, K). Then we say that w' lies above w and that w lies below w'. In this case we often identify k_w with the closure of k in $k'_{w'}$.

Let v be a place of k. Let $k' = k(\theta)$ with $\theta \in k'$, and let $f(X)$ be the minimal polynomial of θ in X over k. Let $f_1(X), f_2(X), \ldots, f_r(X)$ be the irreducible polynomials in $k_v[X]$ such that $f(X) = f_1(X) \cdot f_2(X) \cdots f_r(X)$. Then we have the following canonical isomorphisms over k_v:

$$k_v \otimes_k k' \xrightarrow{\sim} k_v \otimes_k k[X]/f(X)k[X] \xrightarrow{\sim} k_v[X]/f(X)k_v[X]$$
$$\xrightarrow{\sim} \bigoplus_{i=i}^{r} k_v[X]/f_i(X)k_v[X] = \bigoplus_{i=i}^{r} K'_i,$$

$$K'_i = k_v[X]/f_i(X)k_v[X], \quad 1 \le i \le r.$$

For $j \in N$, $1 \le j \le r$, let λ'_j be the composition of the canonial injection $k' \hookrightarrow k_v \otimes_k k' : x' \mapsto 1 \otimes x'$, the isomorphism $k_v \otimes_k k' \xrightarrow{\sim} \bigoplus_{i=1}^r K'_i$ and the canonical projection $\bigoplus_{i=1}^r K'_i \to K'_j$. Then, for $1 \le j \le r$, (λ'_j, K'_j) is a completion of k'. Let $w_1, w_2, \ldots, w_r$ be the places of k' determined by $(\lambda'_1, K'_1), (\lambda'_2, K'_2), \ldots, (\lambda'_r, K'_r)$ respectively. Then $w_1, w_2, \ldots, w_r$ are all the distinct places of k' lying above v (see [W, Chap. III, Section 4, Theorem 4, p. 56]).

Let v be a place of k. If k_v is isomorphic to $\boldsymbol{R}$ (resp. $\boldsymbol{C}$), then we call v a real (resp. an imaginary) place of k. If v is real or imaginary, then we call v an infinite place of k. If v is not infinite, then we say that v is finite.

Let O_k denote the integer ring of k, that is, the integral closure of $\boldsymbol{Z}$ in k. Then there is a canonical one-to-one correspondence between the set of prime ideals of O_k other than (0) and the set of finite places of k.

In fact, let P be a prime ideal of $O_k \neq (0)$. Let $x \in k$. Then there exist ideals A, B of O_k such that $P+A = P+B = O_k$ and $(x) = xO_k = P^n AB^{-1}$ for some $n \in \boldsymbol{Z}$, where

$$B^{-1} = \{y \in k \mid yB \subset O_k\}.$$

Fix $c \in \boldsymbol{R}$ with $0 < c < 1$. Put $|x|_P = c^n$. Put $|0|_P = 0$. Then $|\ |_P : k \to \boldsymbol{R}_{\ge 0}$ is a non-archimedean absolute value of k. Let k_P denote the completion of k with respect to the distance function $(x, y) \mapsto |x - y|_P$ on k, and let $\lambda : k \hookrightarrow k_P$ the natural embedding. Then (λ, k_P) is a completion of k. Let v be the place of k which is determined by (λ, k_P). Then k_v is isomorphic to k_P and v is a finite place of k. Let

$$R_v = \bigl\{x \in k_v \mid \mathrm{mod}_{k_v}(x) \le 1\bigr\}$$

and

$$P_v = \bigl\{x \in k_v \mid \mathrm{mod}_{k_v}(x) < 1\bigr\}.$$

Then P_v is the unique maximal ideal of R_v and $P = P_v \cap O_k$.

Conversely, let v' be a finite place of k, and let $R_{v'}$ and $P_{v'}$ be as above. Put $P' = P_{v'} \cap O'_k$. Then P' is a prime ideal of $O_k \neq (0)$.

The place of k which is obtained by the above procedure is just v'.

1.5.

Let K be a local field. We recall the definition of "the" Hasse invariant of an element of $B(K)$.

If K is isomorphic to $\boldsymbol{C}$, then $B(K) = \{[K]\}$ (see, e.g., [W, Chap. IX, Section 1, Corollary 2 to Proposition 3, p. 165]), and we set $\mathrm{inv}_K[K] = 0 \bmod 1$ $(\in \boldsymbol{Q}/\boldsymbol{Z})$.

If K is isomorphic to $\boldsymbol{R}$, then $B(K) = \{[K], [H_K]\}$, where H_K denotes the quaternion algebra over K (see, e.g., [W, Chap. IX, Section 4, p. 184]), and we set $\mathrm{inv}_K[K] = 0 \bmod 1$ and $\mathrm{inv}_K[H_K] = \frac{1}{2} \bmod 1$ $(\in \boldsymbol{Q}/\boldsymbol{Z})$.

Assume that K is a finite algebraic extension of $\boldsymbol{Q}_p$ for some prime number p. Let D be a finite-demensional division algebra over K with centre K. Let $[D : K] = m^2$ with $m \in \boldsymbol{N}$ (cf. [W, Chap. IX, Section 1, Corollary 3 to Proposition 3, p. 165]); m is called the (Schur) index of D. Then D contains a maximal commutative subfield $L \supset K$ such that $[L : K] = m$ and L is unramified over K (see, e.g., [W, Chap. I, Section 4, Proposition 5, pp. 20–21]). (If we set $R = \{x \in K \mid \mathrm{mod}_K(x) \leq 1\}$ and $P = \{x \in K \mid \mathrm{mod}_K(x) < 1\}$, then R/P is the residual field of K, and if we put $q = |R/P|$, then $L = K(\omega)$, where ω is a primitive $(q^m - 1)$-th root of 1 in D (see [W, Chap. I, Section 4, Corollary 3 to Theorem 7, pp. 19]).) Let $\sigma = \sigma_{L/K}$ be the Frobenius automorphism of L over $K : \sigma(\omega) = \omega^q$. Then, by a theorem of Skolem and Noether (see [Bour I, Chap. 8, Section 10, $n^o 1$, Theorem 1] or [R, (7.21), p. 103]), we see that there exists an element $u \in D^\times$ such that

$$uxu^{-1} = \sigma(x), \quad x \in L. \tag{1.5.1}$$

We see that $1, u, u^2, \ldots, u^{m-1}$ are linearly independent over L and $c = u^m \in K$. Therefore D is the cyclic algebra $(L/K, \sigma, c)$ over K (cf. [R, Section 30]). Let $v_K : K^\times \to \boldsymbol{Z}$ be the normalized valuation of K. Then we set

$$\mathrm{inv}_K[D] = \frac{v_K(c)}{m} \bmod 1 \quad (\in \boldsymbol{Q}/\boldsymbol{Z}). \tag{1.5.2}$$

This definition of $\mathrm{inv}_K[D]$ is due to Reiner [R, p. 266]. We see that this definition coincides with Serre's description of the invariant of $[D]$ on page 138 of [Serre I], where it is not so hard to verify the statements there by using statements on page 130 of [Serre I].

In [W], instead of u in (1.5.1), an element $v \in D^\times$ is chosen so that

$$v^{-1}xv = \sigma(x), \quad x \in L,$$

and the elements 1, v, $v^2, \ldots, v^{m-1}$ are used as basis of D over L (cf. [W, Chap. IX, Section 4, Proposition 11, P. 183]). So if $h(D)$ denotes the Hasse invariant of D in the sense of Weil in [W, p. 224], we see that

$$h(D) = \exp\big(-2\pi\sqrt{-1}\cdot \mathrm{inv}_K[D]\big).$$

Similarly if $d{-}\mathrm{inv}_K\, D$ denotes the invariant of D in the sense of M. Deuring in [Deu, p. 113], we see that

$$d - \mathrm{inv}_K\, D = -\,\mathrm{inv}_K[D].$$

Another definition of invariant of D on page 148 of [R] is different from $\mathrm{inv}_K[D]$. (If $\mathrm{inv}_K[D] = \frac{r}{m} \bmod 1$ with $(r,m) = 1$, then the invariant of $[D]$ there is $\frac{s}{m} \bmod 1$, where s is an integer such that $rs \equiv 1 \pmod{m}$.)

The description of invariants on page 742 of [CR II] is incorrect.

We have an isomorphism

$$\mathrm{inv}_K : B(K) \overset{\sim}{\to} \boldsymbol{Q}/\boldsymbol{Z}$$

(see [R, (31.8), p. 266] or [Serre I, Section 1, Theorem 1 and Corollary to Theorem 2, p. 130]). If K' is a finite algebraic extension of K of degree n, then

$$\mathrm{inv}_{K'}[K' \otimes_K D] = n \cdot \mathrm{inv}_K[D] \tag{1.5.3}$$

(see [R, (31.9), p. 267] or [Serre I, Section 1, (1.1), Theorem 3, p. 131] or [W, Chap. XII, Section 2, Corollary 2 to Theorem 2, p. 225]).

1.6.

Let k be a finite algebraic extension of $\boldsymbol{Q}$, and let $P(k)$ denote the set of places of k. For $[A] \in B(k)$ and $v \in P(k)$, let $A_v = k_v \otimes_k A$ and set $\mathrm{inv}_v[A] = \mathrm{inv}_{k_v}[A_v]$. For $v \in P(k)$, there is a homomorphism

$$\mathrm{res}_v; B(k) \to B(k_v) : [A] \mapsto [A_v]$$

(cf. [Bour I, Chap. 8, Section 10, $n^o 5$, Proposition 6]). For $[A] \in B(k)$, we have that $[A_v] = [k_v]$ for almost all $v \in P(k)$ (see [W, Chap. XI, Section 1, Theorem 1, p. 202]). Therefore the family $(\mathrm{res}_v)_{v\in P(k)}$ defines a homomorphism

$$r : B(k) \to \bigoplus_{v\in P(k)} B(k_v),$$

which is injective (see [W, Chap. XI, Section 2, Theorem 2, p. 206]). Let

$$\mathrm{inv} : \bigoplus_{v\in P(k)} B(k_v) \to \boldsymbol{Q}/\boldsymbol{Z}$$

be the homomorphism which is given by

$$\mathrm{inv}\left(([B_v])_{v\in P(k)}\right) = \sum_{v\in P(k)} \mathrm{inv}_{k_v}[B_v].$$

Then inv is subjective and its kernel coincides with the image of r (see [W, Chap. XIII, Section 3, Theorem 2, p. 255, and Section 6, Theorem 4, p. 264]). Thus we have the following exact sequence of abelian groups:

$$1 \to B(k) \xrightarrow{r} \bigoplus_{v\in P(k)} B(k_v) \xrightarrow{\mathrm{inv}} \boldsymbol{Q}/\boldsymbol{Z} \to 0. \tag{1.6.1}$$

Let K be a field. Let A be a central simple alegebra over K, and assume that A as isomorphic over K to $M_n(D)$, where D is a finite-dimenshonal division algebra over K with centre K and $n \in \boldsymbol{N}$. Let $[D : K] = m^2$ with $m \in \boldsymbol{N}$. m is called the (Schur) index of A. Call e the order of $[A] = [D]$ in $B(K)$. Then e divides m (see [R, (29.22), p. 253]) and, for a prime number p, p divides m if and only if p divides e (see [R, (29.24), p. 254]).

Assume that $K = k$. Then, for $v \in P(k)$, the index m_v of $D_v = k_v \otimes_k D$ is equal to the order of $[D_v]$ in $B(k_v)$ and to the order of $\mathrm{inv}_{k_v}[D_v]$ in $\boldsymbol{Q}/\boldsymbol{Z}$ (see [R, (31.4), p. 265]). We have that $m = e$ (see [R, (32.19), p. 280]) and m is equal to the least common multiple of the m_v, $v \in P(k)$ (see [R, (32.17), p. 279]).

1.7.

Let k be a field of characteristic 0. Let G be a finite group, and let χ

be an (absolutely) irreducible character of G over an algebraic closure $\bar{k}$ of k. We set

$$k(\chi) = k(\{\chi(g) \mid g \in G\}).$$

We denoted by $A(\chi, k)$ the simple component of $k[G]$ corresponding to χ.

For an irreducible character ζ of G over $\bar{k}$, set

$$e(\zeta) = \frac{\zeta(1)}{|G|} \sum_{g \in G} \zeta(g^{-1})g \quad (\in \bar{k}[G]).$$

Set

$$a(\chi) = \sum_{\sigma \in \mathrm{Gal}(k(\chi)/k)} e(\sigma \circ \chi) \quad (\in k[G]).$$

Then $a(\chi)$ is a central primitive idempotent of $k[G]$ and we have that

$$A(\chi, k) = k[G]a(\chi)$$

(see [Y, Proposition 1.1, pp. 4–5]).

Assume that $k(\chi) = k$. Let k' be a field which is an extension of k. Let $\bar{k}'$ be an algebraic closure of k'. Then the natural embedding $k \hookrightarrow k'$ can be extended to an embedding $\rho : \bar{k} \hookrightarrow \bar{k}'$. Let $U : G \to GL(d, \bar{k})$ ($d = \chi(1)$) be a matrix representation of G over $\bar{k}$ whose character is χ. ρ induces an injective homomorphism $\tilde{\rho}$ of $GL(d, \bar{k})$ into $GL(d, \bar{k}')$ given by $\tilde{\rho}([a_{ij}]) = [\rho(a_{ij})]$ for $[a_{ij}] \in GL(d, \bar{k})$. Then $\tilde{\rho} \circ U : G \to GL(d, \bar{k}')$ is a representation of G over $\bar{k}'$ whose character is χ so that we can consider χ as a character of G over $\bar{k}'$. Thus we can say about the simple component $A(\chi, k')$ of $k'[G]$ corresponding to χ. There is a canonical isomorphism f of $k' \otimes_k k[G]$ onto $k'[G]$ and we see easily that f induces an isomorphism of the simple algebra $k' \otimes_k A(\chi, k)$ onto $A(\chi, k')$.

2. Counter Examples

In this section we shall present examples which show that the problem (P) in the introduction generally has a negative answer.

2.1.

The Brauer-Speiser Theorem (see [Y, Corollary 1.8, p. 9] or [CR II, (74.27), p. 750]). *Let χ be a real-valued absolutely irreducible character of a finite group, then the Schur index $m_{\boldsymbol{Q}}(\chi)$ of χ with respect to $\boldsymbol{Q}$ is* 1 *or* 2.

Proposition 1 *Let χ be a rational-valued absolutely irreducible character of a finite group, and let $A = A(\chi, \boldsymbol{Q})$. Then, for $v \in P(\boldsymbol{Q})$, $\mathrm{inv}_v[A_v]$ is $0 \bmod 1$ or $\frac{1}{2} \bmod 1$.*

As $m_{\boldsymbol{Q}}(\chi)$ is equal to the index of A and the index of A is equal to the order of $[A]$ in $B(\boldsymbol{Q})$, the assertion follows from the Brauer-Speiser theorem.

Proposition 2 (M. Benard, K. L. Fields) *Let $S = \{v_1, v_2, \ldots, v_{2n}\}$ be a subset of $P(\boldsymbol{Q})$ whose cardinality is even. Then there exist a finite group G and a rational-valued absolutely irreducible character χ of G such that, for $v \in P(\boldsymbol{Q})$, $\mathrm{inv}_v[A(\chi, \boldsymbol{Q})]$ is $\frac{1}{2} \bmod 1$ or $0 \bmod 1$ according as $v \in S$ or $v \notin S$ respectively.*

For the sake of completeness, we shall give two proofs.

(1) Let p be a prime number and let $\bar{\boldsymbol{F}}_p$ be an algebraic closure of $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$. For a power q of p, let $\boldsymbol{F}_q$ denote the subfield of $\bar{\boldsymbol{F}}_p$ with q elements. Let q be a power of p, and let G_p be the special unitary group $SU(3, q^2)$ of degree 3 with respect to the quadratic extension $\boldsymbol{F}_{q^2}/\boldsymbol{F}_q$. Then G_p has a rational-valued complex irreducible character χ_p of degree $q^2 - q$ such that, for $v \in P(\boldsymbol{Q})$, $\mathrm{inv}_v[A(\chi_p, \boldsymbol{Q})] = \frac{1}{2} \bmod 1$ if $v = \infty$ or p, and $\mathrm{inv}_v[A(\chi_p, \boldsymbol{Q})] = 0 \bmod 1$ if $v \neq \infty$, p (see Gow [G, Theorem 6, p. 114] or Lusztig [Lu, (7.6), p. 153]). Let $S - \{\infty\} = \{p_1, p_2, \ldots, p_r\}$, and let $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_r}$ and $\chi = \chi_{p_1} \otimes \chi_{p_2} \otimes \cdots \otimes \chi_{p_r}$. Then $A(\chi, \boldsymbol{Q}) = A(\chi_{p_1}, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}} A(\chi_{p_2}, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}} \cdots \otimes_{\boldsymbol{Q}} A(\chi_{p_r}, \boldsymbol{Q})$ has the desired distribution of the invariants.

(2) Let $\bar{\boldsymbol{Q}}$ be the algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{C}$.

Let $\sqrt{-1} \in \bar{\boldsymbol{Q}}$ and let $A_2 = (\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q}, \iota, -1)$, where $\langle \iota \rangle = \mathrm{Gal}(\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q})$. Then $\boldsymbol{R} \otimes_{\boldsymbol{Q}} A_2$ is ismorphic over $\boldsymbol{R}$ to $(\boldsymbol{C}/\boldsymbol{R}, \tilde{\iota}, -1)$, where $\langle \tilde{\iota} \rangle = \mathrm{Gal}(\boldsymbol{C}/\boldsymbol{R})$ (see [R, (30.8), p. 261]). Let $N_{\boldsymbol{C}/\boldsymbol{R}} : \boldsymbol{C}^\times \to \boldsymbol{R}^\times$ be the norm map. Then $N_{\boldsymbol{C}/\boldsymbol{R}}(\boldsymbol{C}^\times) = \boldsymbol{R}_{>O} \not\ni -1$. Therefore $[\boldsymbol{R} \otimes_{\boldsymbol{Q}} A_2] \neq [\boldsymbol{R}]$ (see [R, (30.4)(iii), p. 260] or [W, Chap. IX, Section 4, Proposition 10, p. 182]). Therefore $\mathrm{inv}_\infty[A] = \frac{1}{2} \bmod 1$.

Let v be a finite place of $\boldsymbol{Q}$. Let w be a place of $\boldsymbol{Q}(\sqrt{-1})$ which lies above v. We consider $\boldsymbol{Q}_v$ as a subfield of $\boldsymbol{Q}(\sqrt{-1})_w$. Then in $\boldsymbol{Q}(\sqrt{-1})_w$ we have $\boldsymbol{Q}_v\boldsymbol{Q}(\sqrt{-1}) = \boldsymbol{Q}(\sqrt{-1})_w$, so that we can write $\boldsymbol{Q}(\sqrt{-1})_w = \boldsymbol{Q}_v(\sqrt{-1})$. We have a canonical isomorphism h of $\mathrm{Gal}(\boldsymbol{Q}_v(\sqrt{-1})/\boldsymbol{Q}_v)$ onto the subgroup $\langle\iota^s\rangle$ of $\mathrm{Gal}(\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q}) = \langle\iota\rangle$, where s is the smallest positive integer such that $\iota^s \mid \boldsymbol{Q}(\sqrt{-1}) \cap \boldsymbol{Q}_v = 1$. Let $\iota_v = h^{-1}(\iota^s)$. Then $\boldsymbol{Q}_v \otimes_{\boldsymbol{Q}} A_2$ is similar to the cyclic algebra $(\boldsymbol{Q}_v(\sqrt{-1})/\boldsymbol{Q}_v, \iota_v, -1)$ over $\boldsymbol{Q}_v$ (see [R, (30.8), p. 261]).

Assume that $v \neq 2$. Then $\boldsymbol{Q}_v(\sqrt{-1})$ is unramified over $\boldsymbol{Q}_v$ (see [Serre II, Chap. IV, Section 4, Proposition 16, pp. 84–85]). Therefore $\boldsymbol{Z}_v^\times$ is contained in the image of the norm map $N_{\boldsymbol{Q}_v(\sqrt{-1})/\boldsymbol{Q}_v}$ from $(\boldsymbol{Q}_v(\sqrt{-1}))^\times$ into $\boldsymbol{Q}_v^\times$ (see, e.g., [W, Chap. XII, Section 2, Corollary to Proposition 6, p. 226]), and $-1 \in \boldsymbol{Z}_v^\times$. Therefore $[\boldsymbol{Q}_v \otimes_{\boldsymbol{Q}} A_2] = [\boldsymbol{Q}_v]$ (see [R, (30.4)(iii), p. 260]), and $\mathrm{inv}_v[A_2] = 0 \bmod 1$. As $\mathrm{inv}_\infty[A_2] = \frac{1}{2} \bmod 1$, by the exact sequence (1.6.1) in (1.6), we must have that $\mathrm{inv}_2[A_2] = \frac{1}{2} \bmod 1$. We note that A_2 is a cyclotomic algebra over $\boldsymbol{Q}$.

Let p be an odd prime number. Let $\varepsilon_p \in \boldsymbol{C}$ be a primitive p-th root of 1 and let σ_p be a generator of $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p)/\boldsymbol{Q})$. Let $A_p = (\boldsymbol{Q}(\varepsilon_p)/\boldsymbol{Q}, \sigma_p, -1)$. This is a cyclotomic algebra over $\boldsymbol{Q}$.

The natural embedding $\boldsymbol{Q}(\varepsilon_p) \hookrightarrow \boldsymbol{C}$ determines an imaginary place ∞' of $\boldsymbol{Q}(\varepsilon_p)$ which is lying above the infinite place ∞ of $\boldsymbol{Q}$; we may assume that $\boldsymbol{Q}(\varepsilon_p)_{\infty'} = \boldsymbol{C}$. Then in $\boldsymbol{C}$ we have that $\boldsymbol{C} = \boldsymbol{R}\boldsymbol{Q}(\varepsilon_p) = \boldsymbol{R}(\varepsilon_p)$. We have that $\mathrm{Gal}(\boldsymbol{R}(\varepsilon_p)/\boldsymbol{R}) = \langle\tilde{\iota}\rangle$, where $\tilde{\iota}(\varepsilon_p) = \varepsilon_p^{-1}$. We see that $\boldsymbol{R} \otimes_{\boldsymbol{Q}} A_p$ is similar to $(\boldsymbol{R}(\varepsilon_p)/\boldsymbol{R}, \tilde{\iota}, -1)$. Therefore $\mathrm{inv}_\infty[A_p] = \frac{1}{2} \bmod 1$.

Let v' be a finite place of $\boldsymbol{Q}$, and let w' be a place of $\boldsymbol{Q}(\varepsilon_p)$ which lies above v'. We consider $\boldsymbol{Q}_{v'}$, as a subfield of $\boldsymbol{Q}(\varepsilon_p)_{w'}$. Then we have that $\boldsymbol{Q}(\varepsilon_p)_{w'} = \boldsymbol{Q}_{v'}\boldsymbol{Q}(\varepsilon_p) = \boldsymbol{Q}_{v'}(\varepsilon_p)$. We have a canonical isomorphism h' of $\mathrm{Gal}(\boldsymbol{Q}_{v'}(\varepsilon_p)/\boldsymbol{Q}_{v'})$ onto a subgroup H of $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p)/\boldsymbol{Q}) = \langle\sigma_p\rangle$. Let s' be the smallest positive integer such that $\sigma_p^{s'} \mid \boldsymbol{Q}(\varepsilon_p) \cap \boldsymbol{Q}_{v'} = 1$. Then $H = \langle\sigma_p^{s'}\rangle$. Put $\tau_p = h'^{-1}(\sigma_p^{s'})$. Then $\boldsymbol{Q}_{v'} \otimes_{\boldsymbol{Q}} A_p$ is similar to the cyclic algebra $(\boldsymbol{Q}_{v'}(\varepsilon_p)/\boldsymbol{Q}_{v'}, \tau_p, -1)$ ([R, (30.8), p. 261]).

Assume thar $v' \neq p$. Then $\boldsymbol{Q}_{v'}(\varepsilon_p)$ is unramified over $\boldsymbol{Q}_{v'}$. Therefore, as $-1 \in \boldsymbol{Z}_{v'}^\times$, it lies in the image of the norm map $N_{\boldsymbol{Q}_{v'}(\varepsilon_p)/\boldsymbol{Q}_{v'}}$. Thus $\mathrm{inv}_{v'}[A_p] = 0 \bmod 1$. As $\mathrm{inv}_\infty[A_p] = \frac{1}{2} \bmod 1$, we must have that $\mathrm{inv}_p[A_p] = \frac{1}{2} \bmod 1$.

Let $\{p_1, p_2, \ldots, p_r\}$ be as in the proof (1). Then $A = A_{p_1} \otimes_{\boldsymbol{Q}} A_{p_2} \otimes_{\boldsymbol{Q}} \cdots \otimes_{\boldsymbol{Q}} A_{p_r}$ is similar to a cyclotomic algebra over $\boldsymbol{Q}$ which has the desired distribution of invariants.

2.2.

In this subsection, for a prime number p, $\bar{\boldsymbol{Q}}_p$ denotes an algebraic closure of $\boldsymbol{Q}_p$, and for $n \in \boldsymbol{N}$, ε_n denotes a primitive n-th root of 1 in $\boldsymbol{Q}_p$.

Proposition 3 *Let p be a finite place of $\boldsymbol{Q}$. Then there exists a finite algebraic extension k of $\boldsymbol{Q}$ having at least two places v, w lying abolve p such that $[k_v : \boldsymbol{Q}_p^{(v)}] = 1$ and $[k_w : \boldsymbol{Q}_w^{(w)}]$ is even, where $\boldsymbol{Q}_p^{(v)}$ and $\boldsymbol{Q}_p^{(w)}$ are the closure of $\boldsymbol{Q}$ in k_v and k_w respectively.*

Case (a): $(3, p(p-1)) = 1$**.**

Let r be a prime number $\neq p$, and let $f(X) = X^3 - r$, where X is a variable. Then, by Eisenstein's criterion, we see that $f(X)$ is an irreducible polynomial in $\boldsymbol{Q}[X]$. As $(p, r) = 1$, we have that $\mathrm{mod}_{\boldsymbol{Q}_p}(r) = |r|_p = 1$, so $r \in \boldsymbol{Z}_p^{\times}$. Therefore, by Lemma 1 in (1.3), we see that there is an element α in $\boldsymbol{Z}_p^{\times}$ such that $\alpha^3 = r$. We have

$$
\begin{aligned}
f(x) &= (X-\alpha)(X-\varepsilon_3\alpha)\bigl(X-\varepsilon_3^2\alpha\bigr) = (X-\alpha)g(X),\\
g(x) &= X^2 + \alpha X + \alpha^2 \quad (\in \boldsymbol{Q}_p[X]).
\end{aligned}
$$

As $(3, p-1) = 1$, $\varepsilon_3 \notin M^{\times}$ (cf. (1.3)). Therefore $\varepsilon_3 \notin \boldsymbol{Q}_p$. Therefore we see that $g(X)$ is an irreducible polynomial in $\boldsymbol{Q}_p[X]$. Thus $f(X) = (X-\alpha)g(X)$ is the irreducible docomposition of $f(X)$ in $\boldsymbol{Q}_p[X]$. Thus, by (1.4), we see that $k = \boldsymbol{Q}[X]/f(X)\boldsymbol{Q}[X]$ has just two places, say, v, w lying above p. We can arrange them so that $[k_v : \boldsymbol{Q}_p^{(v)}] = 1$ and $[k_w : \boldsymbol{Q}_p^{(w)}] = 2$.

Case (b): $3 \mid p-1$**.**

(b1) Assume that $p+1$ is not a power of 2. Let q be an odd prime number which divides $p+1$. Then, as $(p+1, p-1) = 2$, q does not divide $p-1$. Therefore 2 is equal to the smallest positive integer h such that $p^h \equiv 1 \pmod{q}$. Therefore we have that $[\boldsymbol{Q}_p(\varepsilon_q) : \boldsymbol{Q}_p] = 2$ (see [Serre II, Chap. IV, Section 4, Corollary to Proposition 16, p. 85]).

Let r be a prime number $\neq p$, and let $f(X) = X^q - r$; $f(X)$ is an irreducible polynomial in $\boldsymbol{Q}[X]$. Set $k = \boldsymbol{Q}[X]/f(X)\boldsymbol{Q}[X]$. We have that $r \in \boldsymbol{Z}_p^{\times}$, and as $(q, p(p-1)) = 1$, there is an element $\alpha \in \boldsymbol{Z}_p^{\times}$ such that $\alpha^q = r$. We have that $\boldsymbol{Q}_p(\varepsilon_q\alpha) = \boldsymbol{Q}_p(\varepsilon_q)$ so $[\boldsymbol{Q}_p(\varepsilon_q\alpha) : \boldsymbol{Q}_p] = [\boldsymbol{Q}_p(\varepsilon_q) : \boldsymbol{Q}_p] = 2$. Let $g(X)$ be the minimal polynomial of $\varepsilon_q\alpha$ over $\boldsymbol{Q}_p$. Then we have

$$
f(X) = (x-\alpha)g(X)h_1(X)\cdots h_s(X),
$$

where $h_1(X), \dots, h_s(X)$ are certain irreducible polynomials in $\boldsymbol{Q}_p[X]$ other than $X - \alpha$ and $g(X)$ (possibly such polynomials do not exist). Thus we can conclude that k has the places v, w, $u_1, \dots, u_s$ lying above p such that $[k_v : \boldsymbol{Q}_p^{(v)}] = 1$, $[k_w : \boldsymbol{Q}_p^{(w)}] = \deg g(X) = 2$, $[k_{u_i} : \boldsymbol{Q}_p^{(u_i)}] = \deg h_i(X)$, $1 \le i \le s$ (possibly $u_1, \dots, u_s$ do not exist).

(b2) Assume that $p+1$ is a power of 2. Then we see easily thet p^2+1 is not a power of 2. Let q be an odd prime number which devides p^2+1. Then, as $(p-1, p^2+1) = 2$, q does not divide $p-1$. We see easily that the smallest positive integer h such that $p^h \equiv 1 \pmod q$ is equal to 4. Therefore $[\boldsymbol{Q}_p(\varepsilon_p) : \boldsymbol{Q}_p] = 4$.

Let r be a prime number $\neq p$ and let $f(X) = X^q - r$. Then $f(X)$ is irreducible in $\boldsymbol{Q}[X]$. Set $k = \boldsymbol{Q}[X]/f(X)\boldsymbol{Q}[X]$. We have that $r \in \boldsymbol{Z}_p^\times$ and $(q, p(p-1)) = 1$. Let $\alpha \in \boldsymbol{Z}_p^\times$ be such that $\alpha^q = r$. Then $[\boldsymbol{Q}_p(\varepsilon_q\alpha) : \boldsymbol{Q}_p] = [\boldsymbol{Q}_p(\varepsilon_q) : \boldsymbol{Q}_p] = 4$. Let $g(X)$ be the minimal polynomial of $\varepsilon_q\alpha$ over $\boldsymbol{Q}_p$. Then in $\boldsymbol{Q}_p[X]$ we have $f(X) = (X-\alpha)g(X)h_1(X)\cdots h_s(X)$, where $h_1(X), \dots, h_s(X)$ are certain irreducible polynomials in $\boldsymbol{Q}_p[X]$ other than $X - \alpha$ and $g(X)$ (possibly $h_1(X), \dots, h_s(X)$ do not exist). Thus we conclude that k has at least two places v, w such that $[k_v : \boldsymbol{Q}_p^{(v)}] = 1$ and $[k_w : \boldsymbol{Q}_p^{(w)}] = 4$.

Case (C): $p = 3$.

Let r be a prime number $\neq 3$, and let $f(X) = X^5 - r$. Then $f(X)$ is irreducible in $\boldsymbol{Q}[X]$. Set $k = \boldsymbol{Q}[X]/f(X)\boldsymbol{Q}[X]$. We have that $r \in \boldsymbol{Z}_3^\times$. As $(5, 3(3-1)) = 1$, there is an element $\alpha \in \boldsymbol{Z}_3^\times$ such that $\alpha^5 = r$. We see that $[\boldsymbol{Q}_3(\varepsilon_5) : \boldsymbol{Q}_3] = 4$. Let $g(X)$ be the minimal polynomial of $\varepsilon_5\alpha$ over $\boldsymbol{Q}_3$. Then we have $f(X) = (X-\alpha)g(X)$. Thus we can conclude that k has just two places v, w such that $[k_v : \boldsymbol{Q}_3^{(v)}] = 1$ and $[k_w : \boldsymbol{Q}_3^{(w)}] = 4$.

This completes the proof of Proposition 3.

2.3.

Proposition 4 *Let χ be a rational-valued absolutely irreducible character of a finite group G such that $[A(\chi, \boldsymbol{Q})] \neq [\boldsymbol{Q}]$ (cf. Proposition 2 in (2.1)). Let p be a finite place of $\boldsymbol{Q}$ such that $\mathrm{inv}_p[A(\chi, \boldsymbol{Q})] = \frac{1}{2} \bmod 1$. Then there exists a finite algebraic extension k of $\boldsymbol{Q}$ having at least two places v, w lying above p such that $\mathrm{inv}_v[A(\chi, k)] = \frac{1}{2} \bmod 1$ and $\mathrm{inv}_w[A(\chi, k)] = 0 \bmod 1$.*

In fact, let k, v, w be as in Proposition 3. We note that $\boldsymbol{Q}_p^{(v)}$ and $\boldsymbol{Q}_p^{(w)}$

are canonically isomorphic to $\boldsymbol{Q}_p$ as topological fields. In (1.7), we observed that $k \otimes_{\boldsymbol{Q}} A(\chi, \boldsymbol{Q})$ is canonically isomorphic to $B = A(\chi, k)$. Thus, by (1.5.3) in (1.5), we have:

$$\begin{aligned}
\mathrm{inv}_v[B] &= \left[k_v : \boldsymbol{Q}_p^{(v)}\right] \cdot \mathrm{inv}_{\boldsymbol{Q}_p^{(v)}} \left[\boldsymbol{Q}_p^{(v)} \otimes_{\boldsymbol{Q}} A(\chi, \boldsymbol{Q})\right] \\
&= 1 \cdot \mathrm{inv}_{\boldsymbol{Q}_p} \left[\boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} A(\chi, \boldsymbol{Q})\right] = \frac{1}{2} \bmod 1
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{inv}_w[B] &= \left[k_w : \boldsymbol{Q}_p^{(w)}\right] \cdot \mathrm{inv}_{\boldsymbol{Q}_p^{(w)}} \left[\boldsymbol{Q}_p^{(w)} \otimes_{\boldsymbol{Q}} A(\chi, \boldsymbol{Q})\right] \\
&= (\text{even number}) \cdot \mathrm{inv}_{\boldsymbol{Q}_p} \left[\boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} A(\chi, \boldsymbol{Q})\right] \\
&= (\text{even number}) \cdot \left(\frac{1}{2} \bmod 1\right) \\
&= 0 \bmod 1.
\end{aligned}$$

This proves Proposition 4.

Proposition 5 *Let χ be a rational-valued absolutely irreducible character of a finite group such that $\mathrm{inv}_\infty[A(\chi, \boldsymbol{Q})] = \frac{1}{2} \bmod 1$. Then there exists a finite algebraic extension k of $\boldsymbol{Q}$ having (at least) two infinite places ∞_1, ∞_2 such that $\mathrm{inv}_{\infty_1}[A(\chi, k)] = \frac{1}{2} \bmod 1$ and $\mathrm{inv}_{\infty_2}[A(\chi, k)] = 0 \bmod 1$.*

In fact, let $f(X) = x^q - r$ be as in the proof of Proposition 3 in (2.2). We note that q is an odd prime number and r is an integer > 1. Let $\sqrt[q]{r}$ be the unique element in $\boldsymbol{R}$ such that $(\sqrt[q]{r})^q = r$ and let ε_q be a primitive q-th root of 1 in an algebraic closure $\bar{\boldsymbol{R}}$ of $\boldsymbol{R}$. Then in $\bar{\boldsymbol{R}}[X]$ we have:

$$\begin{aligned}
f(X) &= \left(X - \sqrt[q]{r}\right)\left(X - \varepsilon_q \sqrt[q]{r}\right)\left(x - \varepsilon_q^2 \sqrt[q]{r}\right) \cdots \left(X - \varepsilon_q^{q-1} \sqrt[q]{r}\right) \\
&= \left(X - \sqrt[q]{r}\right) g_1(X) g_2(X) \cdots g_{(q-1)/2}(X), \\
g_i(X) &= X^2 - \left(\varepsilon_q^i + \varepsilon_q^{-i}\right) \sqrt[q]{r} X + \sqrt[q]{r}^2 \quad (1 \leq i \leq (q-1)/2).
\end{aligned}$$

As $\varepsilon_q \notin \boldsymbol{R}$ and $\varepsilon_q^i + \varepsilon_q^{-i} \in \boldsymbol{R}$ for $1 \leq i \leq (q-1)/2$, we see that the $g_i(X)$ are irreducible polynomials in $\boldsymbol{R}[X]$. Therefore, by (1.4), we find that $k = \boldsymbol{Q}[X]/f(X)\boldsymbol{Q}[X]$ has just one real place ∞_1 and $(q-1)/2$ imaginary places. Let ∞_2 be any one of the imaginary places. Then the assertion is clear (cf. [W, Chap. XII, Section 2, Corollary 2 to Theorem 2, p. 225]).

3. Proof of Theorem 3

In this section we give a proof of Theorem 3 in the introduction which is based on the Brauer-Witt theorem.

3.1.

Let K be a field. Let D be a finite-dimensional division algebra over K with centre K. Call m the index of $D : m^2 = [D : K]$. Let

$$m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s},$$

where $p_1, p_2, \ldots, p_s$ are mutually different prime numbers and $e_1, e_2, \ldots, e_s \in \boldsymbol{N}$. Then there exist division algebras $D_1, D_2, \ldots, D_s$ over K with centre K such that, for $1 \leq i \leq s$, the index of D_i is $p_i^{e_i}$, and that D is isomorphic over K to $D_1 \otimes_K D_2 \otimes_K \cdots \otimes_K D_s$ (see, e.g., [R, p. 256] or [Deu, V, Section 3, Satz 3, p. 59]). For such $D_1, D_2, \ldots, D_s$, we have

$$[D] = [D_1][D_2] \cdots [D_s],$$

where, for $1 \leq i \leq s$, the order of $[D_i]$ in $B(K)$ (> 1) divides $p_i^{e_i}$ (see [R, (29.22), p. 253]). Therefore $[D_1], [D_2], \ldots, [D_s]$ are uniquely determined by $[D]$. For a prime number p, we set

$$[D]_p = \begin{cases} [K] & \text{if } p \notin \{p_1, p_2, \ldots, p_s\}, \\ [D_i] & \text{if } p = p_i \text{ for some } i. \end{cases}$$

3.2.

Let K be a field, L a finite Galois extension of K with Galois group G, K' a subfield of L over K and $H = \mathrm{Gal}(L/K')$. Let $f : G \times G \to L^\times$ be a 2-cocycle of G with values in $L^\times$. Let $\mathrm{res}(f) : H \times H \to L^\times$ be the 2-cocycle of H with values in $L^\times$ which is defined by

$$(\mathrm{res}(f))(\sigma, \tau) = f(\sigma, \tau), \quad \sigma, \tau \in H.$$

Then

$$[K' \otimes_K (L/K, f)] = [(L/K', \mathrm{res}(f))]$$

in $B(K')$ (see [R, (29.13), p. 248]). We can define:

$$\mathrm{res}([L/K, f)] = [(L/K', \mathrm{res}(f))].$$

Put $t = (G : H) = [K' : K]$. Assume that

$$G = \bigcup_{\theta \in \Sigma} H\theta, \quad \Sigma = \{\theta_1, \theta_2, \ldots, \theta_t\}, \quad \theta_1, \theta_2, \ldots, \theta_t \in G.$$

For $\sigma \in G$ and $\theta \in \Sigma$, let

$$\theta\sigma = h(\theta, \sigma)\theta^\sigma$$

with $h(\theta, \sigma) \in H$ and $\theta^\sigma \in \Sigma$. Let $g : H \times H \to L^\times$ be a 2-cocycle of H with values in $L^\times$. We define a map $\mathrm{cor}_\Sigma(g) : G \times G \to L^\times$ by

$$(\mathrm{cor}_\Sigma(g))(\sigma, \tau) = \prod_{\theta \in \Sigma} \theta^{-1}\bigl(g(h(\theta, \sigma), h(\theta^\sigma, \tau))\bigr), \quad \sigma, \tau \in G.$$

Then we see that $\mathrm{cor}_\Sigma(g)$ is a 2-cocycle of G with values in $L^\times$, and we can define

$$\mathrm{cor}([L/K', g]) = \bigl[(L/K, \mathrm{cor}_\Sigma(g))\bigr],$$

which is independent of the choice of Σ. We can verify:

$$(\mathrm{cor} \circ \mathrm{res})([L/K, f]) = [(L/K, f)]^t \tag{3.2.1}$$

(cf. [Serre II, Chap. VII, Section 7, Proposition 6, p. 127]).

Assume that, in the situation $L \supset K' \supset K$ as above, K' is a Galois extension of K with Galois group $\bar{G}$. $\pi : \sigma \mapsto \sigma \mid K'$ induces a canonical isomorphism of G/H onto $\bar{G}$. Let $h : \bar{G} \times \bar{G} \to K'^\times$ be a 2-cocycle of $\bar{G}$ with values in $K'^\times (\subset L^\times)$. We define the 2-cocycle $\inf(h) : G \times G \to L^\times$ by

$$(\inf(h))(\sigma, \tau) = h(\pi(\sigma), \pi(\tau)), \quad \sigma, \tau \in G.$$

Then

$$\inf([(K'/K, h)]) := [(L/K, \inf(h))] = [(K'/K, h)]$$

(see [R, (29.16), p. 249]).

3.3.

Let k be a field of characteristic 0. Let p be a prime number. Then we say that a finite group H is k-elementary with respect to p if the following two conditions are satisfied:

(i) H is a semidirect product AP, where A is a cyclic, normal subgroup of H whose order is relatively prime to p and P is a p-group.

(ii) Let $A = \langle a \rangle$, and let ε be a primitive $|A|$-th root of 1 in an extension-field of k. If a^i and a^j are conjugate in H $(i, j \in \boldsymbol{Z})$, then there exists $\sigma \in \mathrm{Gal}(k(\varepsilon)/k)$ such that $\sigma(\varepsilon^i) = \varepsilon^j$.

3.4.

We quote from [Y, pp. 31–32] the following theorem:

The Brauer-Witt Theorem. *Let k be a field of characteristic* 0 *and $\bar{k}$ an algebraic closure of k. Let G be a finite group of exponent n. Let ε be a primitive n-th root of* 1 *in $\bar{k}$. Let χ be an irreducible character of G over $\bar{k}$ such that $k(\chi) = k$. Let p be a prime number.*

(I) *Let L_p be the subfield of $k(\varepsilon)$ which contains k such that $[k(\varepsilon) : L_p]$ is a power of p and $t_p = [L_p : k]$ is relatively prime to p. Then there is a subgroup F_p of G which is L_p-elementary with respect to p and an irreducible character θ_p of F_p over $\bar{k}$ with $L_p(\theta_p) = L_p$ such that the inner product $(\chi \mid F_p, \theta_p)_{F_p} \not\equiv 0 \pmod{p}$, and the following statement* (II) *holds.*

(II) *There is a normal subgroup N_p of F_p and a linear character ψ_p of N_p over $\bar{k}$ such that* (i) *$\theta_p = \psi_p^{F_p} = \mathrm{Ind}_{N_p}^{F_p}(\psi_p)$ (the induced character),* (ii) *for $f \in F_p$, there exists $\tau(f) \in \mathrm{Gal}(L_p(\psi_p)/L_p)$ such that $\psi_p^f = \psi_p^{\tau(f)} = \tau(f) \circ \psi_p$ $(\psi_p^f(x) = \psi_p(fxf^{-1}), x \in N_p)$, and by the mapping $f \mapsto \tau(f)$, $F_p/N_p \xrightarrow{\sim} \mathrm{Gal}(L_p(\psi_p)/L_p)$,* (iii) *$A(\theta_p, L_p)$ is isomorphic over L_p to the cyclotomic algebra $(L_p(\psi_p)/L_p, \beta_p)$ over L_p, where, if T_p is a complete set of coset representatives of N_p in F_p $(1 \in T_p)$, with $ff' = n(f.f')f''$ for f, f', $f'' \in T_p$, $n(f, f') \in N_p$, then $\beta_p(\tau(f), \tau(f')) = \psi_p(n(f, f'))$.*

(III) *$[A(\chi, L_p)] = [A(\theta_p, L_p)] = [(L_p(\psi_p)/L_p, \beta_p)]$ in $B(L_p)$, and the p-part of the Schur index $m_k(\chi)$ of χ with respect to k (i.e. the heighest power of p dividing $m_k(\chi)$) is equal to $m_{L_p}(\theta_p)$.*

3.5.

Let us prove Theorem 3. We repeat the argument in the proof of Corollary 3.10 of [Y, pp. 32–33] which shows that $A(\chi, k)$ is similar to a cyclotomoic algebra over k. Let the notation be as in the Brauer-Witt theorem.

Consider the homomorphism

$$\mathrm{res} : B(k) \to B(L_p) : [B] \mapsto [L_p \otimes_k B]$$

(cf. [Bour I, Chap. 8, Section 10, $n^0 5$, Proposition 6]). We show that

$$\mathrm{res}([A(\chi, k)]_p) = [A(\chi, L_p)]. \tag{3.5.1}$$

In fact, we have

$$\mathrm{res}([A(\chi, k)]) = \big[L_p \otimes_k A(\chi, k)\big] = [A(\chi, L_p)]$$

and

$$\mathrm{res}([A(\chi, k)]) = \mathrm{res}\left(\prod_q [A(\chi, k)]_q\right) = \prod_q \mathrm{res}([A(\chi, k)]_q),$$

where q ranges over all prime numbers. For a prime number q, the order of $\mathrm{res}([A(\chi, k)]_q)$ is a power of q so that $\mathrm{res}([A(\chi, k)]_q) = \mathrm{res}([A(\chi, k)])_q = [A(\chi, L_p)]_q$. Therefore it sufficies to show that the index of $A(\chi, L_p)$ is a power of p.

By a theorem of R. Brauer (see, e.g., [CR I, (41.1), p. 292]), we see that χ is realizable in $k(\varepsilon)$, that is, there is a matrix representation $G \to GL(d, k(\varepsilon))$ $(d = \chi(1))$ of G over $k(\varepsilon)$ whose character is χ. Therefore $k(\varepsilon)$ is a splitting field of $A(\chi, L_p)$ (cf. [CR I, (70.11), p. 469]). Therefore the index m_p of $A(\chi, L_p)$ divides $[k(\varepsilon) : L_p]$ (see, e.g., [CR I, (68.7), p. 457]), which is a power of p.

By the assertion (III) of the Brauer-Witt theorem, we have $[A(\chi, L_p)] = [B_p]$, where $B_p = (L_p(\psi_p)/L_p, \beta_p)$. In the situation $k(\varepsilon) \supset L_p(\psi_p) \supset L_p$, put $\tilde{\beta}_p = \inf(\beta_p)$; $\tilde{\beta}_p$ is a 2-cocycle of $\mathrm{Gal}(k(\varepsilon)/L_p)$ whose values are in $L_p(\psi_p)^\times$ $(\subset k(\varepsilon)^\times)$. Put $\tilde{B}_p = (k(\varepsilon)/L_p, \tilde{\beta}_p)$; $\tilde{B}_p$ is similar to B_p.

In the situation $k(\varepsilon) \supset L_p \supset k$, put $\gamma_p = \mathrm{cor}_\Sigma(\tilde{\beta}_p)$, where Σ is a complete set of coset representatives of $\mathrm{Gal}(k(\varepsilon)/L_p)$ in $\mathrm{Gal}(k(\varepsilon)/k)$. Put $C_p = (k(\varepsilon)/k, \gamma_p)$; $[C_p] = \mathrm{cor}([\tilde{B}_p]) = \mathrm{cor}([B_p]) = \mathrm{cor}([A(\chi, L_p)]$.

Let D_p be a finite-dimensional division algebra over k with centre k such that $[A(\chi,k)]_p = [D_p]$. We show that $k(\varepsilon)$ is a splitting field of D_p.

In fact, we have $[A(\chi,k)] = \prod_q [A(\chi,k)]_q = \prod_q [D_q]$, where q ranges over all prime numbers and, for a prime number q, D_q denotes a finite-dimensional division algebra over k with centre k such that $[A(\chi,k)]_q = [D_q]$. We have

$$[k(\varepsilon)] = [k(\varepsilon)\otimes_k A(\chi,k)] = \prod_q [k(\varepsilon)\otimes_k D_q],$$

and, for each prime number q, the order of $[k(\varepsilon)\otimes_k D_q]$ in $B(k(\varepsilon))$ is a power of q. Thus, for each q, $[k(\varepsilon)\otimes_k D_q] = [k(\varepsilon)]_q = [k(\varepsilon)]$. In particular, $k(\varepsilon)$ is a splitting field of D_p.

Therefore, we find that there exists a 2-cocycle f of $\mathrm{Gal}(k(\varepsilon)/k)$ with values in $k(\varepsilon)$ such that $[D_p] = [(k(\varepsilon)/k, f)]$ (cf. Proof of (29.12) of [R, pp. 246–247]). Thus, in the situation $k(\varepsilon)\supset L_p \supset k$, we have:

$$\begin{aligned}(\mathrm{cor}\circ\mathrm{res})([A(\chi,k)]_p) &= (\mathrm{cor}\circ\mathrm{res})([D_p]) = (\mathrm{cor}\circ\mathrm{res})([k(\varepsilon)/k,f)])\\ &= [(k(\varepsilon)/k,f)]^{t_p} = [A(\chi,k)]_p^{t_p} \quad (\text{cf. } (3.2.1)).\end{aligned}$$

Let $[k(\varepsilon) : L_p] = p^a$, where a is a non-negative integer. Let u_p be an integer such that $u_p t_p \equiv 1 \pmod{p^a}$. Then

$$\begin{aligned}\big[(k(\varepsilon)k, \gamma_p^{u_p})\big] &= [(k(\varepsilon)/k,\gamma_p)]^{u_p} = [C_p]^{u_p} = \big(\mathrm{cor}([\tilde{B}_p])\big)^{u_p} = (\mathrm{cor}([B_p]))^{u_p}\\ &= (\mathrm{cor}(\mathrm{res}([A(\chi,k)]_p)))^{u_p} = ((\mathrm{cor}\circ\mathrm{res})([A(\chi,k)]_p))^{u_p}\\ &= ([A(\chi,k)]_p)^{u_p t_p} = [A(\chi,k)]_p.\end{aligned}$$

Here the last equality follows from the following consideration.

The index m_p of D_p ($[A(\chi,k)]_p = [D_p]$) is the p-part of the index of m of $A(\chi,k)$. As $k(\varepsilon)$ is a splitting field of $A(\chi,k)$, we see that m divides $[k(\varepsilon):k] = p^a t_p$, and $(t_p,p)=1$. As m_p is a power of p, m_p must divide p^a. Therefore the order of $[D_p] = [A(\chi,k)]_p$ in $B(k)$ divides p^a. As $t_p u_p \equiv 1 \pmod{p^a}$, we have that $t_p u_p = 1 + p^a v$ from some $v\in \boldsymbol{Z}$. Therefore we have:

$$([A(\chi,k)]_p)^{t_p u_p} = ([A(\chi,k)]_p)^{1+p^a v} = [A(\chi,k)]_p.$$

Thus we have:

$$[A(\chi,k)] = \prod_q [A(\chi,k)]_q = \prod_q \left[(k(\varepsilon)/k, \gamma_q^{u_q})\right] = \left[\left(k(\varepsilon)/k, \prod_q \gamma_q^{u_q}\right)\right]$$
$$= [(k(\varepsilon)/k, \gamma)], \qquad \gamma = \prod_q \gamma_q^{u_q},$$

where q ranges over all prime numbers (note that if q does not divide $[k(\varepsilon) : k]$, then $[A(\chi,k)]q = [k]$ so that we may take as $\gamma_q = 1$). We note that γ is a 2-cocycle of $\mathrm{Gal}(k(\varepsilon)/k)$ whose values are in $\langle\varepsilon\rangle$.

Let r be an integer such that $(r,n) = 1$. Then there is an automorphism α of $\boldsymbol{Q}^{(k)}(\varepsilon)$ such that $\alpha(\varepsilon) = \varepsilon^r$ where $\boldsymbol{Q}^{(k)}$ denotes the prime field of k. We have $\Psi^r(\chi) = \chi^\alpha =: \alpha\circ\chi$. Applying the Brauer-Witt theorem and the above argument to $\Psi^r(\chi)$, we find that $L_p, F_p, \theta_p, N_p, \psi_p, \beta_p, \tilde{\beta}_p, \gamma_p$ and γ will be replaced with $L_p, F_p, \theta_p^\alpha, N_p, \psi_p^\alpha, \beta_p^\alpha, \tilde{\beta}_p^\alpha, \gamma_p^\alpha$ and γ^α respectively ($\theta_p^\alpha = \alpha\circ\theta_p$, $\psi_p^\alpha = \alpha\circ\psi_p$, $\beta_p = \alpha\circ\beta_p$, $\tilde{\beta}_p^\alpha = \alpha\circ\tilde{\beta}_p$, $\gamma_p^\alpha = \alpha\circ\gamma_p$ and $\gamma^\alpha = \alpha\circ\gamma$).

In fact, in the statement (I) of the Brauer-Witt theorem, we have

$$\left(\chi^\alpha \mid F_p, \theta_p^\alpha\right)_{F_p} = \alpha\big((\chi \mid F_p, \theta_p)_{F_p}\big) = \left(\chi \mid F_p, \theta_p\right)_{F_p}.$$

In the statement (II) of the Brauer-Witt theorem, we have $\theta_p^\alpha = (\psi_p^\alpha)^{F_p}$, for $f \in F_p$, we have $(\psi_p^\alpha)^f = (\psi_p^f)^\alpha = (\psi_p^{\tau(f)})^\alpha = (\psi_p^\alpha)^{\tau(f)}$, and $\beta_p^\alpha(\tau(f),\tau(f')) = \alpha(\beta_p(\tau(f),\tau(f'))) = \alpha(\psi_p(n(f,f')) = \psi_p^\alpha(n(f.f'))$.

And $\inf(\beta_p^\alpha) = (\inf(\beta_p))^\alpha = \tilde{\beta}_p^\alpha$, $\mathrm{cor}_\Sigma(\tilde{\beta}_p^\alpha) = (\mathrm{cor}_\Sigma(\tilde{\beta}_p))^\alpha = \gamma_p^\alpha$, and $\prod_q (\gamma_q^\alpha)^{u_q} = \prod_q (\gamma_q^{u_q})^\alpha = \gamma^\alpha$.

Thus we have

$$[A(\Psi^r(\chi),k)] = [(k(\varepsilon)/k, \gamma^\alpha)] = [(k(\varepsilon)/k, \gamma^r)] = [(k(\varepsilon)/k, \gamma)]^r = [A(\chi,k)]^r.$$

This completes the proof of Theorem 3.

3.6.

We show that the assertion in Theorem 3 follows from the assertion in the case where k is a finite algebraic extension of its prime field $\boldsymbol{Q}^{(k)}$.

In fact, assume that k is a field of characteristic 0 and let χ be an absolutely irreducible character of a finite group G over an extension-field of k such that $\chi(g) \in k$ for all $g \in G$. Then $\boldsymbol{Q}^{(k)}(\chi)$ is well-defined and is a subfield of k of a finite degree over $\boldsymbol{Q}^{(k)}$. Applying the homomorphism res : $B(Q^{(k)}(\chi)) \to B(k)$ to the equalithy $[A(\Psi^r(\chi), \boldsymbol{Q}^{(k)}(\chi))] = [A(\chi, \boldsymbol{Q}^{(k)}(\chi))]^r$, we obtain:

$$\begin{aligned}[A(\Psi^r(\chi), k)] &= \left[k \otimes_{\boldsymbol{Q}^{(k)}(\chi)} A(\Psi^r(\chi), \boldsymbol{Q}^{(k)}(\chi))\right] = \operatorname{res}\left([A(\Psi^r(\chi), \boldsymbol{Q}^{(k)}(\chi))]\right) \\ &= \operatorname{res}\left([A(\chi, \boldsymbol{Q}^{(k)}(\chi))]^r\right) = \left(\operatorname{res}(A(\chi, \boldsymbol{Q}^{(k)}(\chi)])\right)^r = [A(\chi, k)]^r.\end{aligned}$$

3.7.

We show that Theorem 4 follows from Theorem 3.

In fact, let k' be a splitting field of $A(\chi, k)$ such that $[k' : k]$ is equal to the index m of $A(\chi, k)$ (cf. [R, (7.15), p. 97]). Applying the homomorphism res : $B(k) \to B(k')$ to the equality $[A(\Psi^r(\chi), k)] = [A(\chi, k)]^r$, we obtain:

$$\begin{aligned}\left[k' \otimes_k A(\Psi^r(\chi), k)\right] &= \operatorname{res}\left([A(\Psi^r(\chi), k)]\right) = \operatorname{res}([A(\chi, k)]^r) \\ &= \left(\operatorname{res}([A(\chi, k)])\right)^r = [k' \otimes_k A(\chi, k)]^r = [k']^r = [k'].\end{aligned}$$

Therefore k' is a splitting field of $A(\Psi^r(\chi), k)$ so that we see that m is divisible by the index m_r of $A(\Psi^r(\chi), k)$. Conversely, we have $\chi = \Psi^s(\Psi^r(\chi))$ for an integer s such that $rs \equiv 1 \pmod{|G|}$, so that we see that m divides m_r. Thus $m = m_r$.

Remark In [Oh] Theorem 4 is proved directly by using the Brauer-Witt theorem. Serre ([Serre V]) and Delingne ([De]) have an alternating proof of Theorem 4 by using properties of Adams operators (cf. [Serre IV, 9, 9.1, Exercices 3), a), p. 86] or [CR II, (12.7), p. 316]).

3.8.

(a) Usualy, by an algebraic number field, we mean a finite algebraic extension of $\boldsymbol{Q}$. Thus, for an algebraic number field k and a complex irreducible character χ of a finite group G, "the field $\boldsymbol{Q}(\chi)$" cannot be defined canonically, since generally there exist no fields containing both of k and $\chi(g)$, $g \in G$. Similarly, if F is a field of characteristic 0, then, for a complex irreducible character χ of a finite group, "$F(\chi)$" cannot be defined canonically (cf. [Oh, Theorem 1]). In particular, when χ is a complex irreducible character of a finite group, for a prime number p, we must be careful in using the notation "$\boldsymbol{Q}_p(\chi)$".

Let v be a place of $\boldsymbol{Q}(\chi)$ lying above p, and we identify $\boldsymbol{Q}_p$ with the closure of $\boldsymbol{Q}$ in $\boldsymbol{Q}(\chi)_v$. Then $\boldsymbol{Q}(\chi)_v = \boldsymbol{Q}_p \cdot \boldsymbol{Q}(\chi) = \boldsymbol{Q}_p(\chi)$.

(b) Let p be a prime number and let k be an algebraic number field. Then "$k \cdot \boldsymbol{Q}_p$" cannot be defined canonically.

Let v be a place of k lying above p. If we identify $\boldsymbol{Q}_p$ with the closure $\boldsymbol{Q}_p^{(v)}$ of $\boldsymbol{Q}$ in k_v, then $k_v = k \cdot \boldsymbol{Q}_p$. But, if w is another place of k lying above p, then, as we have seen in Proposition 3 in (2.2), $[k_v : \boldsymbol{Q}_p^{(v)}] \neq [k_w : \boldsymbol{Q}_p^{(w)}]$ generally.

(c) As to "$E \cdot F$" where E and F are extension-fields for some field, there is some discussion in [W, pp. 49–].

Appendix A

In this appendix we shall give another example which shows that the problem (P) in the introduction has a negative answer.

A.1.

First, following Isaacs ([Is, (10.16), p. 169]), we construct, for a given odd prime number p, an irreducible character ζ of a finite group with $m_{\boldsymbol{Q}}(\zeta) = p$.

Let p be an odd prime number and let q be a prime number such that $q \equiv 1 \pmod{p}$ and $q \not\equiv 1 \pmod{p^2}$. By a theorem of Dirichlet, we see that there exists infinite number of such q of the form

$$q = tp^2 + p + 1, \quad t \in N. \tag{A.1.1}$$

Let $\langle x \rangle$ be a cyclic group of order p^2, $\langle y \rangle$ a cyclic group of order q and $f : \langle x \rangle \to \mathrm{Aut}\langle y \rangle$ a homomorphism of $\langle x \rangle$ into $\mathrm{Aut}\langle y \rangle \cong \boldsymbol{Z}/(q-1)\boldsymbol{Z}$ whose image has order p. Let

$$G = \big\langle x, y \mid x^{p^2} = y^q = 1,\ xyx^{-1} = (f(x))(y) \big\rangle. \tag{A.1.2}$$

Assume that

$$xyx^{-1} = y^r, \quad r \in \boldsymbol{Z}, \quad (r, q) = 1, \quad r^p \equiv 1 \pmod{q}. \tag{A.1.3}$$

Then G is a finite group of order $p^2 q$ and contains the normal subgroup $H = \langle x^p, y \rangle = \langle x^p \rangle \times \langle y \rangle$ of order pq. Let C be an algebraic closure of $\boldsymbol{Q}$, and let ε_p and ε_q be a primitive p-th root of 1 in C and a primitive q-th root of 1 in C respectively. Let $\lambda : H \to C^\times$ be the linear character of H

over C which is given by

$$\lambda((x^p)^i y^j) = \varepsilon_p^i \varepsilon_q^j, \quad i, j \in \boldsymbol{Z}, \tag{A.1.4}$$

and put

$$\zeta = \lambda^G = \mathrm{Ind}_H^G(\lambda). \tag{A.1.5}$$

Set

$$k = \boldsymbol{Q}(\zeta) = \boldsymbol{Q}(\{\zeta(g) \mid g \in G\}). \tag{A.1.6}$$

Lemma A.1.1 *ζ is an irreducible character of G over C of degree p.*

In fact, for $g \in G$, let λ^g be the linear character of H over C which is defined by $\lambda^g(h) = \lambda(ghg^{-1})$, $h \in H$. Then we have that

$$\zeta \mid H = \sum_{i=0}^{p-1} \lambda^{x^i} \tag{A.1.7}$$

and $\zeta \mid (G - H) = 0$. For i, $j \in \boldsymbol{Z}$, $0 \leq i \neq j \leq p-1$, we have that

$$\lambda^{x^i}(y) = \lambda(x^i y x^{-i}) = \varepsilon_q^{r^i} \neq \varepsilon_q^{r^j} = \lambda(y^{r^j}) = \lambda^{x^j}(y),$$

so that $\lambda^{x^i} \neq \lambda^{x^j}$. Therefore, by Frobenius reciprocity law, we have that

$$(\zeta, \zeta)_G = (\zeta \mid H, \lambda)_H = \left(\sum_{i=0}^{p-1} \lambda^{x^i}, \lambda \right)_H = 1.$$

Therefore ζ is absolutely irreducible.

Let σ be the element of $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/\boldsymbol{Q}(\varepsilon_p))$ which is given by

$$\sigma(\varepsilon_q) = \varepsilon_q^r. \tag{A.1.7}$$

Lemma A.1.2 *We have that*

$$\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k) = \langle \sigma \rangle \cong \boldsymbol{Z}/p\boldsymbol{Z}.$$

Thus $k = \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)^{\langle\sigma\rangle} = \{z \in \boldsymbol{Q}(\varepsilon_p, \varepsilon_q) \mid \sigma(z) = z\}$ *contains* ε_p.

In fact, for $\tau \in \mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/\boldsymbol{Q})$, let $\lambda^\tau = \tau \circ \lambda$. Then $\lambda^{x^i} = \lambda^{\sigma^i}$ for $i \in \boldsymbol{Z}$, $0 \le i \le p-1$. As $\zeta \mid (G - H) = 0$, we have that

$$k = \boldsymbol{Q}\Bigl(\sum_{i=0}^{p-1} \lambda^{x^i}\Bigr) = \boldsymbol{Q}\Bigl(\sum_{i=0}^{p-1} \lambda^{\sigma^i}\Bigr) \subset \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)^{\langle\sigma\rangle}.$$

Therefore the inclusion $\langle\sigma\rangle \subset \mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k)$ is clear.

Conversely, let τ be any element of $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k)$. Then

$$\sum_{i=0}^{p-1} \lambda^{\sigma^i} = \zeta \mid H = (\zeta \mid H)^\tau = \sum_{i=0}^{p-1} \lambda^{\sigma^i \tau}.$$

Therefore, by the linearly independence of the irreducible characters of H over C, we see that we must have that $\lambda^\tau = \lambda^{\sigma^i}$ for some $i \in \boldsymbol{Z}$, $0 \le i \le p-1$. But, as $\boldsymbol{Q}(\lambda) = \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$, we must have that $\tau = \sigma^i \in \langle\sigma\rangle$. Thus $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k) \subset \langle\sigma\rangle$.

Lemma A.1.3 *$A(\zeta, k)$ is isormorphic over k to the cyclic algebra $(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k, \sigma, \varepsilon_p)$ over k.*

Proof. We repeat the argument in the proof of Proposition 3.5 of [Y, p. 24].

Let $\psi : G \to C$ be the function on G with values in C which is defined by

$$\psi(g) = \begin{cases} \lambda(g) & \text{if } g \in H, \\ 0 & \text{if } g \notin H. \end{cases}$$

For $g \in G$, let $U(g)$ be the $p \times p$ matrix whose (i,j)-th entry is $\psi(x^{i-1} g x^{-(j-1)})$, $1 \le i,\ j \le p$. Then the mapping $g \mapsto U(g)$, $g \in G$, is the representation of G over C which is induced by λ. As

$$k[G] = \sum_{i=0}^{p-1} k[H] x^i,$$

we have

$$\mathrm{env}_k(U) := U(k[G]) = \sum_{i=0}^{p-1} U(k[H])U(x)^i,$$

where U is extended to a representation of $k[G]$ by linearlity. For $h \in H$, we have

$$\begin{aligned} U(h) &= \mathrm{diag}\left(\lambda(h), \lambda(xhx^{-1}), \lambda(x^2hx^{-2}), \ldots, \lambda(x^{p-1}hx^{-(p-1)})\right) \\ &= \mathrm{diag}\left(\lambda(h), \sigma(\lambda(h)), \sigma^2(\lambda(h)), \ldots, \sigma^{p-1}(\lambda(h))\right). \end{aligned}$$

Put

$$\Xi = \left\{ \mathrm{diag}(\xi, \sigma(\xi), \sigma^2(\xi), \ldots, \sigma^{p-1}(\xi)) \mid \xi \in k(\lambda) \right\} = U(k[H]).$$

Then the mapping $\rho : \xi \mapsto \mathrm{diag}(\xi, \sigma(\xi), \sigma^2(\xi), \ldots, \sigma^{p-1}(\xi))$, $\xi \in k(\lambda)$, induces an isomorphism of $k(\lambda) = \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$ onto Ξ. We have that $\mathrm{env}_k(U) = \sum_{i=1}^{p-1} \Xi \cdot U(x)^i$. Let

$$\sigma' = \rho \circ \sigma \circ \rho^{-1} : \Xi \to \Xi.$$

Then, for $\xi = \lambda(h)$, $h \in H$, we have:

$$U(x)\rho(\xi)U(x)^{-1}$$

$$= \begin{bmatrix} 0 & 1 & & & & \\ & 0 & 1 & & O & \\ & & \cdot & \cdot & & \\ & & & \cdot & \cdot & 1 \\ & O & & & \cdot & \\ \varepsilon_p & & & & & 0 \end{bmatrix} \begin{bmatrix} \xi & & & & \\ & \sigma(\xi) & & & O \\ & & \cdot & & \\ & & & \cdot & \\ & O & & & \cdot \\ & & & & \sigma^{p-1}(\xi) \end{bmatrix} \begin{bmatrix} 0 & & & & & \varepsilon_p^{-1} \\ 1 & 0 & & & O & \\ & 1 & \cdot & & & \\ & & \cdot & \cdot & & \\ & O & & \cdot & \cdot & \\ & & & & 1 & 0 \end{bmatrix}$$

$$= \mathrm{diag}\left(\sigma(\xi), \sigma^2(\xi), \ldots, \sigma^{p-1}(\xi), \xi\right) = \rho\big(\sigma(\rho^{-1}(\rho(\xi)))\big) = \sigma'(\rho(\xi)).$$

Therefore we see that, for all $X \in \Xi$, we have

$$U(x)XU(x)^{-1} = \sigma'(X).$$

Thus we see that the matrics $U(1)$, $U(x)$, $U(x)^2, \ldots, U(x)^{p-1}$ are linearly independent over the field Ξ. And we have

$$U(x)^p = \mathrm{diag}(\varepsilon_p, \varepsilon_p, \ldots, \varepsilon_p) = \varepsilon_p \cdot 1_p = \rho(\varepsilon_p).$$

Thus

$$A(\zeta, k) \underset{U}{\cong} \mathrm{env}_k(U) = (k(\lambda) \cdot 1_p / k \cdot 1_p, \sigma', \varepsilon_p \cdot 1_p) \underset{k}{\cong} (k(\lambda)/k, \sigma, \varepsilon_p).$$

Lemma A.1.4 (see Proof of (10.16) of [Is]) *We have that*

$$\varepsilon_p \notin N_{k(\lambda)/k}(k(\lambda)^\times).$$

Proposition A.1.1 *$D = (k(\lambda)/k, \sigma, \varepsilon_p)$ is a division algebra over k with the index p. Thus $m_k(\zeta) = p$.*

Proof. By Lemma A.1.4, we see that the index m of D is > 1. But, as $[D : k] = p^2$ and $[k(\lambda) : k] = p$, we see that $k(\lambda)$ is a maximal commutative subfield of D. Therefore $k(\lambda)$ is a splitting field of D. Therefore m divides $p = [k(\lambda) : k]$, and, as $m > 1$, we must have that $m = p$. And we see that D is a division algebra over k with centre k.

Proposition A.1.2 *Let v be a place of k and let $D_v = k_v \otimes_k D$. Then, if v is not lying above q, the index of D_v is 1. If v lies above q, then the index of D_v is equal to p.*

Proof. If v is infinite, then v is imaginary so that the index of D_v is 1. Assume that v is finite. If v is not lying above q, then, as $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q) \supset k \supset \boldsymbol{Q}(\varepsilon_p)$, v is unramified in $k(\lambda) = \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$ over k, so that the index of D_v is 1. Assume that v lies above q. By Proposition A.1.1, the index of D is p, so that, the index of D_v must be p for some v. Thus, by Benard's theorem (Theorem 1 in the introduction), the index of D_v must be p for all v.

A.2.

Let the notation be as in (A.1). We assume that q is of the form tp^2+p+1 for some $t \in \boldsymbol{N}$. We prove

Proposition A.2.1 *Let v be a place of k lying above q. Then there exists a finite algebraic extension k' of k which has at least two places w, w' lying above v such that $[k'_w : k_v^{(w)}] = 1$ and $[k'_{w'} : k_v^{(w')}] = p$, where $k_v^{(w)}$ and $k_v^{(w')}$ are the closures of k in k'_w and $k'_{w'}$ respectively.*

Let v' be a place of $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$ lying above v and let C' be an algebraic closure of $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)_{v'}$. We identify k_v with the closure of k in $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)_{v'}$ and $\boldsymbol{Q}_q$ with the closure of $\boldsymbol{Q}$ in $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)_{v'}$. Thus $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)_{v'} = \boldsymbol{Q}_p(\varepsilon_p, \varepsilon_q) = k_v(\varepsilon_q)$. Put

$$n = (q^p - 1)/(q-1) = q^{p-1} + q^{p-2} + \cdots + q + 1 \quad (> q+1 > p+2).$$

Then $(q-1, n) = (q-1, (q^{p-1}-1) + (q^{p-2}-1) + \cdots + (q-1) + p) = p$ and n is odd. As $q = p(tp+1)+1$, we have:

$$\begin{aligned} q^p - 1 &= p^p(tp+1)^p + p \cdot p^{p-1}(tp+1)^{p-1} + \cdots + (p(p-1)/2) \cdot p^2(tp+1)^2 \\ &\qquad + p \cdot p(tp+1) + 1 - 1 \\ &= p^2(tp+1)(pa+1), \end{aligned}$$

where a is some positive integer. Therefore $\mathrm{ord}_p(q^p-1) = 2$. Therefore, as $\mathrm{ord}_p(q-1) = 1$, we have that $\mathrm{ord}_p n = 1$.

Let m be an odd prime number $\neq p$ which divides n. We note that $(m, pq) = 1$. Let s be a prime number $\neq q$, and let $f(X) = X^m - s \in \boldsymbol{Q}[X]$, where X is a variable. Then $f(X)$ is an irreducible polynomial in $\boldsymbol{Q}[X]$. Let ε_m be a primitive m-th root of 1 in C'. As m divides $n = (q^p-1)/(q-1)$ and as $(n, q-1) = p$, we have that $q^p \equiv 1 \pmod m$ and $q \not\equiv 1 \pmod m$. Let h_0 be the smallest positive integer such that $q^{h_0} \equiv 1 \pmod m$. Then we see that h_0 divides p and $h_0 \neq 1$. Therefore $h_0 = p$, and we see that $[\boldsymbol{Q}_q(\varepsilon_m) : \boldsymbol{Q}_q] = p$. As $\boldsymbol{Q}_q(\varepsilon_q)$ is totally ralified over $\boldsymbol{Q}_q$ and $\boldsymbol{Q}_q(\varepsilon_m)$ is unramified over $\boldsymbol{Q}_q$, we have $\boldsymbol{Q}_q(\varepsilon_q) \cap \boldsymbol{Q}_q(\varepsilon_q) = \boldsymbol{Q}_q$. Therefore we have that $[\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m) : \boldsymbol{Q}_q(\varepsilon_q)] = [\boldsymbol{Q}_q(\varepsilon_m) : \boldsymbol{Q}_q] = p$.

Lemma A.2.1 *We have that* $[\boldsymbol{Q}_q(\varepsilon_q) : k_v] = p$ *(note that* $\varepsilon_p \in \boldsymbol{Q}_q$*) and there is a canonical isomorphism of* $\mathrm{Gal}(\boldsymbol{Q}_q(\varepsilon_q)/k_v)$ *onto* $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k)$.

For example, we can argue as follow.

Let ρ be the canonical homomorphism of $\mathrm{Gal}(\boldsymbol{Q}_q(\varepsilon_q)/k_v)$ into $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k) = \langle \sigma \rangle$ given by $\rho(\tau) = \tau \mid \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$. Let u be the smallest positive integer such that σ^u is a generator of the image of ρ, and put $\tilde{\sigma} = \rho^{-1}(\sigma^u)$. Then $D_v = k_v \otimes_k D = k_v \otimes_k (\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k, \sigma, \varepsilon_p)$ is similar to the cyclic algebra $(\boldsymbol{Q}_q(\varepsilon_q)/k_v, \tilde{\sigma}, \varepsilon_p)$ over k_v. But, by Propisition A.1.2, we see that D_v has the index p. Therefore we conclude that $\boldsymbol{Q}_q(\varepsilon_q) \neq k_v$, hence $[\boldsymbol{Q}_q(\varepsilon_q) : k_v] = \rho$ and ρ is an isomorphism of $\mathrm{Gal}(\boldsymbol{Q}_q(\varepsilon_q)/k_v)$ onto $\mathrm{Gal}(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k)$ ($\cong \boldsymbol{Z}/p\boldsymbol{Z}$).

As $(s,q) = 1$, we have that $\mathrm{mod}_{\boldsymbol{Q}_q}(s) = |s|_q = 1$, so $s \in \boldsymbol{Z}_q^\times$. As $(m, q-1) = 1$, by Lemma 1 in (1.3), we see that there is an element α of $\boldsymbol{Z}_q^\times$ such that $\alpha^m = s$. We have

$$f(X) = x^m - s = \prod_{j=0}^{m-1} (X - \varepsilon_m^j \alpha)$$

in $C'[X]$.

Lemma A.2.2 *For $j \in N$, $1 \leq j \leq m-1$, we have that $[\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m^j \alpha) : k_v(\varepsilon_m^j \alpha)] = [k_v(\varepsilon_m^j \alpha) : k_v] = p$.*

In fact, put $K = k_v(\varepsilon_m^j \alpha)$, and consider the following diagram

$$\begin{tikzcd}[column sep=small]
 & \boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m^j \alpha) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \boldsymbol{Q}_q(\varepsilon_q) \arrow[dl, dash] \\
 & K \cap \boldsymbol{Q}_q(\varepsilon_q) =: K_0 \arrow[d, dash] & \\
 & k_v. &
\end{tikzcd} \tag{$*$}$$

By Lemma A.2.1, we have that $[\boldsymbol{Q}_q(\varepsilon_q) : k_v] = p$, so that $k_0 = \boldsymbol{Q}_q(\varepsilon_q)$ or $K_0 = k_v$. Suppose that $K_0 = \boldsymbol{Q}_q(\varepsilon_q)$. Then $K \supset \boldsymbol{Q}_q(\varepsilon_q)$, so $K = \boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m)$. Therefore we have:

$$\begin{aligned} p &= [\boldsymbol{Q}_q(\varepsilon_m) : \boldsymbol{Q}_q] \geq [k_v(\varepsilon_m) : k_v] \text{ (cf. (}**\text{) below) } = [K : k_v] \\ &= [\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m) : k_v] = \left[\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m^j) : \boldsymbol{Q}_q(\varepsilon_q)\right] \cdot [\boldsymbol{Q}_q(\varepsilon_q) : k_v] = p^2, \end{aligned}$$

which is a contradiction.

$$
\begin{tikzcd}[column sep=small]
 & k_v(\varepsilon_m) \arrow[dl, dash] \arrow[dr, dash] & \\
\boldsymbol{Q}_q(\varepsilon_m) \arrow[dr, dash] & & k_v \arrow[dl, dash] \\
 & \boldsymbol{Q}_q(\varepsilon_m) \cap k_v \arrow[d, dash] & \\
 & \boldsymbol{Q}_q &
\end{tikzcd}
\tag{$**$}
$$

In view of the diagra $(*)$, we find:

$$
\begin{aligned}
[K : k_v] &= \left[\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m^j\alpha) : \boldsymbol{Q}_v(\varepsilon_q)\right] = \left[\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m^j) : \boldsymbol{Q}_q(\varepsilon_q)\right] \\
&= [\boldsymbol{Q}_q(\varepsilon_q, \varepsilon_m) : \boldsymbol{Q}_q(\varepsilon_q)] = [\boldsymbol{Q}_q(\varepsilon_m) : \boldsymbol{Q}_q] = p.
\end{aligned}
$$

This proves Lemma A.2.2.

We can consider k as a subfield of k_v, and $\alpha \in \boldsymbol{Q}_q \subset k_v$.

Lemma A.2.3 *We have that $\alpha \notin k$.*

In fact, suppose, on the contrary that $\alpha \in k$. As $f(X) = x^m - s$ $(= \prod_{j=0}^{m-1}(X - \varepsilon_m^j\alpha))$ is irreducible in $\boldsymbol{Q}[X]$, the conjugates of α over $\boldsymbol{Q}$ are α, $\varepsilon_m\alpha$, $\varepsilon_m^2\alpha, \dots, \varepsilon_m^{m-1}\alpha$. For $j \in \boldsymbol{N}$, $1 \le j \le m-1$, let τ_j be the embedding of $\boldsymbol{Q}(\alpha)$ into the algebraic closure $\bar{k}$ of k in C' which is given by $\tau_j(\alpha) = \varepsilon_m^j\alpha$. Then τ_j can be extended to an embedding $\tilde{\tau}_j$ of k into $\bar{k}$. As k is a Galois extension of $\boldsymbol{Q}$, k is a normal extension of $\boldsymbol{Q}$ so that $\tilde{\tau}_j(k) = k$. Therefore $\varepsilon_m^j\alpha \in k$. This holds for all j, $1 \le j \le m-1$. But, by Lemma A.2.2, we see that $\varepsilon_m^j\alpha \notin k_v$ for $1 \le j \le m-1$. Therefore $\varepsilon_m^j\alpha \notin k$ for $1 \le j \le m-1$. This is a contradiction. Therefore $\alpha \notin k$.

Let $f(X) = f_1(X) \cdots f_u(X)$ be the irreducible decomposition of $f(X) = x^m - s$ in $k[X]$. As $f(\alpha) = 0$ in $k_v[X]$, we must have that $f_i(\alpha) = 0$ for some i, $1 \le i \le u$. By Lemma A.2.3, we see that $\deg(f_i(X)) > 1$. Therefore $f_i(\varepsilon_m^j\alpha) = 0$ for some j, $1 \le j \le m-1$. Let $g(X)$ be the minimal polynomial of $\varepsilon_m^j\alpha$ over k_v. Then, in $k_v[X]$, $X - \alpha$ and $g(X)$ divide $f_i(X)$. By Lemma A.2.2, we see that $\deg(g(X)) = p$. Therefore, by (1.4), we see that $k' := k[X]/f_i(X)k[X]$ has (at least) two places w, w' lying above v such that $[k'_w : k_v^{(w)}] = 1$ and $[k'_{w'} : k_v^{(w')}] = p$.

This completes the proof of Proposition A.2.1.

Let $A = A(\zeta, k)$ and $A' = k(\zeta, k')$ ($\cong k' \otimes_k A$). Let v, k', w, w' be as in Proposition A.2.1. Then, by (1.5.3) in (1.5), we have:

$$\mathrm{inv}_w[A'] = \left[k'_w : k_v^{(w)}\right] \cdot \mathrm{inv}_v[A] = 1 \cdot \left(\frac{i}{p} \bmod 1\right) = \frac{i}{p} \bmod 1$$

for some interger i such that $(i, p) = 1$, and

$$\mathrm{inv}_{w'}[A'] = \left[k'_{w'} : k_v^{(w')}\right] \cdot \mathrm{inv}_v[A] = p \cdot \left(\frac{i}{p} \bmod 1\right) = 0 \bmod 1.$$

Thus we have obtained a new example which shows that the problem (P) in the introduction has a negative answer.

Appendix B

Let the notation be as in Appendix A. In this opportunity, it will be interesting to know the Hasse invariants of D. To do so, it will be convenient to use the concept of a prime of an algebraic number field instead of a place. For a prime P of an algebraic number field k'', let k''_P denote the completion of k'' at P.

B.1.

Let a be an interger such that

$$ra^{\frac{q-1}{p}} \equiv 1 \pmod{q}$$

and $a \bmod q\boldsymbol{Z}$ has the order p in $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$. $\boldsymbol{Z}[\varepsilon_p]$ is the integral closure of $\boldsymbol{Z}$ in $\boldsymbol{Q}(\varepsilon_p)$. Let

$$\mathfrak{q}_i = (q, \varepsilon_p - a^i) = q\boldsymbol{Z}[\varepsilon_p] + (\varepsilon_p - a^i)\boldsymbol{Z}[\varepsilon_p], \quad 1 \leq i \leq p-1.$$

Then we see that $\mathfrak{q}_1, \ldots, \mathfrak{q}_{p-1}$ are all the distinct prime ideals of $\boldsymbol{Z}[\varepsilon_p]$ lying above $q\boldsymbol{Z}$ (cf., e.g., [La, p. 11]). $\boldsymbol{Z}[\varepsilon_p, \varepsilon_q]$ is the integral clousure of $\boldsymbol{Z}[\varepsilon_p]$ in $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$. Let

$$\begin{aligned} Q_i &= \bigl(q, \varepsilon_p - a^i, \varepsilon_q - 1\bigr) \\ &= q\boldsymbol{Z}[\varepsilon_p, \varepsilon_q] + (\varepsilon_p - a^i)\boldsymbol{Z}[\varepsilon_p, \varepsilon_q] + (\varepsilon_q - 1)\boldsymbol{Z}[\varepsilon_p, \varepsilon_q], \quad 1 \le i \le p-1. \end{aligned}$$

Then we see that, for $i \in \boldsymbol{N}$, $1 \le i \le p-1$, Q_i is the unique prime ideal of $\boldsymbol{Z}[\varepsilon_p, \varepsilon_q]$ lying above $\mathfrak{q}_i$. $Q_1, \dots, Q_{p-1}$ are all the distinct prime ideals of $\boldsymbol{Z}[\varepsilon_p, \varepsilon_q]$ lying above $q\boldsymbol{Z}$.

Let O_k be the integral closure of $\boldsymbol{Z}$ in k, and let

$$\mathfrak{q}'_i = Q_i \cap O_k, \quad 1 \le i \le p-1.$$

Then $\mathfrak{q}'_1, \dots, \mathfrak{q}'_{p-1}$ are all the dinstinct prime ideals of O_k lying above $q\boldsymbol{Z}$ and $\mathfrak{q}'_i\boldsymbol{Z}[\varepsilon_p, \varepsilon_q] = Q_i^p$, $1 \le i \le p-1$.

B.2.

Recall that

$$A(\zeta, k) \cong D = \bigl(\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)/k, \sigma, \varepsilon_p\bigr) = \sum_{i=0}^{p-1} \boldsymbol{Q}(\varepsilon_p, \varepsilon_q) u^i,$$

$$u\xi u^{-1} = \sigma(\xi), \quad \xi \in \boldsymbol{Q}(\varepsilon_p, \varepsilon_q),$$

$$u^p = \varepsilon_p.$$

We note that any $\mathfrak{q}'_i$ is totally ramified in $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)$ over k.

Let $k[u]$ be the subalgebra of D over k which is generated over k by u. Then we see that $k[u]$ is a maximal commutative subfield of D over k in which any $\mathfrak{q}'_i$ is unramified over k. We may write as $k[u] = k(u)$. Let τ be the automorphism of $k(u)$ over k which is given by

$$\tau(u) = u^q = \varepsilon_p^{(q-1)/p} u.$$

Then we see that, for $i \in \boldsymbol{N}$, $1 \le i \le p-1$, if Q'_i denotes a prime of $k(u)$ lying above $\mathfrak{q}'_i$, then τ can be canonically identified with the Frobenius automorphism of $k(u)_{Q'_i}$ over $k_{\mathfrak{q}'_i}$. Put

$$\delta = \sum_{i=0}^{p-1} \varepsilon_p^{i(q-1)/p} \varepsilon_q^{r^i}.$$

Then we see that $\delta \neq 0$. Put

$$v_\tau = \sum_{i=0}^{p-1} \delta u^i \quad (\in D^\times).$$

Then we see that

$$v_\tau \xi v_\tau^{-1} = \tau(\xi), \quad \xi \in k(u)$$

and

$$v_\tau^p = \delta^p N_{K(u)/k}\left(\sum_{i=0}^{p-1} u^i\right).$$

Therefore we have that

$$D = \big(k(u)/k, \tau, v_\tau^p\big),$$

which is similar to

$$D' = (k(u)/k, \tau, \delta^p).$$

Let $\mathfrak{q}' = \mathfrak{q}_1'$ and $Q = Q_1$. Let $v_Q : \boldsymbol{Q}(\varepsilon_p, \varepsilon_q)_Q^\times \to \boldsymbol{Z}$ be the normalized valuation of $\boldsymbol{Q}(\varepsilon_p, \varepsilon_q)_Q$ and by using the condition that $r \cdot a^{q-1/p} \equiv 1 \pmod{q}$, we see, by a relatively long calculation, that

$$v_Q(\delta) = 1.$$

Let $v_{\mathfrak{q}'} : k_{\mathfrak{q}'}^\times \to \boldsymbol{Z}$ be the normalized valation of $k_{q'}$. Then it follows that

$$v_{\mathfrak{q}'}(\delta^p) = 1.$$

Thus

$$\mathrm{inv}_{q'}[D] = \mathrm{inv}_{q'}[D'] = \frac{v_{\mathfrak{q}'}(\delta^p)}{p} \bmod 1 = \frac{1}{p} \bmod 1.$$

Let $i \in \boldsymbol{Z}$, $1 \leq i \leq p-1$, and let i' be an integer such that $i'i \equiv 1$

(mod p). Then by Theorem 2 in the introduction, we see that

$$i' \cdot \mathrm{inv}_{\mathfrak{q}'_i}[D] = \mathrm{inv}_{\mathfrak{q}'}[D] = \frac{1}{p} \bmod 1.$$

Thus

$$\mathrm{inv}_{\mathfrak{q}'_i}[D] = \frac{i}{p} \bmod 1.$$

B.3.

Remark (a) If we use Fontaine's describtion on page 131, lines 3–7, in [F], we can obtain the same result as above more speedily.

(b) In [Is], Isaacs constructed the character ζ as an example which shows that the Schur index may become large. In [Br], R. Brauer constructed, for each $n \in \boldsymbol{N}$, an irreducible character χ of a finite group whose Schur index is n. By the above Fontaine's method, we can calculate the Hasse invariants of the simple algebra corresponding to χ.

Acknowledgement I wish to dedicate this paper to my daughter Fumiko.

References

[Be] Benard M., *The Schur subgroup I.* J. Algebra **22** (1972), 374–377.

[BS] Benard M. and Schacher M. M., *The Schur subgroup II.* J. Algebra **22** (1972), 378–385.

[Bour I] Bourbaki N., Algèbre. Hermann, Paris, 1958.

[Bour II] Bourbaki N., Intégration. Hermann, Paris, 1963.

[Br] Brauer R., Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen. Collected Papers Vol. I, pp. 88–102. The MIT Press, 1980.

[CR I] Curtis C. W. and Reiner I., Representation theory of finite groups and associative algebras. Interscience, Wiley & Sons, 1962.

[CR II] Curtis C. W. and Reiner I., Methods of representation theory with applications to finite groups and orders, Vol. I, II. Interscience, Wiley & Sons, 1981.

[De] Deligne P., A letter to the author.

[Deu] Deuring M., Algebren. Springer-Verlag, 1968.

[F] Fontaine J. M., *Sur la décomposition des algèbres de groupes.* Ann. Scient. Éc. Norm. Sup., 4^0 série, t.4 (1971), 122–180.

[G] Gow R., *Schur indices of some groups of Lie type.* J. Algebra **42** (1976), 102–120.

[Is] Isaacs I. M., Character theory of finite groups. Academic Press, Inc., (London) LTD., 1976.

[La] Lang S., Algebraic number theory. Addison-Wesley Publishing Company, INC., 1970.

[Lu] Lusztig G., *Coxeter orbits and eigenspaces of Frobenius.* Invent. Math. **38** (1976), 101–151.

[Oh] Ohmori J., *On Feit's definition of the Schur index.* Hokkaido Math. J. **33** (2004), 299–317.

[R] Reiner I, Maximal orders. Oxford, 2003.

[Sch] Schmid P., *Represetation groups for the Schur index.* J. Algebra **97** (1985), 101–115.

[Serre I] Serre J.-P., Local class field theory. In Algebraic Number Theory, ed., by Cassels and Fröhlich, Chap. VI, pp. 128–161. Academic Press, 1967.

[Serre II] Serre J.-P., Corps locaux. Hermann, Paris, 1968.

[Serre III] Serre J.-P., Cours d'artithmétique. Universitaires de France, 1970.

[Serre IV] Serre J.-P., Représenations linéaires des groupes finis. Hermann. Paris, 1971.

[Serre V] Serre J.-P., A letter to the author.

[W] Weil A., Basic number theory. 2nd ed., Springer-Verlag, 1973.

[Y] Yamada T., The Schur subgroup of the Brauer group. Lecture Notes in Mathematics **397**, Springer-Verlag, 1974.

Mathematics Department
Hokkaido University of Education
Sapporo Campus
5-3-1-5 Ainosato, Kita-ku
Sapporo 002-8502
Hokkaido, Japan