Hokkaido Mathematical Journal Vol. 28 (1999) p. 39–55

On the Schur indices of certain irreducible characters of finite Chevalley groups

Zyozyu OHMORI

(Received September 27, 1996; Revised March 23, 1998)

Abstract. Let G be a finite Chevalley group of split type. We shall give some sufficient conditions subject for that G has irreducible characters of the Schur index equal to 2.

Key words: Chevalley groups, irreducible characters, Schur index.

Introduction

Let F_q be a finite field with q elements of characteristic p. Let $\boldsymbol{G}$ be a connectecd, reductive algebraic group defined over F_q, and let $F : \boldsymbol{G} \rightarrow \boldsymbol{G}$ be the corresponding Frobenius endomorphism of $\boldsymbol{G}$. In the following, if H denotes an F-stable subgroup of $\boldsymbol{G}$, then the group of F-fixed points of $\boldsymbol{H}$ will be denoted by H. Let $\boldsymbol{B}$ be an F-stable Borel subgroup of $\boldsymbol{G}$, and let $\boldsymbol{U}$ be the unipotent radical of $\boldsymbol{B}$. Then $\boldsymbol{U}$ is F-stable and U is a Sylow p-subgroups of $\boldsymbol{G}$. According to a theorem of Gel'fand-Graev-Yokonuma-Steinberg, if λ is a linear character of U in "general position", then the character λ^G of G induced by λ is multiplicity-free (see Steinberg [13, Theorem 49, p. 258] and Carter [2, Theorem 8.1.3]). In [5], R. Gow has initiated to study the rationality-properties of the characters λ^G where λ runs over certain linear characters of U and, using the results obtained there, he obtained some informations about the Schur indices of some irreducible characters of G (also cf. A. Helversen-Pasoto [7]). He has treated the case that $\boldsymbol{G} = GL_n$, SL_n and Sp_{2n}. In [10], we have obtained some results about the rationality of the λ^G when $\boldsymbol{G}$ is a general reductive group. Our intension here is to get more precise results when $\boldsymbol{G}$ is a simple algebraic group. The twisted cases are treated in [12]. So, in this paper, we shall treat the untwisted cases. We shall obtain some sufficient conditions subject for that the Schur index of any irreducible character of G is equal to one and some sufficient conditions subject for that G has irreducible characters of the Schur index equal to 2.

1991 Mathematics Subject Classification : 20G05.

We note that the results of this paper have been announced in [11].

1. Linear characters of $\boldsymbol{U}$

Let K be an algebraic closure of F_q. Let $\boldsymbol{G}$ be an simple algebraic group over K. We assume that G is defined and split over F_q. Let $F : \boldsymbol{G} \to \boldsymbol{G}$ be the corresponding Frobenius endomorphism of $\boldsymbol{G}$. We shall fix an F-stable Borel subgroup $\boldsymbol{B}$ of G and an F-stable maximal torus $\boldsymbol{T}$ of $\boldsymbol{G}$ contained in $\boldsymbol{B}$. Let $\boldsymbol{U}$ be the unipotent radical of $\boldsymbol{B}$. Let R, R^+ and Δ be respectively the set of roots of $\boldsymbol{G}$ with respect to $\boldsymbol{T}$, the set of positive roots determined by $\boldsymbol{B}$ and the set of corresponding simple roots. For a root α, let $\boldsymbol{U}_\alpha$ be the root subgroup of $\boldsymbol{G}$ associated with α. Let $X = \mathrm{Hom}(\boldsymbol{T}, K^\times)$ be the character module of $\boldsymbol{T}$. Then F acts on X by $(F\chi)(t) = \chi(F(t))$ for $\chi \in X$, $t \in \boldsymbol{T}$. As $\boldsymbol{T}$ splits over F_q, we have $F(t) = t^q$, $t \in \boldsymbol{T}$, so we have $F\chi = q\chi$, $\chi \in X$.

Let $\boldsymbol{U}. = \langle \boldsymbol{U}_\alpha \mid \alpha \in R^+ - \Delta \rangle$. Then $\boldsymbol{U}.$ is an F-stable normal subgroup of $\boldsymbol{U}$ and contains the derived group of $\boldsymbol{U}$. It is known that if p is not a bad prime for $\boldsymbol{G}$, then $\boldsymbol{U}.$ coincides with the commutator subgroup of $\boldsymbol{U}$. We have $\boldsymbol{U}/\boldsymbol{U}. = \prod_{\alpha\in\Delta} \boldsymbol{U}_\alpha = \prod_{\alpha\in\Delta} F_q$ (we note that each $\boldsymbol{U}_\alpha$ is F-stable since $\boldsymbol{G}$ splits over F_q).

Let Λ be the set of all linear characters λ of U such that $\lambda \mid U. = 1$, and let Λ_0 be the set of all λ in Λ such that $\lambda \mid U_\alpha \neq 1$ for all $\alpha \in \Delta$.

Lemma 1 (Gel'fand-Graev [4], Yokonuma [15], Steinberg [13]) *If $\lambda \in \Lambda_0$, then λ^G is multiplicity-free.*

For a subset J of Δ, put $\boldsymbol{T}_J = \bigcap_{\alpha\in J} \mathrm{Ker}\,\alpha$ (we put $\boldsymbol{T}_\phi = \boldsymbol{T}$). Then, for any such J, $\boldsymbol{T}_J$ is an F-stable subgroup of $\boldsymbol{T}$.

Lemma 2 (cf. Yokonuma [15], Steinberg [13, Exercise on p. 263]) *If $\lambda \in \Lambda_0$, then there is a set S of subsets J of Δ such that S contains Δ and ϕ and that $(\lambda^G, \lambda^G)_G = \sum_{J\in S} |T_J|$.*

This is proved in [12]. The next lemma is also proved in [12].

Lemma 3 ([12, Proposition 1]) *Let c be the order of the centre Z of G. Then if $\lambda \in \Lambda_0$, there is a positive integer r such that $(\lambda^G, \lambda^G)_G = r(q-1) + c$.*

Let $\lambda \in \Lambda_0$. Let $\eta_1, \ldots, \eta_c$ be all the irreducible characters of the centre

Z. For $1 \leqq i \leqq c$, put $\Gamma_{\lambda,i} = \mathrm{Ind}_{UZ}^{G}(\lambda\eta_i)$. Then it is easy to see that $\lambda^G = \Gamma_{\lambda,1} + \cdots + \Gamma_{\lambda,c}$ and that (by using Lemma 3)

$$(\Gamma_{\lambda,i}, \Gamma_{\lambda,j})_G = \delta_{ij} \cdot \frac{1}{c} \cdot (\lambda^G, \lambda^G)_G = \delta_{ij}\left\{\frac{r(q-1)}{c} + 1\right\} \qquad (1 \leqq i,\ j \leqq c).$$

(δ_{ij} denotes Kronecker's delta.)

Our purpose is to study the rationality properties of the $\lambda^G, \lambda \in \Lambda$. For that purpose we study the rationality of the λ^B. If $p = 2$, then $U/U.$ is an elementary abelian 2-group, so that all the λ^B are realizable in Q. Therefore in the rest of this paper, we shall assume that $p \neq 2$.

Let ζ_p be a fixed primitive p-th root of unity, and let π be the Galois group of $Q(\zeta_p)$ over Q. Then π acts on $\widehat{F}_q = \mathrm{Hom}(F_q, C^\times)$ naturally. Let $\chi \in \widehat{F}_q$, $\chi \neq 1$. For $a \in F_q$, we define $\chi_a \in \widehat{F}_q$ by $\chi_a(x) = \chi(ax)$, $x \in F_q$. Then we have $\widehat{F}_q = \{\chi_a \mid a \in F_q\}$ and $\{\chi^\sigma \mid \sigma \in \pi\} = \{\chi_a \mid a \in {F_p}^\times\}$.

B acts on Λ by $\lambda^b(u) = \lambda(bub^{-1})$, $b \in B$, $\lambda \in \Lambda$; B fixes Λ_0. Fix a character λ in Λ_0, and set $L = \{b \in B \mid \lambda^b = \lambda^{\tau(b)}$ for some $\tau(b) \in \pi\}$. Put $M = L \cap T$. Then we have $L = MU$ (semidirect product) and we see easily that

$$M = \{t \in T \mid \text{for some } x \in {F_p}^\times : \alpha(t) = x \text{ for all } \alpha \in \Delta\}.$$

This shows that L is independent of the choice of λ in Λ_0 and the mapping $b \to \tau(b)$ is a homomorphism of L into π with kernel ZU (Z is the centre of G). Let f be an element of T such that $\langle\tau(f)\rangle = \tau(L)$ and put $\sigma = \tau(f)$.

Let λ be any character in Λ such that $\lambda \neq 1$. Let $\eta_1, \ldots, \eta_c$ be as before all the irreducible characters of Z ($c = |Z|$). For $1 \leqq i \leqq c$, put $\mu_i = \mathrm{Ind}_{ZU}^{L}(\eta_i\lambda)$. Then we see easily that $\mu_1, \ldots, \mu_c$ are mutually different irreducible characters of L and we have $\lambda^L = \mu_1 + \cdots + \mu_c$.

Now, if χ is an ordinary character of a finite group and k is a field of characteristic 0, tnen $k(\chi)$ denotes the field generated over k by the values of χ. Then we see easily that $Q(\lambda^L) = Q(\zeta_p)^{\langle\sigma\rangle}$ and, for $1 \leqq i \leqq c$, $Q(\mu_i) = Q(\lambda^L)(\eta_i)$. Put $k = Q(\lambda^L)$ and $k_i = Q(\mu_i)$ $(1 \leqq i \leqq c)$. For $1 \leqq i \leqq c$, let A_i be the simple direct summand of the group algebra $k_i[L]$ of L over k_i associated with μ_i. Let $h = (M : Z)$. Then f^h is an element of Z. For $1 \leqq i \leqq c$, put $\theta_i = \eta_i(f^h)$. Then we see that, for $1 \leqq i \leqq c$, A_i is isomorphic over k_i to the cyclic algebra $(\theta_i, k_i(\zeta_p), \sigma_i)$ over k_i, where σ_i is a certain extension of σ to $k_i(\zeta_p)$ over k_i (see Yamada [14, Proposition 3.5]).

2. Calculation of the group M

Let X denote as before the character module $\mathrm{Hom}(\boldsymbol{T}, K^{\times})$ of $\boldsymbol{T}$. Let $P(R)$ and $Q(R)$ denote respectively the weight-lattice of R and the root-lattice of R. Then $P(R) \supset X \supset Q(R)$. We say that $\boldsymbol{G}$ is adjoint if $X = Q(R)$. By [9], we see that if $\boldsymbol{G}$ is adjoint, then τ induces an isomorphism of M with π and f can be chosen so that $\langle f \rangle = M$.

Let $Y = \mathrm{Hom}(K^{\times}, T)$ be the cocharacter module of $\boldsymbol{T}$ written additively. Then the pairing $\langle \chi, \lambda \rangle = \deg(\chi \circ \lambda)$ defines a perfect pairing $\langle\, , \rangle : X \times Y \to Z$. Suppose that $\dim \boldsymbol{T} = \ell$. Let $\{\chi_1, \dots, \chi_\ell\}$ be a basis of X over Z and let $\{\lambda_1, \dots, \lambda_\ell\}$ be the basis of Y dual to it, i.e., $\langle \chi_i, \lambda_j \rangle = \delta_{ij}$. Then each element t of $\boldsymbol{T}$ can be written uniquely as

$$t = h(x_1, \dots, x_\ell) = \lambda_1(x_1) \cdots \lambda_\ell(x_\ell) \quad (x_1, \dots, x_\ell \in K^{\times}).$$

Recall that we have $F\chi_i = q\chi_i$, $1 \leqq i \leqq \ell$.

Lemma 4 *Assume that $\Delta = \{\alpha_1, \dots, \alpha_\ell\}$ and, for $1 \leqq i \leqq \ell$, let $\alpha_i = \sum_{j=1}^{\ell} s_{ij}\chi_j (s_{ij} \in Z)$. Then, for $t \in \boldsymbol{T}$, $t = h(x_1, \dots, x_\ell)$, t lies in M if and only if ${x_j}^q = x_j$ for $1 \leqq j \leqq \ell$ and $\prod_{j=1}^{\ell} {x_j}^{s_{1j}} = \cdots = \prod_{j=1}^{\ell} {x_j}^{s_{\ell j}} = x$ for some $x \in {F_p}^{\times}$.*

Proof. Let $t = h(x_1, \dots, x_\ell)$ be an element of $\boldsymbol{T}$. Then, as $F(t) = t^q$, it is easy to see that $F(h(x_1, \dots, x_\ell)) = h({x_1}^q, \dots, {x_\ell}^q)$. Therefore $F(t) = t$ if and only if ${x_i}^q = x_i$ for $1 \leqq i \leqq \ell$. Next, we have

$$\begin{aligned} \alpha_i(t) &= \alpha_i\left(\prod_{j=1}^{\ell} \lambda_j(x_j)\right) \\ &= \prod_{j=1}^{\ell} {x_j}^{\langle \alpha_i, \lambda_j \rangle} \\ &= \prod_{j=1}^{\ell} {x_j}^{s_{ij}}. \end{aligned}$$

Therefore the assertion in the lemma follows. □

In the following, η is a fixed primitive element of F_q and $\nu = \eta^{(q-1)/(p-1)}$, a primitive element of F_p. If m is an integer, then we denote by $\mathrm{ord}_2 m$ the exponent of the 2-part of m. Put $d = (X : Q(R))$.

Lemma 5 (cf. Gow [5, 6]) *Assume that $\boldsymbol{G}$ is of type (A_ℓ), $\ell \geqq 1$. Then*

$Z \simeq \boldsymbol{Z}/(d, q-1)\boldsymbol{Z}$ *and we have*: (i) *if* $2 \mid \ell(\ell+1)/d$ *or* $\mathrm{ord}_2 d > \mathrm{ord}_2(p-1)$, *then* $\tau(M) = \pi$ *and* f *can be chosen so that* $M = \langle f \rangle \times Z$ *and* $f^{p-1} = 1$. *Assume that* $2 \nmid \ell(\ell+1)/d$ *and* $\mathrm{ord}_2 d \leqq \mathrm{ord}_2(p-1)$. *Then*: (ii) *if* q *is square, then* $\tau(M) = \pi$ *and* f *can be chosen so that* $f^{p-1} = \varepsilon$, *where* ε *is the unique element of* Z *of order* 2; (iii) *if* q *is non-square and* $\mathrm{ord}_2 d = \mathrm{ord}_2(p-1)$, *then* $(\pi : \tau(M)) = 2$ *and* f *can be chosen so that* $M = \langle f \rangle \times Z$ *and* $f^{(p-1)/2} = 1$; (iv) *if* q *is non-square and* $\mathrm{ord}_2 d < \mathrm{ord}_2(p-1)$, *then* $(\pi : \tau(M)) = 2$ *and* f *can be chosen so that* $f^{(p-1)/2} = \varepsilon$.

Proof. We use the notation of Bourbaki [1]. By [1, P1.I, (VIII)], we have $P(R) = \langle \alpha_1, \ldots, \alpha_{\ell-1}, \overline{\omega} \rangle_Z$, where

$$\overline{\omega} = \varepsilon_1 - \frac{1}{\ell+1}(\varepsilon_1 + \cdots + \varepsilon_{\ell+1}) = \frac{1}{\ell+1}\sum_{i=1}^{\ell}(\ell - i + 1)\alpha_i,$$

so that $P(R)/Q(R) = \langle \overline{\omega} + Q(R) \rangle = \boldsymbol{Z}/(\ell+1)\boldsymbol{Z}$. Therefore, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ for $1 \leqq i \leqq \ell - 1$ and $\chi_\ell = \frac{1}{d}\sum_{i=1}^{\ell}(\ell - i + 1)\alpha_i$. Thus $\alpha_i = \chi_i$ for $1 \leqq i \leqq \ell - 1$ and $\alpha_\ell = d\chi_\ell - \sum_{i=1}^{\ell-1}(\ell - i + 1)\chi_i$. It follows from Lemma 4 that, for $t = h(x_1, \ldots, x_\ell) \in \boldsymbol{T}$, we have $t \in M$ if and only if $x_1, \ldots, x_\ell \in {F_q}^\times$ and, for some $x \in {F_p}^\times$, $x_1 = \cdots = x_{\ell-1} = x$ and $x^{-\ell}x^{-(\ell-1)} \cdots x^{-2}{x_\ell}^d = x$, i.e.,

$$ {x_\ell}^d = x^{\ell(\ell+1)/2}. \tag{1}$$

First, as $\boldsymbol{Z} = \bigcap_{\alpha \in \Delta} \operatorname{Ker} \alpha$ ($\boldsymbol{Z}$ is the centre of $\boldsymbol{G}$; we see easily that Z is equal to the group of F_q-rational points of $\boldsymbol{Z}$), we have $Z = \{h(1, \ldots, 1, y) \mid y \in {F_q}^\times,\ y^d = 1\} = \boldsymbol{Z}/(d, q-1)\boldsymbol{Z}$.

Next, we note that we have $\tau(M) = \pi$ if and only if the equation (1) has a solution in ${F_q}^\times$ for $x = \nu$, and when $\tau(M) = \pi$ f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{p-1} = 1$ if and only if that solution can be found in ${F_p}^\times$. We also note that when $\tau(M) \neq \pi$ we have $(\pi : \tau(M)) = 2$ if and only if the equation (1) has a solution in ${F_q}^\times$ for $x = \nu^2$, and if this is the case, then f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{(p-1)/2} = 1$ if and only if that solution can be found in $({F_p}^\times)^2$.

Now the group $({F_p}^\times)^d = \{y^d \mid y \in {F_p}^\times\}$ is the cyclic subgroup of ${F_p}^\times$ of order $a = (p-1)/(d, p-1)$ and the element $\nu^{\ell(\ell+1)/2}$ of ${F_p}^\times$ has the order $b = (p-1)/(\ell(\ell+1)/2, p-1)$. Therefore, for $x = \nu$, the equation (1) has a solution in ${F_p}^\times$ if and only if $b \mid a$, i.e., $(d, p-1) \mid (\ell(\ell+1)/2, p-1)$. But, as $d \mid \ell(\ell+1)$, the latter condition is satisfied if and only if $d \mid \ell(\ell+1)/2$

(i.e. $2 \mid \ell(\ell+1)/d$) or $\mathrm{ord}_2 d > \mathrm{ord}_2(p-1)$ (Case (i)).

Suppose therefore that $2 \nmid \ell(\ell+1)/d$ and $\mathrm{ord}_2 d \leqq \mathrm{ord}_2(p-1)$. If q is square, then $y = \eta^{((q-1)/2(p-1))\ell(\ell+1)/d}$ is a solution of the equation (1) for $x = \nu$ in $F_q{}^{\times}$ and $y^{p-1} = -1$ (Case (ii)). Assume that q is non-square. Then $(q-1)/(p-1)$ is odd and $(d, q-1) \nmid (((q-1)/(p-1))\ell(\ell+1)/2, q-1)$. This means that the equation (1) has no solutions in $F_q{}^{\times}$ for $x = \nu$. But, for $x = \nu^2$, the equation (1) has a solution in $F_p{}^{\times}$, e.g., $y = \nu^{\ell(\ell+1)/d}$ (cf. $y^{(p-1)/2} = -1$). As $(F_p{}^{\times})^{2d}$ is a cyclic group of order $((p-1)/2)/(d, (p-1)/2)$ and $\nu^{2 \cdot \ell(\ell+1)/2}$ is of order $((p-1)/2)/(\ell(\ell+1)/2, (p-1)/2)$, the equation (1) has a solution in $(F_p{}^{\times})^2$ for $x = \nu^2$ if and only if $(d, (p-1)/2) \mid (\ell(\ell+1)/2, (p-1)/2)$, i.e., $\mathrm{ord}_2 d > \mathrm{ord}_2(p-1)/2$, i.e., $\mathrm{ord}_2 d = \mathrm{ord}_2(p-1)$ (Cases (iii), (iv)).

This proves Lemma 5. □

We note that the case $G = SL_{\ell+1}$ of Lemma 5 was treated by Gow ([5, 6]).

Lemma 6 *Assume that G is non-adjoint and of type (B_ℓ), $\ell \geqq 2$ (i.e. $G = \mathrm{Spin}_{2\ell+1}$). Then $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z}$. And:* (i) *if $4 \mid \ell(\ell+1)$, then $\tau(M) = \pi$ and f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{p-1} = 1$. Assume that $4 \nmid \ell(\ell+1)$. Then:* (ii) *if q is square, we have $\tau(M) = \pi$ and $f^{p-1} = \varepsilon$, where ε is the generator of Z;* (iii) *if q is non-square and $p \equiv -1 \pmod 4$, we have $(\pi : \tau(M)) = 2$ and f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{(p-1)/2} = 1$;* (iv) *if q is non-square and $p \equiv 1 \pmod 4$, we have $(\pi : \tau(M)) = 2$ and $f^{(p-1)/2} = \varepsilon$.*

Proof. By [1, PL.2, (VIII)], we have $P(R) = \langle \overline{\omega}, \alpha_2, \ldots, \alpha_\ell \rangle$, where $\overline{\omega} = \frac{1}{2}\sum_{i=1}^{\ell} i\alpha_i$. So $P(R)/Q(R) = \langle \overline{\omega} + Q(R) \rangle = \boldsymbol{Z}/2\boldsymbol{Z}$. As G is non-adjoint, we have $X = P(R)$. Therefore, as a basis $\{\chi_i\}$ of X, we can take: $\chi_1 = \frac{1}{2}\sum_{i=1}^{\ell} i\alpha_i$, $\chi_i = \alpha_i$ ($2 \leqq i \leqq \ell$). So se have $\alpha_1 = 2\chi_1 - \sum_{i=2}^{\ell} i\chi_i$, $\alpha_i = \chi_i$ ($2 \leqq i \leqq \ell$). Therefore, by Lemma 4, we see that M consists of those elements $h(y, x, \ldots, x)$ with $x \in F_p{}^{\times}$ and $y \in F_q{}^{\times}$ such that $y^2 = x^{\ell(\ell+1)/2}$. In particular, by solving the last equation for $x = 1$, we get $Z = \{h(\pm 1, 1, \ldots, 1)\} \simeq \boldsymbol{Z}/2\boldsymbol{Z}$. For $x = \nu$, a solution y of the equation $y^2 = x^{\ell(\ell+1)/2}$ can be found in $F_p{}^{\times}$ if and only if $2 \mid \ell(\ell+1)/2$, and if this is the case, then $y = \nu^{\ell(\ell+1)/4}$ is a solution of that equation (Case (i)). Assume that $4 \nmid \ell(\ell+1)$. Then $\ell(\ell+1)/2$ is odd. Hence we see that, for $x = \nu$, solutions y of that equation can be found in $F_q{}^{\times}$ if and only if

$(q-1)/(p-1)$ is even, i.e., q is square, and if this is the case, then $y = \eta^i$ with $i = (\ell(\ell+1)/2) \cdot (q-1)/2(p-1)$ is a solution and $y^{p-1} = -1$ (Case (ii)). Assume that q is non-square. Then, for $x = \nu^2$, we can find a solution y of the equation $y^2 = x^{\ell(\ell+1)/2}$ in $F_p{}^\times$, and we see that a solution y can be found in $(F_p{}^\times)^2$ if and only if $(p-1)/2$ is odd, i.e., $p \equiv -1 \pmod 4$, and if this is the case, then $y = \nu^{(\ell(\ell+1)+p-1)}$ is a solution in $(F_p{}^\times)^2$ (Cases (iii), (iv); in case (iv), $y = \nu^{\ell(\ell+1)/2}$ is a solution in $F_p{}^\times$).

This proves Lemma 6. $\square$

Lemma 7 (cf. Gow [5]) *Assume that $\boldsymbol{G}$ is non-adjoint and of type (C_ℓ), $\ell \geqq 2$ (i.e., $\boldsymbol{G} = Sp_{2\ell}$). Then $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ and:* (i) *if q is square, we have $\tau(M) = \pi$ and $f^{p-1} = \varepsilon$, where ε is the generator of Z;* (ii) *if q is non-square and $p \equiv -1$* (mod 4), *we have $(\pi : \tau(M)) = 2$ and f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{(p-1)/2} = 1$;* (iii) *if q is non-square and $p \equiv 1$* (mod 4), *then $(\pi : \tau(M)) = 2$ and $f^{(p-1)/2} = \varepsilon$.*

Proof. By [1, PL.3, (VIII)], we have $P(R) = \langle \alpha_1, \ldots, \alpha_{\ell-1}, \overline{\omega}_1 \rangle$, where $\overline{\omega}_1 = \sum_{i=1}^{\ell-1} \alpha_i + \frac{1}{2}\alpha_\ell \equiv \frac{1}{2}\alpha_\ell \pmod{Q(R)}$, hence $P(R)/Q(R) = \langle \frac{1}{2}\alpha_\ell + Q(R) \rangle \simeq \boldsymbol{Z}/2\boldsymbol{Z}$. Since $\boldsymbol{G}$ is non-adjoint, we have $X = P(R)$. So, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ $(1 \leqq i \leqq \ell - 1)$, $\chi_\ell = \frac{1}{2}\alpha_\ell$. Therefore we have $\alpha_i = \chi_i$ $(1 \leqq i \leqq \ell-1)$, $\alpha_\ell = 2\chi_\ell$. Hence, by Lemma 4, we see that M consists of those elements $h(x, \ldots, x, y)$ with $x \in F_p{}^\times$ and $y \in F_q{}^\times$ with $y^2 = x$. Clearly we have $Z = \langle h(1, \ldots, 1, \pm 1) \rangle \simeq \boldsymbol{Z}/2\boldsymbol{Z}$. We see easily that, for $x = \nu$, the equation $y^2 = x$ has no solutions in $F_p{}^\times$ and has a solution in $F_q{}^\times$ if and only if q is square. Thus case (i). Assume that q is non-square. Then we see that, for $x = \nu^2$, the equation $y^2 = x$ has a solution in $F_p{}^\times$ and has a solution in $(F_p{}^\times)^2$ if and only if $(p-1)/2$ is odd, i.e., $p \equiv -1 \pmod 4$. Thus (ii) and (iii). (We can take: (i) $y = \eta^{(q-1)/2(p-1)}$; (ii) $y = \nu^{(p+1)/2}$; (iii) $y = \nu$.)

This proves Lemma 7. $\square$

Lemma 8 *Assume that $\boldsymbol{G}$ is non-adjoint and of type (D_ℓ), $\ell \geqq 3$. Then $Z \simeq \boldsymbol{Z}/(d, q-1)\boldsymbol{Z}$ $(d = (P(R) : X))$ if $2 \nmid \ell$, $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ if $2 \mid \ell$ and $d = 4$, and $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ if $2 \mid \ell$ and $d = 2$. And the following holds:*

(I) $X = P(R)$ $(G = \mathrm{Spin}_{2\ell})$; (i) *either* (a) *if* $4 \mid \ell(\ell-1)$ *or* (b) *if* $\mathrm{ord}_2(\ell-1) = 1$ *and $p \equiv -1$* (mod 4), *then $\tau(M) = \pi$ and f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{p-1} = 1$;* (ii) *if q is square and either* (a) *if* $\mathrm{ord}_2 \ell = 1$ *or* (b) *if* $\mathrm{ord}_2(\ell - 1) = 1$ *and $p \equiv 1$* (mod 4), *then $\tau(M) = \pi$ and*

f can be chosen so that $|\langle f^{p-1}\rangle| = 2$; (iii) *if q is non-square and either* (a) *if* $\mathrm{ord}_2(\ell-1) = 1$ *and* $\mathrm{ord}_2(p-1) = 2$ *or* (b) *if* $\mathrm{ord}_2\ell = 1$ *and* $p \equiv -1 \pmod 4$, *then* $(\pi : \tau(M)) = 2$ *and f can be chosen so that* $M = \langle f\rangle \times Z$ *and* $f^{(p-1)/2} = 1$; (iv) *if q is non-square and either* (a) *if* $\mathrm{ord}_2(\ell-1) = 1$ *and* $\mathrm{ord}_2(p-1) \geqq 3$ *or* (b) *if* $\mathrm{ord}_2\ell = 1$ *and* $p \equiv 1 \pmod 4$, *then* $(\pi : \tau(M)) = 2$ *and f can be chosen such that* $|\langle f^{(p-1)/2}\rangle| = 2$.

(II) $\boldsymbol{G} = SO_{2\ell}$ $(d = 2)$: *We have* $\tau(M) = \pi$ *and f can be chosen so that* $M = \langle f\rangle \times Z$ *and* $f^{p-1} = 1$.

(III) $\boldsymbol{G} = \mathrm{HSpin}_{2\ell}(2 \mid \ell,\ d = 2)$: (i) *if* $4 \mid \ell$, *then* $\tau(M) = \pi$ *and f can be chosen so that* $M = \langle f\rangle \times Z$ *and* $f^{p-1} = 1$; (ii) *if* $\mathrm{ord}_2\ell = 1$ *and q is square, then* $\tau(M) = \pi$ *and* $f^{p-1} = \varepsilon$, *where ε is the generator of Z*; (iii) *if* $\mathrm{ord}_2\ell = 1$, *q is non-square and* $p \equiv -1 \pmod 4$, *then* $(\pi : \tau(M)) = 2$ *and f can be chosen so that* $M = \langle f\rangle \times Z$ *and* $f^{(p-1)/2} = 1$; (iv) *if* $\mathrm{ord}_2\ell = 1$, *q is non-square and* $p \equiv 1 \pmod 4$, *then* $(\pi : \tau(M)) = 2$ *and* $f^{(p-1)/2} = \varepsilon$.

Proof. First we assume that ℓ is odd. Then, by [1, PL.4, (VIII)], we have $P(R) = \langle Q(R), \overline{\omega}_\ell\rangle$, where

$$\overline{\omega}_\ell = \frac{1}{2}\left\{\alpha_1 + 2\alpha_2 + \cdots + (\ell-2)\alpha_{\ell-2} + \frac{1}{2}(\ell-2)\alpha_{\ell-1} + \frac{1}{2}\ell\alpha_\ell\right\}.$$

$\overline{\omega}_\ell$ is congruent modulo $Q(R)$ to $\overline{\omega}$, where

$$\overline{\omega} = \begin{cases} \frac{1}{2}\Big(\alpha_1 + \alpha_3 + \cdots + \alpha_{\ell-2} - \frac{1}{2}\alpha_{\ell-1} + \frac{1}{2}\alpha_\ell\Big) & (4 \mid \ell - 1), \\ \frac{1}{2}\Big(\alpha_1 + \alpha_3 + \cdots + \alpha_{\ell-2} + \frac{1}{2}\alpha_{\ell-1} - \frac{1}{2}\alpha_\ell\Big) & (4 \mid \ell + 1). \end{cases}$$

Therefore we have $P(R) = \langle \alpha_1, \ldots, \alpha_{\ell-1}, \overline{\omega}\rangle$.

The case $X = P(R)$: As a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ $(1 \leqq i \leqq \ell-1)$, $\chi_\ell = \overline{\omega}$. So we have $\alpha_i = \chi_i$ for $1 \leqq i \leqq \ell - 1$ and

$$\alpha_\ell = \begin{cases} 4\chi_\ell - 2(\chi_1 + \chi_3 + \cdots + \chi_{\ell-2}) + \chi_{\ell-1} & (4 \mid \ell - 1), \\ -4\chi_\ell + 2(\chi_1 + \chi_3 + \cdots + \chi_{\ell-2}) + \chi_{\ell-1} & (4 \mid \ell + 1). \end{cases}$$

Therefore we see that M consists of those elements $h(x, \ldots, x, y)$ with $x \in F_p{}^\times$ and $y \in F_q{}^\times$ such that

$$y^4 = x^{\ell-1}. \tag{2}$$

By solving the equation (2) for $x = 1$, we see that $Z = \{h(1, \ldots, 1, y \mid y^4 = 1,\ y \in F_q{}^\times\} \simeq \boldsymbol{Z}/(4, q-1)\boldsymbol{Z}$. Let us calculate the group M. We see easily that the equation (2) has a solution y in $F_p{}^\times$ for $x=\nu$ if and only if (a) $4 \mid \ell-1$ or (b) $4 \mid \ell+1$ and $(p-1)/2$ is odd, and that in case (a) (resp. in case (b)) $y=\nu^{(\ell-1)/4}$ (resp. $y=\nu^{(\ell-p)/4}$) is a solution of the equation (2) for $x=\nu$ (Case (i)). Assume that $4 \nmid \ell-1$ and $p \equiv 1 \pmod 4$. Then we see that the equation (2) has a solution y in $F_q{}^\times$ for $x=\nu$ if and only if q is square, and if this is the case $y=\eta^i$ with $i=\frac{q-1}{2(p-1)}\cdot\frac{\ell-1}{2}$ is a solution and $y^{p-1}=-1$. Assume that q is non-square ($4 \nmid \ell-1$ and $p\equiv 1 \pmod 4$). Then we see that the equation (2) for $x=\nu^2$ has a solution y in $F_p{}^\times$ and y can be found in $(F_q{}^\times)^2$ if and only if $\mathrm{ord}_2(p-1)=2$. If $\mathrm{ord}_2(p-1)=2$, then we may take $y=\nu^i$ with $i=\frac{\ell-1}{2}+\frac{p-1}{4}$ (then $y^{(p-1)/2}=1$), and if $\mathrm{ord}_2(p-1)\geqq 3$, then we may take $y=\nu^{(\ell-1)/2}$ (then $y^{(p-1)/2}=-1$).

The case $d=2(SO_{2\ell})$: We have $X=\langle\alpha_1,\dots,\alpha_{\ell-1},\frac{1}{2}(\alpha_{\ell-1}-\alpha_\ell)\rangle$. So, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i=\alpha_i$ $(1\leqq i\leqq \ell-1)$, $\chi_\ell=\frac{1}{2}(\alpha_{\ell-1}-\alpha_\ell)$. Hence we have $\alpha_i=\chi_i$ for $1\leqq i\leqq \ell-1$ and $\alpha_\ell=-2\chi_\ell+\chi_{\ell-1}$. Therefore we see that M consists of those elements $h(x,\dots,x,y)$ with $x\in F_p{}^\times$ and $y\in F_q{}^\times$ such that $y^2=1$, and that $Z=\{h(1,\dots,1,\pm1)\}\simeq \boldsymbol{Z}/2\boldsymbol{Z}$. Clearly we can take $f=h(\nu,\dots,\nu,1)$.

Next we assume that ℓ is even. Then we have $P(R)=\langle Q(R),\overline{\omega}_{\ell-1},\overline{\omega}_\ell\rangle$, where $\overline{\omega}_\ell$ is as above and

$$\overline{\omega}_{\ell-1}=\frac{1}{2}\left\{\alpha_1+2\alpha_2+\cdots+(\ell-2)\alpha_{\ell-2}+\frac{1}{2}\ell\alpha_{\ell-1}+\frac{1}{2}(\ell-2)\alpha_\ell\right\}.$$

Put:

$$\begin{aligned}\overline{\omega}' &= \frac{1}{2}(\alpha_1+\alpha_3+\cdots+\alpha_{\ell-3}+\alpha_{\ell-1}),\\ \overline{\omega}'' &= \frac{1}{2}(\alpha_1+\alpha_3+\cdots+\alpha_{\ell-3}+\alpha_\ell).\end{aligned}$$

Then $\overline{\omega}_{\ell-1}\equiv\overline{\omega}''$, $\overline{\omega}_\ell\equiv\overline{\omega}'$ (mod $Q(R)$) if $4\,|\,\ell$, and $\overline{\omega}_{\ell-1}\equiv\overline{\omega}'$, $\overline{\omega}_\ell\equiv\overline{\omega}''$ (mod $Q(R)$) if $\mathrm{ord}_2\ell=1$. Therefore we have $P(R)=\langle Q(R),\overline{\omega}',\overline{\omega}''\rangle$.

The case $X=P(R)(\mathrm{Spin}_{2\ell})$: Let $\chi_i=\alpha_i$ for $1\leqq i\leqq \ell-2$, $\chi_{\ell-1}=\overline{\omega}'$ and $\chi_\ell=\overline{\omega}''$. Then $\{\chi_1,\dots,\chi_\ell\}$ is a basis of X, and we have: $\alpha_i=\chi_i$ $(1\leqq i\leqq \ell-2)$, $\alpha_{\ell-1}=2\chi_{\ell-1}-(\chi_1+\chi_3+\cdots+\chi_{\ell-3})$ and $\alpha_\ell=2\chi_\ell-(\chi_1+\chi_3+\cdots+\chi_{\ell-3})$. Therefore, by Lemma 4, we see that M consists of those elements $h(x,\dots,x,y,z)$ with $x\in F_p{}^\times$ and $y,z\in F_q{}^\times$ such that $y^2=z^2=x^{\ell/2}$. It is clear that $Z=\{h(1,\dots,1,\pm1,\pm1)\}\simeq \boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$. Let us calculate the group M. First, it is easy to see that, for $x=\nu$, the equations $y^2=z^2=x^{\ell/2}$ have solutions y, z in $F_p{}^\times$ if and only if $\ell/2$ is even and if this is the case then $y = z = \nu^{\ell/4}$ are solutions (Case (I), (i)). Suppose therefore $\mathrm{ord}_2\ell = 1$. Then we see that, for $x = \nu$, the equations $y^2 = z^2 = x^{\ell/2}$ have solutions y, z in ${F_q}^\times$ if and only if $(q-1)/(p-1)$ is even, i.e., q is square, and if this is the case then $y = z = \eta^i$ with $i = \frac{1}{2}(\frac{q-1}{p-1} \cdot \frac{\ell}{2} + q - 1)$ are solutions and $y^{p-1} = z^{p-1} = -1$ (Case (I), (ii)). Assume that q is non-square ($\mathrm{ord}_2\ell = 1$). Then we see that, for $x = \nu^2$, the equations $y^2 = z^2 = x^{\ell/2}$ have solutions y, z in ${F_p}^\times$ and that y, z can be found in $({F_p}^\times)^2$ if and only if $(p-1)/2$ if odd. In fact, if $p \equiv -1 \pmod 4$, then taking $y = z = \nu^i$ with $i = \frac{\ell}{2} + \frac{p-1}{2}$, we have $y^{(p-1)/2} = z^{(p-1)/2} = 1$, and if $p \equiv 1 \pmod 4$, taking $y = z = \nu^{\ell/2}$, we have $y^{(p-1)/2} = z^{(p-1)/2} = -1$ (Cases (I), (iii), (iv)).

The case $d = 2$: Three cases occur: (α) $\overline{\omega}' + \overline{\omega}'' \in X(SO_{2\ell})$, ($\beta$) $\overline{\omega}_{\ell-1} \in X(\mathrm{HSpin}_{2\ell})$, ($\gamma$) $\overline{\omega}_\ell \in X(\mathrm{HSpin}_{2\ell})$.

Case (α): We have $X = \langle \alpha_1, \dots, \alpha_{\ell-1}, \frac{1}{2}(\alpha_{\ell-1} + \alpha_\ell) \rangle$. So, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ $(1 \leqq i \leqq \ell-1)$, $\chi_\ell = \frac{1}{2}(\alpha_{\ell-1} + \alpha_\ell)$. Then we have $\alpha_i = \chi_i$ for $1 \leqq i \leqq \ell - 1$ and $\alpha_\ell = 2\chi_|\ell - \chi_{\ell-1}$. Therefore, by Lemma 4, we see that M consists of those elements $h(x, \dots, x, y)$ with $x \in {F_p}^\times$ and $y \in {F_q}^\times$ such that $y^2 = x^2$. Thus we have $Z = \{h(1, \dots, 1, \pm 1)\} \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ and we can take: $f = h(\nu, \dots, \nu, \nu)$.

Case (β): Assume that $4 \mid \ell$. Then we have $X = \langle \alpha_1, \dots, \alpha_{\ell-1}, \overline{\omega}'' \rangle$. And, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ $(1 \leqq i \leqq \ell - 1)$, $\chi_\ell = \overline{\omega}''$. So we have $\alpha_i = \chi_i$ for $1 \leqq i \leqq \ell - 1$ and $\alpha_\ell = 2\chi_\ell - (\chi_1 + \chi_3 + \cdots + \chi_{\ell-3})$. Hence, by Lemma 4, we see that M consists of those elements $h(x, \dots, x, y)$ with $x \in {F_p}^\times$ and $y \in {F_q}^\times$ such that $y^2 = x^{\ell/2}$. Hence we have $Z = \{h(1, \dots, 1, \pm 1)\} \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ and we have take: $f = h(\nu, \dots, \nu, \nu^{\ell/4})$.

Assume that $\mathrm{ord}_2\ell = 1$. Then we have $X = \langle \alpha_1, \dots, \alpha_{\ell-2}, \overline{\omega}', \alpha_\ell \rangle$. So, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ $(1 \leqq i \leqq \ell - 2)$, $\chi_{\ell-1} = \overline{\omega}'$, $\chi_\ell = \alpha_\ell$. Then we have $\alpha_i = \chi_i$ for $1 \leqq i \leqq \ell - 2$ and $i = \ell$ and $\alpha_{\ell-1} = 2\chi_{\ell-1} - (\chi_1 + \chi_3 + \cdots + \chi_{\ell-3})$. Therefore, by Lemma 4, we see that M consists of those elements $h(x, \dots, x, y, x)$ with $x \in {F_p}^\times$ and $y \in {F_q}^\times$ such that $y^2 = x^{\ell/2}$. Thus we have $Z = h(1, \dots, 1, \pm 1, 1)\} \simeq \boldsymbol{Z}/2\boldsymbol{Z}$. As $\ell/2$ is odd, we see that, for $x = \nu$, the equation $y^2 = x^{\ell/2}$ has no solutions in ${F_p}^\times$ and has a solution in ${F_q}^\times$ if and only if $(q-1)/(p-1)$ is even, i.e., q is square. If q is square, then $y = \eta^i$ with $i = \frac{1}{2}(\frac{q-1}{p-1} \cdot \frac{\ell}{2})$ is a solution of that equation for $x = \nu$ and $y^{p-1} = -1$. Assume therefore that q is non-square. Then we see that, for $x = \nu^2$, that equation has a solution y in ${F_p}^\times$ and y can be found in $({F_p}^\times)^2$ if and only if $(p-1)/2$ is odd. In fact, if $p \equiv -1 \pmod 4$, then $y = \nu^{(\ell+p-1)/2}$ is a solution and $y^{(p-1)/2} = 1$. If $p \equiv 1 \pmod 4$, then $y = \nu^{\ell/2}$ is a solution.

Case (γ): Similar to the case (β).

This completes the proof of Lemma 8. □

Lemma 9 *Assume that* $\boldsymbol{G}$ *is a non-adjoint group of type* (E_6). *Then* $Z \simeq \boldsymbol{Z}/(3, q-1)\boldsymbol{Z}$ *and* $\tau(M) = \pi$ *and* f *can be chosen so that* $M = \langle f \rangle \times Z$ *and* $f^{p-1} = 1$.

This lemma is proved in [10].

Lemma 10 *Assume that* $\boldsymbol{G}$ *is a non-adjoint group of type* (E_7). *Then* $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ *and we have*: (i) *if* q *is square, then* $\tau(M) = \pi$ *and* $f^{p-1} = \varepsilon$, *where* ε *is the generator of* Z; (ii) *if* q *is non-square and* $p \equiv -1 \pmod 4$, *then* $(\pi : \tau(M)) = 2$ *and* f *can be chosen so that* $M = \langle f \rangle \times Z$ *and* $f^{(p-1)/2} = 1$; (iii) *if* q *is non-square and* $p \equiv 1 \pmod 4$, *then* $(\pi : \tau(M)) = 2$ *and* $f^{(p-1)/2} = \varepsilon$.

Proof. By [1, PL.6, (VIII)], we have $P(R) = \langle Q(R), \overline{\omega}_2 \rangle$, where $\overline{\omega}_2 \equiv \frac{1}{2}(\alpha_2 + \alpha_5 + \alpha_7) \pmod{Q(R)}$, so that we have $P(R) = \langle \alpha_1, \ldots, \alpha_6, \frac{1}{2}(\alpha_2 + \alpha_5 + \alpha_7) \rangle$. Therefore, as a basis $\{\chi_i\}$ of X, we can take: $\chi_i = \alpha_i$ $(1 \leqq i \leqq 6)$, $\chi_7 = \frac{1}{2}(\alpha_2 + \alpha_5 + \alpha_7)$. Hence we have $\alpha_i = \chi_i$ for $1 \leqq i \leqq 6$ and $\alpha_7 = 2\chi_7 - \chi_2 - \chi_5$. Therefore, by Lemma 4, we see that M consists of those elements $h(x, \ldots, x, y)$ with $x \in {F_p}^\times$ and $y \in {F_q}^\times$ such that $y^2 = x^3$. Hence $Z = \{h(1, \ldots, 1, \pm 1)\} = Z/2Z$. It is easy to see that, for $x = \nu$, the equation $y^2 = x^3$ has no solutions y in ${F_p}^\times$ and has a solution y in ${F_q}^\times$ if and only if q is square. If q is square, then $y = \eta^i$ with $i = \frac{q-1}{p-1} \cdot 3 \cdot \frac{1}{2}$ is a solution and $y^{p-1} = -1$. We see that, for $x = \nu^2$, that equation has a solution y in ${F_p}^\times$ and y can be found in $({F_p}^\times)^2$ if and only if $(p-1)/2$ is odd. In fact, if $p \equiv -1 \pmod 4$, then $y = \nu^i$ with $i = 3 + \frac{p-1}{2}$ is a solution and $y^{(p-1)/2} = 1$ and if $p \equiv 1 \pmod 4$, then $y = \nu^3$ is a solution and $y^{(p-1)/2} = -1$.

This proves Lemma 10. □

3. The Hasse invariants of the algebras A_i

Let $\lambda \in \Lambda$, $\lambda \neq 1$. Let the μ_i, k, the k_i and the A_i be as in §1.

First we assume that $\tau(M)=\pi$ and f can be chosen so that $M=\langle f\rangle\times Z$ and $f^{p-1}=1$ (this occurs when $\boldsymbol{G}$ is adjoint or $\boldsymbol{G}$ is non-adjoint of any one of the following types: (A_ℓ) $2\mid \ell(\ell+1)/d$ or $\mathrm{ord}_2 d>\mathrm{ord}_2(p-1)$; (B_ℓ) $4\mid\ell(\ell+1)$, (D_ℓ) $(\mathrm{Spin}_{2\ell})$ either (a) $4\mid\ell(\ell-1)$ or (b) $\mathrm{ord}_2(\ell-1)=1$ and $p\equiv -1 \pmod 4$; (D_ℓ) $(SO_{2\ell})$; (D_ℓ) $(\mathrm{HSpin}_{2\ell})4\mid\ell$; (E_6)). Put $\sigma=\tau(f)$. Then, as $\tau(\langle f\rangle)=\pi=\mathrm{Gal}(Q(\zeta_p)/Q)$, σ is a generator of $\mathrm{Gal}(Q(\zeta_p)/Q)$, so we see easily that $k=Q$ and, for $1\leqq i\leqq c$, $k_i=Q(\eta_i)$ (= the field generator over Q by the values of η_i). Let us fix i $(1\leqq i\leqq c)$. Then, as $f^{p-1}=1$, we have $\theta_i=\eta_i(1)=1$. So A_i is isomorphic over k_i to the cyclic algebra $(1,k_i(\zeta_p),\sigma_i)\sim k_i$ (similar). Thus we have $m_Q(\mu_i)=m_{k_i}(\mu_i)=1$. Here, if ξ is an irreducible character of a finite group and E is a field of characteristic 0, then $m_E(\xi)$ denotes the Schur index of ξ with respect to E.

Let $\overline{Q}$ denote an algebraic closure of Q. Then $\mathrm{Gal}(\overline{Q}/Q)$ acts on the set $C=\{\mu_1,\ldots,\mu_c\}$. Let X be the set of orbits of $\mathrm{Gal}(\overline{Q}/Q)$ on C. For $x\in X$, put $\mu_x=\sum_{\mu\in x}\mu$. Then, as $m_Q(\mu)=1$ for all $\mu\in C$, by a theorem of Schur (see, e.g., Feit [3, (11.4)]), each μ_x is a Q-irreducible character of L. Therefore $\lambda^L=\sum_{x\in X}\mu_x$ is realizable in Q. Therefore $\lambda^G=(\lambda^L)^G$ is realizable in Q.

Thus we get

Proposition 1 *Recall that $p\neq 2$. Assume that $\boldsymbol{G}$ is adjoint or a non-adjoint group of any one of the following types:* (A_ℓ) $2\mid\ell(\ell+1)/d$ *or* $\mathrm{ord}_2 d>\mathrm{ord}_2(p-1)$; (B_ℓ) $4\mid\ell(\ell+1)$; (D_ℓ) $(\mathrm{Spin}_{2\ell})$ *either* (a) $4\mid\ell(\ell-1)$ *or* (b) $\mathrm{ord}_2(\ell-1)=1$ *and* $p\equiv-1 \pmod 4$; (D_ℓ) $(SO_{2\ell})$; (D_ℓ) $(\mathrm{HSpin}_{2\ell})4\mid\ell$; (E_6). *Then, for any $\lambda\in\Lambda$, λ^G is realizable in Q.*

Next, we assume that $\boldsymbol{G}$ is a non-adjoint group of any one of the following types: (A_ℓ) $2\nmid\ell(\ell+1)/d$, $\mathrm{ord}_2 d\leqq\mathrm{ord}_2(p-1)$ and q square; (B_ℓ) $4\nmid\ell(\ell+1)$ and q square; (C_ℓ) q square; (D_ℓ) $(\mathrm{Spin}_{2\ell})q$ square and (a) $\mathrm{ord}_2\ell=1$ or (b) $\mathrm{ord}_2(\ell-1)=1$ and $p\equiv 1 \pmod 4$; (D_ℓ) $(\mathrm{HSpin}_{2\ell})q$ square and $\mathrm{ord}_2\ell=1$; (E_7) q square. Then, by Lemmas 5–10, we see that $\tau(M)=\pi$ but there is no f such that $M=\langle f\rangle\times Z$ and $f^{p-1}=1$.

In the following, if E is a finite extension of Q (that is E is an algebraic number field of finite degree) and B is a finite dimensional central simple algebra over E, then, for any place v of E, $h_v(B)$ denotes the Hasse invariant of E at E_v.

We arrange the characters $\eta_1,\ldots,\eta_c$ of Z $(c=|Z|)$ as follows: If Z is cyclic, then we fix a generator z of Z and a primitive c-th root ζ_c of unity and we assume that $\eta_i(z) = \zeta_c{}^i$ for $1 \leqq i \leqq c$. If $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ (this case occurs when $G = \mathrm{Spin}_{2\ell}$ with $\mathrm{ord}_2\ell = 1$, and in this case we have $Z = \{h(1,\ldots,1,\pm 1,\pm 1)\}$), then we assume that $\eta_i(h(1,\ldots,1,-1,-1)) = (-1)^i$, $1 \leqq i \leqq 4$ (we note that f can be chosen so that $f^{p-1} = h(1,\ldots,1,-1,-1)$). Then we have $k = Q$, $k_i = Q(\eta_i)$ $(1 \leqq i \leqq c)$ and $A_i \sim k_i \otimes_Q ((-1)^i, Q(\zeta_p), \sigma)$ $(1 \leqq i \leqq c)$.

If i is even, then A_i splits in k_i. Suppose that i is odd. Put $A = (-1, Q(\zeta_p), \sigma)$. Then we have $h_\infty(A) \equiv h_p(A) \equiv \frac{1}{2} \pmod 1$ and $h_r(A) \equiv 0 \pmod 1$ for any finite place r of Q different from p. If $Z \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ or $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$, then $k_i = Q$ and $A_i = A$. Suppose that Z is cyclic and that $Z \not\simeq \boldsymbol{Z}/2\boldsymbol{Z}$. Let v be any place of k_i. Then if v is infinite, we have $h_v(A_i) \equiv \frac{1}{2} \pmod 1$ or $\equiv 0 \pmod 1$ according as v is real or imaginary. If v is a finite place of k_i such that $v \nmid p$, then $h_v(A_i) \equiv 0 \pmod 1$. Suppose that $v \mid p$ and put $f_i = [(k_i)_v : Q_p]$. Then $h_v(A_i) \equiv \frac{1}{2} f_i \pmod 1$.

Lemma 11 *Assume that* $\boldsymbol{G}$ *is of type* (A_ℓ) *where* $2 \nmid \ell(\ell+1)/d$, $1 \leqq \mathrm{ord}_2(\ell+1) \leqq \mathrm{ord}_2(p-1)$ *and* q *is square or* $G = \mathrm{Spin}_{2\ell}$ *where* $\mathrm{ord}_2(\ell-1) = 1$, $p \equiv 1 \pmod 4$ *and* q *is square. Let* $q = p^{2^t s}$ *with* $(2, s) = 1$. *Recall that* i *is odd. Then* $2 \nmid f_i$ *if and only if any odd prime divisor of* $c/(c,i)$ *divides* $p^s - 1$. *In particular, if* $\boldsymbol{G} = \mathrm{Spin}_{2\ell}$, *then* f_i *is odd.*

Proof. Put $c_i = c/(c,i)$. c_i is equal to the order of $\zeta_c{}^i$. Then f_i is equal to the smallest positive integer h such that $p^h \equiv 1 \pmod{c_i}$. The integers $h \geqq 1$ such that $p^h \equiv 1 \pmod{c_i}$ form the semigroup generated by f_i. So f_i divides $2^t s$ since $q \equiv 1 \pmod{c_i}$. Hence f_i is odd if and only if f_i divides s. But, if $f_i \,|\, s$, then $p^{f_i} - 1 \mid p^s - 1$, so $p^s \equiv 1 \pmod{c_i}$, hence $f_i \,|\, s$ again. Therefore it suffices to show that the condition that $c_i \mid p^s - 1$ is equivalent to the condition which is stated in the lemma. For an integer m, let $V(m)$ be the set of odd prime divisors of m. Then we have $V(p^s-1) \cap V((q-1)/(p^s-1)) = \emptyset$ since $(p^s-1, (q-1)/(p^s-1)) = (p^s-1, 2^t) =$ a power of 2. Suppose that $V(c_i) \subset V(p^s-1)$. Then, for any $r \in V(c_i)$, r divides p^s-1, so that the r-part r^e of c_i divides p^s-1 since r is an odd divisor of $q-1 = (p^s-1)((q-1)/(p^s-1))$. And we have $\mathrm{ord}_2 c_i$ $(\leqq \mathrm{ord}_2(\ell+1)) \leqq \mathrm{ord}_2(p-1) = \mathrm{ord}_2(p^s-1)$. Thus we have seen that $\mathrm{ord}_r c_i \leqq \mathrm{ord}_r(p^s-1)$ for any prime divisor r of c_i. Hence c_i divides p^s-1. Conversely, if c_i divides p^s-1, then clearly $V(c_i) \subset V(p^s-1)$. This proves the lemma. □

Suppose that $\boldsymbol{G}$ is of type (A_ℓ) where q is square, $2 \nmid \ell(\ell+1)/d$ and $\mathrm{ord}_2 d \leqq \mathrm{ord}_2(p-1)$. Let i be the odd part of c. Then c_i is equal to the 2-part of c, so $V(c_i) = \emptyset$. Hence f_i is odd and $h_v(A_i) \equiv \frac{1}{2} \pmod 1$ if v is any place of k_i lying above p. Hence we have $m_{Q_p}(\mu_i) = 2$. Here, if χ is an irreducible character of a finite group and if E is a field of characteristic 0, then $m_E(\chi)$ denotes the Schur index of χ with respect to E.

Suppose that $G = \mathrm{Spin}_{2\ell}$ where $\mathrm{ord}_2(\ell-1) = 1$ and q is an even power of $p \equiv 1 \pmod 4$ (cf. Lemma 8). Then $Z \simeq \boldsymbol{Z}/4\boldsymbol{Z}$. Suppose that i is odd. Then $c_i = 4$, so $V(c_i) = \emptyset$. Hence f_i is odd and we have $m_{Q_p}(\mu_i) = 2$.

Thirdly, we assume that $\boldsymbol{G}$ is a non-adjoint group of any one of the following types: (A_ℓ) $2 \nmid \ell(\ell+1)/d$, $\mathrm{ord}_2 d = \mathrm{ord}_2(p-1)$ and q non-square; (B_ℓ) $4 \nmid \ell(\ell+1)$, q non-square and $p \equiv -1 \pmod 4$; (C_ℓ) q non-square and $p \equiv -1 \pmod 4$; (D_ℓ) $(\mathrm{Spin}_{2\ell})q$ non-square, $\mathrm{ord}_2(\ell-1) = 1$ and $\mathrm{ord}_2(p-1) = 2$; $(\mathrm{Spin}_{2\ell})q$ non-square, $\mathrm{ord}_2\ell = 1$ and $p \equiv -1 \pmod 4$; $(\mathrm{HSpin}_{2\ell})q$ non-square, $\mathrm{ord}_2\ell = 1$ and $p \equiv -1 \pmod 4$; (E_7) q non-square and $p \equiv -1 \pmod 4$. Then we have $(\pi : \tau(M)) = 2$ and f can be chosen so that $M = \langle f \rangle \times Z$ and $f^{(p-1)/2} = 1$ (cf. Lemmas 5–10). In this case k is the quadratic subfield of $Q(\zeta_p)$, i.e., $k = Q(\sqrt{(-1)^{(p-1)/2}p})$. For $1 \leqq i \leqq c$, we have $\theta_i = 1$, so A_i splits in k_i. Hence any λ^G is realizable in k.

Finally, we assume that $\boldsymbol{G}$ is a non-adjoint group of any one of the following types: (A_ℓ) $e \nmid \ell(\ell+1)/d$, $\mathrm{ord}_2 d < \mathrm{ord}_2(p-1)$ and q non-square; (B_ℓ) $4 \nmid \ell(\ell+1)q$ non-square and $p \equiv 1 \pmod 4$; (C_ℓ) q non-square and $p \equiv 1 \pmod 4$; (D_ℓ) $(\mathrm{Spin}_{2\ell})q$ non-square, $\mathrm{ord}_2(\ell-1) = 1$ and $\mathrm{ord}_2(p-1) \geqq 3$; $(\mathrm{Spin}_{2\ell})q$ non-square, $\mathrm{ord}_2\ell = 1$ and $p \equiv \pmod 4$; $(\mathrm{HSpin}_{2\ell})q$ non-square, $\mathrm{ord}_2\ell = 1$ and $p \equiv 1 \pmod 4$; (E_7) q non-square and $p \equiv 1 \pmod 4$. Then we have $(\pi : \tau(M)) = 2$ and f can be chosen so that $|\langle f^{(p-1)/2} \rangle| = 2$. We arrange the characters $\eta_1, \ldots, n_c$ of Z as before. Then k is the quadratic sub-field of $Q(\zeta_p)$ and if i is even A_i splits in k_i. Assume that i is odd. Then we have $A_i \sim k_i \otimes_k B$, where B is the cyclic algebra $(-1, k(\zeta_p), \sigma)$ over k. By [8, Proposition 1], we see that B has non-zero Hasse invariants only at two real places of k and no others. Thus we have $m_R(\mu_i) = 2$ or 1 according as μ_i is real or not.

Assume that $\boldsymbol{G}$ is of type (A_ℓ) and $\mathrm{ord}_2 d = 1$. Let i be the odd part of c. Then $c_i = 2$ and $A_i = B$. Hence we have $m_R(\mu_i) = 2$. Assume that $\boldsymbol{G}$ is of type (B_ℓ). Then $i = 1$ and $A_1 = B$. So we have $m_R(\mu_1) = 2$. Similarly, if G is of type (C_ℓ), then we have $m_R(\mu_1) = 2$. Assume that $\boldsymbol{G}$ is of type (D_ℓ). If $Z \not\simeq \boldsymbol{Z}/4\boldsymbol{Z}$, then k_i is real, so we have $m_R(\mu_i) = 2$. If $Z \not\simeq \boldsymbol{Z}/4\boldsymbol{Z}$, then k_i is not real, so we have $m_R(\mu_i) = 1$. Assume that $\boldsymbol{G}$ is of type (E_7). Then $k_i = k$, so we have $m_R(\mu_1) = 2$.

4. The Schur index

Let $\boldsymbol{G}$ be a simple algebraic group, defined and split over a finite field F_q, and let G be the group of its F_q-rational points. Let χ be any irreducible character of G. We assume that there is a linear character λ in Λ such that $(\lambda^G, \chi)_G = 1$ or that when p is a good prime for $\boldsymbol{G}$ $p \nmid \chi(1)$. We assume that $p \neq 2$.

Theorem 1 ([10]) *We have the following.*
(i) *We have* $m_Q(\chi) \leqq 2$.
(ii) *If* $p \equiv -1 \pmod 4$, *then we have* $m_{Q(\sqrt{-p})}(\chi) = 1$.
(iii) *If* $p \equiv 1 \pmod 4$, *then, for any finite place* v *of* $Q(\sqrt{p})$, *we have* $m_{Q(\sqrt{p})_v}(\chi) = 1$.
(iv) *If* q *is square, then, for any prime number* $r \neq p$, *we have* $m_{Q_r}(\chi) = 1$.

By proposition 1 and the argument in the proof of Corollary 4 in [10], we get:

Theorem 2 *In the following cases, we have* $m_Q(\chi) = 1:$ (i) $\boldsymbol{G}$ *adjoint*; (ii) (A_ℓ) $2 \mid \ell(\ell+1)/d$ *or* $\mathrm{ord}_2 d > \mathrm{ord}_2(p-1)$; (B_ℓ) $4 \mid \ell(\ell+1)$; (D_ℓ) $(\mathrm{Spin}_{2\ell})$ *either* $4 \mid \ell(\ell-1)$, *or*, $\mathrm{ord}_2(\ell-1) = 1$ *and* $p \equiv -1 \pmod 4$; $(SO_{2\ell})$; $(\mathrm{HSpin}_{2\ell}) 4 \mid \ell$; (E_6).

Similarly, by the arguments in §3, we get:

Theorem 3 *Let* k *be the quadratic subfield of* $Q(\zeta_p)$. *Then in the following cases we have* $m_k(\chi) = 1 :$ (A_ℓ) $2 \nmid \ell(\ell+1)/d$, $\mathrm{ord}_2 d = \mathrm{ord}_2(p-1)$ *and* q *non-square*; $(\mathrm{Spin}_{2\ell}) q$ *non-square,* $\mathrm{ord}_2(\ell-1) = 1$ *and* $\mathrm{ord}_2(p-1) = 2$.

Theorem 4 *Assume that* $\boldsymbol{G}$ *is non-adjoint. Let* $\lambda \in \Lambda_0$. *Then in any one of the following cases* λ^G *contains an irreducible character of the Schur index* 2 *over* Q : (A_ℓ) *either* (a) q *square,* $2 \nmid \ell(\ell+1)/d$, $\mathrm{ord}_2 d \leqq \mathrm{ord}_2(p-1)$, *or* (b) q *non-square,* $2 \nmid \ell(\ell+1)/d$, $\mathrm{ord}_2 d = 1 < \mathrm{ord}_2(p-1)$; (B_ℓ) *either* (a) $4 \nmid \ell(\ell+1)$, q *square, or* (b) $4 \nmid \ell(\ell+1)$, q *non-square,* $p \equiv 1 \pmod 4$; (C_ℓ) *either* (a) q *square, or* (b) q *non-square,* $p \equiv 1 \pmod 4$; $(\mathrm{Spin}_{2\ell})$ *either* (a) $\mathrm{ord}_2 \ell = 1$, q *square, or* (b) $\mathrm{ord}_2 \ell = 1$, q *non-square,* $p \equiv 1 \pmod 8$, *or*

(c) $\mathrm{ord}_2(\ell-1)=1$, *q square, $p\equiv 1 \pmod 4$*; ($\mathrm{HSpin}_{2\ell}$) *either* (a) $\mathrm{ord}_2\ell=1$, *q square, or* (b) $\mathrm{ord}_2\ell=1$, *q non-square, $p\equiv 1 \pmod 4$*; (E_7) *either* (a) *q square, or* (b) *q non-square, $p\equiv 1 \pmod 4$*.

Proof. We repeat the argument in the proof of Theorem 4 of [12]. Assume that $\boldsymbol{G}$ is a non-adjoint simple group of type (A_ℓ) where q is square, $2\nmid \ell(\ell+1)/d$ and $\mathrm{ord}_2 d \leqq \mathrm{ord}_2(p-1)$. Then we see from the argument in §3 that $k=Q$ and there is an irreducible character μ_i of L such that $m_{k_i}(\mu_i)=2$ $(\lambda\in\Lambda_0)$. By the arguments in §1, we see that $\Gamma_{\lambda,i}$ is multiplicity-free and $(\Gamma_{\lambda,i},\Gamma_{\lambda,i})_G$ is odd. Let X be the set of all the irreducible components of $\Gamma_{\lambda,i}$. Then, by Schur's lemma, we see that, for any $\chi\in X$, we must have $\chi\mid Z=\chi(1)\eta_i$. Therefore we find that $Q(\Gamma_{\lambda,i})\subset k_i$. We show that there is a character χ in X such that $m_{k_i}(\chi)=2$. Suppose, on the contrary, that we have $m_{k_i}(\chi)=1$ for all $\chi\in X$ (cf. Theorem 1 (i)). Then we see from the theorem of Schur that $\Gamma_{\lambda,i}$ is realizable in k_i. But, then, as $(\Gamma_{\lambda,i}\mid L,\mu_i)_L=(\Gamma_{\lambda,i},\Gamma_{\lambda,i})_G$ is odd, we must have $m_{k_i}(\mu_i)=1$, a contradiction. Therefore X must contains a character χ such that $m_{k_i}(\chi)=2$. The remaining cases can be treated similarly. □

References

[1] Bourbaki N., *Groupes et Algèbres de Lie.* Chapitres 4, 5 et 6. Hermann, Paris, 1968.

[2] Carter R.W., *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters.* John Wiley and Sons, 1985.

[3] Feit W., *Characters of Finite Groups.* Benjamin, New York-Amsterdam, 1967.

[4] Gal'fand I.M. and Graev M.I., *Constructions of irreducible representations of simple algebraic groups over a finite field.* Soviet Math. Dokl. **3** (1962), 1646–1649.

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

[6] Gow R., *On the Schur indices of characters of finite classical groups.* J. London Math. Soc. (2), **24** (1981), 135–147.

[7] Helversen-Pasotto A., *Sur l'indices de Schur des représentations de $GL(n,F_q)$.* C. R. Acad. Sc. Paris, t. **283** (20 septembre 1976), Serie A, 233–235.

[8] Janusz G.J., *Simple components of $Q[SL(2,q)]$.* Commun. Algebra **1** (1974), 1–22.

[9] Ohmori Z., *On the Schur indices of reductive groups.* Quart. J. Math. Oxford (2), **28** (1977), 357–361.

[10] Ohmori Z., *On the Schur indices of certain irreducible characters of reductive groups over finite fields.* Osaka J. Math. **25** (1988), 149–159.

[11] Ohmori Z., *On the Schur indices of certain irreducible characters of simple algebraic groups over finite fields.* Proceed. Japan Acad. **64**, Ser. A, No. 7, (1988), 253–255.

[12] Ohmori Z., *On the Schur indices of $SU_{\ell+1}(F_q)$ and* $\mathrm{Spin}_{2\ell}^-(F_q)$. Tokyo J. Math. **18** (1995), 11–29.

[13] Steinberg R., *Lectures on Chevalley Groups.* Yale Univ., 1967.

[14] Yamada T., *The Schur Subgroup of the Brauer Group.* Lecture Notes in Math. **397**, Springer, Berlin-Heidelberg-New York, 1974.

[15] Yokonuma T., *Sur le commutant d'une représentation d'un groupe de Chevalley fini.* J. Fac. Sci. Univ. Tokyo **15** (1968), 115–129.

Iwamizawa College
Hokkaido University of Education
Midorigaoka, Iwamizawa 068-0835, Hokkaido
Japan