Journal of Algebra 557 (2020) 129–164

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On the calculation of local invariants of irreducible characters

Alexandre Turull

Department of Mathematics, University of Florida, Gainesville, FL 32611, USA

ARTICLE INFO

Article history:
Received 30 August 2019
Available online 18 April 2020
Communicated by Markus Linckelmann

MSC:
20C11

Keywords:
Brauer group
Finite groups
Representations
Schur index

ABSTRACT

Let K be a finite extension of the field $\mathbf{Q}_p$ of p-adic numbers. Let χ be an irreducible character of a finite group whose values are in K. Associated with χ and K is an element of the Brauer group of K, and therefore by standard results a local invariant in $\mathbf{Q}/\mathbf{Z}$. The paper defines some classes of finite groups, that the paper calls *p-basic* groups, and gives formulas to calculate the local invariant of their characters. It also shows how one can calculate the local invariant of any irreducible character of any finite group that has values in K by reducing the problem to the case where the groups are p-basic and using the explicit formulas given in the paper.

1. Introduction

Let K be a finite extension of the field $\mathbf{R}$ of real numbers, or of a field $\mathbf{Q}_p$ of p-adic numbers, for some prime p. Let G be a finite group, and let $\chi \in \mathrm{Irr}(G)$ be an irreducible character of G, and assume that the values of χ are all in K (we write $\chi \in \mathrm{Irr}_K(G)$ to indicate this). An element $[\chi]_K$ of the Brauer group $\mathrm{Br}(K)$ of K is naturally associated

E-mail address: turull@ufl.edu.

https://doi.org/10.1016/j.jalgebra.2020.03.032

with χ (Definition 2.1). It is a standard result that given K, there exists a unique corresponding injective group homomorphism

$$\mathrm{inv}\colon \mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}.$$

In the present paper, we discuss a method to calculate explicitly the local invariant $\mathrm{inv}([\chi]_K)$ of the Brauer element $[\chi]_K$. This method is described in Section 9.

Before we discuss a little the details of the paper, we look briefly at the role of this invariant in the representation theory of finite groups generally. Let G be a finite group, and let $\chi \in \mathrm{Irr}(G)$ be an irreducible character of G. It is known that important information can be obtained from the study of representations associated to χ over arbitrary fields of characteristic 0. Let F be a field of characteristic 0 and assume that the values of χ are in F. It is natural to consider the Brauer element $[\chi]_F \in \mathrm{Br}(F)$, the element of the Brauer group over F corresponding to the character χ. (See Definition 2.1 below for the definition of this Brauer invariant). This invariant works well with respect to field extensions. Furthermore, the Schur index $m_F(\chi)$ with respect to F can be found from $[\chi]_F$. It follows that $[\chi]_F$ gives the Schur index of χ over every field extension of F. As a result the invariant $[\chi]_{\mathbf{Q}(\chi)} \in \mathrm{Br}(\mathbf{Q}(\chi))$ over the smallest field $\mathbf{Q}(\chi)$ yields basic information about the representations over fields of characteristic zero.

Hence, the element $[\chi]_{\mathbf{Q}(\chi)}$ plays an important role in the representation theory associated to χ. It follows that $\mathrm{Br}(\mathbf{Q}(\chi))$ is of particular importance for our purposes, or more generally $\mathrm{Br}(F)$ for F a finite extension of $\mathbf{Q}$. Important results tell us how to describe in detail these Brauer groups. Details about this can be found, for example, in Pierce [5]. When F is a finite extension of $\mathbf{Q}$, the Brauer group $\mathrm{Br}(F)$ is best understood in terms of the Brauer groups $\mathrm{Br}\left(\hat{F}_v\right)$ where v runs through the non-trivial normalized valuations of F, and $\hat{F}_v$ is the completion of F under v. Now the fields $\hat{F}_v$ are isomorphic to finite extensions of $\mathbf{R}$ or of $\mathbf{Q}_p$ the field of p-adic numbers, for some prime p, and for such fields K we have an injective group homomorphism

$$\mathrm{inv}\colon \mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}.$$

We note here that this group homomorphism is uniquely defined by the field K, and has excellent compatibility properties with respect to field extensions.

It follows from the details of what we describe above that $[\chi]_{\mathbf{Q}(\chi)}$ can effectively be calculated from the knowledge of $[\chi]_{\hat{F}_v}$, where v runs through the non-trivial normalized valuations of F. The present article describes a method to calculate explicitly these $[\chi]_{\hat{F}_v}$ and their invariant $\mathrm{inv}\left([\chi]_{\hat{F}_v}\right)$ once an identification of $\hat{F}_v$ with a finite extensions of $\mathbf{R}$ or $\mathbf{Q}_p$ for some prime p has been chosen.

A theorem of Benard–Schacher (see for example Theorem 6.1 in Yamada's book [15]) tells us that the invariant varies in predictable ways as we take different valuations v above the same prime p. However, we argue in [13] that, as soon as we fix a prime p and

p-Brauer characters are defined, then a natural single value of $\operatorname{inv}\left([\chi]_{\hat{F}_v}\right)$ is associated to each χ.

In addition to their intrinsic interest, and their use in calculating the whole family of invariants, as described above, the invariants $[\chi]_K$, where K is a finite extension of the field $\mathbf{Q}_p$ of p-adic numbers, for some prime p, have recently been shown to be closely related to some of the fundamental conjectures in representation theory of finite groups. In particular, the celebrated McKay Conjecture has been strengthened by Turull [10] to incorporate these invariants in a natural way. Although this conjecture remains open in general (as is the original weaker McKay Conjecture open in general) the strengthened version was proved by Turull [11] in 2013 in a very strong form including the Alperin strengthening and others for p-solvable groups. In addition, a refinement of Dade's Projective Conjecture that incorporates these invariants was proposed and proved for all p-solvable groups by Turull in 2017 [12].

It is well known that the knowledge of these invariants implies the knowledge of the Schur indices. In particular, these conjectures have a corresponding weaker version that replaces the element of the Brauer group by the corresponding Schur index. Furthermore, our calculation of the invariants implies a calculation of the Schur indices.

The author is not aware of any earlier attempt to find an algorithm to calculate these invariants for arbitrary finite groups. The calculation of the Schur indices, however, has been the subject of substantial research. The 'wedderga'-package [1] for the computer algebra system GAP has functionality to calculate Schur indices over $\mathbf{Q}$ or $\mathbf{Q}_p$. Similarly, a general practical algorithm for the calculation of the Schur indices for arbitrary finite groups has also recently been proposed by Unger [14] and implemented within MAGMA. We refer the interested reader to [14] for more information on the work to date on the techniques to calculate Schur indices.

We now turn to describing the content of this paper. Let K be a finite extension of the field $\mathbf{R}$ of real numbers, or of a field $\mathbf{Q}_p$ of p-adic numbers, for some prime p. Let G be a finite group, and let $\chi \in \operatorname{Irr}_K(G)$. We describe a method to explicitly calculate the local invariant $\operatorname{inv}([\chi]_K)$.

While our method calculates the invariant in every case, its practical implementation requires control over certain subgroups of the group in question, and, in particular, the use of the Brauer-Witt reduction. Hence, the practical implementation of this method is mostly suitable for groups that are not too large. We believe that it has theoretical interest for all finite groups.

In Section 4 we define some classes of finite groups, which we name *p-basic groups*. They come in various types, namely, type 0, 1, 2, 3 and 4. (For convenience, we allow these various types to have some overlap, and some finite groups can be p-basic of more than one type.) Their definition is related to some ideas of Schmid [8] and Riese and Schmid [6]. However, our goals here are different than those in these papers and the classes of groups we obtain are different from theirs. Our goal is to define classes of finite groups which are broad enough to include all groups obtained as terminal cases of our reductions but narrow enough that the local invariants of their irreducible characters can be explicitly given by a formula. After a section on uniformizers and a section on crossed products, these invariants are calculated in Section 8.

It follows from well known results (Yamada [15]) that the p-local Schur indices for $p = \infty$ or $p = 2$ are always at most 2. In this case, the knowledge of the Schur index over K is enough to give the invariant $\operatorname{inv}([\chi]_K)$. See Theorem 2.7 below. Hence, we set ourselves in the case when K is a finite extension of $\mathbf{Q}_p$, for some odd prime p. Then again, from work of Yamada [15], we know that the order of $\operatorname{inv}([\chi]_K)$ divides $p-1$. See also Theorem 2.7 below. It follows that it is enough to calculate $\operatorname{inv}([\chi]_K)_q$, the q-part of $\operatorname{inv}([\chi]_K)$, for each prime q dividing $p-1$.

So we consider the case when p and q are distinct primes and we describe how to calculate $\operatorname{inv}([\chi]_K)_q$. Using ideas from the Brauer-Witt Theorem, we can reduce to the case where G is q-quasi-elementary. We can then apply the reductions from Theorem 3.1 repeatedly to the resulting situation until they no longer produce a smaller group. At this point, the group we have is a p-basic group, and the invariant of its irreducible character is given explicitly in Section 8. This process is described in more detail in Section 9.

When K is a finite extension of $\mathbf{Q}_p$ for some odd prime p, our algorithm does not rely on the prior calculation of the p-local Schur index. Hence, in this case it can be viewed as giving in addition an alternative calculation of the p-local Schur index. On the other hand, when K is a finite extension of $\mathbf{R}$ or of $\mathbf{Q}_2$, the algorithm simply uses the known local Schur index to calculate the invariant.

Our proof relies on a limited number of properties of the Schur indices. Namely, it relies only on the fact that the real Schur index is at most two and the fact that the p-part of the p-local Schur index is always 1 except possibly when $p = 2$, when it could be 2. These facts follow from the more precise facts proved by Yamada [15] about p-local Schur indices.

Finally, we note that a careful reading of our proofs shows that they give an independent proof of the fact proved by Yamada [15] that the p'-part of the p-local Schur index always divides $p-1$ for every (finite) prime p (including $p = 2$, where, of course, we recover the fact that it is 1).

2. Notation and basic results

If F is any field, we denote by $\operatorname{Br}(F)$ the Brauer group of F. In the present paper, $\mathbf{Q}_p$ means the field of p-adic numbers, where p is a prime. We will often be working over a particular field F of characteristic zero, and in this case we will take the irreducible characters of every finite group to have values in some fixed algebraic closure of F, so that for every finite group G the elements of $\operatorname{Irr}(G)$ have values in the algebraic closure of F. We denote by $\operatorname{Irr}_F(G)$ the set of all elements of $\operatorname{Irr}(G)$ whose values are all in F. If $\chi \in \operatorname{Irr}_F(G)$, we denote by $m_F(\chi)$ the Schur index of χ with respect to F.

Definition 2.1. Let F be a field of characteristic 0, let G be a finite group, and let $\chi \in \operatorname{Irr}_F(G)$. Then the *Brauer element of* χ with respect to F is $[\chi]_F$ the class in

$\mathrm{Br}(F)$ of the central simple algebra $\mathrm{End}_{FG}(M)$ where is M is any non-zero FG-module affording as character a multiple of χ. (The Brauer element does not depend on our choice of M.)

Some authors find more natural to assign to χ the element of the Brauer group coming from the simple ideal of FG associated to χ. The following lemma shows that both definitions give closely related results.

Lemma 2.2. *Let F be a field of characteristic* 0*, G be a finite group, and let $\chi \in \mathrm{Irr}_F(G)$. Let $e \in \mathrm{Z}(FG)$ be the central idempotent associated with χ. Let $[eFG]$ be the class of eFG in $\mathrm{Br}(F)$. Then $[\chi]_F$ is the inverse of $[eFG]$ in $\mathrm{Br}(F)$.*

Proof. Let $M = eFG$ viewed as a left FG-module. Then M affords the character $\chi(1)\chi$. Now $\mathrm{End}_F(M)$ is a full matrix algebra over F of dimension $\chi(1)^4$. $\mathrm{End}_{FG}(M)$ is a central simple subalgebra of $\mathrm{End}_F(M)$ of dimension $\chi(1)^2$. Likewise, eFG is a central simple algebra of dimension $\chi(1)^2$, and the action of eFG on M by left multiplication provides an isomorphic copy of itself in $\mathrm{End}_F(M)$ that commutes with $\mathrm{End}_{FG}(M)$. By a dimension argument, it follows that, as an algebra over F, $\mathrm{End}_F(M)$ is isomorphic to $\mathrm{End}_{FG}(M) \otimes_F eFG$. The lemma follows. □

For some fields, the Brauer group can be described in terms of the group $\mathbf{Q}/\mathbf{Z}$. Let K be isomorphic to a finite extension of either $\mathbf{R}$ or some $\mathbf{Q}_p$ for some prime p. Then there is a standard uniquely defined injective group homomorphism

$$\mathrm{inv}\colon\ \mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}.$$

This is well known, and can be found for example in Serre [9] or Pierce [5]. When K is isomorphic to a finite extension of $\mathbf{R}$, then $|\,\mathrm{Br}(K)| \leq 2$, and this determines inv uniquely in this case. We use crossed products to describe inv for the case when K is a finite extension of $\mathbf{Q}_p$ for some prime p. We use the notation of Pierce [5] for crossed products.

Definition 2.3. Let F/K be a finite cyclic field extension of degree n, let σ be a generator for $\mathrm{Gal}(F/K)$, and let $a \in K^{\times}$. Then the *crossed product* (F, σ, a) is a central simple algebra over K that is generated by a subalgebra identified with F, and an invertible element u such that $u^n = a$, and, for all $d \in F$, we have $d^u = u^{-1}du = \sigma(d)$, and, we set, by convention, $d^{\tau} = \tau(d)$ for all $\tau \in \mathrm{Gal}(F/K)$.

Theorem 2.4. *Let p be a prime, and let K be a finite extension of $\mathbf{Q}_p$. Then the map*

$$\mathrm{inv}\colon\ \mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}$$

is a group isomorphism. Furthermore, let $\pi \in K$ *be a uniformizer, let* $k \in \mathbf{Z}$*, let* F/K *be an unramified finite extension of degree* n*, and let* σ *be the Frobenius automorphism of* F/K*. Then*

$$\mathrm{inv}\left([(F,\sigma,\pi^k)]\right) = \frac{k}{n}.$$

Proof. See Section 17.10 in [5]. $\square$

Let K be a finite extension of $\mathbf{Q}_p$ for some prime p. From Serre [9] we know that we have the *valuation* v_K of K

$$v_K \colon K \to \mathbf{Z} \cup \{+\infty\}.$$

v_K is such that $v_K(0) = +\infty$, and, the restriction of v_K yields a surjective homomorphism $K^\times \to \mathbf{Z}$. We note that this definition is slightly different than the one used in Pierce [5] where all valuations take values in the multiplicative semigroup of real numbers.

Using v_K we can describe the invariant of many crossed products.

Corollary 2.5. *Assume the hypotheses of Theorem 2.4. Let* $a \in K^\times$*. Then*

$$\mathrm{inv}\left([(F,\sigma,a)]\right) = \frac{v_K(a)}{n}.$$

Proof. Let $k = v_K(a)$. We can write $a = \pi^k b$ where $b \in K^\times$ with $v_K(b) = 0$. By for example Section 17.9 of [5], we know that b is a norm from $F^\times$. It then follows from Section 15.1 of [5], for example, that

$$\mathrm{inv}\left([(F,\sigma,a)]\right) = \mathrm{inv}\left([(F,\sigma,\pi^k)]\right).$$

Hence, the corollary follows from the theorem. $\square$

Using inv, for appropriate fields, we can define the local invariant to be an element of $\mathbf{Q}/\mathbf{Z}$.

Definition 2.6. Let K be isomorphic to a finite extension of either $\mathbf{R}$ or $\mathbf{Q}_p$ for some prime p. Let G be a finite group, and let $\chi \in \mathrm{Irr}_K(G)$. Then the *local invariant of* χ *with respect to* K is $\mathrm{inv}\left([\chi]_K\right)$ the invariant in $\mathbf{Q}/\mathbf{Z}$ corresponding to $[\chi]_K \in \mathrm{Br}(K)$.

Theorem 2.7. *Let* K *be isomorphic to a finite extension of either* $\mathbf{R}$ *or* $\mathbf{Q}_p$ *for some prime* p*. Let* G *be a finite group, and let* $\chi \in \mathrm{Irr}_K(G)$*. Then the following hold.*

(1) *If* $e \in \mathrm{Z}(KG)$ *is the central idempotent associated to* χ*, then*

$$\mathrm{inv}\left([\chi]_K\right) = -\,\mathrm{inv}\left([eKG]\right).$$

(2) *If F is a finite extension of K, then*

$$\operatorname{inv}([\chi]_F) = [F : K] \operatorname{inv}([\chi]_K).$$

(3) *Suppose $a, b \in \mathbf{Z}$, where $b > 0$, a and b are relatively prime, and $\frac{a}{b}$ is a representative of* $\operatorname{inv}([\chi]_K)$. *Then $b = m_K(\chi)$.*

(4) *Assume that $m_K(\chi) \leq 2$. Then*

$$\operatorname{inv}([\chi]_K) = \frac{1}{m_K(\chi)} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

(5) *If K is isomorphic to a finite extension of* $\mathbf{R}$ *then $m_K(\chi) \leq 2$.*

(6) *If K is isomorphic to a finite extension of $\mathbf{Q}_p$, for some prime p, and $p \nmid |G|$ then $m_K(\chi) = 1$.*

(7) *(Yamada) If K is isomorphic to a finite extension of $\mathbf{Q}_2$ then $m_K(\chi) \leq 2$.*

(8) *(Yamada) If K is isomorphic to a finite extension of $\mathbf{Q}_p$ where p is an odd prime, then $m_K(\chi) \mid p - 1$.*

Proof. (1) follows from Lemma 2.2, the fact that inv is a group homomorphism, and the fact that $\mathbf{Q}/\mathbf{Z}$ is an additive group.

(2) Of course, $\chi \in \operatorname{Irr}_F(G)$. Let M be any non-zero KG-module affording as character a multiple of χ. Then $F \otimes_K M$ is a non-zero FG-module affording as character a multiple of χ. The central simple algebra $\operatorname{End}_{FG}(F \otimes_K M)$ is isomorphic to $F \otimes_K \operatorname{End}_{KG}(M)$, and so the equation follows from the corresponding property of inv as given, for example, in Section 17.10 of Pierce [5].

(3) From Section 17.10 of Pierce [5], for example, we obtain that the order of $\operatorname{inv}([\chi]_K)$ is $m_K(\chi)$, and the result follows.

(4) Follows directly from (3).

(5) It is well known that the Schur indices over $\mathbf{R}$ are at most 2.

(6) See, for example, Corollary 9.4, page 186 in [2].

(7) and (8) See Yamada [15] Theorem 5.14 for (7), and Theorem 4.4 for (8). □

Since there are methods to calculate the Schur indices, the previous theorem tells us how to calculate $\operatorname{inv}([\chi]_K)$ when K is a finite extension of $\mathbf{R}$ or of $\mathbf{Q}_2$, a fact that was noted in [15].

In the rest of the paper, we focus on the calculation of this invariant when K is a finite extension of $\mathbf{Q}_p$ for some odd prime p.

3. Reductions for the local invariant of a character

Let K be a field of characteristic 0, and let characters take values in $\overline{K}$, an algebraic closure of K. Let G be a finite group, and let χ be a character of G. Then we say that χ

is *K-quasi-homogeneous* if $\chi \neq 0$, χ takes its values in K, and there exists a $\psi \in \mathrm{Irr}(G)$ such that χ is a sum of characters of the form $\sigma\psi$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Theorem 3.1. *Let K be a field of characteristic 0, and let characters take values in $\overline{K}$, an algebraic closure of K. Then there is an algorithm that works as follows. Let G and $\chi \in \mathrm{Irr}_K(G)$, and assume any of the following:*

(1) $\ker(\chi) \neq 1$.
(2) *$H \neq G$ is a subgroup of G such that $\mathrm{Res}^G_H(\chi) \in \mathrm{Irr}(H)$.*
(3) *N is a normal subgroup of G and $\mathrm{Res}^G_N(\chi)$ is not K-quasi-homogeneous.*

Then the algorithm produces a group H and some $\psi \in \mathrm{Irr}_K(H)$ with all the following properties.

(1) $|H| < |G|$.
(2) *H is a section of G.*
(3) $[\chi]_K = [\psi]_K$.

Proof. Suppose first that $\ker(\chi) \neq 1$. Then we set $H = G/\ker(\chi)$ and set $\psi \in \mathrm{Irr}(G)$ to be the character corresponding to χ, and, of course, we then have all the stated properties. Suppose next that $H \neq G$ is a subgroup of G such that $\mathrm{Res}^G_H(\chi) \in \mathrm{Irr}(H)$. Now set $\psi = \mathrm{Res}^G_H(\chi)$. Let M be any non-zero KG-module affording as character a multiple $r\chi$ of χ. Then $\dim_K(\mathrm{End}_{FG}(M)) = r^2$, and setting $N = \mathrm{Res}^G_H(M)$, we have that $\mathrm{End}_{KG}(M) = \mathrm{End}_{KH}(N)$ because they have the same dimension, and so $[\chi]_K = [\psi]_K$.

Suppose now that N is a normal subgroup of G and $\mathrm{Res}^G_N(\chi)$ is not K-quasi-homogeneous. Let $\theta \in \mathrm{Irr}(N)$ be contained in $\mathrm{Res}^G_N(\chi)$. Using the notation of [11], we set $H = \tilde{I}_G(\theta, K)$, so that H is the set of all elements of G that conjugate θ to a Galois conjugate of θ. Now since $\mathrm{Res}^G_N(\chi)$ is not K-quasi-homogeneous but $\chi \in \mathrm{Irr}_K(G)$, we know that $H \neq G$. It then follows from [11, Proposition 2.1] that there exists a corresponding $\psi \in \mathrm{Irr}_K(H)$ to χ, and that we also have $[\chi]_K = [\psi]_K$. Hence, the theorem holds. □

Let q be a prime. Recall that a finite group is *q-quasi-elementary* if it has cyclic normal q'-complement. See Definition 8.8 in [4].

The following result is well known.

Theorem 3.2. *Let K be a field of characteristic zero, assume that characters take values in some algebraic closure $\overline{K}$ of K, and let q be a prime. Let G be a finite group, and let $\chi \in \mathrm{Irr}_K(G)$. Then there exists some q-quasi-elementary subgroup H of G and some $\psi \in \mathrm{Irr}(H)$ such that*

$$[K(\psi) : K][\psi, \mathrm{Res}^G_H(\chi)] \not\equiv 0 \pmod{q}.$$

Proof. By Solomon's Theorem [4, Theorem 8.10], there exist $n > 0$, $m, n_i \in \mathbf{Z}$ and H_i q-quasi-elementary subgroups of G for $i \in \{1, \ldots, n\}$ such that $q \nmid m$ and

$$m1_G = \sum_{i=1}^{n} n_i \operatorname{Ind}_{H_i}^{G}(1_{H_i}).$$

This implies, using Frobenius reciprocity, that

$$m = [m\chi, \chi] = \sum_{i=1}^{n} n_i [\operatorname{Res}_{H_i}^{G}(\chi), \operatorname{Res}_{H_i}^{G}(\chi)].$$

Since $q \nmid m$, this, in turn, implies that there exists some $i \in \{1, \ldots, n\}$ such that

$$q \nmid n_i [\operatorname{Res}_{H_i}^{G}(\chi), \operatorname{Res}_{H_i}^{G}(\chi)].$$

Since $\chi \in \operatorname{Irr}_K(G)$, it follows that there exists some $\psi \in \operatorname{Irr}(H_i)$ such that

$$q \nmid n_i [K(\psi) : K][\psi, \operatorname{Res}_{H_i}^{G}(\chi)],$$

and the theorem follows. $\square$

Proposition 3.3. *Let K be a finite extension of $\mathbf{R}$ or $\mathbf{Q}_p$ for some p prime. Assume that characters take values in an algebraic closure $\overline{K}$ of K. Let G be a finite group, let $\chi \in \operatorname{Irr}(G)$, let H be a subgroup of G, and let $\psi \in \operatorname{Irr}(H)$. Then*

$$[\operatorname{Res}_{H}^{G}(\chi), \psi][K(\chi, \psi) : K(\chi)] \operatorname{inv}\left([\chi]_{K(\chi)}\right) = [\operatorname{Res}_{H}^{G}(\chi), \psi][K(\chi, \psi) : K(\psi)] \operatorname{inv}\left([\psi]_{K(\psi)}\right) \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Set $L = K(\chi, \psi)$, and set $d = [\operatorname{Res}_{H}^{G}(\chi), \psi]$. If $d = 0$, the result holds, so we assume $d \neq 0$. By Theorem 2.7, we know that

$$\operatorname{inv}([\chi]_L) = [L : K(\chi)] \operatorname{inv}\left([\chi]_{K(\chi)}\right)$$

and

$$\operatorname{inv}([\psi]_L) = [L : K(\psi)] \operatorname{inv}\left([\psi]_{K(\psi)}\right).$$

Let M be a LG-module affording as character $\mathrm{m}_L(\chi)\chi$. Set $D = \operatorname{End}_{LG}(M)$. Then D is a central division algebra over L, and

$$\operatorname{inv}([\chi]_L) = \operatorname{inv}([D]).$$

Let N be the ψ-homogeneous component of $\mathrm{Res}_H^G(M)$. Then N can be viewed as a LH-module affording the character $\mathrm{m}_L(\chi)d\psi$. In particular, $N \neq 0$. Set $E = \mathrm{End}_{LH}(N)$. Then

$$\mathrm{inv}\left([\psi]_L\right) = \mathrm{inv}\left([E]\right).$$

Now D acts naturally on N, and this identifies D with a subalgebra of E. Set $C = \mathrm{C}_E(D)$. Since D is a central simple algebra over L, it follows that C is a central simple algebra over L and

$$E = D \otimes_L C.$$

We know that

$$\dim_L(E) = \mathrm{m}_L(\chi)^2 d^2 = \dim_L(D) d^2.$$

It follows that $\mathrm{inv}\left([C]\right)$ has a representative that is a fraction whose denominator is d. Since $\mathrm{inv}\left([E]\right) = \mathrm{inv}\left([D]\right) + \mathrm{inv}\left([C]\right)$, it follows that $d\,\mathrm{inv}\left([E]\right) = d\,\mathrm{inv}\left([D]\right) \in \mathbf{Q}/\mathbf{Z}$. This proves our proposition. □

Proposition 3.4. *Let K be a finite extension of $\mathbf{R}$ or $\mathbf{Q}_p$ for some p prime. Assume that characters take values in an algebraic closure $\overline{K}$ of K. Let G be a finite group, and let $\chi \in \mathrm{Irr}_K(G)$. Let q be a prime, and let H, and $\psi \in \mathrm{Irr}(H)$ be as in Theorem 3.2, so that H is a q-quasi-elementary subgroup of G, and*

$$[K(\psi) : K][\psi, \mathrm{Res}_H^G(\chi)] \not\equiv 0 \pmod{q}.$$

Then all the following hold.

(1) *$m_K(\psi)$ is a power of q;*
(2) *There is some $a \in \mathbf{Z}$ such that a is the inverse of $[K(\psi) : K]$ modulo $m_K(\psi)$;*
(3) *The q-part of $\mathrm{inv}\left([\chi]_K\right)$ is*

$$\mathrm{inv}\left([\chi]_K\right)_q = a\,\mathrm{inv}\left([\psi]_{K(\psi)}\right),$$

where a is any integer as in (2).

Proof. Since H is a q-quasi-elementary group, we know that $\psi(1)$ is a power of q, and this implies that $m_K(\psi)$ is also a power of q, so that (1) holds. Now, by our hypotheses, $[K(\psi) : K]$ is prime to q, and (2) follows. Now by Proposition 3.3, we know that

$$[\mathrm{Res}_H^G(\chi), \psi][K(\psi) : K]\,\mathrm{inv}\left([\chi]_K\right) = [\mathrm{Res}_H^G(\chi), \psi]\,\mathrm{inv}\left([\psi]_{K(\psi)}\right) \in \mathbf{Q}/\mathbf{Z}.$$

Since the right hand side is a q-element, we may replace the left hand side by its own q-part. Now the order of $\operatorname{inv}([\chi]_K)_q$ and the order of $\operatorname{inv}\left([\psi]_{K(\psi)}\right)$ are both $m_K(\psi)$. Multiplying both sides by an integer that is the inverse of $[\operatorname{Res}^G_H(\chi), \psi]$ modulo $m_K(\psi)$, we obtain

$$[K(\psi) : K] \operatorname{inv}([\chi]_K)_q = \operatorname{inv}\left([\psi]_{K(\psi)}\right) \in \mathbf{Q}/\mathbf{Z}.$$

Then the result follows. $\square$

The reductions that we have described allow us to reduce the calculation of the invariant of a character to the case when the group is q-quasi-elementary and the irreducible character satisfies some extra conditions.

Theorem 3.5. *Let K be a finite extension of $\mathbf{R}$ or $\mathbf{Q}_p$ for some p prime. Assume that characters take values in an algebraic closure $\overline{K}$ of K. Let q be a prime. Then there exists an algorithm that, given any finite group G and any $\chi \in \operatorname{Irr}(G)$, produces a field F, a section H of G, and some $\psi \in \operatorname{Irr}_F(H)$ such that all of the following conditions are satisfied:*

(1) $K \subseteq K(\chi) \subseteq F \subseteq \overline{K}$;
(2) $q \nmid [F : K(\chi)]$;
(3) *H is q-quasi-elementary;*
(4) *ψ is faithful;*
(5) $\operatorname{Res}^H_P(\psi)$ *is not irreducible for every proper subgroup P of H;*
(6) $\operatorname{Res}^H_N(\psi)$ *is F-quasi-homogeneous for every normal subgroup N of H;*
(7) $[F : K(\chi)]$ *is invertible modulo the order of* $\operatorname{inv}([\psi]_F)$;
(8) *The q-part of* $\operatorname{inv}\left([\chi]_{K(\chi)}\right)$ *is*

$$\operatorname{inv}\left([\chi]_{K(\chi)}\right)_q = a \operatorname{inv}([\psi]_F),$$

where $a \in \mathbf{Z}$ is any such that $a[F : K(\chi)] \equiv 1$ modulo the order of $\operatorname{inv}([\psi]_F)$.

Proof. By Theorem 3.2, we may find some subgroup H_1 of G and some irreducible character $\psi_1 \in \operatorname{Irr}(H_1)$ such that H_1 is q-quasi-elementary, and

$$[K(\psi_1, \chi) : K(\chi)][\psi_1, \operatorname{Res}^G_{H_1}(\chi)] \not\equiv 0 \pmod{q}.$$

We then set $F = K(\psi_1, \chi)$. Then (1) and (2) hold, and $\psi_1 \in \operatorname{Irr}_F(H_1)$. Now while the hypotheses of Theorem 3.1 (with F instead of K) apply to H_1 and ψ_1, we keep replacing them by those given by the theorem. Since the size of H_1 decreases each time we apply the theorem, after a finite number of steps, we will get H_1 and ψ_1 for which the hypotheses of Theorem 3.1 no longer hold. We then set $H = H_1$ and $\psi = \psi_1$. It follows that (3–6) hold. In addition, from Theorem 3.1, we know $[\psi]_F = [\psi_1]_F$. Since H

is q-quasi-elementary, the order of $\operatorname{inv}([\psi]_F)$ is a power of q, so that (7) also holds. Now the theorem follows from Theorem 3.4 and the construction of H and ψ. $\square$

4. p-basic groups

Let p be a prime number. In this section, we define the following types of finite groups which we call *p-basic groups*. We find it convenient to allow certain finite groups to have more than one type.

Definition 4.1. We say that G is a *p-basic group of type* 0 if G is a finite group and $p \nmid |G|$.

Definition 4.2. We say that G is a *p-basic group of type* 1 if G is a finite group, G has a unique Sylow p-subgroup P, $|P| = p$, and G/P is cyclic.

Definition 4.3. We say that G is a *p-basic group of type* $2-3$ if G is a finite group, and there exist two different primes r and q both different from p such that G has a unique Sylow p-subgroup P, $|P| = p$, G has a unique Sylow r-subgroup R, $|R| = r$, $\mathrm{C}_G(PR)$ is cyclic, and there is some $Q \in \mathrm{Syl}_q(G)$ such that $G = PRQ$, and $\mathrm{C}_Q(R) \subseteq \mathrm{C}_Q(\mathrm{C}_Q(PR))$.

Lemma 4.4. *Suppose G is a p-basic group of type $2-3$, and assume the notation of Definition 4.3. Let $C = \mathrm{C}_Q(PR)$. Then, at least one of the following holds:*

(1) *There exists a cyclic subgroup X of Q such that $\mathrm{C}_X(P) \subseteq \mathrm{Z}(G)$, and $G = X\,\mathrm{C}_G(P) = X\,\mathrm{C}_G(R)$; or*
(2) *There exists a cyclic subgroup Y of Q such that $\mathrm{C}_Y(R) \subseteq C$, and $Y\,\mathrm{C}_G(R) = G$.*

Proof. Assume that G is a counterexample. Set $Q_1 = Q/\mathrm{C}_Q(P)$ and $Q_2 = Q/\mathrm{C}_Q(R)$, and notice that they both are cyclic q-groups. Let $x \in Q$ be such that $x\,\mathrm{C}_Q(P)$ generates Q_1, and let $y \in Q$ be such that $y\,\mathrm{C}_Q(R)$ generates Q_2.

Suppose that y can be chosen so that $y^{|Q_2|} \in \mathrm{C}_Q(P)$. Then we set $Y = \langle y \rangle$. We have $\mathrm{C}_Y(R) = \left\langle y^{|Q_2|} \right\rangle \subseteq C$. By our choice of y, $Y\,\mathrm{C}_Q(R) = Q$, and it follows that $Y\,\mathrm{C}_G(R) = G$, so that Y satisfies (2), against our hypothesis. Hence, for any choice of y we have $y^{|Q_2|} \notin \mathrm{C}_Q(P)$. In particular, $|Q_1| > |Q_2|$.

Suppose that $x\,\mathrm{C}_Q(R)$ is a generator for Q_2. Set $X = \langle x \rangle$. Then $\mathrm{C}_X(P) = \left\langle x^{|Q_1|} \right\rangle \subseteq C$, and $\mathrm{C}_G(C_X(P)) \supseteq X\,\mathrm{C}_Q(R)PR = G$. Since this implies that X satisfies the conditions of (1), it follows that $x\,\mathrm{C}_Q(R)$ is not a generator for Q_2.

There is some integer n such that $y\,\mathrm{C}_Q(P) = x^n\,\mathrm{C}_Q(P)$. Since $x\,\mathrm{C}_Q(R)$ is not a generator for Q_2, $x^{-n}y \in Q$ is such that $x^{-n}y\,\mathrm{C}_Q(R)$ is a generator for Q_2, and $x^{-n}y \in \mathrm{C}_Q(P)$. By replacing y by $x^{-n}y$, if necessary, we may choose $y \in \mathrm{C}_Q(P)$. This contradicts the second paragraph, and completes the proof of the lemma. $\square$

Definition 4.5. We say that G is a *p-basic group of type* 2 if G is a p-basic group of type 2-3, and, in the notation of Definition 4.3, there exists a cyclic subgroup X of Q such that $\mathrm{C}_X(P) \subseteq \mathrm{Z}(G)$, and $G = X\,\mathrm{C}_G(P) = X\,\mathrm{C}_G(R)$.

Definition 4.6. We say that G is a *p-basic group of type* 3 if G is a p-basic group of type $2-3$, and, in the notation of Definition 4.3, and setting $C = \mathrm{C}_Q(PR)$, there exists a cyclic subgroup Y of Q such that $\mathrm{C}_Y(R) \subseteq C$, and $Y\,\mathrm{C}_G(R) = G$.

Of course, in the terminology we just introduced, Lemma 4.4 tells us that every p-basic group of type $2-3$ is either a p-basic group of type 2 or a p-basic group of type 3. Note that there exist non-abelian finite groups that are both of type 2 and of type 3. Even more strikingly, if we take two distinct primes p and r, any cyclic group of order pr is p-basic of types 1, 2, and 3, as well as r-basic of types 1, 2, and 3. (We believe that it would unnecessarily complicate the definitions to set up our terminology to exclude these possibilities.)

The last type of p-basic groups only occurs when $p \equiv 3 \pmod 4$.

Definition 4.7. We say that G is a *p-basic group of type* 4 if $p \equiv 3 \pmod 4$, G is a finite group, G has a unique Sylow p-subgroup P, $|P| = p$, G/P is a 2-group, $G \neq \mathrm{C}_G(P)$, and, letting $D \in \mathrm{Syl}_2(\mathrm{C}_G(P))$ and, setting 2^n to be the 2-part of p^2-1, D is isomorphic to a non-abelian subgroup of a semidihedral group of order 2^{n+1}, and D has a cyclic maximal subgroup M such that $G = D\,\mathrm{C}_G(M)$.

Note that in Definition 4.7, $\mathrm{C}_G(P)$ is a normal subgroup of index 2 in G, and that D is the unique Sylow 2-subgroup of $\mathrm{C}_G(P)$.

Definition 4.8. We say that G is a *p-basic group*, if it is a p-basic group of type 0, 1, 2, 3, or 4.

5. From quasi-elementary to basic

In this section, we prove that whenever p and q are primes, $p \neq q$, we are working over a finite extension of $\mathbf{Q}_p$, and we start with a q-quasi-elementary group and one of its irreducible characters, and we repeatedly apply the algorithm of Theorem 3.1, we will reach a p-basic group and one of its irreducible characters.

Lemma 5.1. *Let p be a prime, let K be a finite extension of $\mathbf{Q}_p$, and assume all characters take values in some algebraic closure $\overline{K}$ of K. Let G be a finite group. Let $\psi \in \mathrm{Irr}_K(G)$ be faithful. Let N be a normal abelian p'-subgroup of G, and assume that the restriction of ψ to N is K-quasi-homogeneous. Then $G/\,\mathrm{C}_G(N)$ is cyclic.*

Proof. Let $\lambda \in \mathrm{Irr}(N)$ be contained in the restriction of ψ to N. Since ψ is K-quasi-homogeneous, and ψ is faithful, we know that λ is faithful. It follows that N is cyclic.

Let $F = K(\lambda)$. Now the action of G on N by conjugation yields a faithful action of $G/\operatorname{C}_G(N)$ by conjugation on N, and this in turn yields through λ a group isomorphism from $G/\operatorname{C}_G(N)$ to $\operatorname{Gal}(F/K)$. Since N is a p'-group, F is an extension of K by a p'-th root of unity. By, for example, Proposition 16 Chapter IV in [9], we obtain the well known facts that the extension F/K is unramified and that $\operatorname{Gal}(F/K)$ is cyclic. The lemma follows. $\square$

Lemma 5.2. *Let p be a prime, let K be a finite extension of $\mathbf{Q}_p$, and assume all characters take values in some algebraic closure $\overline{K}$ of K, and let G be a finite group and let $\psi \in \operatorname{Irr}_K(G)$ be faithful. Let q be a prime number. Assume that G has a normal cyclic subgroup C such that $q \nmid |C|$ and G/C is a q-group. Suppose that the restriction of ψ to every normal subgroup of G is K-quasi-homogeneous. Let $Q \in \operatorname{Syl}_q(G)$. Then there exists some subgroup C_0 of C such that, setting $H = QC_0$, we have that $|C_0| \mid pr$ for some prime $r \notin \{p, q\}$, and $\operatorname{Res}^G_H(\psi) \in \operatorname{Irr}(H)$.*

Proof. Let $P \in \operatorname{Syl}_p(C)$, and set $P_0 = P$ if $|P| = 1$, and P_0 to be the unique subgroup of C of order p of P otherwise. Then $\operatorname{C}_Q(P) = \operatorname{C}_Q(P_0)$. Let C_1 be the Hall p'-subgroup of C. Let $\theta \in \operatorname{Irr}(C_1)$ be contained in the restriction of ψ to C_1. Since this restriction is K-quasi-homogeneous, it follows from Lemma 5.1 that $Q/\operatorname{C}_Q(C_1)$ is a cyclic q-group. If $Q/\operatorname{C}_Q(C_1) \neq 1$, then there exists some subgroup R of prime order (r say) of C_1 such that $\operatorname{C}_Q(C_1) = \operatorname{C}_Q(R)$, and we set $C_0 = P_0R$. If $Q/\operatorname{C}_Q(C_1) = 1$, then we set $C_0 = P_0$, and we let r be any prime different from p and different from q. In either case, we have $r \notin \{p, q\}$, $|C_0| \mid pr$, and $\operatorname{C}_Q(C) = \operatorname{C}_Q(C_0)$. We set $H = QC_0$. Let $\zeta_1 \in \operatorname{Irr}(C)$ be contained in the restriction of ψ to C. Then the inertia subgroup of ζ_1 in G is $\operatorname{C}_Q(C)C$, a nilpotent subgroup of G. There exists some $\nu \in \operatorname{Irr}(\operatorname{C}_Q(C))$ such that $\nu \otimes \zeta_1$ is contained in the restriction of ψ to $\operatorname{C}_Q(C)C$. By Clifford's Theorem, it follows that $\psi = \operatorname{Ind}^G_{\operatorname{C}_Q(C)C}(\nu \otimes \zeta_1)$. In particular,

$$\psi(1) = [Q : \operatorname{C}_Q(C)]\nu(1).$$

Let $\zeta_2 \in \operatorname{Irr}(C_0)$ be the restriction of ζ_1 to C_0. Then the inertia group of ζ_2 in H is $\operatorname{C}_Q(C)C_0$, and the character $\nu \otimes \zeta_2$ is contained in the restriction of ψ to $\operatorname{C}_Q(C)C_0$. It follows that $\operatorname{Ind}^H_{\operatorname{C}_Q(C)C_0}(\nu \otimes \zeta_2) \in \operatorname{Irr}(H)$ and it is contained in the restriction of ψ to H. It follows that $\operatorname{Res}^G_H(\psi) \in \operatorname{Irr}(H)$. Hence, the lemma holds. $\square$

The following lemma follows from P. Hall's classification of the q-groups all of whose abelian characteristic subgroups are cyclic [3, Satz III.13.10]. It is very close to [7, Lemma 4], and follows easily from it. We offer a full proof of our version for completeness.

Lemma 5.3. *Let q be a prime number, let G be a finite q-group, and suppose that Q is a normal non-cyclic subgroup of G. Assume that every G-invariant abelian subgroup of Q is cyclic. Then $q = 2$, Q contains a G-invariant subgroup of order 4 not in the center of Q, and Q is dihedral, semidihedral or generalized quaternion.*

Proof. Assume the lemma is false, and consider a counterexample with $|Q|$ as small as possible. By Hall's classification of the q-groups all of whose abelian characteristic subgroups are cyclic [3, Satz III.13.10], we know that Q is a central product of a group Q_1 that is either extraspecial or cyclic of order q, and a group $Q_2 \neq 1$ that is either cyclic or else $q = 2$, $|Q_2| \geq 16$, and Q_2 is dihedral, semidihedral or generalized quaternion, and where the central subgroups of order q of Q_1 and of Q_2 are identified. Suppose that Q_1 is cyclic of order q, so that $Q = Q_2$. Since we have a counterexample, it must be that Q_2 is not cyclic, and it follows that $q = 2$, and Q is dihedral, semidihedral or generalized quaternion and $|Q| \geq 16$. This in turn implies that Q has a non-central characteristic subgroup of order 4, a contradiction. So $|Q_1| \geq q^3$. Looking at the possibilities, we see that $|Q| \geq q^4$.

Suppose that Q_2 is cyclic of order at least q^2. Then, the subgroup of Q generated by all elements of order q and q^2 has exponent q^2 and contains a G-invariant subgroup S such that $|S| = q^3$ and $|S \cap \mathrm{Z}(Q)| = q^2$. But then S is abelian but not cyclic, contradicting our hypotheses. So Q_2 is not cyclic of order at least q^2.

Let $|Q| = q^n$. If $|Q_2| = q$, then $|Q_1| \geq q^5$ and the exponent of Q is at most q^2. If $|Q_2| \neq q$, then, since Q_2 is not cyclic, the exponent of Q is at most q^{n-3}. Hence, in any case, the exponent of Q is at most q^{n-3}.

There is a maximal G-invariant subgroup M of Q. Since G is a q-group, we have $[Q : M] = q$, so that $|M| = q^{n-1}$. By the previous paragraph, M is not cyclic. It follows that, by our choice of counterexample, we know that $q = 2$, and M is dihedral, semidihedral or generalized quaternion. Again, by the previous paragraph, it follows that $|M| \leq q^{n-2}$. This final contradiction completes the proof of the lemma. $\square$

Theorem 5.4. *Let p be a prime, let K be a finite extension of $\mathbf{Q}_p$, and assume all characters take values in some algebraic closure $\overline{K}$ of K. Let G be a finite group, let q be a prime with $q \neq p$, and suppose that $C \trianglelefteq G$ is cyclic of q'-order and G/C is a q-group. Let $\psi \in \mathrm{Irr}_K(G)$ be faithful. Suppose that the restriction of ψ to every normal subgroup of G is K-quasi-homogeneous, and the restriction of ψ to every proper subgroup of G is not irreducible. Then G is a p-basic group.*

Proof. Assume we have a counterexample. If $p \nmid |C|$, then G is a p-basic group of type 0 (Definition 4.1). Hence, $p \mid |C|$. It follows from Lemma 5.2 that there exists some prime $r \notin \{p, q\}$ such that $|C| \in \{p, pr\}$. Let $P \in \mathrm{Syl}_p(G)$, $R \in \mathrm{Syl}_r(G)$, $Q \in \mathrm{Syl}_q(G)$, and $D = \mathrm{C}_Q(C)$. Now $|P| = p$, $|R| \mid r$, both P and R are normal subgroups of G, and $C = PR$.

Suppose that D is cyclic. Then ψ is induced from an irreducible linear character of CD. It follows that $\psi(1) = [Q : D]$. Suppose that Q/D is cyclic. Let $x \in Q$ be such that xD generates the cyclic group Q/D. Then ψ restricts irreducibly to $\langle x \rangle C$, so that $G = \langle x \rangle C$ and $Q = \langle x \rangle$. Suppose that Q/D acts faithfully on R. Then ψ restricts irreducibly to $\langle x \rangle R$, against our hypothesis. Now, since Q/D is a cyclic q-group, this implies that it acts faithfully on P, and this in turn implies that $R = 1$.

It follows that G is p-basic of type 1 (Definition 4.2). Hence Q/D is not cyclic. This implies that $R \neq 1$, so that $|R| = r$. By Lemma 5.1, $Q/\mathrm{C}_Q(RD)$ is cyclic. Suppose that $\mathrm{C}_Q(R) \nsubseteq \mathrm{C}_Q(D)$. Then $\mathrm{C}_Q(RD) = \mathrm{C}_Q(D)$, and it follows that ψ restricts irreducibly to PQ, against our hypothesis. Hence, $\mathrm{C}_Q(R) \subseteq \mathrm{C}_Q(D)$. Now G is a p-basic group of type 2-3 (Definition 4.3). Lemma 4.4 then tells us that G is p-basic of type 2 (Definition 4.5) or p-basic of type 3 (Definition 4.6). This contradiction shows that D is not cyclic.

Let A be any Q-invariant abelian subgroup of D. Then A is normal in G, and it follows that $\mathrm{Res}^G_A(\chi)$ is K-quasi-homogeneous, by hypothesis, so that A is cyclic, and, if further K contains a primitive $|A|$-th root of unity, then $A \subseteq \mathrm{Z}(G)$. By Lemma 5.3, it follows that $q = 2$, D is a non-abelian dihedral, semidihedral, or generalized quaternion group, $|D| \geq 8$, D contains a cyclic maximal subgroup M that is normal in G, and K does not contain a primitive 4-th root of unity. In particular, $p \equiv 3 \pmod 4$, and we set $2^n = (p^2 - 1)_2$. Let k be the residue field of K. Then, since k does not have a primitive 4-th root of unity, $|k|$ is an odd power of p, and $(|k|^2 - 1)_2 = 2^n$. Then $|M| \mid 2^n$, and D is isomorphic to a subgroup of a semidihedral group of order 2^{n+1}. Since ψ does not restrict irreducibly to Q, we know that $Q \neq \mathrm{C}_Q(C)$.

Now CM is a self centralizing normal cyclic subgroup of G. There exists a linear character $\lambda \in \mathrm{Irr}(CM)$ such that $\mathrm{Ind}^G_{CM}(\lambda) = \psi$. Since D acts non-trivially on M, $\mathrm{C}_G(R)$ is not contained in $\mathrm{C}_G(M)$. By Lemma 5.1, $G/\mathrm{C}_G(RM)$ is a cyclic 2-group. It follows that $\mathrm{C}_G(M) \subseteq \mathrm{C}_G(R)$. Hence, the restriction of ψ to PQ is irreducible. It follows that $R = 1$.

Since Q is a 2-group, and $Q/\mathrm{C}_Q(C)$ acts faithfully on a group of order p, it follows that $|Q/\mathrm{C}_Q(C)| = 2$. Consider the homomorphism $\phi\colon G \to \mathrm{Aut}(M)$, such that, for each $g \in G$ and $m \in M$, $\phi(g)(m) = m^{g^{-1}}$. Since M is a normal p'-subgroup of G, $\mathrm{Aut}(M)$ is canonically isomorphic to $(\mathbf{Z}/|M|\mathbf{Z})^\times$, and the image of ϕ corresponds exactly to the cyclic subgroup of $(\mathbf{Z}/|M|\mathbf{Z})^\times$ generated by the class of $|k|$. If $x \in Q$, then $x^2 \in D$ and x^2 centralizes the two elements of order 4 of M. It follows that $x^2 \in M$. This implies that the image of ϕ is cyclic of order 2, and $\phi(G) = \phi(D)$. It follows from this that $G = D\,\mathrm{C}_G(M)$, and that D is isomorphic to a subgroup of a semidihedral group of order 2^{n+1}. This tell us that G is a p-basic group of type 4 (Definition 4.7). This contradiction completes the proof of the theorem. □

Combining this theorem with Theorem 3.5 we obtain the following corollary.

Corollary 5.5. *Let p be a prime, let K be a finite extension of $\mathbf{Q}_p$, and assume all characters take values in some algebraic closure $\overline{K}$ of K. Let q be a prime with $q \neq p$. Then there exists an algorithm that, given any finite group G and any $\chi \in \mathrm{Irr}(G)$, produces a field F, a section H of G, and some $\psi \in \mathrm{Irr}_F(H)$ such that all of the following conditions are satisfied:*

(1) $K \subseteq K(\chi) \subseteq F \subseteq \overline{K}$;
(2) $q \nmid [F : K(\chi)]$;

(3) *H is a p-basic group;*
(4) *ψ is faithful;*
(5) $\mathrm{Res}_P^H(\psi)$ *is not irreducible for every proper subgroup P of H;*
(6) $\mathrm{Res}_N^H(\psi)$ *is F-quasi-homogeneous for every normal subgroup N of H;*
(7) *$[F : K(\chi)]$ is invertible modulo the order of* $\mathrm{inv}\left([\psi]_F\right)$*;*
(8) *The q-part of* $\mathrm{inv}\left([\chi]_{K(\chi)}\right)$ *is*

$$\mathrm{inv}\left([\chi]_{K(\chi)}\right)_q = a\,\mathrm{inv}\left([\psi]_F\right),$$

where $a \in \mathbf{Z}$ is any such that $a[F : K(\chi)] \equiv 1$ modulo the order of $\mathrm{inv}\left([\psi]_F\right)$*.*

Proof. The algorithm is the same as that of Theorem 3.5. By Theorem 5.4, the section H it produces is a p-basic group. Hence the corollary holds. □

6. Roots of unity and uniformizers

In this section, we set up notation for the relevant roots of unity in local fields, and we establish the existence of suitable uniformizers for our purposes.

Definition 6.1. Let p be a prime, and let $t \in \mathbf{Z}$ be relatively prime to p. Then there exists a unique p'-th root of unity $\rho \in \mathbf{Q}_p$ such that $\rho \equiv t \pmod{p\mathbf{Z}_p}$. When p is clear from the context, we denote $\epsilon_t = \rho$.

The facts about $\mathbf{Q}_p$ used in the above definition are well known and can be found, for example, in Serre's book [9, II §4 Proposition 8]. We note that ϵ_t depends only on the class of t modulo p, and that if $t, s \in \mathbf{Z}$ are both relatively prime to p then $\epsilon_{ts} = \epsilon_t \epsilon_s$.

Lemma 6.2. *Let p be a prime, let F and K be finite extensions of $\mathbf{Q}_p$, with $K \subseteq F$, let e' be the ramification index of F/K and let e be the ramification index of $K/\mathbf{Q}_p$, let v_F be the valuation on F, and let $\zeta_p \in F$ be a primitive p-th root of 1. Then $\mathbf{Q}_p\left(\zeta_p\right)/\mathbf{Q}_p$ is totally ramified of degree $p-1$, and*

$$v_F\left(\zeta_p - 1\right) = \frac{ee'}{p-1}.$$

Proof. We know, for example, from [9, IV §4 Proposition 17] that $\zeta_p - 1$ is a uniformizer for $\mathbf{Q}_p\left(\zeta_p\right)$, and $\mathbf{Q}_p\left(\zeta_p\right)/\mathbf{Q}_p$ is totally ramified of degree $p-1$. It follows for example from Corollary b in Section 17.7 of [5] that the ramification indices are multiplicative, so that, in particular, ee' is the ramification index of $F/\mathbf{Q}_p$, and $\frac{ee'}{p-1}$ the ramification index of $F/\mathbf{Q}_p\left(\zeta_p\right)$. Hence the lemma holds. □

Lemma 6.3. *Let p be a prime, let F be a finite extension of $\mathbf{Q}_p$, let v_F be the valuation on F, let $\zeta_p \in F$ be a primitive p-th root of 1, and we set $\pi_0 = \zeta_p - 1$. For each $\sigma \in \mathrm{Gal}\left(F/\mathbf{Q}_p\right)$, we set $\lambda(\sigma) = \epsilon_t$ where $t \in \mathbf{Z}$ is such that $\sigma\left(\zeta_p\right) = \zeta_p^t$.*

Then, $v_F(\pi_0) > 0$,

$$\lambda\colon\ \mathrm{Gal}(F/\mathbf{Q}_p) \to \mathbf{Q}_p$$

is a well defined linear character, and for all $\sigma \in \mathrm{Gal}(F/\mathbf{Q}_p)$,

$$v_F(\sigma(\pi_0) - \lambda(\sigma)\pi_0) > v_F(\pi_0).$$

Proof. It follows from Lemma 6.2 that $v_F(\pi_0) > 0$. For each $\sigma \in \mathrm{Gal}(F/\mathbf{Q}_p)$ there exists some $t \in \mathbf{Z}$ such that $\sigma(\zeta_p) = \zeta_p^t$, and this t is relatively prime to p and uniquely defined modulo p. Hence, λ is well defined, and it follows that λ is a linear character.

Let $\sigma \in \mathrm{Gal}(F/\mathbf{Q}_p)$. There exists some $t \in \mathbf{Z}$ such that $\sigma(\zeta_p) = \zeta_p^t$ and $t > 0$. Then $\lambda(\sigma) = \epsilon_t$. It follows, using the binomial expansion of $\sigma(1+\pi_0) = (1+\pi_0)^t$, that

$$v_F(\sigma(\pi_0) - \lambda(\sigma)\pi_0) = v_F(\sigma(1+\pi_0) - (1+\epsilon_t\pi_0)) > v_F(\pi_0).$$

Hence the lemma holds. □

Lemma 6.4. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that $\sigma_1(\zeta_r) = \zeta_r$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$, and let $m = |\,\mathrm{C}_{\langle\sigma_2\rangle}(\zeta_r)\,|$. We set L to be the fixed field in F of $\langle\sigma_2\rangle$. Let v_F be the valuation on F.*

Then there exists some $\pi \in L$ such that

$$v_F(\pi) = m\, v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F(\sigma_1^n(\pi) - \epsilon_s^{mn}\pi) > v_F(\pi).$$

Proof. Let $G = \langle\sigma_2\rangle$, let $C = \mathrm{C}_G(\zeta_r)$, and let $\overline{G} = G/C$. Set $\pi_0 = \zeta_p - 1$. Set $G_1 = \mathrm{Gal}(F/K)$. Then, by Lemma 6.3, $v_F(\pi_0) > 0$, and there exists a linear character λ of G_1 such that for all $\sigma \in G_1$, there exists some $t \in \mathbf{Z}$ such that $\sigma(\zeta_p) = \zeta_p^t$, and for any such t we have $\lambda(\sigma) = \epsilon_t$, and

$$v_F(\sigma(\pi_0) - \lambda(\sigma)\pi_0) > v_F(\pi_0).$$

The restriction of λ to C is faithful. Note that the product of all the values of λ on C is exactly $(-1)^{m+1}$. We set

$$\pi_1 = \prod_{\sigma \in C} \sigma(\pi_0).$$

Now $v_F(\pi_1) = m\, v_F(\zeta_p - 1) > 0$, and, for all $\sigma \in G_1$,

$$v_F\left(\sigma(\pi_1) - (-1)^{m+1}\lambda(\sigma^m)\,\pi_0^m\right) > v_F(\pi_1).$$

Now from the case $\sigma = 1$, we obtain

$$v_F\left(\lambda(\sigma^m)\,\pi_1 - (-1)^{m+1}\lambda(\sigma^m)\,\pi_0^m\right) > v_F(\pi_1).$$

Combining this with the previous inequality, we obtain that, for all $\sigma \in G_1$,

$$v_F\left(\sigma(\pi_1) - \lambda(\sigma^m)\,\pi_1\right) > v_F(\pi_1).$$

Notice that $\overline{G}$ acts on $\mathbf{Q}_p(\zeta_r)$ as the Galois group of the extension $\mathbf{Q}_p(\zeta_r)/\mathbf{Q}_p(\zeta_r) \cap L$. Since r is prime to p, the extension is unramified. Applying the Normal Basis Theorem to the corresponding extension of residue fields, it follows that there exists some p'-th root of unity $\omega \in \mathbf{Q}_p(\zeta_r)$, such that its projection into the residue field of $\mathbf{Q}_p(\zeta_r)$ generates a normal basis for the entension of residue fields of $\mathbf{Q}_p(\zeta_r)/\mathbf{Q}_p(\zeta_r) \cap L$.

Now both π_1 and ω are in the fixed field of C in F. We let

$$\pi = \sum_{\sigma \in \overline{G}} \sigma(\pi_1 \omega),$$

so that π is the trace under $\overline{G}$ of $\pi_1\omega$. In particular $\pi \in L$.

Notice that C is contained in the kernel of the restriction of the linear character λ^m to G, so that we may define μ as the linear character of $\overline{G}$ corresponding to λ^m. With this notation, we rewrite some special cases of one of our earlier inequalities as, for all $\sigma \in \overline{G}$,

$$v_F\left(\sigma(\pi_1\omega) - \mu(\sigma)\sigma(\omega)\pi_1\right) > v_F(\pi_1).$$

Set

$$\pi' = \pi_1 \sum_{\sigma \in \overline{G}} \mu(\sigma)\sigma(\omega).$$

It follows from the above inequalities that

$$v_F(\pi - \pi') > v_F(\pi_1).$$

Since the values of μ are roots of unity in $\mathbf{Q}_p$, the choice of ω implies that π'/π_1 projects to a non-zero element of the residue field of $\mathbf{Q}_p(\zeta_r)$. It follows that $v_F(\pi) = v_F(\pi') = v_F(\pi_1)$. In particular, $v_F(\pi) = m\, v_F(\zeta_p - 1) > 0$.

By one of our earlier inequalities, we know that for all $n \in \mathbf{Z}$,

$$v_F\left(\sigma_1^n(\pi_1) - \epsilon_s^{mn}\pi_1\right) > v_F(\pi).$$

Note that, by hypothesis, σ_1 fixes ω and all its Galois conjugates. It follows that

$$v_F(\sigma_1^n(\pi) - \epsilon_s^{mn}\pi) > v_F(\pi).$$

Hence, the lemma holds. $\square$

Lemma 6.5. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that*

$$\langle\sigma_1\rangle \times \langle\sigma_2\rangle = \mathrm{Gal}(F/K),$$

$\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_p) = 1$ and $\sigma_2(\zeta_p) = \zeta_p$. For $i \in \{1,2\}$, we set $d_i = |\langle\sigma_i\rangle|$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$. We set L to be the fixed field in F of $\langle\sigma_2\rangle$. Let v_F be the valuation on F.

Then L/K is a finite Galois extension of degree d_1 with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, where τ is the restriction to L of σ_1. Furthermore, there exists some $\pi \in L$ such that

$$v_F(\pi) = v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F(\tau^n(\pi) - \epsilon_s^n\pi) > v_F(\pi).$$

In addition, ϵ_s is a primitive d_1-th root of unity, and $L = K(\pi)$.

Proof. It follows from elementary Galois theory, that L/K is a finite Galois extension with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, where τ is the restriction to L of σ_1, and that $[L : K] = d_1$. Since $\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_p) = 1$, the order of s modulo p is d_1. We set $\pi = \zeta_p - 1$. Then $\pi \in L$, and by Lemma 6.3, we know that $v_F(\pi) > 0$ and that, for all $n \in \mathbf{Z}$,

$$v_F(\tau^n(\pi) - \epsilon_s^n\pi) > v_F(\pi).$$

Now if $\tau^n(\pi) = \pi$, we know that $v_F(1 - \epsilon_s^n) > 0$, and this implies that n is a multiple of d_1. Hence $K(\pi) = L$, and the lemma follows. $\square$

Lemma 6.6. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that*

$$\langle\sigma_1\rangle \times \langle\sigma_2\rangle = \mathrm{Gal}(F/K),$$

$\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_p) = 1$ and $\sigma_2(\zeta_p) = \zeta_p$. For $i \in \{1,2\}$, we set $d_i = |\langle\sigma_i\rangle|$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$, and let $m = |\,\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_r)\,|$. Suppose that $\beta \in \mathbf{Z}$ is such that $\sigma_1^\beta\sigma_2(\zeta_r) = \zeta_r$. We set L to be the fixed field in F of $\langle\sigma_1\rangle$. Let v_F be the valuation on F.

Then L/K is a finite Galois extension of degree d_2 with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, where τ is the restriction to L of σ_2. Furthermore, there exists some $\pi \in L$ such that

$$v_F(\pi) = m\,v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F\left(\tau^n(\pi) - \epsilon_s^{\beta mn}\pi\right) > v_F(\pi).$$

In addition, $\epsilon_s^{\beta m}$ is a primitive d_2-th root of unity, and $L = K(\pi)$.

Proof. It follows from elementary Galois theory, that L/K is a finite Galois extension with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, where τ is the restriction to L of σ_2, and that $[L:K] = d_2$. We apply Lemma 6.4, with $\sigma_1^\beta\sigma_2$ and σ_1 in the place of σ_1 and σ_2 in the lemma. This tells us that there exists some $\pi \in L$ such that

$$v_F(\pi) = m\,v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F\left(\tau^n(\pi) - \epsilon_s^{\beta mn}\pi\right) > v_F(\pi).$$

Since $\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_p) = 1$, the order of ϵ_s is d_1. The order of the restriction to $\mathrm{Gal}(K(\zeta_r)/K)$ of σ_1^β is $d_1/(d_1, m\beta)$. Since $\sigma_2(\zeta_p) = \zeta_p$, it follows that $d_2 = d_1/(d_1, m\beta)$. Hence, the order of $\epsilon_s^{m\beta}$ is d_2. Now if $\tau^n(\pi) = \pi$, we know that $v_F\left(1 - \epsilon_s^{\beta mn}\right) > 0$, and this implies that n is a multiple of d_2. Hence $K(\pi) = L$, and the lemma follows. □

Lemma 6.7. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that*

$$\langle\sigma_1\rangle \times \langle\sigma_2\rangle = \mathrm{Gal}(F/K),$$

$\sigma_1(\zeta_r) = \zeta_r$, and let $\mathrm{C}_{\langle\sigma_2\rangle}(\zeta_r) = 1$. For $i \in \{1,2\}$, we set $d_i = |\langle\sigma_i\rangle|$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$. We set L to be the fixed field in F of $\langle\sigma_2\rangle$. Let v_F be the valuation on F.

Then L/K is a finite Galois extension of degree d_1 with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, where τ is the restriction to L of σ_1. Furthermore, there exists some $\pi \in L$ such that

$$v_F(\pi) = v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F(\tau^n(\pi) - \epsilon_s^n \pi) > v_F(\pi).$$

In addition, ϵ_s *is a primitive* d_1*-th root of unity, and* $L = K(\pi)$.

Proof. It follows from elementary Galois theory, that L/K is a finite Galois extension with cyclic Galois group $\langle \tau \rangle = \mathrm{Gal}(L/K)$, where τ is the restriction to L of σ_1, and that $[L : K] = d_1$. Since $\mathrm{C}_{\langle \sigma_1 \rangle}(\zeta_p) = 1$, the order of s modulo p is d_1. We apply Lemma 6.4 and it tells us that there exists some $\pi \in L$ such that

$$v_F(\pi) = v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F(\tau^n(\pi) - \epsilon_s^n \pi) > v_F(\pi).$$

Now if $\tau^n(\pi) = \pi$, we know that $v_F(1 - \epsilon_s^n) > 0$, and this implies that n is a multiple of d_1. Hence $K(\pi) = L$, and the lemma follows. □

7. Some cross products

In this section, we study certain cross products that will be useful for our calculations, with particular emphasis on their invariants.

Theorem 7.1. *Let p be a prime, and let F and K be finite extensions of $\mathbf{Q}_p$. Assume that the extension F/K is unramified, that $\mathrm{Gal}(F/K)$ is generated by σ, and that $\alpha \in K$ is a p'-th root of unity. Then the crossed product (F, σ, α) is isomorphic to a full matrix algebra over K.*

Proof. Since α is a root of unity, we know that $v_K(\alpha) = 0$. Hence, the theorem follows immediately from Corollary 2.5. □

Lemma 7.2. *Let p be a prime, let F, L, K be finite extensions of $\mathbf{Q}_p$, with $F \supseteq L \supseteq K$. Let k be the residue field of K. Let v_F be the valuation on F, and let e' be the ramification index of F/K. Assume that L/K is a Galois extension with cyclic Galois group of order d generated by τ, and that $d \mid p - 1$. Let $\epsilon \in \mathbf{Q}_p$ be a primitive d-th root of unity. Let $\pi \in L$ and assume that $v_F(\pi) > 0$, and that, for all $n \in \mathbf{Z}$, we have*

$$v_F(\tau^n(\pi) - \epsilon^n \pi) > v_F(\pi).$$

Suppose that $\alpha \in K$ is such that $\alpha^{(|k|-1)/d} = \epsilon^{-1}$. Let A be the crossed product (L, τ, α). Then A is a central simple algebra over K and its invariant is

$$\mathrm{inv}(A) = \frac{v_F(\pi)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Set $G = \mathrm{Gal}(L/K)$. We view L as a subfield of A, and K as the center of A. We let $u \in A$ be such that $u^d = \alpha$, and, for all $a \in L$, we have $a^u = a^\tau$, where by convention we have $a^\tau = \tau(a)$. We know that A is generated by L and u, and that $\dim_K(A) = d^2$.

$\langle u \rangle$ is a finite group of order dividing $d(|k| - 1)$, and, in particular, of order relatively prime to p. Let $K(u)$ be the subalgebra of A generated by K and u. Since $u^d \in K$, it is clear that $\dim_K(K(u)) \leq d$. By Maschke's Theorem, $K(u)$ is a direct sum of fields that are isomorphic to field extensions of K by $(|k| - 1)$-th roots of ϵ^{-1}. Let K_1 be any field extension of K by a $(|k| - 1)$-th root of ϵ^{-1}. Let k_1 be the residue field of K_1, and let δ be the projection in k_1 of a $(|k| - 1)$-th root of ϵ^{-1} in K_1. Now $\delta^{|k|} = \delta\epsilon'$, where $\epsilon' \in k$ is the projection in k of ϵ^{-1} and is a primitive d-th root of unity. It follows that $[k_1 : k] = d$. This implies that $[K_1 : K] = d$ and K_1/K is unramified. It follows that $K(u)$ is a field extension of K, that $[K(u) : K] = d$, and that $K(u)/K$ is unramified.

Since ϵ is a primitive d-th root of unity in K, there exists a unique faithful character $\mu \in \mathrm{Irr}(G)$ with values in K such that $\mu(\tau) = \epsilon^{-1}$. It follows from our hypotheses that, for $g \in G$, we have

$$v_F\left(\mu(g)\pi^g - \pi\right) > v_F(\pi).$$

We set

$$\beta := \sum_{g \in G} \mu(g)\pi^g.$$

Hence

$$v_F\left(\beta - |G|\pi\right) > v_F(\pi).$$

Since $p \nmid |G|$, it follows that $v_F(\beta) = v_F(\pi)$, and, in particular, $\beta \neq 0$. Note that $\beta \in L$ and therefore β is invertible in A. Now, it follows from the definition of β that

$$\beta^u = \sum_{g \in G} \mu(g)\pi^{g\tau} = \epsilon\beta.$$

It then follows that

$$\left(u^{-1}\right)^\beta = \epsilon u^{-1},$$

and, therefore, $u^\beta = \epsilon^{-1}u = u^{|k|}$ using that $\epsilon^{-1} = u^{|k|-1}$.

Since $|k| \equiv 1 \pmod{d}$, d divides $(|k|^d - 1)/(|k| - 1)$. It follows that the order of u divides $|k|^d - 1$, so that β^d commutes with u. As β commutes with every element of L, it then follows that $\beta^d \in K$. Let $\phi \in \mathrm{Gal}(K(u)/K)$ be the Frobenius automorphism. Then A is isomorphic to the crossed product $(K(u), \phi, \beta^d)$. Since $K(u)$ is an unramified extension of K of degree d, by Corollary 2.5, it follows that A is a central simple algebra over K whose invariant is

$$\mathrm{inv}(A) = \frac{v_K\left(\beta^d\right)}{d} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Since the ramification index of F/K is e', we have

$$\frac{v_K\left(\beta^d\right)}{d} = \frac{v_F\left(\beta^d\right)}{e'd} = \frac{v_F(\pi)}{e'},$$

because $v_F(\beta) = v_F(\pi)$, as noted above. The lemma then follows. $\square$

Theorem 7.3. *Let p be a prime, let F, L, K be finite extensions of $\mathbf{Q}_p$, with $F \supseteq L \supseteq K$. Let k be the residue field of K. Let v_F be the valuation on F, and let e' be the ramification index of F/K. Assume that L/K is a Galois extension with cyclic Galois group of order d generated by τ, and that $d \mid p - 1$. Let $\epsilon \in \mathbf{Q}_p$ be a primitive d-th root of unity. Let $\pi \in L$ and assume that $v_F(\pi) > 0$, and that, for all $n \in \mathbf{Z}$, we have*

$$v_F\left(\tau^n(\pi) - \epsilon^n \pi\right) > v_F(\pi).$$

Suppose that $\alpha \in K$ is a p'-th root of unity in K. Let A be the crossed product (L, τ, α).

Then there exists some integer a such that $\alpha^{(|k|-1)/d} = \epsilon^a$, and, for any such a, we have that A is a central simple algebra over K and

$$\mathrm{inv}(A) = \frac{-a v_F(\pi)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Note that $d \mid |k| - 1$. Since ϵ is a primitive d-th root of unity and α is a $(|k|-1)$-th root of unity, we know that a exists. A is a central simple algebra over K.

Note that K contains a primitive $(|k| - 1)$-th root of unity, and that its $(|k| - 1)/d$-th power is a primitive d-th root of unity. Taking an appropriate power of it, it follows that there exists $\beta \in K$ a primitive $(|k| - 1)$-th root of unity such that $\beta^{(|k|-1)/d} = \epsilon^{-1}$. By Lemma 7.2, it follows that the cross product (L, τ, β) is a central simple division algebra over K and that its invariant is $\frac{v_F(\pi)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$.

Since α is a $(|k| - 1)$-th root of unity, there exists some integer b such that $\alpha = \beta^b$. It follows that $\alpha^{(|k|-1)/d} = \epsilon_r^{-b}$, so that

$$-b \equiv a \pmod{d}.$$

Furthermore, $A = (L, \tau, \beta^b)$ is a central simple algebra over K and its invariant is $\frac{bv_F(\pi)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$. Since the denominator of $\frac{v_F(\pi)}{e'}$ in lowest terms divides d, the invariant of A is also $\frac{-av_F(\pi)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$, as desired. $\square$

Recall that Definition 6.1 gives special meaning to ϵ_s when $p \nmid s$. We continue to use this notation in what follows.

Theorem 7.4. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that*

$$\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle = \mathrm{Gal}(F/K),$$

and $\mathrm{C}_{\langle \sigma_1 \rangle}(\zeta_p) = 1$, and $\sigma_2(\zeta_p) = \zeta_p$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$. We set L to be the fixed field in F of $\langle \sigma_2 \rangle$, and let $\tau \in \mathrm{Gal}(L/K)$ be the restriction of σ_1 to L. Set $d_1 = |\langle \sigma_1 \rangle|$. Suppose that $\alpha \in K$ is a p'-th root of unity in K. Let A be the crossed product (L, τ, α).

Then there exists some integer a such that $\alpha^{(|k|-1)/d_1} = \epsilon_s^a$, and, for any such a, we have that A is a central simple algebra over K of dimension d_1^2 and

$$\mathrm{inv}(A) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Let v_F be the valuation on F, and let e' be the ramification index of F/K. By Lemma 6.5, L/K is a finite Galois extension of degree d_1 with cyclic Galois group $\langle \tau \rangle = \mathrm{Gal}(L/K)$, and, there exists some $\pi \in L$ such that

$$v_F(\pi) = v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F(\tau^n(\pi) - \epsilon_s^n \pi) > v_F(\pi).$$

In addition, ϵ_s is a primitive $[L : K]$-th root of unity, and $L = K(\pi)$. It follows that by Theorem 7.3 there exists some integer a such that $\alpha^{(|k|-1)/d_1} = \epsilon_s^a$, and, for any such a, we have that A is a central simple algebra over K and

$$\mathrm{inv}(A) = \frac{-av_F(\pi)}{e'} + \mathbf{Z} = \frac{-av_F(\zeta_p - 1)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

By Lemma 6.2, $v_F(\zeta_p - 1) = \frac{ee'}{p-1}$. Hence the theorem holds. $\square$

Of particular interest is the case when $r = 1$ in the previous theorem.

Corollary 7.5. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p)$. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Suppose that $\sigma \in \mathrm{Gal}(F/K)$ is such that $\langle\sigma\rangle = \mathrm{Gal}(F/K)$. Let $s \in \mathbf{Z}$ be such that $\sigma(\zeta_p) = \zeta_p^s$. Set $d = |\langle\sigma\rangle|$. Suppose that $\alpha \in K$ is a p'-th root of unity in K. Let A be the crossed product (F, σ, α).*

Then there exists some integer a such that $\alpha^{(|k|-1)/d} = \epsilon_s^a$, and, for any such a, we have that A is a central simple algebra over K and

$$\mathrm{inv}(A) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. This follows immediately from Theorem 7.4 by setting $r = 1$, $\zeta_r = 1$, and $L = F$. $\square$

Theorem 7.6. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that*

$$\langle\sigma_1\rangle \times \langle\sigma_2\rangle = \mathrm{Gal}(F/K),$$

$\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_p) = 1$, and $\sigma_2(\zeta_p) = \zeta_p$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$, and let $m = |\,\mathrm{C}_{\langle\sigma_1\rangle}(\zeta_r)|$. Suppose that $\beta \in \mathbf{Z}$ is such that $\sigma_1^\beta\sigma_2(\zeta_r) = \zeta_r$. We set L to be the fixed field in F of $\langle\sigma_1\rangle$, and let $\tau \in \mathrm{Gal}(L/K)$ be the restriction of σ_2 to L. Set $d_2 = |\langle\sigma_2\rangle|$. Suppose that $\alpha \in K$ is a p'-th root of unity in K. Let A be the crossed product (L, τ, α).

Then there exists some integer a such that $\alpha^{(|k|-1)/d_2} = \epsilon_s^{\beta ma}$, and, for any such a, we have that A is a central simple algebra over K of dimension d_2^2 and

$$\mathrm{inv}(A) = \frac{-aem}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Let v_F be the valuation on F, and let e' be the ramification index of F/K. By Lemma 6.6, L/K is a finite Galois extension of degree d_2 with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, and, there exists some $\pi \in L$ such that

$$v_F(\pi) = m\, v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F\left(\tau^n(\pi) - \epsilon_s^{\beta mn}\pi\right) > v_F(\pi).$$

In addition, $\epsilon_s^{\beta mn}$ is a primitive d_2-th root of unity, and $L = K(\pi)$. It follows that by Theorem 7.3 there exists some integer a such that $\alpha^{(|k|-1)/d_2} = \epsilon_s^{\beta ma}$, and, for any such a, we have that A is a central simple algebra of dimension d_2^2 over K and

$$\operatorname{inv}(A) = \frac{-a\, v_F(\pi)}{e'} + \mathbf{Z} = \frac{-am\, v_F(\zeta_p - 1)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

By Lemma 6.2, $v_F(\zeta_p - 1) = \frac{ee'}{p-1}$. Hence the theorem holds. $\square$

Theorem 7.7. *Let p be a prime, let F, K be finite extensions of $\mathbf{Q}_p$, let $\zeta_p \in F$ be a primitive p-th root of 1, let r be a positive integer prime to p, let $\zeta_r \in F$ be a primitive r-th root of 1, and assume that $F \supseteq K$ and $F = K(\zeta_p, \zeta_r)$. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ are such that*

$$\langle\sigma_1\rangle \times \langle\sigma_2\rangle = \mathrm{Gal}(F/K),$$

$\sigma_1(\zeta_r) = \zeta_r$ and $\mathrm{C}_{\langle\sigma_2\rangle}(\zeta_r) = 1$. Let $s \in \mathbf{Z}$ be such that $\sigma_1(\zeta_p) = \zeta_p^s$. We set L to be the fixed field in F of $\langle\sigma_2\rangle$, and let $\tau \in \mathrm{Gal}(L/K)$ be the restriction of σ_1 to L. Set $d_1 = |\langle\sigma_1\rangle|$. Suppose that $\alpha \in K$ is a p'-th root of unity in K. Let A be the crossed product (L, τ, α).

Then there exists some integer a such that $\alpha^{(|k|-1)/d_1} = \epsilon_s^a$, and, for any such a, we have that A is a central simple algebra over K of dimension d_1^2 and

$$\operatorname{inv}(A) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Let v_F be the valuation on F, and let e' be the ramification index of F/K. By Lemma 6.7, L/K is a finite Galois extension of degree d_1 with cyclic Galois group $\langle\tau\rangle = \mathrm{Gal}(L/K)$, and, there exists some $\pi \in L$ such that

$$v_F(\pi) = v_F(\zeta_p - 1) > 0,$$

and, for all $n \in \mathbf{Z}$,

$$v_F(\tau^n(\pi) - \epsilon_s^n \pi) > v_F(\pi).$$

In addition, ϵ_s is a primitive d_1-th root of unity, and $L = K(\pi)$. It follows that by Theorem 7.3 there exists some integer a such that $\alpha^{(|k|-1)/d_1} = \epsilon_s^a$, and, for any such a, we have that A is a central simple algebra of dimension d_1^2 over K and

$$\operatorname{inv}(A) = \frac{-a\, v_F(\pi)}{e'} + \mathbf{Z} = \frac{-a\, v_F(\zeta_p - 1)}{e'} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

By Lemma 6.2, $v_F(\zeta_p - 1) = \frac{ee'}{p-1}$. Hence the theorem holds. $\square$

8. The invariants of p-basic groups

In this section, we explicitly calculate the invariants for all the relevant irreducible characters of the p-basic groups. These characters include all of the characters of p-basic groups that are needed to calculate the invariant of an arbitrary irreducible character of any finite group, and many other irreducible characters of the p-basic groups.

While it would be sufficient for our purposes here to assume that all these characters are faithful, in view of making applications easier, we relax this condition a little. We use the following convention. Let G be a group, H be a subgroup of G, and χ be a character of G. We say that χ *is faithful for* H if the restriction of χ to H is faithful.

Theorem 8.1. *Let p be a prime, let K be a finite extension of $\mathbf{Q}_p$. Let G be a p-basic group of type* 0*, and let $\chi \in \operatorname{Irr}_K(G)$. Then*

$$\operatorname{inv}\left([\chi]_K\right) = 0 + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. By definition, $p \nmid |G|$. Then, by Theorem 2.7, the Schur index $m_K(\chi) = 1$, and the invariant is as described. $\square$

Theorem 8.2. *Let p be a prime, and let K be a finite extension of $\mathbf{Q}_p$. Let G be a p-basic group of type* 1*, assume the notation of Definition 4.2, and let $\chi \in \operatorname{Irr}_K(G)$. Assume that the restriction of χ to P is faithful and K-quasi-homogeneous. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Let $1 \neq u \in P$, and let $x \in G$ be a p'-element such that xP is a generator for G/P. Let $r \in \mathbf{Z}$ be such that $u^x = u^r$, let $d = \chi(1)$, and let $\alpha = \chi\left(x^{|k|-1}\right)/d$.*

Then, there exists some $a \in \mathbf{Z}$ such that $\alpha = \epsilon_r^a$, and for any such a we have

$$\operatorname{inv}\left([\chi]_K\right) = \frac{ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. $G = P\langle x\rangle$, the normal subgroup $\mathrm{C}_G(P)$ is abelian, χ is induced from a linear character of $\mathrm{C}_G(P)$, and $d = \chi(1) = |G/\mathrm{C}_G(P)|$. Notice that $x^d \in \mathrm{Z}(G)$, and we set $\beta = \chi\left(x^d\right)/d$. Then $\beta \in K$ is a p'-th root of unity. Since d is the order of r modulo p, we know that $d \mid |k| - 1$, and $\alpha = \beta^{(|k|-1)/d}$. Let A be the simple ideal of the group algebra KG associated with χ. Then $\dim_K(A) = d^2$. For each $a \in KG$, we denote by $\overline{a}$ its projection in A. A has a central subalgebra isomorphic to K, and we denote it also by K. Similarly, if $\gamma \in K$, we may denote $\overline{\gamma}$ also by γ. We set $F = \overline{KP}$, the projection in A of the group algebra of the normal cyclic subgroup P of G. Since the restriction of χ to P is K-quasi-homogeneous, F is a finite field extension of K. F is a field extension of K by $\overline{u}$, a primitive p-th root of unity. Furthermore $\overline{x}^d = \beta$. G acts by conjugation on F as Galois automorphisms over K. Furthermore, the kernel of this action is $\mathrm{C}_G(P)$, and the image of this action is exactly $\operatorname{Gal}(F/K)$. In addition, this action provides an isomorphism $\langle x\rangle/\mathrm{C}_{\langle x\rangle}(P) \simeq \operatorname{Gal}(F/K)$.

We let $\sigma \in \mathrm{Gal}(F/K)$ be the action of x on F. (To be precise, we define $\sigma(f) = f^x$ for all $f \in F$.) We notice that

$$\mathrm{Gal}(F/K) = \langle \sigma \rangle,$$

and that $|\,\mathrm{Gal}(F/K)| = d$. Now A is the crossed product of (F, σ, β). By Corollary 7.5 and Theorem 2.7 the result follows. □

Corollary 8.3. *In the notation of Theorem 8.2, assume furthermore that K is contained in an extension of $\mathbf{Q}_p$ by a primitive p-th root of unity. Then, there exists some integer a such that $\alpha = \epsilon_r^a$, and for any such a we have*

$$\mathrm{inv}\left([\chi]_K\right) = \frac{a}{d} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. By Lemma 6.2, $F/\mathbf{Q}_p$ is a totally ramified extension of degree $p-1$. Therefore, the ramification index e of $K/\mathbf{Q}_p$ is exactly $\frac{p-1}{d}$, so the corollary follows immediately from Theorem 8.2. □

Lemma 8.4. *Let p be an odd prime, and let G be a p-basic group of type 2, assume the notation of Definition 4.5, and $C = \mathrm{C}_Q(PR)$. Let $m = |\,\mathrm{C}_X(R)/X \cap C|$, $x \in X$ be a generator for X, and let $1 \neq u \in P$. Then there exist $s \in \mathbf{Z}$ such that $u^x = u^s$, there exists $y \in \mathrm{C}_Q(P)$ such that yC is a generator for the cyclic group $\mathrm{C}_Q(P)/C$, and there exists $\beta \in \mathbf{Z}$ such that $x^\beta y \in \mathrm{C}_Q(R)$.*

Proof. The group $\mathrm{C}_Q(P)/C$ is cyclic because it is isomorphic to a subgroup of the automorphism group of R, and we pick some $y \in \mathrm{C}_Q(P)$ such that yC is a generator for $\mathrm{C}_Q(P)/C$. Since $G = X\,\mathrm{C}_G(R)$, there exists $\beta \in \mathbf{Z}$ such that $x^\beta y \in \mathrm{C}_Q(R)$. □

Recall the meaning of *faithful for* described in the second paragraph of this section.

Theorem 8.5. *Let p be an odd prime, and let K be a finite extension of $\mathbf{Q}_p$. Let G be a p-basic group of type 2, assume the notation of Lemma 8.4. Let $\chi \in \mathrm{Irr}_K(G)$ be faithful for PR. Assume that the restriction of χ to PRC is K-quasi-homogeneous. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Let e_χ be the central idempotent associated with χ. We set*

$$\alpha_1 = \chi\left(x^{|k|-1}\right)/\chi(1).$$

Then, $e_\chi KR$ is a field, there exists some p'-root of unity $\gamma \in e_\chi KR$ such that $y\gamma$ commutes with x, and we set

$$\alpha_2 = \chi\left((y\gamma)^{|k|-1}\right)/\chi(1).$$

Furthermore, there exists some integer a_1 such that $\alpha_1 = \epsilon_s^{a_1}$, there exists some integer a_2 such that $\alpha_2 = \epsilon_s^{\beta m a_2}$, and for any such a_1 and a_2 we have

$$\mathrm{inv}\left([\chi]_K\right) = \frac{(a_1 + ma_2)e}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. Notice that χ is induced from a linear character of PRC, and that $\chi(1) = |Q/C|$. Let $A = e_\chi KG$ be the simple ideal of the group algebra KG associated with χ. Then $\dim_K(A) = \chi(1)^2$. For each $a \in KG$, we denote $\overline{a}$ its projection $e_\chi a$ in A. A has a central subalgebra $e_\chi K$ isomorphic to K, and we denote it also by K. Similarly, if $\gamma \in K$, we may denote $\overline{\gamma}$ also by γ. We set $F = \overline{KPRC}$, the projection in A of the group algebra of the normal cyclic subgroup PRC of G. Since the restriction of χ to PRC is K-quasi-homogeneous, F is a finite field extension of K. G acts by conjugation on F as Galois automorphisms over K. Furthermore, the kernel of this action is PRC, and the image of this action is exactly $\mathrm{Gal}(F/K)$. In addition, this action provides an isomorphism $Q/C \simeq \mathrm{Gal}(F/K)$.

We let $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ be the action respectively of x and of y on F. (To be precise, we define $\sigma_1(f) = f^x$ for all $f \in F$, and similarly for σ_2.) We notice that

$$\mathrm{Gal}(F/K) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle.$$

We set $d_i = |\langle\sigma_i\rangle|$ for $i \in \{1, 2\}$. We have $\chi(1) = |Q/C| = d_1 d_2$. Let $z = [y, x]$. Since Q/C is abelian, $z \in C$ and $\overline{z}$ is a p'-th root of unity in F. For $i \in \{1, 2\}$, we let L_i be the fixed field of $\langle\sigma_{3-i}\rangle$ in F, and we let $\tau_i \in \mathrm{Gal}(L_i/K)$ be the restriction to L_i of σ_i.

Set $U = e_\chi KR$. Therefore $U = \overline{KR} \subseteq F$. Then U is the extension field of K by $\overline{R}$, so that U is an unramified extension of K contained in F. It follows that U is K extended by a primitive r-th root of unity. We let $\sigma_3, \sigma_4 \in \mathrm{Gal}(U/K)$ be the restrictions of respectively σ_1 and σ_2 to U. From the definition of p-basic group of type 2, it follows that $\langle\sigma_3\rangle = \mathrm{Gal}(U/K)$, and, in particular $\sigma_4 \in \langle\sigma_3\rangle$. Again from the definition of p-basic group of type 2, it follows that $\overline{C} \subseteq U$. Furthermore σ_4 has order d_2.

Let L be the fixed field in U of $\langle\sigma_4\rangle$. The extension U/L is unramified. Now $\overline{y}^{d_2}$ is a p'-th root of unity in L. It follows that $\overline{y}^{d_2}$ is the norm under $\langle\sigma_4\rangle$ of some p'-th root of unity in U. Therefore, there exists some $z_1 \in U$, a p'-th root of unity, such that, setting $y_1 = \overline{y} z_1 \in A^\times$, we have that $y_1^{d_2} = 1$. Notice that, for all $f \in F$, we have $f^{y_1} = \sigma_2(f)$. Now $y_1^x = y_1 z_2$ where $z_2 \in U$ is a p'-th root of unity. Since $y_1^{d_2} = 1$, it follows that the norm under $\langle\sigma_4\rangle$ of z_2 is also 1. This implies that the norm under $\langle\sigma_3\rangle$ of z_2 is also 1. It then follows that there exists a p'-th root of unity $z_3 \in U$ such that $(y_1 z_3)^x = y_1 z_3$. It follows that $z_1 z_3$ is a p'-th root of unity in U such that x centralizes $y z_1 z_3$. Hence a γ as described in the theorem exists. We set γ to be any one of them.

We set $\delta_1 = \overline{x}^{d_1}$. Now $\delta_1 \in \overline{C} \subseteq U$. Since δ_1 is fixed by σ_1, it follows that $\delta_1 \in K$. Note that $\alpha_1 = \delta_1^{(|k|-1)/d_1}$. We let B be the subalgebra of A generated by L_1 and $\overline{x}$. Then B is isomorphic to the cross product (L_1, τ_1, δ_1). By Theorem 7.4, B is a central simple algebra over K, with $\dim_K(B) = d_1^2$, there exists some $a_1 \in \mathbf{Z}$ such that $\delta_1^{(|k|-1)/d_1} = \epsilon_s^{a_1}$, and, for any such a_1,

$$\operatorname{inv}(B) = \frac{-a_1 e}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

We set $\delta_2 = (y\gamma)^{d_2}$. Now $\delta_2 \in F$ is fixed both by x and by σ_2, so that δ_2 is a p'-th root of unity in K. Note that $\alpha_2 = \delta_2^{(|k|-1)/d_2}$. Let D be the subalgebra of A generated by L_2 and $y\gamma$. Now, D is isomorphic to the crossed product (L_2, τ_2, δ_2). By Theorem 7.6, D is a central simple algebra over K, with $\dim_K(D) = d_2^2$, there exists some $a_2 \in \mathbf{Z}$ such that $\delta_2^{(|k|-1)/d_2} = \epsilon_s^{\beta m a_2}$, and, for any such a,

$$\operatorname{inv}(D) = \frac{-a_2 e m}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Since B and D centralize each other, it follows that

$$\operatorname{inv}(A) = \frac{-a_1 e}{p-1} + \frac{-a_2 e m}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Theorem 2.7 then completes the proof of the theorem. □

Lemma 8.6. *Let p be a prime, and let K be a finite extension of $\mathbf{Q}_p$. Let G be a finite group, and let R be a normal subgroup of G, with $|R| = r$ where r is a prime $r \neq p$. Assume Y is a subgroup of G such that $G = Y\,\mathrm{C}_G(R)$. Let $\chi \in \operatorname{Irr}_K(G)$, and assume that the restriction of χ to R is faithful and K-quasi-homogeneous. Let k be the residue field of K. Let $1 \neq v \in R$. Then there exists some $y \in Y$ such that $v^y = v^{|k|}$. Furthermore, for any such y, $y\,\mathrm{C}_G(R)$ is a generator for $G/\mathrm{C}_G(R)$.*

Proof. Let $e = e_\chi$ be the central idempotent associated with χ. Since the restriction of χ is faithful and K-quasi-homogeneous, it follows that eKR is a field extension of eK by a primitive r-th root of unity. Therefore eKR is an unramified extension of eK. The Galois group $\mathrm{Gal}(eKR/eK)$ is cyclic and generated by its unique element σ such that, for all p'-th roots of unity ρ in eKR, we have $\sigma(\rho) = \rho^{|k|}$. Now G acts by conjugation on eKR by Galois automorphisms over eK. So we get a natural homomorphism from G to $\mathrm{Gal}(eKR/eK)$. Since the values of χ are all in K, we know that this homomorphism is surjective. Its kernel is $\mathrm{C}_G(R)$. Since $G = Y\,\mathrm{C}_G(R)$, it follows that the lemma holds. □

Theorem 8.7. *Let p be an odd prime, and let K be a finite extension of $\mathbf{Q}_p$. Let G be a p-basic group of type 3, assume the notation of Definition 4.6. Let $\chi \in \operatorname{Irr}_K(G)$ be faithful for PR. Assume that the restriction of χ to PRC is K-quasi-homogeneous. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Let $1 \neq u \in P$, let $1 \neq v \in R$, let $y \in Y$ be such that $v^y = v^{|k|}$, let $x \in \mathrm{C}_Q(R)$ be such that $\langle x, y, C\rangle = Q$, let $s \in \mathbf{Z}$ be such that $u^x = u^s$, and let $z = [x, y]$. We set*

$$\alpha = \chi\left(x^{|k|-1}z^{-1}\right)/\chi(1).$$

Then, there exists some integer a such that $\alpha = \epsilon_s^a$, and for any such a we have

$$\operatorname{inv}\left([\chi]_K\right) = \frac{ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. For completeness, we first check that the notation can indeed be set up as described in the theorem. It follows from Lemma 8.6 and our hypotheses that y can be chosen as described, and that $y\,\mathrm{C}_Q(R)$ is a generator of $Q/\,\mathrm{C}_Q(R)$. Now $\mathrm{C}_Q(R)/C$ acts faithfully on P so that it is a cyclic group, and so the x can be chosen as described. The existence of s, z, and α requires no comment.

Notice that χ is induced from a linear character of PRC, and that $\chi(1) = |Q/C|$. Let A be the simple ideal of the group algebra KG associated with χ. Then $\dim_K(A) = \chi(1)^2$. For each $a \in KG$, we denote $\overline{a}$ its projection in A. A has a central subalgebra isomorphic to K, and we denote it also by K. For $\gamma \in K$, we may also denote $\overline{\gamma}$ by γ. We set $F = \overline{KPRC}$, the projection in A of the group algebra of the normal cyclic subgroup PRC of G. Since the restriction of χ to PRC is K-quasi-homogeneous, F is a finite field extension of K. G acts by conjugation on F as Galois automorphisms over K. Furthermore, the kernel of this action is PRC, and the image of this action is exactly $\mathrm{Gal}(F/K)$. In addition, this action provides an isomorphism $Q/C \simeq \mathrm{Gal}(F/K)$.

We let $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ be the action respectively of x and of y on F. (To be precise, we define $\sigma_1(f) = f^x$ for all $f \in F$, and similarly for σ_2.) We notice that

$$\mathrm{Gal}(F/K) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle.$$

We set $d_i = |\langle\sigma_i\rangle|$ for $i \in \{1, 2\}$. We have $\chi(1) = |Q/C| = d_1 d_2$. Since Q/C is abelian, $z \in C$ and $\overline{z}$ is a p'-th root of unity in F.

Let U be the extension of K by $\overline{R}$, so that U is an unramified extension of K contained in F. Then U is K extended by a primitive r-th root of unity. We let $\sigma_3, \sigma_4 \in \mathrm{Gal}(U/K)$ be the restrictions of respectively σ_1 and σ_2 to U. Since $x \in \mathrm{C}_Q(R)$, σ_3 is the identity. It follows that $\langle\sigma_4\rangle = \mathrm{Gal}(U/K)$. From the definition of p-basic group of type 3, we know that σ_4 has order d_2. From the definition of p-basic group of type 3, we also know that $\overline{C} \subseteq U$. In particular, $\overline{y}^{d_2} \in \overline{C}$ is a p'-th root of unity in K.

Now $\overline{y}^{d_2} = (\overline{y}^x)^{d_2}$, and since $y^x = yz^{-1}$, this implies that the $\langle\sigma_4\rangle$-norm of $\overline{z}^{-1}$ is 1. Hence, there exists $z_1 \in U$ such that z_1 is a p'-th root of unity and $\overline{z}^{-1} = z_1^{-1} z_1^y = z_1^{|k|-1}$. We set $x_1 = \overline{x} z_1$. Then $x_1^y = \overline{xz} z_1^y = \overline{x} z_1 = x_1$. We notice that x_1 centralizes U and $\overline{y}$.

We let D be the subalgebra of A generated by U and $\overline{y}$. D is isomorphic to the crossed product $\left(U, \sigma_4, \overline{y}^{d_2}\right)$, and $\dim_K(D) = d_2^2$. By Theorem 7.1, since U/K is unramified and $\overline{y}^{d_2}$ is a p'-th root of unity, D is isomorphic to a full matrix algebra over K.

Let L be the fixed field in F of $\langle\sigma_2\rangle$. Let B be the subalgebra of A generated by L and x_1. Let τ be the restriction of σ_1 to L. Then, for all $l \in L$, we have $\tau(l) = l^{x_1}$, and $|\langle\tau\rangle| = d_1$. Since $\overline{y}$ centralizes x_1, $x_1^{d_1} \in K$, and $x_1^{d_1}$ is a p'-th root of unity. We set $\delta = x_1^{d_1}$. B is isomorphic to the crossed product (L, τ, δ), and $\dim_K(B) = d_1^2$. By Theorem 7.7, there exists some integer a such that $\delta^{(|k|-1)/d_1} = \epsilon_s^a$, and, for any such a, we have that B is a central simple algebra over K of dimension d_1^2 and

$$\mathrm{inv}(B) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Notice that

$$\delta^{(|k|-1)/d_1} = x_1^{|k|-1} = \chi\left(x^{|k|-1}z^{-1}\right)/\chi(1) = \alpha.$$

Since B and D centralize each other, it follows that

$$\mathrm{inv}(A) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Theorem 2.7 then completes the proof of the theorem. □

Theorem 8.8. *Let p be a prime with $p \equiv 3 \pmod 4$, and let K be a finite extension of $\mathbf{Q}_p$. Let G be a p-basic group of type 4, assume the notation of Definition 4.7. Let $\chi \in \mathrm{Irr}_K(G)$ be faithful for PM. Assume that the restriction of χ to PM is K-quasi-homogeneous. Let e be the ramification index of $K/\mathbf{Q}_p$, and let k be the residue field of K. Let $Q \in \mathrm{Syl}_2(G)$, let $x \in \mathrm{C}_Q(M)$ with $x \notin M$, and let $y \in D$ with $y \notin M$, and let $z = [x, y]$. We set*

$$\alpha = \chi\left(x^{|k|-1}z^{-1}\right)/\chi(1).$$

Then, if e is odd and $\alpha = -1$, then

$$\mathrm{inv}\left([\chi]_K\right) = \frac{1}{2} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z},$$

and otherwise

$$\mathrm{inv}\left([\chi]_K\right) = 0 + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Proof. For completeness, we first check that the notation can indeed be set up as described in the theorem. Note first that $D \trianglelefteq G$, $D \subseteq Q$, and PM is a cyclic normal subgroup of G. Since $p \equiv 3 \pmod 4$, $[G : \mathrm{C}_G(P)] = 2$, so that $[Q : D] = 2$, $G = PQ$, $\mathrm{C}_Q(M) \in \mathrm{Syl}_2(\mathrm{C}_G(M))$, and $[\mathrm{C}_Q(M) : M] = 2$. Since we also know that $[D : M] = 2$, it follows x and y can be chosen as described. The existence of z, and α requires no comment. We also note that x inverts by conjugation every element of P, and that $Q = \langle x, y\rangle M$.

Notice that χ is induced from a linear character of PM, and that $\chi(1) = 4$. Let A be the simple ideal of the group algebra KG associated with χ. Then $\dim_K(A) = 16$. For each $a \in KG$, we denote $\overline{a}$ its projection in A. A has a central subalgebra isomorphic to K, and we denote it also by K. We set $F = \overline{KPM}$, the projection in A of the group algebra of the normal cyclic subgroup PM of G. Since the restriction of χ to PM is K-quasi-homogeneous, F is a finite field extension of K. G acts by conjugation on F as Galois automorphisms over K. Furthermore, the kernel of this action is PM, and the image of this action is exactly $\mathrm{Gal}(F/K)$. In addition, this action provides an isomorphism $Q/M \simeq \mathrm{Gal}(F/K)$.

We let $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ be the action respectively of x and of y on F. We notice that

$$\mathrm{Gal}(F/K) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle.$$

We have $2 = |\langle\sigma_i\rangle|$ for $i \in \{1, 2\}$. Since Q/M is abelian, $z \in M$ and $\overline{z}$ is a p'-th root of unity in F.

Let U be the extension of K by $\overline{M}$, so that U is an unramified extension of K contained in F. Then U is K extended by a primitive 2^α-th root of unity, where $2 \leq \alpha \leq n$. We let $\sigma_3, \sigma_4 \in \mathrm{Gal}(U/K)$ be the restrictions of respectively σ_1 and σ_2 to U. Since $x \in \mathrm{C}_Q(M)$, σ_3 is the identity. It follows that $\langle\sigma_4\rangle = \mathrm{Gal}(U/K)$. From the definition of p-basic group of type 4, we know that σ_4 has order 2. It follows that $|k|$ is not a square, and that, for every p'-th root of unity $\rho \in U$, we have $\sigma_4(\rho) = \rho^{|k|}$. Now, $\overline{y}^2 \in \overline{M}$ is a p'-th root of unity in K.

Now $\overline{y}^2 = (\overline{y}^x)^2$, and since $y^x = yz^{-1}$, this implies that the $\langle\sigma_4\rangle$-norm of $\overline{z}^{-1}$ is 1. Hence, there exists $z_1 \in U$ such that z_1 is a p'-th root of unity and $\overline{z}^{-1} = z_1^{-1} z_1^y = z_1^{|k|-1}$. We set $x_1 = \overline{x} z_1$. Then $x_1^y = \overline{xz} z_1^y = \overline{x} z_1 = x_1$. We notice that x_1 centralizes U and $\overline{y}$.

We let D be the subalgebra of A generated by U and $\overline{y}$. D is isomorphic to the crossed product $\left(U, \sigma_4, \overline{y}^2\right)$, and $\dim_K(D) = 4$. By Theorem 7.1, since U/K is unramified and $\overline{y}^2$ is a p'-th root of unity, D is isomorphic to a full matrix algebra over K.

Let L be the fixed field in F of $\langle\sigma_2\rangle$. Let B be the subalgebra of A generated by L and x_1. Let τ be the restriction of σ_1 to L. Then, for all $l \in L$, we have $\tau(l) = l^{x_1}$, and $|\langle\tau\rangle| = 2$. Since $\overline{y}$ centralizes x_1, $x_1^2 \in K$, and it is a p'-th root of unity. We set $\delta = x_1^2$. B is isomorphic to the crossed product (L, τ, δ), and $\dim_K(B) = 4$. By Theorem 7.7, there exists some integer a such that $\delta^{(|k|-1)/2} = (-1)^a$, and, for any such a, we have that B is a central simple algebra over K of dimension 4 and

$$\mathrm{inv}(B) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Notice that

$$\delta^{(|k|-1)/2} = x_1^{|k|-1} = \chi\left(x^{|k|-1} z^{-1}\right) / \chi(1) = \alpha.$$

Since B and D centralize each other, it follows that

$$\mathrm{inv}(A) = \frac{-ae}{p-1} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

By Lemma 6.2, we know that $p-1$ divides the ramification index of $F/\mathbf{Q}_p$. Since $\mathrm{Gal}(F/K)$ is a 2-group, it follows that $(p-1)/2$ divides e. Hence $\mathrm{inv}(A) = \mathbf{Z}$ if e is even or $\alpha \neq -1$, and $\mathrm{inv}(A) = \frac{1}{2} + \mathbf{Z}$ otherwise. Theorem 2.7 then completes the proof of the theorem. □

9. Calculating the local invariant for an arbitrary character

In this section, we describe how one can find the local invariant for an arbitrary irreducible character of a finite group. We let K be a finite extension of either $\mathbf{R}$ or $\mathbf{Q}_p$ for some prime p. We let G be an arbitrary finite group, and let $\chi \in \mathrm{Irr}_K(G)$.

Suppose first that K is a finite extension of $\mathbf{R}$, the field of real numbers. It is well know that the local Schur index $m_K(\chi) \in \{1, 2\}$, and there exists a formula to calculate it. Then we know from Theorem 2.7 that

$$\mathrm{inv}\left([\chi]_K\right) = \frac{1}{m_K(\chi)} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

Suppose next that K is a finite extension of $\mathbf{Q}_2$, the field of dyadic numbers. Then we know from Theorem 2.7 that the local Schur index $m_K(\chi) \in \{1, 2\}$ (Yamada's Theorem), and that

$$\mathrm{inv}\left([\chi]_K\right) = \frac{1}{m_K(\chi)} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}.$$

We also note that there exist methods to calculate the Schur index $m_K(\chi)$.

Finally, suppose that K is a finite extension of $\mathbf{Q}_p$, the field of p-adic numbers, where p is any odd prime. By Yamada's Theorem (Theorem 2.7) we know that the order of $\mathrm{inv}\left([\chi]_K\right)$, which is the local Schur index $m_K(\chi)$, divides $p-1$. Hence to calculate $\mathrm{inv}\left([\chi]_K\right)$ it is enough to calculate the q-part $\mathrm{inv}\left([\chi]_K\right)_q$ of $\mathrm{inv}\left([\chi]_K\right)$ for all primes $q \mid p-1$.

Let us then fix some prime $q \mid p-1$. By Corollary 5.5, there exists an algorithm that produces a field F, a section H of G, some $\psi \in \mathrm{Irr}_F(H)$, and some integer a satisfying all the conditions of the corollary, and, in particular, such that F is a finite extension of K, H is p-basic and the q-part of $\mathrm{inv}\left([\chi]_K\right)$ is

$$\mathrm{inv}\left([\chi]_K\right)_q = a\,\mathrm{inv}\left([\psi]_F\right).$$

The conditions given in the corollary also imply that $\mathrm{inv}\left([\psi]_F\right)$ is given by a formula in Section 8.

Hence, this method calculates the local invariant for an arbitrary character of a finite group.

References

[1] G.K. Bakshi, O.B. Cristo, A. Herman, A. Konovalov, S. Maheshwary, A. Olivieri, G. Olteanu, Á. del Río, I. Van Gelder, Wedderga – Wedderburn decomposition of group algebras, version 4.9.5. 2018, https://gap-packages.github.io/wedderga/.
[2] W. Feit, The Representation Theory of Finite Groups, North-Holland, Amsterdam-New York-Oxford, 1982.
[3] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.
[4] I.M. Isaacs, Character Theory of Finite Groups, Dover, New York, 1994.
[5] Richard S. Pierce, Associative Algebras, Springer-Verlag, New York, Heidelberg, Berlin, 1982.
[6] Udo Riese, Peter Schmid, Schur indices and Schur groups, II, J. Algebra 182 (1996) 183–200.
[7] Peter Schmid, Representation groups for the Schur index, J. Algebra 97 (1985) 101–115.
[8] Peter Schmid, Schur indices and Schur groups, J. Algebra 169 (1994) 226–247.
[9] J.-P. Serre, Local Fields, Springer-Verlag, New York, Heidelberg, Berlin, 1979.
[10] A. Turull, Strengthening the McKay Conjecture to include local fields and local Schur indices, J. Algebra 319 (2008) 4853–4868.
[11] A. Turull, The strengthened Alperin-McKay conjecture for p-solvable groups, J. Algebra 394 (2013) 79–91.
[12] A. Turull, Refinements of Dade's Projective Conjecture for p-solvable groups, J. Algebra 474 (2017) 424–465.
[13] A. Turull, Characters, Brauer characters, and local Brauer groups, submitted for publication.
[14] W.R. Unger, An algorithm for computing Schur indices of characters, J. Symb. Comput. 93 (2019) 148–160.
[15] T. Yamada, The Schur Subgroup of the Brauer Group, Lecture Notes in Mathematics, vol. 397, Springer-Verlag, Berlin-New York, 1974.