Galois Algebras, Hasse Principle and Induction–Restriction Methods

E. Bayer-Fluckiger and R. Parimala

Received: May 9, 2011
Revised: August 29, 2011

Communicated by Ulf Rehmann

Let k be a field of characteristic $\neq 2$, and let L be a Galois extension of k with group G. Let us denote by $q_L : L \times L \to k$ the *trace form*, defined by $q_L(x,y) = \mathrm{Tr}_{L/k}(xy)$. Let $(gx)_{g \in G}$ be a normal basis of L over k. We say that this is a *self–dual normal basis* if $q_L(gx, hx) = \delta_{g,h}$. If the order of G is odd, then L always has a self–dual normal basis over k (cf. [1]). This is no longer true in general if the order of G is even; some partial results are given in [2].

If k is a global field, then it is natural to ask whether a local–global principle holds for this problem. In order to make this question precise, we have to consider G–Galois algebras and not only field extensions. Moreover, it is useful to note that q_L is a G*–quadratic form*, in other words $q_L(gx, gy) = q_L(x,y)$ for all $x, y \in L$ and $g \in G$. The G–Galois algebra has a self–dual normal basis if and only if the G–form q_L is isomorphic to the unit G–form. This leads to the following question:

Question. Suppose that k is a global field, and let L and L' be two G–Galois algebras. Assume that for all places v of k, the G–forms q_{L_v} and $q_{L'_v}$ are isomorphic over k_v. Are the G–forms q_L and $q_{L'}$ isomorphic over k ?

Note that a similar Hasse principle does not hold for arbitrary G–forms, cf. Morales [5]. In the context of trace forms of G–Galois algebras, positive results are obtained in [2] in some special cases. However, the problem is open in general.

The starting point of this paper is to investigate this question. The main tool, which is of independent interest, is to develop induction–restriction methods for arbitrary G–forms, generalizing some results of [2] and of Lequeu in [4]. The key ingredient is an *odd determinant property* of the group G (cf. §2) which is shown to hold for instance if the normalizer of a 2–Sylow subgroup S controls the fusion of S in G. We obtain the following :

Theorem. *Suppose that k is a global field of characteristic $\neq 2$. Let G be a finite group, and suppose that G has the odd determinant property if* $\mathrm{char}(k) = 0$*. Let L and L' be two G–Galois algebras such that for all places v of k, the G–forms q_{L_v} and $q_{L'_v}$ are isomorphic over k_v. Then the G–forms q_L and $q_{L'}$ are isomorphic over k.*

Corollary. *Suppose that k and G are as above. Then a G–Galois algebra has a self–dual normal basis over k if and only if such a basis exists over all the completions of k.*

We thank Jean–Pierre Serre for many fruitful conversations and correspondence. We also thank Emmanuel Lequeu for very interesting conversations, and for showing us a preliminary version of his paper [4]. The authors acknowledge hospitality of Emory University and the École Polytechnique Fédérale de Lausanne, institutions in which the work was carried out. The first named author was partially supported by the Swiss National Science Fundation, grant 200020-109174/1, and the second named author was partially supported by NSF grant DMS 1001872.

§1. Definitions and basic facts

Let k be a field of characteristic $\neq 2$, let G be a finite group, and let $k[G]$ be the associated group ring. We refer to [7] for basic facts on $k[G]$–modules.

Group ring and involution

Let $\iota : k[G] \to k[G]$ be the canonical involution of the group ring, in other words the k–linear involution of $k[G]$ characterized by $\iota(g) = g^{-1}$ for all $g \in G$. Let R be the radical of $k[G]$. Then $k[G]/R$ is a semi–simple k–algebra, hence we have a decomposition $k[G]/R = \prod_{i=1,\dots,r} M_{n_i}(D_i)$, where $D_1, \dots, D_r$ are division algebras. Let us denote by K_i the center of D_i, and let D_i^{op} be the opposite algebra of D_i.

Note that $\iota(R) = R$, hence ι induces an involution $\iota : k[G]/R \to k[G]/R$. Therefore $k[G]/R$ decomposes into a product of involution invariant factors. These can be of two types: either an involution invariant matrix algebra $M_{n_i}(D_i)$, or a product $M_{n_i}(D_i) \times M_{n_i}(D_i^{op})$, with $M_{n_i}(D_i)$ and $M_{n_i}(D_i^{op})$ exchanged by the involution. We say that a factor is *unitary* if the restriction of the involution to its center is not the identity: in other words, either an involution invariant $M_{n_i}(D_i)$ with $\iota|K_i$ not the identity, or a product $M_{n_i}(D_i) \times M_{n_i}(D_i^{op})$. Otherwise, the factor is said to be of the first kind. In this case, the component is of the form $M_{n_i}(D_i)$ and the restriction of ι to K_i is the identity. We say that the component is *orthogonal* if after base change to a separable closure ι is given by the transposition, and *symplectic* otherwise.

We say that a component $M_{n_i}(D_i)$ is *split* if D_i is a commutative field.

G–quadratic forms

A *G–quadratic form* is a pair (V, q), where V is a $k[G]$–module that is a finite dimensional k–vector space, and $q : V \times V \to k$ is a non–degenerate symmetric bilinear form such that

$$q(gx, gy) = q(x, y)$$

for all $x, y \in V$ and all $g \in G$. We say that two G–quadratic forms (V, q) and (V', q') are *isomorphic* if there exists an isomorphism of $k[G]$–modules $f : V \to V'$ such that $q'(f(x), f(y)) = q(x, y)$ for all $x, y \in V$. If this is the case, we write $(V, q) \simeq_G (V', q')$, or $q \simeq_G q'$.

Let S be a subgroup of G. We have two operations, induction and restriction (see for instance [2], 1.2 for details):

If (V, q) is an S–quadratic form, then $\mathrm{Ind}_S^G(V, q)$ is a G–quadratic form;

If (V, q) is a G–quadratic form, then $\mathrm{Res}_S^G(V, q)$ is an S–quadratic form.

The following result will be used in the sequel

Theorem 1.1. (see [1], th. 4.1) *Let q and q' be two G–quadratic forms. If they become isomorphic over an odd degree extension, then they are isomorphic.*

It is well–known that S–quadratic forms correspond bijectively to $k[S]$–hermitian forms with respect to the involution $\iota : k[S] \to k[S]$. We will use the same notation for the S–quadratic form and the corresponding hermitian form.

Trace forms

Let L be a G–Galois algebra, and let

$$q_L : L \times L \to k, \quad q_L(x, y) = \mathrm{Tr}_{L/k}(xy)$$

be its trace form. Then q_L is a G–quadratic form.

Let us recall a result from [2] that will be basic for the proof of the main theorem:

Lemma 1.2. (cf. [2], 2.1.1.): *Let S be a 2–Sylow subgroup of G. For any G–Galois algebra L, there exists an odd degree field extension k'/k and an S–Galois algebra M over k' such that the G–form $(L, q_L) \otimes_k k'$ is isomorphic to the G–form $\mathrm{Ind}_S^G(q_M)$.*

§2. The induction-restriction functor and the odd determinant property

The aim of this section is to introduce the odd determinant property, and to state a result (th. 2.2), which will be used in the proof of the Hasse principle result of §3.

Let G be a finite group, let S be a 2–Sylow subgroup of G, and let $N = N_G(S)$ be the normalizer of S in G. Then N acts on S, and we denote by Σ the set of orbits of S under the action of N.

Let X be the Z–module of Z–valued functions on S invariant under conjugation by N, and let $\Phi : X \to X$ be $\mathrm{Res}^G_S \, \mathrm{Ind}^G_S$ considered as an endomorphism of X (cf. [7], 7.2).

Definition 2.1 We say that G has the *odd determinant property* if the determinant of $\Phi : X \to X$ is an odd integer.

One of the main results of this paper is the following

Theorem 2.2 *Suppose that G has the odd determinant property. Let (V_1, q_1) and (V_2, q_2) be two S–quadratic spaces. Suppose that*

$$\mathrm{Res}^G_S \, \mathrm{Ind}^G_S(V_1, q_1) \simeq_S \mathrm{Res}^G_S \, \mathrm{Ind}^G_S(V_2, q_2).$$

Then

$$\mathrm{Ind}^G_S(V_1, q_1) \simeq_G \mathrm{Ind}^G_S(V_2, q_2).$$

This result is used in the proof of the Hasse principle stated in the introduction, see th. 3.1. The proof relies on an analysis of the odd determinant property, and is the subject matter of sections 4-11. The structure of the proof of th. 2.2 is as follows. Sections 5 and 6 study induction and restriction properties of S–quadratic forms. Section 7 is concerned with the odd determinant property in the special case where all the characters of S over k are absolutely irreducible. Using a filtration introduced in §9 and the quadratic descent argument of §8, we obtain a general result (see th. 10.1) based on the case considered in §7. This is then used in §11 to prove th. 2.2.

We next show that the odd determinant property holds if N controls the fusion of S in G.

Definition 2.3 We say that N *controls the fusion of S in G* if for all subsets T and T' of S, if there exists $g \in G$ with $gTg^{-1} = T'$ then there exists $n \in N$ such that $nTn^{-1} = T'$.

There are many examples of groups G in which the normalizer controls the fusion of the 2–Sylow subroups; see for instance Thévenaz [8] for a survey.

REMARK. Note that we only use the following property, which is clearly satisfied if N controls the fusion of S in G :

(*) For all $s, t \in S$, if there exists $g \in G$ with $gsg^{-1} = t$ then there exists $n \in N$ such that $nsn^{-1} = t$.

It does not seem to be known whether there exist groups G having property (*) where N does not control the fusion of S in G.

PROPOSITION 2.4 *Suppose that N controls the fusion of S in G. Then G has the odd determinant property.*

In order to prove this proposition, we need the following lemma:

LEMMA 2.5 *Suppose that N controls the fusion of S in G, and let $x \in S$. Then $C_S(x)$ is a 2–Sylow subgroup of $C_G(x)$.*

PROOF. Let S_0 be a 2–Sylow subgroup of $C_G(x)$ containing x and let S_1 be a 2–Sylow subgroup of G containing S_0. Let $g \in G$ be such that $gS_1g^{-1} = S$. In view of the fusion hypothesis, there exists $n \in N$ such that $ngxg^{-1}n^{-1} = x$. Let us consider $\mathrm{Int}(ng) : G \to G$. Then, as $\mathrm{Int}(ng)(x) = x$, we have $\mathrm{Int}(ng)(C_G(x)) = C_G(x)$. We have $\mathrm{Int}(ng)(S_1) = S$, hence $\mathrm{Int}(ng)(S_0) = \mathrm{Int}(ng)(S_1 \cap C_G(x)) = S \cap C_G(x) = C_S(x)$. This implies that $C_S(x)$ is a 2–Sylow subgroup of $C_G(x)$, as claimed.

PROOF OF PROP. 2.4 For $\sigma \in \Sigma$, let q_σ be the function on S which is equal to 1 on σ and 0 otherwise. Note that the set $(q_\sigma)_{\sigma \in \Sigma}$ is a basis of the Z–module X. Let $\sigma, \sigma' \in \Sigma$, and fix $x \in \sigma'$. By definition, the coefficient of q_σ in $\Phi(q_{\sigma'})$ is equal to

$$\frac{1}{\#S} \#\{g \in G \mid gxg^{-1} \in \sigma \}.$$

As N controls the fusion of S in G, we have $gxg^{-1} \in \sigma$ if and only if $x \in \sigma$. Therefore the coefficient of q_σ in $\Phi(q_{\sigma'})$ is equal to 0 if $\sigma \neq \sigma'$.

The coefficient of q_σ in $\Phi(q_\sigma)$ is equal to

$$\frac{1}{\#S}\ \#C_G(x)\ \#\sigma = \frac{1}{\#S}\ \#C_G(x)\ \frac{\#N}{\#C_N(x)} = \frac{\#N}{\#S}\ \frac{\#C_G(x)}{\#C_S(x)}\ \frac{\#C_S(x)}{\#C_N(x)}.$$

Therefore it suffices to check that $\frac{\#C_G(x)}{\#C_S(x)}$ is odd, and this follows from lemma 2.5.

§3. Hasse principle

In this section, we suppose that k is a global field of characteristic $\neq 2$. Let G be a finite group, and let us denote by $k[G]$ the associated group ring. One of the main results of this paper is the following

Theorem 3.1 *Suppose that G has the odd determinant property if* $\mathrm{char}(k) = 0$, *and let L and L' be two G–Galois algebras. Then $q_L \simeq_G q_{L'}$ over k if and only if $q_L \simeq_G q_{L'}$ over all the completions of k.*

As an immediate consequence, we get

Corollary 3.2 *Suppose that G has the odd determinant property if* $\mathrm{char}(k) = 0$. *Then a G–Galois algebra has a self–dual normal basis over k if and only if it has a self–dual normal basis over every completion of k.*

By prop. 2.3, we know that G has the odd determinant property whenever for a 2–Sylow subgroup S, the normalizer $N_G(S)$ controls the fusion of S in G. Hence we have

Corollary 3.3 *Suppose that for a 2–Sylow subgroup S of G, the normalizer $N_G(S)$ controls the fusion of S in G. Then the trace forms of two G–Galois algebras are G–isomorphic over k if and only if they are G–isomorphic over each completion of k. In particular, a G–Galois algebra has a self–dual normal basis over k if and only if it has a self–dual normal basis over every completion of k.*

Corollary 3.4 *Suppose that G has a normal 2–Sylow subgroup. Then the trace forms of two G–Galois algebras are isomorphic over k if and only if they are isomorphic over each completion of k. In particular, a G–Galois algebra has a self–dual normal basis over k if and only if it has a self–dual normal basis over every completion of k.*

Proof. This is an immediate consequence of 3.3.

The proof of th. 3.1 relies on th. 2.2, and on some properties of group rings and of quadratic and hermitian forms that we recall in this section. Let us first note that the Hasse principle holds for *any* G–form provided the orthogonal components of the group ring are split:

Theorem 3.5 *Suppose that all the orthogonal components of $k[G]$ are split, and let q, q' be two G–forms. Then $q \simeq_G q'$ over k if and only if $q \simeq_G q'$ over all the completions of k.*

Proof. This follows from the Hasse principle for unitary and symplectic forms, as well as the Hasse principle for quadratic forms over global fields (see for instance [6], chap. 10).

Therefore th. 3.1 is new for number fields only – indeed, if $\mathrm{char}(k) > 0$, then all the orthogonal components of $k[G]$ are split.

Proposition 3.6 *Let S be a 2–group. Then the orthogonal and unitary components of $k[S]$ are split, and the symplectic components of $k[S]$ are either split, or of the form $M_n(H)$ where H is a quaternion division algebra over its center.*

Proof. Note that $k[S] = Q[S] \otimes_Q k$ if $\mathrm{char}(k) = 0$, and $k[S] = F_p[S] \otimes_{F_p} k$ if $\mathrm{char}(k) = p \neq 0$. Therefore it is sufficient to prove the proposition when $k = Q$ or $k = F_p$. As the Brauer group of a finite field is trivial, every component is split if $k = F_p$.

Suppose that $k = Q$. Then each component of $Q[S]$ is invariant under ι (cf. [6], Chap 8, 13.2.).

Let $M_n(D)$ be a symplectic component of $Q[S]$. This implies that the algebra $M_n(D)$ is of order one or two in the Brauer group of Q, and it is well–known that this can only happen if D is a commutative field or a quaternion algebra.

Let us now show that the orthogonal and unitary components of $Q[S]$ are split. Let v be a non–dyadic place of Q, and let O_v be the ring of integers of Q_v. Since $\#S$ is invertible in O_v, it follows that $O_v[S]$ is Azumaya over its center. This implies that this algebra is split mod π, where π is a uniformizer at v, therefore it is split over O_v. In particular every component of $Q_v[S]$ is split.

If v is the real place of Q, then every orthogonal and unitary component of $Q_v[S] = R[S]$ is split (cf. [6], Chap 8, 13.5).

Let $M_n(D)$ be an orthogonal or unitary component of $Q[S]$, and let $Z(D) = K$. As S is a 2–group, K is a subfield of a 2–cyclotomic field, hence K admits a unique dyadic place. Since D is split at all the other places, D is split at the dyadic place as well, hence D is split.

Corollary 3.7 *Let S be a 2–group, and let q, q' be two S–forms. Then $q \simeq_S q'$ over k if and only if $q \simeq_S q'$ over all the completions of k.*

Proof. This follows from 3.5 and 3.6.

We are now ready to prove 3.1. The proof uses th. 2.2, which will be proved in section 11.

Proof of th. 3.1 Suppose first that $\mathrm{char}(k) > 0$. Then all the components of $k[G]$ are split, hence th. 3.5 implies the desired result.

Suppose now that $\mathrm{char}(k) = 0$, in other words that k is an algebraic number field. By lemma 1.2, there exists an odd degree field extension k'/k and S–Galois algebras M and M' over k' such that $(L, q_L) \otimes_k k' \simeq_G \mathrm{Ind}_S^G(M, q_M)$, and $(L,' q_{L'}) \otimes_k k' \simeq_G \mathrm{Ind}_S^G(M', q_{M'})$. Recall that by hypothesis the G–forms (L, q_L) and $(L', q_{L'})$ are isomorphic over all the completions of k. This implies that the G–forms $(L, q_L) \otimes_k k'$ and $(L,' q_{L'}) \otimes_k k'$ are isomorphic over all the completions of k'. Hence the S–forms $\mathrm{Res}^G_S(L, q_L) \otimes_k k' \simeq_S \mathrm{Res}^G_S \mathrm{Ind}^G_S(M, q_M)$, and $\mathrm{Res}^G_S(L', q_{L'}) \otimes_k k' \simeq_S \mathrm{Res}^G_S \mathrm{Ind}^G_S(M', q_{M'})$ are isomorphic over all the completions of k'. By corollary 3.7, this implies that the S forms $\mathrm{Res}^G_S(L, q_L) \otimes_k k' \simeq_S \mathrm{Res}^G_S \mathrm{Ind}^G_S(M, q_M)$, and $\mathrm{Res}^G_S(L', q_{L'}) \otimes_k k' \simeq_S \mathrm{Res}^G_S \mathrm{Ind}^G_S(M', q_{M'})$ are isomorphic over k'. As G has the odd determinant property, th. 2.2 implies that the G–forms $\mathrm{Ind}^G_S(M, q_M)$ and $\mathrm{Ind}^G_S(M', q_{M'})$ are isomorphic. As $(L, q_L) \otimes_k k' \simeq_G \mathrm{Ind}^G_S(M, q_M)$ and $(L,' q_{L'}) \otimes_k k' \simeq_G \mathrm{Ind}^G_S(M', q_{M'})$, we get $(L, q_L) \otimes_k k' \simeq_G (L,' q_{L'}) \otimes_k k'$. By th. 1.1, this implies that $(L, q_L) \simeq_G (L,' q_{L'})$, and this completes the proof of th. 3.1.

§4. Properties of determinants in characteristic 2

This section is concerned with properties of determinants of linear transformations over rings of characteristic 2 that will be needed in the following sections. Let F be a field of characteristic 2, and let $R = F[X]/(X^2 + 1)$. We start by recalling a result of linear algebra :

Proposition 4.1 *Let $M = R^n$ be the free R–module of rank n, and let $f : M \to M$ be an R–linear map. Then*

$$N_{R/F}(\det(f)) = \det(f_F),$$

where $\det(f_F)$ is the determinant of f considered as an F–linear map.

Corollary 4.2 *Let*

$$A = \begin{pmatrix} a_{1,1} & b_{1,1} & \dots & a_{1,n} & b_{1,n} \\ b_{1,1}, & a_{1,1} & \dots & b_{1,n} & a_{1,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & b_{n,1} & \dots & a_{n,n} & b_{n,n} \\ b_{n,1} & a_{1,n} & \dots & b_{n,n} & a_{n,n} \end{pmatrix}$$

and

$$B = \begin{pmatrix} a_{1,1} + b_{1,1} & \dots & a_{1,n} + b_{1,n} \\ \dots & \dots & \dots \\ a_{n,1} + b_{n,1} & \dots & a_{n,n} + b_{n,n} \end{pmatrix}$$

with $a_{i,j}, b_{i,j} \in F$. Then

$$\det(B)^2 = \det(A).$$

Proof. Let $f : R^n \to R^n$ be defined by $f(e_j) = \Sigma_{1 \le i \le n}(a_{i,j} + b_{i,j}X)e_i$, where $e_1, \dots, e_n$ is the standard basis of R^n. The matrix of f with respect to the basis $e_1, \dots, e_n$ is $(a_{i,j} + b_{i,j}X)$. We have

$$N_{R/F}(\det(a_{i,j} + b_{i,j}X)) = (\det(a_{i,j} + b_{i,j}))^2,$$

which is equal to $\det(B)^2$. By 4.1, this is the determinant of f as an F–linear map. On the other hand, the determinant of f in the basis $e_1, e_1X, e_2, e_2X, \ldots, e_n, e_nX$ is equal to $\det(A)$; hence we have $\det(B)^2 = \det(A)$, as claimed.

We also need the following observation:

LEMMA 4.3 *Let $n \in N$, and suppose that the group $\{1, \iota\}$ of order 2 acts on the set $\{1, \ldots, n\}$ in such a way that $\{1, \ldots, r\}$ is the set of fixed points. Let $(d_{i,j})_{1 \le i,j \le n}$ be an integral matrix such that $d_{\iota(i),\iota(j)} = d_{i,j}$ for all i, j. Then*

$$\det(d_{i,j})_{1 \le i,j \le n} \equiv \det(d_{i,j})_{1 \le i,j \le r} \det(d_{i,j})_{r+1 \le i,j \le n} \pmod 2.$$

PROOF. Let S be the set of permutations of $\{1, 2, ...n\}$. For $s \in S$ and $1 \le i \le n$, set $\iota * s(i) = \iota s \iota(i)$. We have

$$\det(d_{i,j})_{1 \le i,j \le n} \equiv \Sigma_{s \in S}(\prod_{1 \le i \le n} d_{si,i}) \mod 2.$$

Set

$$H = \{s \in S \mid s(i) \le r \text{ for } i \le r\}.$$

Then

$$\Sigma_{s \in S}(\prod_{1 \le i \le n} d_{si,i}) = \Sigma_{s \in H}(\prod_{1 \le i \le n} d_{si,i}) + \Sigma_{s \notin H}(\prod_{1 \le i \le n} d_{si,i}).$$

For $s \notin H$, we have $\iota * s \notin H$ and $s \ne \iota * s$. In view of $d_{i,j} = d_{\iota(i),\iota(j)}$ for all i, j, we get

$$\Sigma_{s \notin H}(\prod_{1 \le i \le n} d_{si,i}) \equiv 0 \mod 2.$$

Let

$$S^1 = \{s \in S \mid s(i) = i \text{ for } i \ge r+1\},$$

and

$$S^2 = \{s \in S \mid s(i) = i \text{ for } i \le r\}.$$

Then we have

$$\Sigma_{s \in H}(\prod_{1 \le i \le n} d_{si,i}) = [\Sigma_{s \in S^1}(\prod_{1 \le i \le r} d_{si,i})].[\Sigma_{s \in S^2}(\prod_{r+1 \le i \le n} d_{si,i})].$$

This completes the proof of the lemma.

Lemma 4.3 is used in the next sections, in particular in the proofs of 7.1, 8.4 and 8.5.

§5. Group rings of 2–groups and decomposition of S–quadratic forms

The aim of this section is to introduce some tools and notation that will be used in the sequel. In particular, we set up a decomposition of the quadratic forms invariant by a 2–group, generalizing the approach of [2], §5.

Group rings of 2–groups

Let k be a field of characteristic $\neq 2$, and let S be a 2–group. Recall that $\iota : k[S] \to k[S]$ is the canonical involution of the group ring.

As the characteristic of k is not 2, the algebra $k[S]$ is semi–simple. We have a decomposition of $k[S]$ into simple factors, corresponding to the irreducible representations of S over k, hence also to the irreducible characters of S over k. Let us denote by S'_k the set of these irreducible characters. Each of them determines a component $M_{n_x}(\Delta_x)$ of $k[S]$, where Δ_x is a division algebra. Let $K_x = Z(\Delta_x)$ be the center of Δ_x. Recall that the orthogonal and unitary components are split, and that the symplectic components are either split, or of the form $M_n(H)$ where H is a quaternion division algebra (see prop. 3.6).

Let us denote by U_x the simple $k[S]$–module associated to the irreducible character $x \in S'_k$. Note that it is isomorphic to $\Delta_x^{n_x}$. Let Y_k be the free Z–module generated by S'_k.

Note that ι acts on S'_k by $\iota(x)(s) = x(s^{-1})$ for all $x \in S'_k$ and $s \in S$. We say that $x \in S'_k$ is *self–dual* if $\iota(x) = x$. This is equivalent to requiring that the corresponding component $M_{n_x}(\Delta_x)$ is stable by ι. If $x \in S'_k$ is not self–dual, then there exists $x' \in S'_k$ such that $x' \neq x$ and $\iota(x) = x'$. In this case, set $\overline{x} = (x, x')$. If x is self–dual, then set $\overline{x} = x$. Let us denote by $\overline{S}'_k$ the set of $\overline{x}$ for $x \in S'_k$.

Set $M_{n_x}(\Delta_{\overline{x}}) = M_{n_x}(\Delta_x)$ if x is self–dual, and $M_{n_x}(\Delta_{\overline{x}}) = M_{n_x}(\Delta_x) \times M_{n_{x'}}(\Delta_{x'})$ if $\iota(x) = x' \neq x$. Similarly, set $K_{\overline{x}} = K_x$ is x is self–dual and $K_{\overline{x}} = K_x \times K_{x'}$ if $\overline{x} = (x, x')$. Note that $K_{\overline{x}}$ is an étale algebra, but not necessarily a field. Let $K^0_{\overline{x}} = \{a \in K_{\overline{x}} \mid \iota(a) = a\}$ be the invariants of ι in $K_{\overline{x}}$. When x is not self–dual, then we have $K_x \simeq K_{x'} \simeq K^0_{\overline{x}}$.

The involution ι of $k[S]$ restricts to the factors $M_{n_x}(\Delta_{\overline{x}})$, and it is adjoint to a hermitian or skew–hermitian form, which we fix in the different cases as follows.

If x is orthogonal, then $\Delta_{\overline{x}} = K_x$. In this case, we set $D_{\overline{x}} = K_x$, and we chose the involution $\tau_{\overline{x}} : D_{\overline{x}} \to D_{\overline{x}}$ to be the identity. The restriction of the involution ι to this factor is adjoint to a symmetric form on $D_{\overline{x}}^{n_x}$ which we denote by $\rho_{\overline{x}}$. We define $m_x = n_x$, and the symmetric form is supported on the simple module U_x.

If x is symplectic, then $\Delta_{\overline{x}} = K_x$ or a quaternion division algebra. We set $D_{\overline{x}} = M_2(K_x)$ in the first case, and $D_{\overline{x}} = \Delta_x$ in the second case. In both cases, we choose the involution $\tau_{\overline{x}} : D_{\overline{x}} \to D_{\overline{x}}$ to be the standard symplectic involution of $D_{\overline{x}}$. In this case, the restriction of the involution ι to this factor is adjoint to a hermitian form over $D_{\overline{x}}^{m_x}$ with respect to the involution $\tau_{\overline{x}}$ which we denote by $\rho_{\overline{x}}$. The form $\rho_{\overline{x}}$ is supported on the module $U_x \oplus U_x$ and $n_x = 2m_x$ if $D_{\overline{x}}$ is not division, it is supported on the module U_x and $m_x = n_x$ if $D_{\overline{x}}$ is division.

If x is unitary, then $\Delta_{\overline{x}} = K_{\overline{x}}$, and $K_{\overline{x}}$ is a quadratic algebra over $K_{\overline{x}}^0$. We set $D_{\overline{x}} = K_{\overline{x}}$, and we fix the involution $\tau_{\overline{x}} : D_{\overline{x}} \to D_{\overline{x}}$ to be the non–trivial automorphism of this quadratic algebra. Then the restriction of the involution ι to this factor is adjoint to a hermitian form on $D_{\overline{x}}^{n_x}$ with respect to the involution $\tau_{\overline{x}}$ which we denote by $\rho_{\overline{x}}$. We set $m_x = n_x$ in this case. The form $\rho_{\overline{x}}$ is supported on U_x if x is self–dual, and on $U_{x_1} \oplus U_{x_2}$ if $\overline{x} = (x_1, x_2)$ with $x_1 \neq x_2$ and $\iota(x_1) = x_2$.

Set $U_{\overline{x}} = U_x \oplus U_x$ if x is symplectic and $D_{\overline{x}}$ not division, $U_{\overline{x}} = U_{x_1} \oplus U_{x_2}$ if $\overline{x}$ is unitary with $\overline{x} = (x_1, x_2)$ such that $\iota(x_1) = x_2$ and $x_1 \neq x_2$, and $U_{\overline{x}} = U_x$ in all other cases. Note that $U_{\overline{x}} \simeq D_{\overline{x}}^{m_x}$. Therefore in all cases we have a hermitian form $\rho_{\overline{x}} : U_{\overline{x}} \times U_{\overline{x}} \to D_{\overline{x}}$ which we fix throughout. We denote the hermitian form $(U_{\overline{x}}, \rho_{\overline{x}})$ by $\rho_{\overline{x}}$.

We also fix a quadratic form $n_{\overline{x}} : D_{\overline{x}} \to K_{\overline{x}}^0$ to be the one–dimensional unit form if x is orthogonal, the reduced norm form of the quaternion algebra $D_{\overline{x}}$ if x is symplectic, and the norm form of the quadratic algebra $D_{\overline{x}}$ if x is unitary.

Decomposition of S–quadratic forms

Let (V, q) be an S–quadratic form. Then (V, q) decomposes as an orthogonal sum of hermitian forms $(M_{\overline{x}}, Q_{\overline{x}})$ for $x \in S'_k$, over $M_{m_x}(D_{\overline{x}})$ with respect to the restriction of ι to this factor. By Morita theory, fixing $\rho_{\overline{x}}$, the hermitian form $(M_{\overline{x}}, Q_{\overline{x}})$ is uniquely determined up to isomorphism by a hermitian form $h_{\overline{x}}$ over a free $D_{\overline{x}}$–module $W_{\overline{x}}$ of finite rank with respect to the involution $\tau_{\overline{x}}$, and conversely the hermitian form $(W_{\overline{x}}, h_{\overline{x}})$ is uniquely determined up to isomorphism by $(M_{\overline{x}}, Q_{\overline{x}})$. Moreover, by Jacobson's theorem the hermitian form $(W_{\overline{x}}, h_{\overline{x}})$ corresponds to a quadratic form $(V_{\overline{x}}, g_{\overline{x}})$ over $K_{\overline{x}}^0$ with the property that $(V_{\overline{x}}, g_{\overline{x}}) \otimes n_{\overline{x}}$ is uniquely determined by $(W_{\overline{x}}, h_{\overline{x}})$ (cf. [6], 10.1.1 and 10.1.7) . We have $(M_{\overline{x}}, Q_{\overline{x}}) \simeq \rho_{\overline{x}} \otimes_{K_{\overline{x}}^0} (V_{\overline{x}}, g_{\overline{x}})$, and $(V_{\overline{x}}, g_{\overline{x}}) \otimes n_{\overline{x}}$ is uniquely determined by $(M_{\overline{x}}, Q_{\overline{x}})$, hence by (V, q). In other words, we have

$$(V, q) \simeq \bigoplus_{\overline{x} \in \overline{S}'_k} \rho_{\overline{x}} \otimes_{K_{\overline{x}}^0} (V_{\overline{x}}, g_{\overline{x}}),$$

and if (V_1, q_1) and (V_2, q_2) are two S–quadratic forms with

$$(V_1, q_1) \simeq \bigoplus_{\overline{x} \in \overline{S}'_k} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V^1_{\overline{x}}, g^1_{\overline{x}}) \text{ and } (V_2, q_2) \simeq \bigoplus_{\overline{x} \in \overline{S}'_k} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V^2_{\overline{x}}, g^2_{\overline{x}}),$$

then

$$(V_1, q_1) \simeq_S (V_2, q_2)$$

if and only if

$$n_{\overline{x}} \otimes g^1_{\overline{x}} \simeq n_{\overline{x}} \otimes g^2_{\overline{x}}$$

for all $\overline{x} \in S'_k$.

§6. Induction of S–forms

Let k be a field of characteristic $\neq 2$. Let G be a finite group, and let S be a 2–Sylow subgroup of G, We use the notation introduced in §5. In particular, S'_k is the set of irreducible characters of S over k. Recall that $\iota : k[S] \to k[S]$ is the standard involution, and that for $x \in S'_k$ we set $\overline{x} = x$ if x is selfdual, and $\overline{x} = (x, x')$ if $\iota(x) = x' \neq x$.

Let $N = N_G(S)$ be the normalizer of S in G. Then N acts on S'_k by $n(x)(s) = x(nsn^{-1})$ for all $n \in N$, $x \in S'_k$ and $s \in S$. Note that the actions of N and ι commute. We need the following lemmas:

Lemma 6.1 *The orbits of S'_k under N have odd cardinality.*

Proof. Let $x \in S'_k$ and let ω be the orbit of x under N. We have $\sharp(\omega) = \sharp(N/\mathrm{Stab}_N(x))$. As $S \subset Stab_N(x)$, we see that $\sharp(N/\mathrm{Stab}_N(x))$ is odd.

Lemma 6.2 *Let $x, x' \in S'_k$ such that $\iota(x) = x' \neq x$. Let ω, ω' be the orbits of x, respectively x'. Then $\omega \neq \omega'$.*

Proof. Indeed, suppose that $\omega = \omega'$. As the actions of N and ι commute, we see that for every $n \in N$, we have $\iota n(x) \neq n(x)$. This implies that $\iota y \neq y$ for every $y \in \omega$, and therefore ω has even cardinality, contradicting lemma 6.1. Therefore $\omega \neq \omega'$.

Let us denote by Ω_k the set of orbits of S'_k under N. There is an induced action of N on the free Z–module generated by S'_k and the set of orbits under this action is the free Z–module generated by Ω_k.

Let us define an action of ι on Ω_k by letting $\iota\omega$ to be the orbit of $\iota(x)$ for any $x \in \omega$; this is well–defined as the actions of N and ι on S'_k commute. For any

$\omega \in \Omega_k$, set $\overline{\omega} = \omega$ if $\iota\omega = \omega$, and $\overline{\omega} = (\omega_1, \omega_2)$ with $\iota\omega_1 = \omega_2$ and $\omega_1 \neq \omega_2$. Let $\overline{\Omega}_k$ be the set of all $\overline{\omega}$ with $\omega \in \Omega_k$. Let us fix a field extension $K^0_{\overline{\omega}}$ of k such that $K^0_{\overline{\omega}} \simeq K^0_{\overline{x}}$ for all $\overline{x} \in \overline{\omega}$.

Let (V, q) be an S–quadratic form. Then we have an orthogonal decomposition

$$(V, q) \simeq \bigoplus_{\overline{x} \in \overline{S}'_k} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V_{\overline{x}}, g_{\overline{x}}),$$

where $(V_{\overline{x}}, g_{\overline{x}})$ is a quadratic form over $K^0_{\overline{x}}$, and $(V_{\overline{x}}, g_{\overline{x}}) \otimes n_{\overline{x}}$ is uniquely determined by (V, q) (cf. §5).

For all $\overline{\omega} \in \overline{\Omega}_k$, let us consider the orthogonal sum

$$(V_{\overline{\omega}}, g_{\overline{\omega}}) = \bigoplus_{\overline{x} \in \overline{\omega}} (V_{\overline{x}}, g_{\overline{x}}).$$

Then $(V_{\overline{\omega}}, g_{\overline{\omega}})$ is a quadratic form over $K^0_{\overline{\omega}}$.

Note that $\mathrm{Ind}_S^G(\rho_{\overline{x}})$ does not depend on the choice of $\overline{x} \in \overline{\omega}$. Set

$$I(\overline{\omega}) = \mathrm{Ind}_S^G(\rho_{\overline{x}})$$

where $\overline{x}$ is any element of $\overline{\omega}$.

Therefore we have

$$\mathrm{Ind}_S^G(V, q) = \bigoplus_{\overline{\omega} \in \overline{\Omega}_k} I(\overline{\omega}) \otimes_{K^0_{\overline{\omega}}} (V_{\overline{\omega}}, g_{\overline{\omega}}).$$

Set

$$A(V, q) = \mathrm{Res}_S^G \ \mathrm{Ind}_S^G(V, q).$$

Then we have

$$A(V, q) = \bigoplus_{\overline{\omega} \in \overline{\Omega}_k} \mathrm{Res}_S^G(I(\overline{\omega})) \otimes_{K^0_{\overline{\omega}}} (V_{\overline{\omega}}, g_{\overline{\omega}}).$$

Let $\overline{y} \in \overline{S}'_k$, and let us take the $\overline{y}$–component of the equation above. We get

$$A(V, q)_{\overline{y}} = \bigoplus_{\overline{\omega} \in \overline{\Omega}_k} \mathrm{Res}_S^G(I(\overline{\omega}))_{\overline{y}} \otimes_{K^0_{\overline{\omega}}} (V_{\overline{\omega}}, g_{\overline{\omega}}).$$

Let $\overline{\omega}' \in \overline{\Omega}_k$ such that $\overline{y} \in \overline{\omega}'$. Note that the S–quadratic spaces $A(V, q)_{\overline{y}}$ and $\mathrm{Res}_S^G(I_{\overline{\omega}})_{\overline{y}}$ do not depend on the choice of $\overline{y} \in \overline{\omega}'$. Set

$$A(V, q)_{\overline{\omega}'} = A(V, q)_{\overline{y}}$$

and

$$\mathrm{Res}_S^G(I(\overline{\varpi}))_{\overline{\varpi}'} = \mathrm{Res}_S^G(I(\overline{\varpi}))_{\overline{y}}$$

for any $\overline{y} \in \overline{\varpi}'$.

Then we have

$$\mathrm{Res}_S^G(I(\overline{\varpi}))_{\overline{\varpi}'} = \rho_{\overline{y}} \otimes_{K^0_{\overline{\varpi}'}} F_{\overline{\varpi},\overline{\varpi}'}$$

for $\overline{y} \in \overline{\varpi}'$, where $F_{\overline{\varpi},\overline{\varpi}'}$ is a quadratic form over $K^0_{\overline{\varpi}'}$.

Hence

$$A(V,q)_{\overline{\varpi}'} = \rho_{\overline{y}} \otimes_{K^0_{\overline{\varpi}'}} \bigoplus_{\overline{\varpi}\in\overline{\Omega}_k} [F_{\overline{\varpi},\overline{\varpi}'} \otimes_{K^0_{\overline{\varpi}}} (V_{\overline{\varpi}}, g_{\overline{\varpi}})].$$

Notation. Let $\omega, \omega' \in \Omega_k$ be such that $K^0_{\overline{\omega}} = K^0_{\overline{\omega}'} = k$. We define $d_{\overline{\varpi},\overline{\varpi}'}$ to be the dimension of the k–vector space underlying the quadratic form $F_{\overline{\varpi},\overline{\varpi}'}$.

Note that $d_{\overline{\varpi},\overline{\varpi}'}$ is the number of times $\rho_{\overline{y}}$ occurs in $\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(\rho_{\overline{x}})$ for any $\overline{x} \in \overline{\varpi}$, $\overline{y} \in \overline{\varpi}'$. As $U_{\overline{x}}$ is the underlying module of $\rho_{\overline{x}}$, the integer $d_{\overline{\varpi},\overline{\varpi}'}$ can also be seen as the number of times $U_{\overline{y}}$ occurs in $\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(U_{\overline{x}})$ for any $\overline{x} \in \overline{\varpi}$, $\overline{y} \in \overline{\varpi}'$.

Let (V_1, q_1) and (V_2, q_2) be two S–quadratic forms. If $A(V_1, q_1) \simeq A(V_2, q_2)$, then $A(V_1, q_1)_{\overline{\varpi}'} \simeq A(V_2, q_2)_{\overline{\varpi}'}$ for all $\overline{\varpi}' \in \overline{\Omega}_k$. Hence, if we have

$$(V_1, q_1) \simeq \bigoplus_{\overline{x}\in\overline{S}'_k} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V^1_{\overline{x}}, g^1_{\overline{x}}) \quad \text{and} \quad (V_2, q_2) \simeq \bigoplus_{\overline{x}\in\overline{S}'_k} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V^2_{\overline{x}}, g^2_{\overline{x}}),$$

then, for each $\overline{\varpi}' \in \overline{\Omega}_k$,

$$\bigoplus_{\overline{\varpi}\in\overline{\Omega}_k} n_{\overline{\varpi}'} \otimes_{K^0_{\overline{\varpi}'}} [F_{\overline{\varpi},\overline{\varpi}'} \otimes_{K^0_{\overline{\varpi}}} (V^1_{\overline{\varpi}}, g^1_{\overline{\varpi}})] \simeq \bigoplus_{\overline{\varpi}\in\overline{\Omega}_k} n_{\overline{\varpi}'} \otimes_{K^0_{\overline{\varpi}'}} [F_{\overline{\varpi},\overline{\varpi}'} \otimes_{K^0_{\overline{\varpi}}} (V^2_{\overline{\varpi}}, g^2_{\overline{\varpi}})].$$

§7. Odd determinant property – a special case

The aim of this section and the next ones is to establish some technical results relative to the odd determinant property. These will be used in §11 to prove th. 2.2.

We keep the notation of the previous sections, and we suppose that all the characters in S'_k are absolutely irreducible.

Recall that Ω_k is the set of N–orbits of S'_k. The following notation will be important in the sequel:

Notation. Let us define $d_{\omega,\omega'}$ as being the number of times U_y occurs in

$$\mathrm{Res}_S^G \, \mathrm{Ind}_S^G(U_x)$$

for $x \in \omega$, $y \in \omega'$.

The standard involution $\iota : k[S] \to k[S]$ acts on Ω_k. Note that $d_{\iota\omega,\iota\omega'} = d_{\omega,\omega'}$ for all $\omega, \omega' \in \Omega_k$. Let us define

$$\Omega^1 = \{\omega \in \Omega_k \mid \iota\omega = \omega\}$$

and

$$\Omega^2 = \{\omega \in \Omega_k \mid \iota\omega \neq \omega\}.$$

Since all the characters in S'_k are absolutely irreducible and in view of Lemma 6.2, Ω^1 is precisely the set of orbits of irreducible orthogonal and symplectic characters.

Proposition 7.1 *Suppose that*

$$\det_{\omega,\omega' \in \Omega_k}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2.$$

Then

$$\det_{\omega,\omega' \in \Omega^1}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2$$

and

$$\det_{\omega,\omega' \in \Omega^2}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2.$$

Proof. Since the group $\{1, \iota\}$ acts on Ω with fixed points precisely Ω^1, it follows from lemma 4.3 that

$$\det_{\omega,\omega' \in \Omega_k}(d_{\omega,\omega'}) \equiv \det_{\omega,\omega' \in \Omega^1}(d_{\omega,\omega'}) \det_{\omega,\omega' \in \Omega^2}(d_{\omega,\omega'}) \pmod 2.$$

Hence we have

$$\det_{\omega,\omega' \in \Omega^1}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2,$$

and

$$\det_{\omega,\omega' \in \Omega^2}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2.$$

This completes the proof of the proposition.

We define $\Omega^{1,o} = \{\omega \in \Omega^1 \mid \omega \text{ orthogonal}\}$, and $\Omega^{1,s} = \{\omega \in \Omega^1 \mid \omega \text{ symplectic}\}$.

Proposition 7.2 *Suppose that* $\det_{\omega,\omega' \in \Omega^1}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2$. *Then*

$$\det_{\omega,\omega' \in \Omega^{1,o}}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2,$$

and

$$\det_{\omega,\omega'\in\Omega^{1,s}}(d_{\omega,\omega'}) \equiv 1 \pmod 2.$$

Proof. Let ω be orthogonal and ω' symplectic. For $x \in \omega$, $y \in \omega'$, recall that U_x and U_y are the simple $k[S]$–modules associated to x and y respectively. Then $\rho_{\overline{y}}$ is supported on $U_{\overline{y}} = U_y \oplus U_y$ and $\rho_{\overline{x}}$ is supported on $U_{\overline{x}} = U_x$, hence the $\overline{y}$–component of $\mathrm{Res}^G_S\ \mathrm{Ind}^G_S(U_x, \rho_{\overline{x}})$ is isomorphic to $(U_y \oplus U_y, \rho_{\overline{y}}) \otimes_k F_{\overline{\omega},\overline{\omega}'}$. Thus the module U_y occurs with even multiplicity in $\mathrm{Res}^G_S\ \mathrm{Ind}^G_S(U_x)$, so that $d_{\omega,\omega'} \equiv 0 \pmod 2$. Therefore the matrix $(d_{\omega,\omega'})_{\omega,\omega'\in\Omega^1}$ has the shape

$$\begin{pmatrix} A & 0 \\ * & B \end{pmatrix}.$$

mod 2, where $A = \det_{\omega,\omega'\in\Omega^{1,o}}(d_{\omega,\omega'})$ and $B = \det_{\omega,\omega'\in\Omega^{1,s}}(d_{\omega,\omega'})$. This completes the proof of the proposition.

For any $\omega \in \Omega_k$, recall that $\overline{\omega} = \omega$ if $\iota\omega = \omega$, and $\overline{\omega} = (\omega_1, \omega_2)$ with $\iota\omega_1 = \omega_2$ and $\omega_1 \neq \omega_2$. Let $\overline{\Omega}_k$ be the set of all $\overline{\omega}$ with $\omega \in \Omega_k$. Let

$$\overline{\Omega}^2 = \{\overline{\omega} = (\omega_1, \omega_2) \in \overline{\Omega} \mid \ \iota\omega_1 = \omega_2 \ \text{ and } \ \omega_1 \neq \omega_2\}.$$

Proposition 7.3 *Suppose that* $\det_{\omega,\omega'\in\Omega^2}(d_{\omega,\omega'}) \equiv 1 \pmod 2$. *Then we have*

$$\det_{\overline{\omega},\overline{\omega}'\in\overline{\Omega}^2}(d_{\overline{\omega},\overline{\omega}'}) \equiv 1 \pmod 2.$$

Proof. Let $\overline{\omega} = (\omega_1, \omega_2)$ and $\overline{\omega}' = (\omega_1', \omega_2')$, and let $d_{\omega_1,\omega_1'} = a$, $d_{\omega_1,\omega_2'} = b$. Then $d_{\overline{\omega},\overline{\omega}'} = a + b$. For a suitable ordering of the orbits $\overline{\Omega}^2$, and the corresponding ordering of Ω^2, the matrices $d_{\overline{\omega},\overline{\omega}'}$ and $d_{\omega,\omega'}$ are of the shape B and A as in corollary 4.2. Hence $\det(B)^2 \equiv \det(A) \pmod 2$. This gives the desired result.

We have the following

Proposition 7.4 *Suppose that G has the odd determinant property. Then*

$$\det_{\omega,\omega'\in\Omega_k}(d_{\omega,\omega'}) \equiv 1 \pmod 2.$$

For the proof of prop. 7.4, we need the following lemma

Lemma 7.5 *Let K be a field of characteristic 0, and assume that all the characters in S'_K are absolutely irreducible. Suppose that G has the odd determinant property. Then*

$$\det_{\omega,\omega'\in\Omega_K}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2.$$

Proof. Let $X_K = X \otimes_Z K$ be the vector space of K–valued functions on S invariant under conjugation by N. For all $\omega \in \Omega_K$, set $p_\omega = \Sigma_{x\in\omega}x$. Note that as all the characters in S'_K are absolutely irreducible, the set $(p_\omega)_{\omega\in\Omega_K}$ is a basis of X_K.

Let $\Phi : X_K \to X_K$ be $\mathrm{Res}^G_S\ \mathrm{Ind}^G_S$ considered as an endomorphism of X_K. Note that we have

$$\Phi(p_\omega) = (\sharp\omega)\Sigma_{\omega\in\Omega_K} d_{\omega,\omega'}p_{\omega'}.$$

This implies that the matrix of Φ in the basis $(p_\omega)_{\omega\in\Omega_K}$ is equal to $((\sharp\omega)d_{\omega,\omega'})$.

On the other hand, the odd determinant property implies that the determinant of $\Phi : X_Z \to X_Z$ is odd (cf. §2). Hence the determinant of $\Phi : X_K \to X_K$ is also odd. Note that $\sharp\omega$ is odd for all $\omega \in \Omega$ (see lemma 6.1). This implies that $\det_{\omega,\omega'\in\Omega_K}(d_{\omega,\omega'})$ is odd, hence the lemma is proved.

Proof of prop. 7.4 Note that for any field E and any $\omega, \omega' \in \Omega_E$, we have

$$d_{\omega,\omega'} = \langle x, \mathrm{Res}^G_S\ \mathrm{Ind}^G_S x'\rangle_S = \langle \mathrm{Ind}^G_S x, \mathrm{Ind}^S_G x'\rangle_G$$

for any $x \in \omega$, $x' \in \omega'$.

If $\mathrm{char}(k) = 0$, then the proposition follows from lemma 7.5. Suppose that $\mathrm{char}(k) > 0$. Let A be a complete discrete valuation ring of characteristic 0 with residue field k, and let π be a uniformizer of A. Let K be the field of fractions of A. Then all the characters in S'_K are absolutely irreducible. Indeed, we have $k[S] = \prod_{1\le i\le r} M_{n_i}(k)$, where r is the number of irreducible representations of S over k. Since $A[S]$ is complete with respect to the ideal $\pi A[S]$, the isomorphism $A[S]/\pi A[S] \to \prod_{1\le i\le r} M_{n_i}(k)$ can be lifted to an isomorphism $A[S] \simeq \prod_{1\le i\le r} M_{n_i}(A)$, hence we have $K[S] \simeq \prod_{1\le i\le r} M_{n_i}(K)$. Thus every character of S'_K is absolutely irreducible, hence by lemma 7.5 we have

$$\det_{\omega,\omega'\in\Omega_K}(d_{\omega,\omega'}) \;\equiv\; 1 \pmod 2.$$

Let us show that the matrices $(d_{\omega,\omega'})_{\omega,\omega'\in\Omega_k}$ and $(d_{\omega,\omega'})_{\omega,\omega'\in\Omega_K}$ are equal for suitable orderings of the sets Ω_k and Ω_K. As S is a 2–group and $\mathrm{char}(k) \neq 2$, every $k[S]$–module is projective. If P is a projective $k[S]$–module, then $\mathrm{Ind}^G_S(P)$ is projective as well.

Let P be a projective $k[S]$–module. Since $A[S]$ is π–adically complete, there is a projective $A[S]$–module $\tilde P$ such that $\tilde P/\pi\tilde P \simeq P$. Then $\tilde P_K = \tilde P \otimes_A K$ is a projective $K[S]$–module. Moreover, P is simple if and only if $\tilde{P}_K$ is simple. Note that if P and Q are simple $k[S]$–modules, then we have

$$\langle \mathrm{Ind}_S^G(P), \mathrm{Ind}_S^G(Q)\rangle_G = \langle \mathrm{Ind}_S^G \tilde{P}_K, \mathrm{Ind}_S^G \tilde{Q}_K\rangle_G.$$

Therefore the matrices $(d_{\omega,\omega'})_{\omega,\omega'\in\Omega_k}$ and $(d_{\omega,\omega'})_{\omega,\omega'\in\Omega_K}$ are equal for suitable orderings of the sets Ω_k and Ω_K, and this completes the proof of the proposition.

§8. Odd determinant property–behavior under quadratic extension

This section contains a quadratic descent argument. Together with a filtration introduced in §9, this quadratic descent will enable us to reduce to the case where all the characters are absolutely irreducible, cf. §7. Putting these informations together in §10, we obtain a result (th. 10.1) that will be used in §11 to prove th. 2.2. We start by recalling and introducing some notation that will be needed in this section and the next ones.

Let G be a finite group and let S be a 2–Sylow subgroup of G. For any field E with $\mathrm{char}(E) \neq 2$, we denote by S'_E the set of irreducible characters of S over E, and by Ω_E be the set of orbits of S'_E under the action of $N = N_G(S)$. Recall that $\iota : E[S] \to E[S]$ is the standard involution, and that for $x \in S'_E$ we denote $\overline{x} = x$ if x is selfdual, and $\overline{x} = (x, x')$ if $\iota(x) = x' \neq x$.

For any $\omega \in \Omega_E$, recall that $\overline{\omega} = \omega$ if the characters of ω are invariant under ι, and $\overline{\omega} = (\omega_1, \omega_2)$ if there exist $x_1 \in \omega_1$ and $x_2 \in \omega_2$ such that $\iota(x_1) = x_2$ with $x_1 \neq x_2$. Let $\overline{\Omega}_E$ be the set of all $\overline{\omega}$ with $\omega \in \Omega_E$, and let $K^0_{\overline{\omega}} = K^0_{\overline{x}}$ for $\overline{x} \in \overline{\omega}$.

Let us define $d_{\omega,\omega'}$ as being the number of times U_y occurs in

$$\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(U_x)$$

for $x \in \omega$, $y \in \omega'$.

Let us recall that for all $\omega, \omega' \in \Omega_k$ such that $K^0_{\overline{\omega}} = K^0_{\overline{\omega}'} = k$, we denote by $d_{\overline{\omega},\overline{\omega}'}$ the dimension of the k–vector space underlying the quadratic form $F_{\overline{\omega},\overline{\omega}'}$ (see §6).

Set

$$\Omega^0_E = \{\omega \in \Omega_E \mid\ K^0_{\overline{\omega}} = E\}$$

$$\overline{\Omega}^0_E = \{\overline{\omega} \in \overline{\Omega}_E \mid K^0_{\overline{\omega}} = E\}$$

$$\Omega^1_E = \{\omega \in \Omega^0_E \mid \omega\ \text{ orthogonal or symplectic}\}$$

$$\Omega_E^{1,o} = \{\omega \in \Omega_E^0 \mid \omega \ \text{ orthogonal}\}$$

$$\Omega_E^{1,s} = \{\omega \in \Omega_E^0 \mid \omega \ \text{ symplectic}\}$$

$$\Omega_E^{2} = \{\omega \in \Omega_E^0 \mid \omega \ \text{ unitary}\}$$

$$\overline{\Omega}_E^{2} = \{\overline{\omega} \in \overline{\Omega}_E^0 \mid \overline{\omega} \ \text{ unitary}\}$$

and

$$\delta_E^1 = \det_{\omega,\omega' \in \Omega_E^1}(d_{\omega,\omega'})$$

$$\delta_E^2 = \det_{\omega,\omega' \in \Omega_E^2}(d_{\omega,\omega'})$$

$$\overline{\delta}_E^2 = \det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}_E^2}(d_{\overline{\omega},\overline{\omega}'})$$

$$\delta_E^{1,o} = \det_{\omega,\omega' \in \Omega_E^{1,o}}(d_{\omega,\omega'})$$

$$\delta_E^{1,s} = \det_{\omega,\omega' \in \Omega_E^{1,s}}(d_{\omega,\omega'})$$

Let L/K be a quadratic extension, and let $\tau : L \to L$ be the non–trivial automorphism of L/K. Then τ acts on S'_L by $(\tau x)(s) = \tau(x(s))$ for all $s \in S$ and $x \in S'_L$. This induces an action of τ on Ω_L.

Proposition 8.1 *Let $\omega \in \Omega_L$. Then $\tau\omega = \omega$ if and only if there is a character $x \in S'_L$ with $x \in \omega$ such that $\tau x = x$.*

Proof. If there exists $x \in \omega$ such that $\tau x = x$, then we have $\tau\omega = \omega$. Conversely, suppose that $\omega \in \Omega_L$ is such that $\tau\omega = \omega$. If we had $\tau x \neq x$ for every $x \in \omega$, then $\sharp(\omega)$ would be even, contradicting lemma 6.1. This implies that there exists $x \in \omega$ with $\tau x = x$, hence the proposition is proved.

Note that τ acts on the center of $L[S]$, and that the action of τ on S'_L can be described in terms of this action. This leads to the following observation, which will be used in the sequel:

Lemma 8.2 *Let $x \in S'_L$ be an orthogonal or symplectic character such that $\tau x = x$. Let $L = K_x$. Then*

(i) There exists $x_0 \in S'_K$ such that $K_{x_0} = K$.

(ii) If x is orthogonal (resp. symplectic) then x_0 is orthogonal (resp. symplectic).

(iii) If x_0 is orthogonal, then $(x_0)_L = x$

(iv) If x_0 is symplectic, then $(x_0)_L = x$ or $(x_0)_L = 2x$.

Proof. For any field E, let us denote by $Z(E[S]))$ the center of $E[S]$.

The Galois automorphism $\tau : L \to L$ over K acts on $L[S]$, hence also on $Z(L[S])$. Then the subalgebra of $Z(L[S])$ fixed by τ is equal to $Z(K[S])$. The hypothesis implies that L is one of the factors in the decomposition of $Z(L[S])$. Note that the restriction of τ to the factor L in $Z(L[S])$ is non–trivial, and that the fixed field is equal to K. This corresponds to a factor in the decomposition of $K[S]$, and hence to a character x_0 of S'_K. This proves (i). Noting that the base change to L of the factor corresponding to x_0 in $K[S]$ is the factor corresponding to $(x_0)_L$, points (ii) and (iii) are immediate. Suppose now that x is symplectic. Then the same reasoning proves that if Δ_{x_0} is a quaternion division algebra and $\Delta_x = L$, then $(x_0)_L = 2x$; if both Δ_{x_0} and Δ_x are quaternion division algebras, or if $\Delta_{x_0} = K$ and $\Delta_x = L$, then $(x_0)_L = x$. This proves (iv).

Corollary 8.3 *Let $\omega \in \Omega^1_L$ be such that $\tau\omega = \omega$.*

(i) If $\omega \in \Omega^{1,o}_L$, there exists $\omega_0 \in \Omega^{1,o}_K$ such that $(\omega_0)_L = \omega$.

(ii) If $\omega \in \Omega^{1,s}_L$, then there exists $\omega_0 \in \Omega^{1,s}_K$ such that $(\omega_0)_L = \omega$ or $(\omega_0)_L = 2\omega$.

Proof. By prop. 8.1 we can choose $x \in \omega$ such that $\tau x = x$. Let $x_0 \in S'_K$ such that $K_{x_0} = K$ (see lemma 8.2 (i)). Hence we have $K_{(x_0)} \otimes_K L = L = K_x$.
(i) Suppose that $\omega \in \Omega^{1,o}_L$. Then x is orthogonal. Hence x_0 is orthogonal, and $(x_0)_L = x$ (cf. 8.2 (ii) and (iii)). Let ω_0 be the orbit of x_0; then $\omega_0 \in \Omega^{1,o}_K$ and $(\omega_0)_L = \omega$.
(ii) Suppose that $\omega \in \Omega^{1,s}_L$. Then x is symplectic. Hence x_0 is symplectic, and $(x_0)_L = x$ or $(x_0)_L = 2x$ (cf. 8.2 (ii) and (iv)). Let ω_0 be the orbit of x_0. Then $\omega_0 \in \Omega^{1,s}_K$ has the required property.

Proposition 8.4 *Suppose that*

$$\delta^{1,o}_L \equiv 1 \text{ (mod 2)}.$$

Then

$$\delta^{1,o}_K \equiv 1 \text{ (mod 2)}.$$

Proof. The automorphism τ of L/K induces a permutation of $\Omega^{1,o}_L$. Set

$$\Omega^{1,1}_L = \{\omega \in \Omega^{1,o}_L \mid \tau\omega = \omega\}$$

and

$$\Omega_L^{1,2} = \{\omega \in \Omega_L^{1,o} \mid \tau\omega \neq \omega\}.$$

Let S_L be the group of permutations of $\Omega_L^{1,o}$, and let S_L^1 respectively S_L^2 be the group of permutations of $\Omega_L^{1,1}$, respectively $\Omega_L^{1,2}$, regarded as subgroups of S_L. Set

$$\alpha = \Sigma_{s \in S_L^1} (\prod_{\omega \in \Omega_L^{1,1}} d_{s\omega,\omega}),$$

$$\beta = \Sigma_{s \in S_L^2} (\prod_{\omega \in \Omega_L^{1,2}} d_{s\omega,\omega}),$$

By lemma 4.3, we have

$$\delta_L^{1,o} \equiv \alpha\beta \pmod 2.$$

On the other hand, we have

$$\delta_K^{1,o} \equiv \alpha \pmod 2.$$

Indeed, by cor. 8.3 (i) the map $\omega_0 \mapsto (\omega_0)_L$ induces a bijection between $\Omega_K^{1,o}$ and $\Omega_L^{1,1}$ with $d_{\omega_0,\omega_0'} = d_{(\omega_0)_L,(\omega_0')_L}$ for $\omega_0, \omega_0' \in \Omega_K^{1,o}$. It follows that $\delta_K^{1,o} \equiv \alpha \pmod 2$. This completes the proof of the proposition.

Proposition 8.5 *Suppose that*

$$\delta_L^{1,s} \equiv 1 \pmod 2.$$

Then

$$\delta_K^{1,s} \equiv 1 \pmod 2.$$

Proof. The automorphism τ of L/K induces a permutation of $\Omega^{1,s}$. Let

$$\Omega_L^{1,1} = \{w \in \Omega_L^{1,s} \mid \tau\omega = \omega\},$$

$$\Omega_L^{1,2} = \{w \in \Omega_L^{1,s} \mid \tau\omega \neq \omega\}.$$

Let S_L be the group of permutations of $\Omega_L^{1,s}$, and let S_L^1 respectively S_L^2 be the group of permutations of $\Omega_L^{1,1}$, respectively $\Omega_L^{1,2}$, regarded as subgroups of S_L. Set

$$\alpha = \Sigma_{s \in S_L^1} (\prod_{\omega \in \Omega_L^{1,1}} d_{s\omega,\omega}),$$

$$\gamma = \Sigma_{s \in S_L^2} (\prod_{\omega \in \Omega_L^{1,2}} d_{s\omega,\omega}).$$

Arguing as in 8.4, we get

$$\delta_L^{1,s} \equiv \gamma\alpha \pmod 2.$$

Claim. We have

$$\delta_K^{1,s} \equiv \alpha \pmod 2.$$

Let us write

$$\Omega_L^{1,1} = \Omega_{L/K}^s \cup \Omega_{L/K}^{ns},$$

where

$$\Omega_{L/K}^s = \{\omega \in \Omega_L^{1,1} \mid \text{there exists } \omega_0 \in \Omega_K^{1,s} \text{ with } (\omega_0)_L = 2\omega\},$$

and

$$\Omega_{L/K}^{ns} = \{\omega \in \Omega_L^{1,1} \mid \text{there exists } \omega_0 \in \Omega_K^{1,s} \text{ with } (\omega_0)_L = \omega\}.$$

By corollary 8.3 (ii) the above is a disjoint union decomposition.

For $\omega \in \Omega_{L/K}^s$ with $2\omega = (\omega_0)_L$ and $\omega' \in \Omega_{L/K}^{ns}$ with $\omega' = (\omega_0')_L$, $\omega_0, \omega_0' \in \Omega_K$, we have:

If $d_{\omega_0',\omega_0} = r$, then $d_{\omega',\omega} = 2r$.

Thus the matrix $(d_{\omega,\omega'})_{\omega,\omega' \in \Omega_L^1}$ is congruent to the matrix

$$\begin{pmatrix} A & * \\ 0 & B \end{pmatrix}$$

where $A = (d_{\omega,\omega'})_{\omega,\omega' \in \Omega_{L/K}^s}$, and $B = (d_{\omega,\omega'})_{\omega,\omega' \in \Omega_{L/K}^{ns}}$. Therefore

$$\alpha \equiv \det(A)\det(B) \pmod 2.$$

We next determine $\delta_K^{1,s} \pmod 2$. Let us write

$$\Omega_K^{1,s} = \Omega_{K/L}^s \cup \Omega_{K/L}^{ns},$$

with

$$\Omega_{K/L}^s = \{\omega \in \Omega_K \mid \text{there exists } \omega_0 \in \Omega_L^{1,1} \text{ with } (\omega)_L = 2\omega_0\},$$

and

$$\Omega_{K/L}^{ns} = \{\omega \in \Omega_K \mid \text{there exists } \omega_0 \in \Omega_L^{1,1} \text{ with } (\omega)_L = \omega_0\}.$$

For $\omega, \omega' \in \Omega^s_{K/L}$, if $\omega_L = 2\omega_0$, $\omega'_L = 2\omega'_0$ for some $\omega_0, \omega'_0 \in \Omega^s_{L/K}$, we have $d_{\omega,\omega'} = d_{\omega_0,\omega'_0}$. Also, for $\omega, \omega' \in \Omega^{ns}_{K/L}$, if $\omega_L = \omega_0$, $\omega'_L = \omega'_0$ for some $\omega_0, \omega'_0 \in \Omega^{ns}_{L/K}$, we have $d_{\omega,\omega'} = d_{\omega_0,\omega'_0}$. Thus the matrix $(d_{\omega,\omega'})_{\omega,\omega' \in \Omega^s_{K/L}}$ is equal to A, and the matrix $(d_{\omega,\omega'})_{\omega,\omega' \in \Omega^{ns}_{K/L}}$ is equal to B. Further, if $\omega \in \Omega^s_{K/L}$, then $\omega_L = 2\omega_0$ for some $\omega_0 \in \Omega^{1,1}_L$, and if $\omega' \in \Omega^{ns}_{K/L}$, then $\omega'_L = \omega'_0$ for some $\omega'_0 \in \Omega^{1,1}_L$. If $d_{\omega_0,\omega'_0} = r$, then $d_{\omega,\omega'} = 2r$. Thus the matrix $(d_{\omega,\omega'})_{\omega,\omega' \in \Omega^{1,s}_K}$ is congruent to

$$\begin{pmatrix} A & 0 \\ * & B \end{pmatrix}.$$

mod 2. Therefore

$$\delta^{1,s}_K = \det(A)\det(B) \equiv \alpha \pmod 2,$$

and this completes the proof of the claim. Therefore we see that $\delta^{1,s}_L \equiv 1 \pmod 2$ implies $\delta^{1,s}_K \equiv 1 \pmod 2$, hence prop. 8.5 is proved.

Let us recall that for any field E of characteristic $\neq 2$, we denote by $\overline{S}'_E$ the set of $\overline{x}$ for $x \in S'_E$.

The Galois automorphism $\tau : L \to L$ over K induces an action on $\overline{S}'_L$ which we denote by $\overline{y} \mapsto \tau\overline{y}$.

Lemma 8.6 *Let $\overline{y} \in \overline{S}'_L$ with $\overline{y}$ unitary such that $\tau\overline{y} = \overline{y}$. Then there exists $\overline{x} \in \overline{S}'_K$ with $\overline{x}$ unitary such that $\overline{x}_L = \overline{y}$. Moreover, if $K^0_{\overline{y}} = L$, then $K^0_{\overline{x}} = K$.*

Proof. Suppose that $\overline{y} = y$ and $\tau y = y$. Then by the method of lemma 8.2 we see that there is a unitary character $x \in S'_K$ such that $x_L = y$. Moreover, τ restricts to a non–trivial automorphism of K_y which commutes with ι. If $E = (K_y)^\iota$, then $\tau|E$ is non–trivial and $K_x = E$. Since $K_{x_L} = EL = K_y$, we have $x_L = y$. Further, if $K^0_y = L$, then $K^0_x = K$.

Suppose that $\overline{y} = (y, \iota y)$ with $\iota y \neq y$ and $\tau\overline{y} = \overline{y}$. Then $\tau y = y$ or $\tau\iota y = y$. Set $M = K_y \times K_{\iota y}$.

Suppose first that $\tau y = y$. Then there is an $x \in S'_K$ such that $x_L = y$. Further, τ induces an automorphism on M which takes each factor K_y and $K_{\iota y}$ in itself. Moreover, we have $M^\tau = K_x \times K_{\iota x}$. Thus $\overline{x} = (x, \iota x) \in \overline{S}'_K$ is unitary with $\overline{x}_L = \overline{y}$. Moreover, if $K^0_y = M^\iota = L$, then $K^0_x = K$.

Suppose now that $\tau\iota y = y$. Then $\tau y = \iota y$, and τ switches the factors K_y and $K_{\iota y}$ of M. Let $E = M^\tau$. Then E is a field which is a factor of the center of $K[S]$ and ι restricted to E is non–trivial. Let $x \in S'_K$ be the character associated to E. Then x is unitary, $K_x = E$ and $K_{x_L} = EL = M = K_y \times K_{\iota y}$. Thus $x_L = (y, \iota y)$. Further, if $K^0_{\overline{y}} = M^\iota = L$, then $K^0_{\overline{x}} = E^\iota = K$, where $\overline{x} = x$.

The automorphism τ induces an action on $\overline{\Omega}^2_L$ that we denote by $\overline{\omega} \mapsto \tau\overline{\omega}$.

Corollary 8.7 *Let $\overline{\omega} \in \overline{\Omega}^2_L$ be a unitary orbit with $\tau\overline{\omega} = \overline{\omega}$. Then there is a unitary orbit $\overline{\omega}_0 \in \overline{\Omega}^2_K$ such that $(\overline{\omega}_0)_L = \overline{\omega}$.*

Proof. Suppose that $\overline{\omega} = \omega$ and $\tau\omega = \omega$. By proposition 8.1, there is a character $y \in S'_L$ belonging to ω with $\tau y = y$. In this case, the proposition follows from lemma 8.6.

Suppose that $\overline{\omega} = (\omega, \iota\omega)$ with $\iota\omega \neq \omega$. Then $\tau\overline{\omega} = \overline{\omega}$ implies that $\tau\omega = \omega$ or $\tau\iota\omega = \omega$.

Suppose first that $\tau\omega = \omega$. Then by proposition 8.1 there is a $y \in \omega$ such that $\tau y = y$. Further, $\overline{y} = (y, \iota y)$ is unitary with $\tau\overline{y} = \overline{y}$. In this case, we appeal to lemma 8.6 to conclude the proof.

Suppose now that $\tau\iota\omega = \omega$ and that $\tau\omega \neq \omega$. Then $\tau\iota$ induces an action on the characters in ω. As $\sharp\omega$ is odd by lemma 6.1, there exists $y \in \omega$ such that $\tau\iota y = y$ and $\tau y \neq y$, since $\tau\omega \neq \omega$. Then $\overline{y} = (y, \iota y)$ is a unitary pair with $\tau\overline{y} = \overline{y}$ and the proposition follows from lemma 8.6.

Proposition 8.8 *If* $\det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}^2_L}(d_{\overline{\omega},\overline{\omega}'}) \equiv 1 \pmod 2$, *then* $\det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}^2_K}(d_{\overline{\omega},\overline{\omega}'}) \equiv 1 \pmod 2$.

Proof. Recall that $\tau : L \to L$ is the non–trivial automorphism of L/K. Let us write $\overline{\Omega}^2_L = \Omega^{2,1}_L \cup \Omega^{2,2}_L$, where

$$\Omega^{2,1}_L = \{\overline{\omega} \in \overline{\Omega}_L \ | \tau\overline{\omega} = \overline{\omega}\},$$

and

$$\Omega^{2,2}_L = \{\overline{\omega} \in \overline{\Omega}_L \ | \tau\overline{\omega} \neq \overline{\omega}\}.$$

Arguing as in 8.4 and using 4.3, we get

$$\det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}^2_L}(d_{\overline{\omega},\overline{\omega}'}) = [\det_{\overline{\omega},\overline{\omega}' \in \Omega^{2,1}_L}(d_{\overline{\omega},\overline{\omega}'})][\det_{\overline{\omega},\overline{\omega}' \in \Omega^{2,2}_L}(d_{\overline{\omega},\overline{\omega}'})].$$

Note that scalar extension induces a bijection between $\overline{\Omega}^2_K$ and $\Omega^{2,1}_L$, and we have $d_{\overline{\omega},\overline{\omega}'} = d_{\overline{\omega}_L,\overline{\omega}'_L}$ for $\overline{\omega}, \overline{\omega}' \in \overline{\Omega}^2_K$. This proves the proposition.

§9. A filtration

Let k be a field of characteristic $\neq 2$, let G be a finite group and let S be a 2–Sylow subgroup of G. In this section, we introduce a quadratic filtration of the field k that will be needed in the next two sections.

Let κ be the prime field of k, that is, $\kappa = Q$ if $\mathrm{char}(k) = 0$ and $\kappa = F_p$ if $\mathrm{char}(k) = p > 0$. Note that $k[S] = \kappa[S] \otimes_\kappa k$, hence it is interesting to investigate the structure of $\kappa[S]$ in both cases.

Suppose first that $\kappa = Q$. We have the following lemma:

Lemma 9.1 *Let S be a 2–group, and let $Q[S] = \prod_{i=1,\dots,r} M_{n_i}(D_i)$ where the D_i's are division algebras, and let $Z(D_i) = K_i$. Let $\iota : Q[S] \to Q[S]$ be the standard involution. Then each component of $Q[S]$ is invariant under ι. Let us denote by K_i^0 the invariant subfield of K_i under the restriction of ι to K_i. Then there exists $m \in N$ such that K_i^0 is a subfield of the real 2–cyclotomic subfield $Q(\zeta_{2^m} + \zeta_{2^m}^{-1})$.*

Proof. The fact that each component of $Q[S]$ is invariant under ι follows from [6], Chap. 8, 13.2. We know that as S is a 2–group, there exists $m \in N$ such that for all $i = 1, \dots, r$ the field K_i is a subfield of the cyclotomic field $Q(\zeta_{2^m})$. The standard involution $\iota : Q[S] \to Q[S]$ is positive definite, hence its restriction to each component is positive definite as well. This implies (cf [6], Chap 8, 13.5) that $K_i^0 \subset R$ for all i. Hence for all $i = 1, \dots, r$, we have $K_i^0 \subset Q(\zeta_{2^m} + \zeta_{2^m}^{-1})$ as claimed.

With the notation of lemma 9.1, let $L = Q(\zeta_{2^m} + \zeta_{2^m}^{-1})$. Since L/Q is cyclic of degree a power of 2, it has a unique set of subfields which fit into a filtration

$$L_0 = Q \subset L_1 \subset L_2 \subset \dots \subset L_s = L$$

with all inclusions being strict, and L_i/L_{i-1} of degree 2.

Suppose now that $\kappa = F_p$ for some prime number p. We have

$$F_p[S] = \prod_{i=1,\dots,r} M_{n_i}(K_i)$$

where the K_i's are finite degree extensions of F_p. As S is a 2–group, the degrees of these extensions are powers of 2. There exists a finite extension L/F_p of degree a power of 2 containing all the K_i^0's. Note that as F_p is a finite field, the extension L/F_p is cyclic. Hence in this case too, we have a unique set of subfields of L which fit into a filtration

$$L_0 = Q \subset L_1 \subset L_2 \subset \dots \subset L_s = L$$

with all inclusions being strict, and L_i/L_{i-1} of degree 2.

Let

$$k_0 = k \subset k_1 \subset k_2 \subset \dots \subset k_t = Lk$$

be the induced strict filtration of Lk/k. Note that every subfield of Lk containing k is one of the fields k_i. Let k_r be the smallest of these fields containing $K^0_{\overline{x}}$ for all $\overline{x} \in S'_k$.

§10. The odd determinant property revisited

For any field E, set

$$\overline{\delta}_E^{1,o} = \det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}_E^{1,o}}(d_{\overline{\omega},\overline{\omega}'})$$

$$\overline{\delta}_E^{1,s} = \det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}_E^{1,s}}(d_{\overline{\omega},\overline{\omega}'})$$

$$\overline{\delta}_E^{2} = \det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}_E^{2}}(d_{\overline{\omega},\overline{\omega}'})$$

$$d_E^0 = \det_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}_E^{0}}(d_{\overline{\omega},\overline{\omega}'}).$$

The result below will be instrumental in the proof of th. 2.2 in the next section:

Theorem 10.1 *Let G be a finite group having the odd determinant property. Then for any field K of characteristic not 2, we have*

$$d_K^0 \equiv \quad 1 \pmod 2.$$

Proof. We first treat the case where all the characters in S'_K are absolutely irreducible. The reduction to this case is via the filtration introduced in §9, and the quadratic descent of §8.

Suppose first that all the characters in S'_K are absolutely irreducible. For $x \in S'_K$, the form $\rho_{\overline{x}}$ is supported on U_x if x is orthogonal, on $U_x \oplus U_x$ if x is symplectic, and $U_{x_1} \oplus U_{x_2}$ if $\overline{x} = (x_1, x_2)$ with $\iota(x_1) = x_2$ and $x_1 \neq x_2$. Noting that for a general K, the integers $d_{\overline{\omega},\overline{\omega}'}$ can be computed after base changing to an algebraic closure of K, we get the following:

1) $d_{\overline{\omega},\overline{\omega}'} = d_{\omega,\omega'}$ if $\omega, \omega' \in \Omega_K^{1,s}$;

2) $d_{\overline{\omega},\overline{\omega}'} = 2d_{\omega,\omega'}$ if ω is symplectic and ω' is not symplectic;

3) $d_{\overline{\omega},\overline{\omega}'} = 2d_{\omega,\omega'}$ if ω is unitary and ω' is orthogonal;

4) $d_{\overline{\omega},\overline{\omega}'} = d_{\omega,\omega'}$ if ω, ω' are orthogonal.

Thus the matrix $(d_{\overline{\omega},\overline{\omega}'})_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}_K^0}$ has the following shape modulo 2

$$\begin{pmatrix} A & * & * \\ 0 & B & * \\ 0 & 0 & C \end{pmatrix},$$

where

$$A = (d_{\overline{\omega},\overline{\omega}'})_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}^{1,o}_K}$$

$$B = (d_{\overline{\omega},\overline{\omega}'})_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}^{2}_K}$$

$$C = (d_{\overline{\omega},\overline{\omega}'})_{\overline{\omega},\overline{\omega}' \in \overline{\Omega}^{1,s}_K}.$$

Thus $d^0_K \equiv 1 \pmod 2$ if and only if $\overline{\delta}^{1,0}_K = \det(A) \equiv 1 \pmod 2$, $\overline{\delta}^{1,s}_K = \det(C) \equiv 1 \pmod 2$, and $\overline{\delta}^{2}_K = \det(B) \equiv 1 \pmod 2$. We also note that for $\omega, \omega' \in \Omega^{1,o}_K$, or for $\omega, \omega' \in \Omega^{1,s}_K$, we have $d_{\overline{\omega},\overline{\omega}'} = d_{\omega,\omega'}$. Therefore $\overline{\delta}^{1,o}_K = \delta^{1,o}_K$, and $\overline{\delta}^{1,s}_K = \delta^{1,s}_K$. Thus $d^0_K \equiv 1 \pmod 2$ if and only if $\delta^{1,o}_K \equiv 1 \pmod 2$, $\delta^{1,s}_K \equiv 1 \pmod 2$, and $\overline{\delta}^{2}_K \equiv 1 \pmod 2$.

There exists a field extension L/K and a filtration by quadratic extensions

$$K \subset K_2 \subset \ldots \subset K_n = L$$

such that all characters in S'_L are absolutely irreducible (cf. §9). By prop. 7.2 and 7.3, we have $\delta^{1,o}_L \equiv 1 \pmod 2$, $\delta^{1,s}_L \equiv 1 \pmod 2$, and $\overline{\delta}^{2}_L \equiv 1 \pmod 2$. By the quadratic descent results 8.4, 8.5 and 8.8, we get $\overline{\delta}^{1,0}_K = \det(A) \equiv 1 \pmod 2$, $\overline{\delta}^{1,s}_K = \det(C) \equiv 1 \pmod 2$, and $\overline{\delta}^{2}_K = \det(B) \equiv 1 \pmod 2$. Therefore $d^0_K \equiv 1 \pmod 2$.

§11. Proof of the induction–restriction result

The aim of this section is to prove th. 2.2. Let

$$k_0 = k \subset k_1 \subset k_2 \subset \ldots \subset k_r$$

be the filtration introduced in §9, k_r being the smallest of these fields containing $K^0_{\overline{x}}$ for all $\overline{x}$.

Proof of theorem 2.2 Let (V, h) be an S–quadratic form. We have a decomposition (cf. §5)

$$(V, h) \simeq \bigoplus_{\overline{x}} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V_{\overline{x}}, g_{\overline{x}}),$$

where $(V_{\overline{x}}, g_{\overline{x}})$ is a quadratic form over $K^0_{\overline{x}}$ (cf. §5). Recall that the Witt class

$$(V_{\overline{x}}, g_{\overline{x}}) \otimes n_{\overline{x}} \in W(K^0_{\overline{x}})$$

is uniquely determined by (V,h), where $n_{\overline{x}}$ is the reduced norm of $D_{\overline{x}}$ over $K^0_{\overline{x}}$ if $D_{\overline{x}}$ is a quaternion algebra, the norm of $K_{\overline{x}}$ over $K^0_{\overline{x}}$ if $K_{\overline{x}}$ is a quadratic algebra, and $n_{\overline{x}} = 1$ otherwise. We have

$$\mathrm{Ind}_S^G(V,h) = \bigoplus_{\overline{\varpi} \in \overline{\Omega}} I(\overline{\varpi}) \otimes_{K^0_{\overline{\varpi}}} (V_{\overline{\varpi}}, g_{\overline{\varpi}}),$$

where

$$(V_{\overline{\varpi}}, g_{\overline{\varpi}}) = \bigoplus_{\overline{x} \in \overline{w}} (V_{\overline{x}}, g_{\overline{x}})$$

is a quadratic space determined up to multiplication by $n_{\overline{\varpi}} = n_{\overline{x}}$. We have $I(\overline{\varpi}) = \mathrm{Ind}_S^G(\rho_{\overline{x}})$, which does not depend on the choice of $\overline{x} \in \overline{\varpi}$.

We have

$$\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(V,h) = \bigoplus_{\overline{\varpi} \in \overline{\Omega}} \mathrm{Res}_S^G(I(\overline{\varpi})) \otimes_{K^0_{\overline{\varpi}}} (V_{\overline{\varpi}}, g_{\overline{\varpi}}).$$

For $\overline{y} \in \overline{S}'_k$, the $\overline{y}$–component of $\mathrm{Res}_S^G(I_{\overline{\varpi}})$ is $\rho_{\overline{y}} \otimes_{K^0_{\overline{\varpi}'}} F_{\overline{\varpi},\overline{\varpi}'}$, where $\overline{y} \in \overline{\varpi}'$, and where $F_{\overline{\varpi},\overline{\varpi}'}$ is a quadratic space over $K^0_{\overline{\varpi}'}$, determined up to multiplication by $n_{\overline{\varpi}'}$.

Let (V_1, h_1) and (V_2, h_2) be two S–quadratic forms such that

$$\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(V_1,h_1) \simeq_S \mathrm{Res}_S^G\ \mathrm{Ind}_S^G(V_2,h_2).$$

Let

$$(V_1,h_1) \simeq \bigoplus_{\overline{x} \in \overline{S}'} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V^1_{\overline{x}}, g^1_{\overline{x}}) \quad \text{and} \quad (V_2,h_2) \simeq \bigoplus_{\overline{x} \in \overline{S}'} \rho_{\overline{x}} \otimes_{K^0_{\overline{x}}} (V^2_{\overline{x}}, g^2_{\overline{x}})$$

and

$$(V^i_{\overline{\varpi}}, g^i_{\overline{\varpi}}) = \bigoplus_{\overline{x} \in \overline{w}} (V^i_{\overline{x}}, g^i_{\overline{x}})$$

for $i = 1, 2$.

Note that as the $k[S]$–modules $\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(V_1)$ and $\mathrm{Res}_S^G\ \mathrm{Ind}_S^G(V_2)$ are isomorphic, the $k[G]$–modules $\mathrm{Ind}_S^G(V_1)$ and $\mathrm{Ind}_S^G(V_2)$ are also isomorphic (see for instance [3], cor. 6.8). This implies that $\dim(V^1_{\overline{\varpi}}) = \dim(V^i_{\overline{\varpi}})$ for all $\overline{\varpi} \in \overline{\Omega}$.

Claim. We have

$$n_{\overline{\varpi}} \otimes_k (V^1_{\overline{\varpi}}, g^1_{\overline{\varpi}}) \simeq n_{\overline{\varpi}} \otimes_k (V^2_{\overline{\varpi}}, g^2_{\overline{\varpi}}).$$

For the proof, we distinguish two cases

Case 1. Suppose that $K^0_{\overline{x}} = k$ for all $\overline{x} \in S'_k$.

Then we have $\mathrm{Res}^G_S(I(\overline{\omega}))_{\overline{y}} = \rho_{\overline{y}} \otimes_k F_{\overline{\omega},\overline{\omega}'}$, where $\overline{y} \in \overline{\omega}'$, where $F_{\overline{\omega},\overline{\omega}'}$ is a quadratic form over k, and $n_{\overline{\omega}'} \otimes_k F_{\overline{\omega},\overline{\omega}'}$ is determined by $\mathrm{Res}^G_S(I(\overline{\omega}))_{\overline{y}}$. Hence

$$\mathrm{Res}^G_S \ \mathrm{Ind}^G_S(V_i, h_i) = \bigoplus_{\overline{y} \in \overline{S}'_k} \rho_{\overline{y}} \otimes_k [\bigoplus_{\overline{\omega} \in \overline{\Omega}_k} F_{\overline{\omega},\overline{\omega}'} \otimes_k (V^i_{\overline{\omega}}, g^i_{\overline{\omega}})]$$

Suppose that $\mathrm{Res}^G_S \ \mathrm{Ind}^G_S(V_1, h_1) \simeq \mathrm{Res}^G_S \ \mathrm{Ind}^G_S(V_2, h_2)$, and set $g^i_{\overline{\omega}} = (V^i_{\overline{\omega}}, g^i_{\overline{\omega}})$ for $i = 1, 2$. Then

$$n_{\overline{\omega}'} \otimes_k [\bigoplus_{\overline{\omega} \in \overline{\Omega}} F_{\overline{\omega},\overline{\omega}'} \otimes_k g^1_{\overline{\omega}}] \simeq n_{\overline{\omega}'} \otimes_k [\bigoplus_{\overline{\omega} \in \overline{\Omega}} F_{\overline{\omega},\overline{\omega}'} \otimes_k g^2_{\overline{\omega}}].$$

Let us denote by $f_{\overline{\omega},\overline{\omega}'}$ the element of $W(k)$ determined by the quadratic form $F_{\overline{\omega},\overline{\omega}'}$, and let $(\tilde{f}_{\overline{\omega},\overline{\omega}'})$ be the matrix of cofactors of the matrix $(f_{\overline{\omega},\overline{\omega}'})$ in the Witt ring $W(k)$. Then the product $(\tilde{f}_{\overline{\omega},\overline{\omega}'})(n_{\overline{\omega}'} \otimes_k f_{\overline{\omega},\overline{\omega}'})$ is equal to

$$\varphi \begin{pmatrix} n_{\overline{\omega}_1} & 0 & \dots & 0 \\ 0 & n_{\overline{\omega}_2} & \dots & 0 \\ 0 & \dots & \dots & n_{\overline{\omega}_n} \end{pmatrix},$$

a diagonal matrix with diagonal entries $\varphi.n_{\overline{\omega}_j}$, where $\varphi \in W(k)$ is the determinant of the matrix $(f_{\overline{\omega},\overline{\omega}'})$. Let $v^i_{\overline{\omega}}$ be the element of $W(k)$ determined by the quadratic form $g^i_{\overline{\omega}} = (V^i_{\overline{\omega}}, g^i_{\overline{\omega}})$ for $i = 1, 2$. Then we get

$$\varphi.n_{\overline{\omega}} \otimes_k (v^1_{\overline{\omega}} - v^2_{\overline{\omega}}) = 0$$

in $W(k)$, for every $\overline{\omega} \in \overline{\Omega}$.

Note that $\det(\dim((f_{\overline{\omega},\overline{\omega}'})) = \dim(\det((f_{\overline{\omega},\overline{\omega}'}))$, and that

$$\det(\dim((f_{\overline{\omega},\overline{\omega}'})) = \det(d_{\overline{\omega},\overline{\omega}'}) = d^0_k.$$

Since G has the odd determinant property, by prop. 10.1 we have $d^0_k \equiv 1 \pmod 2$. Therefore $\dim(\varphi)$ is odd, hence φ is not a zero divisor in $W(k)$ (see for instance [6], 2.6.5). Therefore we have

$$n_{\overline{\omega}} \otimes_k (v^1_{\overline{\omega}} - v^2_{\overline{\omega}}) = 0$$

in $W(k)$, for all $\overline{\omega} \in \overline{\Omega}$, and hence $n_{\overline{\omega}} \otimes_k (V^1_{\overline{\omega}}, g^1_{\overline{\omega}})$ and $n_{\overline{\omega}} \otimes_k (V^2_{\overline{\omega}}, g^2_{\overline{\omega}})$ are in the same Witt class. Recall that $\dim(V^1_{\overline{\omega}}) = \dim(V^2_{\overline{\omega}})$ for all $\overline{\omega} \in \overline{\Omega}$. Hence the quadratic forms $n_{\overline{\omega}} \otimes_k (V^1_{\overline{\omega}}, g^1_{\overline{\omega}})$ and $n_{\overline{\omega}} \otimes_k (V^2_{\overline{\omega}}, g^2_{\overline{\omega}})$ have the same dimension and are in the same Witt class, therefore we have

$$n_{\overline{\varpi}} \otimes_k (V^1_{\overline{\varpi}}, g^1_{\overline{\varpi}}) \simeq n_{\overline{\varpi}} \otimes_k (V^2_{\overline{\varpi}}, g^2_{\overline{\varpi}})$$

for all $\overline{\varpi} \in \overline{\Omega}$. This completes the proof of the claim in case 1.

General case. Let us consider $(V_i, h_i) \otimes_k k_r$. We have

$$\mathrm{Res}^G_S \ \mathrm{Ind}^G_S(V_1, h_1) \otimes_k k_r \simeq_S \mathrm{Res}^G_S \ \mathrm{Ind}^G_S(V_2, h_2) \otimes_k k_r.$$

Moreover, $K^0_{\overline{\varpi}} \otimes_k k_r \simeq \prod_{\alpha \in \mathrm{Gal}(K^0_{\overline{\varpi}}/k)} k_r^\alpha$. The orbit $\overline{\varpi}$ splits into distinct conjugate orbits over k_r. Each $\overline{\varpi} \in \overline{\Omega}_k$ with $K^0_{\overline{\varpi}} = k_r$ occurs as one of the conjugate orbits over k_r. Using case 1, we get, for orbits $\overline{\varpi}$ with $K^0_{\overline{\varpi}} = k_r$,

$$n_{\overline{\varpi}} \otimes (V^1_{\overline{\varpi}}, g^1_{\overline{\varpi}}) \simeq n_{\overline{\varpi}} \otimes (V^2_{\overline{\varpi}}, g^2_{\overline{\varpi}}).$$

Cancelling these factors, we may assume that

$$\mathrm{Ind}^G_S(V, h) = \bigoplus_{\overline{\varpi} \in \overline{\Omega}} I(\overline{\varpi}) \otimes_{K^0_{\overline{\varpi}}} (V_{\overline{\varpi}}, g_{\overline{\varpi}})$$

with $K^0_{\overline{\varpi}} \subset k_{r-1}$ for all $\overline{\varpi}$ in the above decomposition. Inductively we get, for all $\overline{\varpi}$, that

$$n_{\overline{\varpi}} \otimes (V^1_{\overline{\varpi}}, g^1_{\overline{\varpi}}) \simeq n_{\overline{\varpi}} \otimes (V^2_{\overline{\varpi}}, g^2_{\overline{\varpi}}).$$

This completes the proof of the theorem.

Bibliography

[1] E. Bayer–Fluckiger and H.W. Lenstra, Jr., Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* 112 (1990), 359-373.

[2] E. Bayer–Fluckiger and J–P. Serre, Torsions quadratiques et bases normales autoduales, *Amer. J. Math.* 116 (1994) 1–64.

[3] D.J. Benson, R.A. Parker, The Green ring of a finite group, *J. Algebra* 87 (1984), 290-331.

[4] E. Lequeu, Hermitian G-Forms and Induction, in preparation.

[5] J. Morales, Integral bilinear forms with a group action, *J. Algebra* 98 (1986), 470 - 484.

[6] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss, Springer–Verlag (1985).

[7] J–P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, Vol. 42. Springer-Verlag (1977).

[8] J. Thévenaz, Most finite groups are p-nilpotent. *Exposition. Math.* 11 (1993), 359 - 363.

E. Bayer–Fluckiger
École Polytechnique
Fédérale de Lausanne
Epfl/Fsb/Mathgeom/Csag
Station 8
1015 Lausanne, Switzerland
eva.bayer@epfl.ch

R. Parimala
Department of Mathematics
& Computer Science
Emory University
Atlanta, GA 30322, USA.
parimala@mathcs.emory.edu