Illinois Journal of Mathematics
Volume 58, Number 2, Summer 2014, Pages 413–442
S 0019-2082

HOPF ALGEBRAS AND QUADRATIC FORMS

P. CASSOU-NOGUÈS, T. CHINBURG, B. MORIN AND M. J. TAYLOR

Abstract. Following Serre's initial work, a number of authors have considered twists of quadratic forms on a scheme Y by torsors of a finite group G, together with formulas for the Hasse–Witt invariants of the twisted form. In this paper, we take the base scheme Y to be affine and consider non-constant group schemes G. Our main result describes these twists by a simple and explicit formula. There is a fundamental new feature in this case—in that the torsor may now be ramified over Y. The natural framework for handling the case of a non-constant group scheme over the affine base is provided by the quadratic theory of Hopf-algebras.

1. Introduction

Let Y denote a scheme in which 2 is invertible. Recall that a symmetric bundle (V,q) on Y is an O_Y-vector bundle V endowed with a symmetric morphism of O_Y-modules

$$q : V \otimes_{\mathcal{O}_Y} V \to \mathcal{O}_Y$$

inducing an isomorphism between V and its dual $V^\vee$. For any integer n, we let $(\mathcal{O}_Y^n, t_n = x_1^2 + \cdots + x_n^2)$ denote the sum of squares form of rank n on Y.

An isometry of symmetric bundles $u : (V,q) \to (W,r)$ on Y is an isomorphism of vector bundles $u : V \to W$ such that $r(u(x),u(y)) = q(x,y)$ for any open affine subscheme U of Y and any x and y in $V(U)$. We denote by $\operatorname{Isom}(q,r)$ this set. The functor

$$\mathbf{Isom}(q,r) : T \to \operatorname{Isom}(q_T, r_T)$$

Received October 17, 2013; received in final form January 29, 2015.
Supported by NSF Grant #DMS0801030.
2010 *Mathematics Subject Classification.* 11E81, 16W30.

is a sheaf of sets on $\mathbf{Sch}/Y$, endowed with the fppf-topology. We let Y_{fl} denote the category of such sheaves. We define the orthogonal group of $\mathbf{O}(q)$ as the group $\mathbf{Isom}(q,q)$ of Y_{fl}. We set $\mathbf{O}(n)=\mathbf{O}(t_n)$. Suppose that q is of rank n, then $\mathbf{Isom}(t_n,q)$ supports a right $\mathbf{O}(n)$-action which endows it with the structure of an $\mathbf{O}(n)$-torsor. Let $\mathbf{Quad}_n(Y)$ be the category whose objects are symmetric bundles of rank n over Y and whose morphisms are isometries. Then the canonical functor

$$\begin{gathered}\mathbf{Quad}_n(Y)\to\mathbf{Tors}\big(Y_{fl},\mathbf{O}(n)\big)^{op},\\ q\to\mathbf{Isom}(t_n,q)\end{gathered}\tag{1}$$

is an equivalence of categories.

For a group H of Y_{fl}, we write B_H for the topos of objects of Y_{fl} endowed with a left action of H. By a result due to Grothendieck and Giraud we know that for any topos over Y_{fl}, $f:\mathcal{E}\to Y_{fl}$, there is a canonical equivalence

$$\mathbf{Homtop}_{Y_{fl}}(\mathcal{E},B_H)\simeq\mathbf{Tors}\big(\mathcal{E},f^*(H)\big)^{op},\tag{2}$$

where $\mathbf{Homtop}_{Y_{fl}}(\mathcal{E},B_H)$ denotes the category of morphisms of Y_{fl}-topoi from $\mathcal{E}$ to B_H and where $\mathbf{Tors}(\mathcal{E},f^*(H))$ is the category of $f^*(H)$-torsors of $\mathcal{E}$ (see [CCMT], Theorem 2.2 for instance). It follows from (1) and (2), in the particular case where $\mathcal{E}=Y_{fl}$ and $H=\mathbf{O}(n)$, that we have a canonical equivalence

$$\begin{gathered}\mathbf{Quad}_n(Y)\to\mathbf{Homtop}_{Y_{fl}}(Y_{fl},B_{\mathbf{O}(n)})^{op},\\ q\to\{q\}.\end{gathered}\tag{3}$$

Suppose now that we are additionally given a finite flat group scheme G over Y together with a homomorphism of Y_{fl}-group schemes $\rho: G\to\mathbf{O}(q)$. This then yields a map of topoi $B(\rho): B_G\to B_{\mathbf{O}(q)}$. If $X\to Y$ is a G-torsor then by (2) applied to $H=G$ and $\mathcal{E}=Y_{fl}$ we obtain a morphism $Y_{fl}\to B_G$. Moreover, by observing that $\mathbf{Isom}(t_n,q)$, endowed with the left action of $\mathbf{O}(q)$, is an $\mathbf{O}(n)$-torsor of $B_{\mathbf{O}(q)}$, we once again obtain via (2) a morphism $T_q: B_{\mathbf{O}(q)}\to B_{\mathbf{O}(n)}$. The new form which corresponds via (3) to the composite

$$Y_{fl}\to B_G\to B_{\mathbf{O}(q)}\to B_{\mathbf{O}(n)}$$

is referred to as *the twist of* q *by the torsor* X and is denoted q_X (see [CCMT] for the precise definitions). Using the above theoretical approach, one can attach to any symmetric bundle q Hasse–Witt invariants in the étale cohomology groups $H^i_{et}(Y,\mathbf{Z}/2\mathbf{Z})$. In [CCMT], Section 4, we describe a universal formula relating the Hasse–Witt invariants of q to those of the twist q_X.

The use of classifying topoi to study invariants of symmetric bundles provides us with tools to produce results at a high level of generality. In this paper, we focus on the affine case, when $Y=\operatorname{Spec}(R)$ and $G=\operatorname{Spec}(A)$, where A carries the natural structure of a finite and flat R-Hopf algebra. In this case, a symmetric bundle is given by a locally free R-module V, of finite rank, endowed with a nondegenerate quadratic form q. The group scheme homomorphism $\rho : G \to \mathbf{O}(q)$ may be viewed as providing (V, q) with the structure of an A-equivariant quadratic module, where V is an A-comodule and q is an A-equivariant form (Section 2.2). Our goal is to describe the twist (V_X, q_X), constructed above, by a simple explicit formula in terms of quadratic Hopf theory. We may write the G-torsor $X = \mathrm{Spec}(B)$, so that B may be viewed as a principal homogeneous space for A. Under certain mild hypotheses on G (see Section 3.2, hypothesis $\mathbf{H}$), we will show in Section 3 and Theorem 4.1.

Theorem 1.1. *Suppose that $G = \mathrm{Spec}(A)$ is a group scheme over $\mathrm{Spec}(R)$ which satisfies $\mathbf{H}$. Then:*

(1) *The inverse different $D_{B/R}^{-1}$ admits a square root, $D_{B/R}^{-1/2}$ say, which, when endowed with the trace form $\mathrm{Tr}_{B/R}$, forms a quadratic module.*

(2) *The tensor product $(D_{B/R}^{-1/2} \otimes V, \mathrm{Tr}_{B/R} \otimes q)$ is an A-equivariant quadratic module.*

(3) *There exists an isomorphism of quadratic modules*

$$(V_X, q_X) \cong \left(D_{B/R}^{-1/2} \otimes V, \mathrm{Tr}_{B/R} \otimes q\right)^A,$$

where $(D_{B/R}^{-1/2} \otimes V, \mathrm{Tr}_{B/R} \otimes q)^A$ is the submodule of fixed points by A.

Finally suppose that G is a constant group scheme and suppose initially that R is a field; in this case our results yield the well-known twisting formulas of Serre and Fröhlich, [Se1], [F]. Twisting formulas for more general base rings R are given in [CNET] and again our work enables us to recoup these results by appropriate specializations of the universal twisting formula of [CCMT].

The article then concludes by considering some examples. We begin by extending some well-known results for fields with group action to our situation where a group scheme acts on an affine scheme. In particular, we show that for any principal homogeneous space B for the Hopf algebra A, the quadratic module $(D_{B/R}^{-1/2}, \mathrm{Tr}_{B/R})$ is the twist by B of a standard A-equivariant form of A^D (referred to in the text as the unit form). In the last example, we study in detail the twists of the underlying quadratic form of an orthogonal representation of a non-constant group scheme which is generically of dihedral type. We observe that the quadratic forms we obtain by this process are not in general isometric to the form we start with.

2. Symmetric bundles and fixed points

The goal of this section is to describe how we can associate to any symmetric bundle, equivariant under the action of a finite and flat Hopf algebra, a new symmetric bundle by taking *fixed points*. Prior to describing this procedure in Proposition 2.7 of Section 2.2, in the first subsection we have assembled the main notation of the paper together with some elementary algebraic results on Hopf algebras that we will use later on.

2.1. Algebraic preliminaries. Let R be a commutative noetherian integral domain in which 2 is invertible, with field of fractions K. We consider a finite, locally free R-Hopf algebra A and we denote by A^D the dual algebra. We set $A_K = A \otimes_R K$, $A_K^D = A^D \otimes_R K$ and we identify A_K^D with the dual of A_K. We let Δ, ε and S (resp. Δ^D, ε^D and S^D) be respectively the comultiplication, the counit and the antipode of A (resp. A^D). We assume that $S^2 = I_A$, which implies that $(S^D)^2 = I_{A^D}$. This last condition is fulfilled when A is commutative or cocommutative ([C], Proposition 1.11). A right A-comodule M is a finitely generated, locally free R-module, endowed with an R-module homomorphism (the structure map),

$$\begin{aligned} \alpha_M : M &\to M \otimes_R A, \\ m &\mapsto \sum_{(m)} m_{(0)} \otimes m_{(1)}, \end{aligned}$$

such that $(\alpha_M \otimes 1)\alpha_M = (1 \otimes \Delta)\alpha_M$ (coassociativity) and $(1 \otimes \varepsilon)\alpha_M = id : M \to M \otimes A \to M \otimes_R R \simeq M$ (counitary). Define the R-linear map

$$\begin{aligned} \psi_M : A^D \otimes_R M &\to M, \\ g \otimes m &\mapsto \sum_{m} \langle g, m_{(1)} \rangle m_{(0)}. \end{aligned}$$

One can prove that ψ_M defines a left A^D-module structure on M. Moreover, by Proposition 1.3 in [CEPT], the association $(M, \alpha_M) \to (M, \psi_M)$ gives a bijective correspondence between the A-comodule and the A^D-module structures on a R-module M. For any A-comodule M we define the R-submodule

$$M^A = \{ m \in M \mid \alpha_M(m) = m \otimes 1 \}.$$

Lemma 2.1. *For any A-comodule M, then*

$$M^A = \{ m \in M \mid gm = g(1_A)m \ \forall g \in A^D \}.$$

Proof. Let M' denote the right-hand side of the above the equality. The inclusion $M^A \subset M'$ is immediate. We now use the fact that the map

$$\varphi : A \otimes_R A^D \to \mathrm{Hom}_R(A, A),$$

with $\varphi(h \otimes f)(a) = \langle f, a \rangle h$ is an isomorphism. Therefore, there exist elements $\{h_1, \ldots, h_n\}$ of A and $\{f_1, \ldots, f_n\}$ of A^D such that

$$Id = \sum_{1 \leq i \leq n} \varphi(h_i \otimes f_i).$$

This implies that for any $m \in M$ we have

$$\alpha_M(m) = \sum_i f_i m \otimes h_i.$$

The inclusion $M' \subset M^A$ follows easily. □

Since any Hopf algebra is a left module over itself via the multiplication map, it is a right comodule on its dual. Therefore it follows from the lemma that we may define the left integrals of A and A^D by the following equalities:

$$I(A) = A^{A^D} = \{x \in A \mid ax = \varepsilon(a)x, \forall a \in A\},$$
$$I(A^D) = (A^D)^A = \{f \in A^D \mid uf = \varepsilon^D(u)f = u(1)f, \forall u \in A^D\}.$$

We note that $I(A)$ is not only an R-submodule of A but also a two-sided A-ideal. In a similar way we may define the module of right integrals. A Hopf algebra is called *unimodular* if the modules of left and right integrals coincide. A Hopf algebra is also endowed with a right comodule structure induced by its comultiplication. Therefore it becomes a left module over the dual algebra as explained previously. The description of a finite Hopf R-algebra as a module over its dual holds in general. A theorem of Larson and Sweedler (see [P], Section 3) states that for any finite Hopf R-algebra the action of A^D on A induces an isomorphism

$$A \simeq A^D \otimes_R I(A).$$

This theorem implies that $I(A)$ and $I(A^D)$ are rank one projective R-modules ([C], Corollary 3.4). In the particular case where $I(A)$ is a free R-module with θ as a basis, then A is a free A^D-module on the left integral θ. This is always the case when R is a principal ideal domain.

Lemma 2.2. *The following properties are equivalent*:

(i) *The module of left integrals of A is a free rank one R-module.*
(ii) *The module of left integrals of A^D is a free rank one R-module.*
(iii) *There exists $\theta \in A$ and $\theta^D \in A^D$ such that $\theta^D\theta = 1_A$.*

Proof. We show that (i) implies (ii). The rest of the proof is left to the reader. Let θ be a basis of $I = I(A)$. Since A is a free A^D-module on θ there exists a unique θ^D in A^D such that $1_A = \theta^D\theta$. For any u of A^D we have the equalities:

$$(u\theta^D)\theta = u(\theta^D\theta) = u1_A = \varepsilon^D(u)1_A = (\varepsilon^D(u)\theta^D)\theta.$$

This implies that $u\theta^D = \varepsilon^D(u)\theta^D$ and hence that θ^D is a left integral of A^D. Let u be a nonzero left integral of A^D. Since A^D is a projective R-module, it follows that I^D is contained in $I_K^D = I(A_K^D)$, which is a K-vector space of dimension one. Therefore there exist nonzero elements m and n of R such that $mu = n\theta^D$. We set $t = u\theta$. This is an element of A. We observe that

$$mt = (mu)\theta = n(\theta^D\theta) = n.$$

It follows that $n = m\varepsilon(t)$, and so m divides n in R, and u is a multiple of θ^D. We conclude that θ^D is a free generator of $I(A^D)$. □

Proposition 2.3. *Assume that A is commutative, $I(A)$ is free over R and A_K is separable. Then A^D is unimodular, $I(A^D)$ is free over R and the restriction of S^D (resp. S) to the module of integrals of A^D (resp. A) is the identity map.*

Proof. We start by considering the restriction of S to $I(A_K)$. It follows from [Sw], Theorem 5.1.8, that $A_K = I(A_K) \oplus \mathrm{Ker}(\varepsilon)$ as a direct sum of A_K-ideals. Let x be a nonzero element of $I(A_K)$. Then $S(x)$ can be decomposed as a sum $rx + y$ with $r \in K$ and $y \in \mathrm{Ker}(\varepsilon)$. Since $\varepsilon \circ S = \varepsilon$ we deduce that $r = 1$. Therefore, $S(x)x = x^2 + yx$. We observe that $yx \in I(A) \cap \mathrm{Ker}(\varepsilon)$. Thus $yx = 0$ and $S(x)x = \varepsilon(x)x$. Moreover, we note that $S(S(x)x) = S(x)x = \varepsilon(x)S(x)$. So we conclude that $x = S(x)$. Since $I(A)$ is contained in $I(A_K)$ we deduce that, as required, the restriction of S to $I(A)$ is the identity map. We now consider A^D. It follows from Lemma 2.2, that $I(A^D)$ is R-free. Moreover, since A_K is separable, there exists a finite extension K'/K such that $A_{K'} = A_K \otimes_K K'$ is the algebra $\mathrm{Map}(\Gamma, K')$, where Γ is a finite group, endowed with its natural structure of Hopf algebra. The map

$$\alpha_{K'} : A^D \otimes_R K' \simeq A^D_{K'},$$
$$f \otimes \lambda \to f\lambda$$

is an isomorphism of K'-vector spaces which respects the algebra and coalgebra structure of both sides. Thus we may identify the Hopf algebras $A^D \otimes_R K'$ and $K'[\Gamma]$ and therefore $I(A^D)$ with $I(K'[\Gamma]) \cap A^D$. The unimodularity of A^D follows from the unimodularity of $K'[\Gamma]$. We now want to prove that the restriction of S^D to $I(A^D)$ is the identity map. Let $\theta^D \in I(A^D)$ and $\theta \in I(A)$ be such that $\theta^D\theta = 1_A$. Let $\Delta(\theta) = \sum \theta_{(0)} \otimes \theta_{(1)}$. We deduce from the definitions that

$$\varepsilon\big(\theta^D\theta\big) = 1_R = \sum \varepsilon(\theta_0)\big\langle \theta^D, \theta_{(1)}\big\rangle = \big\langle \theta^D, \theta\big\rangle$$

and

$$\varepsilon\big(S^D\big(\theta^D\big)\theta\big) = \big\langle \theta^D, S(\theta)\big\rangle = \big\langle \theta^D, \theta\big\rangle.$$

Because A^D is unimodular we know that θ^D and $S^D(\theta^D)$ both belong to $I(A^D)$. Since $I(A^D_K)$ is of dimension 1 there exists $\lambda \in K$ such that $S^D(\theta^D) = \lambda\theta^D$. Using that $S^2 = I$, we deduce that $\lambda \in \{\pm 1\}$. Since the characteristic of K is different from 2 we deduce from the previous equalities that $S^D(\theta^D) = \theta^D$. This completes the proof of the proposition. □

Remark. When K is of characteristic 0 and A_K is commutative, it follows from a theorem of Cartier that A_K is separable. Therefore any finite, commutative and locally free R-Hopf algebra, where R is a principal ideal domain of characteristic 0, satisfies the hypotheses of Proposition 2.3. Nevertheless it is easy to construct Hopf algebras, which are not separable, but such that $I(A)$ is free and the restriction of S to $I(A)$ is the identity. It suffices for instance to consider $A = k[\Gamma]$ where k is a field of characteristic p and Γ a finite group of order divisible by p, endowed with its usual Hopf algebra structure. We know from Maschke's theorem that A is not separable. However, we may easily check that $I(A)=k\omega$ where $\omega=\sum_{\gamma\in\Gamma}\gamma$. Since $S(\omega)=\omega$, then S restricts to the identity map on $I(A)$. When A_K is not separable we note that $I(A_K)$ is contained in $\mathrm{Ker}(\varepsilon)$ and thus $I(A_K)^2=I(A)^2=\{0\}$.

Let M be an A-comodule and let M_A be the largest quotient of M on which A^D acts trivially, so that $M_A=M/\ker(\varepsilon^D)M$.

Lemma 2.4. *Suppose that A^D is unimodular and that $I(A^D)$ is free over R with θ^D as a basis. Let M be a projective A^D-module. Then*

(i) $M^A=\theta^D M$,
(ii) *M^A is a locally free R-module,*
(iii) *the map $m\mapsto\theta^D m$ induces an isomorphism of R-modules from M_A onto M^A.*

Proof. We first observe that we can reduce to the case where M is A^D-free and so is a direct sum of copies of A^D. Therefore, in order to prove the lemma, we may assume that $M=A^D$. In this case it follows from the very definition of the set of integrals that $M^A=(A^D)^A=I(A^D)=\theta^D A^D=\theta^D R$ which proves (i) and (ii) of the lemma. Moreover, for $g\in A^D$, the equality $\theta^D g=0$ is equivalent to $\theta^D g(1)=0$ and thus to $g(1)=0$ since A^D is R-torsion free. We then deduce that the kernel of the R-module homomorphism $m\mapsto\theta^D m$ is the submodule $\mathrm{Ker}(\varepsilon^D)M$. Therefore it induces, as required, an isomorphism from M_A onto M^A. □

Let (M,α_M) and (N,α_N) be A-comodules. We shall define a comodule structure on $M\otimes N$ by considering

$$\alpha_{M,N}: M\otimes N \overset{\alpha_M\otimes\alpha_N}{\longrightarrow} M\otimes A\otimes N\otimes A \simeq M\otimes N\otimes A\otimes A \overset{Id\otimes mult}{\longrightarrow} M\otimes N\otimes A.$$

The A^D-module structure associated to this comodule structure is given by:

$$g(m\otimes n)=\sum_{(g)} g_{(0)}m\otimes g_{(1)}n, \quad \forall g\in A^D, m\in M, n\in N,$$

where $\Delta^D(g)=\sum_{(g)} g_{(0)}\otimes g_{(1)}$. We say that *$M\otimes N$ is endowed with the diagonal action of A^D.*

We conclude this subsection by recalling a result of Schneider, [S], Lemmas 2.1 and 2.2, which generalizes to a large family of Hopf algebras a theorem well known when $A=\mathrm{Map}(\Gamma,R)$ and $A^D=R[\Gamma]$ ([Mc], Corollary 3.3, p. 145 and p. 196).

Proposition 2.5. *Let A be a Hopf algebra over R. Let M and N be A^D-modules. Assume that M and N are both projective R-modules and that either M or N is projective as an A^D-module. Then $M\otimes_R N$ endowed with the diagonal action of A^D is a projective A^D-module.*

Proof. For the sake of completeness, we briefly recall the proof. First, one checks that the general case follows the "free case" where one of the modules is A^D itself while the other one is free over R. We assume that $M = A^D$ and that N is free over R and we consider the A^D-modules $X = A^D \otimes_R N$, endowed with the diagonal action and $Y = A^D \otimes_R N$ where A^D acts by multiplication on the left factor. It is clear that Y is a projective A^D-module. Then one proves that the R-linear map $f : Y \to X$, defined by:

$$f : m \otimes n \to \sum_{(m)} m_{(0)} \otimes m_{(1)} n,$$

is an isomorphism of A^D-modules with inverse g given by

$$g : m \otimes n \to \sum_{(m)} m_{(0)} \otimes S^D(m_{(1)}) n.$$

□

2.2. Equivariant symmetric bundles. Let M be an R-module equipped with a bilinear and symmetric form

$$q : M \times M \to R.$$

The form q induces a homomorphism of R-modules

$$\varphi_q : M \to M^D.$$

We call q nondegenerate if φ_q is an isomorphism of R-modules. *A symmetric bundle* over $\mathrm{Spec}(R)$ is associated to a pair (M, q) consisting of a finitely generated and locally free R module M endowed with a nondegenerate form q (see [Kne]). In this set up, for reason of simplicity, we will call symmetric bundle over R the pair (M, q) itself. Let A be a finite and locally free Hopf algebra over R and let (M, q) be a symmetric bundle over R. We shall say that (M, q) is *A-equivariant* if M is an A-comodule and if the following is true:

$$q(gm, n) = q\big(m, S^D(g)n\big), \quad \forall m, n \in M, \forall g \in A^D.$$

If, moreover, M is a projective A^D-module, we shall call (M, q) a *projective A-equivariant bundle.* Note that when $A = \mathrm{Map}(\Gamma, R)$, with Γ a finite group and A^D is the group algebra $R[\Gamma]$, an A-equivariant symmetric bundle is an $R[\Gamma]$-module endowed with a non-degenerate, Γ-invariant, bilinear and symmetric form.

We observe that any A-equivariant symmetric bundle (M, q) defines, after scalar extension by a commutative R-algebra T, an A_T-equivariant symmetric bundle over T that we denote by (M_T, q_T).

We can attach to any R-symmetric bundle (M, q) its orthogonal group which we denote by $\mathbf{O}(q)$. This is a group scheme over R. This group scheme is most easily defined in terms of its associated functor of points. Suppose now that A is a commutative Hopf algebra. Then we can associate to A the group scheme $G = \mathrm{Spec}(A)$. We will say that G is generically étale when A_K

is a separable K-algebra. In this case, the notion of A-equivariant symmetric bundle has an interpretation in terms of orthogonal representations.

Proposition 2.6. *Let A be a commutative Hopf R-algebra and let G be the group scheme defined by A. We assume that G is generically étale. Let (M,q) be an R-symmetric bundle. Then the following properties are equivalent*:

(i) *(M,q) is A-equivariant.*

(ii) *There exists a morphism of group schemes*:

$$\rho : G \to \mathbf{O}(q).$$

Proof. For any R-algebras E and F, we denote by $\mathrm{Hom}_{R,\mathrm{alg}}(E,F)$ the set of morphisms of R-algebras $f : E \to F$. We recall that for any R-algebra T we have the following isomorphism

$$G(T) \simeq \mathrm{Hom}_{R,\mathrm{alg}}(A,T) \simeq \mathrm{Hom}_{T,\mathrm{alg}}(A_T,T).$$

Moreover, since A is a finitely generated projective R-module, we know that

$$\mathrm{Hom}_T(A_T,T) \simeq \mathrm{Hom}_R(A,R) \otimes_R T.$$

With a slight abuse of notation we write

$$G(T) = \mathrm{Hom}_{T,\mathrm{alg}}(A_T,T) \subset \mathrm{Hom}_R(A,R) \otimes_R T.$$

We assume (i). For any R-algebra T, after scalar extension, M_T becomes an A_T^D-module. Therefore, for any $g \in G(T)$, we may define

$$\rho_T(g) : M_T \to M_T, \quad m \mapsto gm.$$

One easily checks that ρ_T induces a group homomorphism from $G(T)$ to $\mathbf{O}(q_T)$, which proves (ii). We now suppose that (ii) is satisfied. It follows from the hypothesis that there exists a group homomorphism

$$\rho_A : G(A) \to \mathrm{Aut}(M_A)$$

(here of course $M_A = M \otimes A$ and not the coinvariant module as defined in Lemma 2.4). For the element Id we obtain an A-linear map $\rho_A(Id) : M \otimes_R A \to M \otimes_R A$ which determines by restriction $\alpha : M \to M \otimes_R A$. The map α endows M with a right A-comodule structure (see [W], Chapter 3) and therefore with a left A^D-module structure. Since there exists a finite extension K'/K such that $A_{K'}^D = K'[\Gamma]$, any element $g \in A^D$ can be written $g = \sum_{\gamma\in\Gamma} r_\gamma \gamma$ with $r_\gamma \in K', \forall \gamma \in \Gamma$. Since every γ belongs to $G(K')$, then $S^D(\gamma) = \gamma^{-1}$. Since $\rho_{K'}(\gamma)$ belongs to $\mathbf{O}(q_{K'})$ for any $\gamma \in \Gamma$ we can write the equalities:

$$q(gm,n) = \sum_{\gamma\in\Gamma} r_\gamma q(\gamma m,n) = \sum_{\gamma\in\Gamma} r_\gamma q\big(m,\gamma^{-1}n\big) = q\big(m,S^D(g)n\big),$$

for any m and $n \in M$ and $g \in A^D$. Hence, we have proved as required that (M,q) is A-equivariant. □

We call any morphism of group schemes $\rho : G \to \mathbf{O}(q)$ an *orthogonal representation of* G. In this paper we shall frequently speak either of equivariant symmetric bundles or equivalently orthogonal representations. Observe that, when G is generically constant, an orthogonal representation, as defined above, induces by restriction to the generic fiber an orthogonal representation in the usual sense.

Let (M,q) be a projective A-equivariant symmetric bundle. We assume that A^D satisfies the properties of Proposition 2.3. We fix an R-basis θ^D of $I(A^D)$. Under these assumptions, we use Lemma 2.4 to define a map

$$q^A : M^A \times M^A \to R$$

by setting

$$q^A(x,y) = q(m,y) = q(x,n),$$

where m (resp. n) is any arbitrary element of M such that $x = \theta^D m$ (resp. $y = \theta^D n$). Observe that if $\theta^D m = \theta^D m'$, then $m - m'$ belongs to $\mathrm{Ker}(\varepsilon^D)M$. Since

$$q\big(gu, \theta^D n\big) = q\big(u, S^D(g)\theta^D n\big) = q\big(u, \varepsilon^D\big(S^D(g)\big)\theta^D n\big) = q\big(u, \varepsilon^D(g)\theta^D n\big) = 0,$$

for any $g \in \mathrm{Ker}(\varepsilon^D)$, we deduce that q^A is well defined. Moreover, we note that

$$q^A(x,y) = q(y,m) = q\big(\theta^D n, m\big) = q\big(n, S^D\big(\theta^D\big)m\big) = q\big(n, \theta^D m\big) = q^A(y,x).$$

Hence q^A is a symmetric bilinear form on M^A.

Proposition 2.7. *Let A be a Hopf algebra and let (M,q) be a projective A-equivariant symmetric bundle. Suppose that A^D is unimodular and that $I(A^D)$ is a free R-module, then (M^A, q^A) is a symmetric R-bundle.*

Proof. From Lemma 2.4, we know that M^A is a locally free R-module. It remains to prove that the adjoint map

$$\varphi_{q^A} : M^A \to \mathrm{Hom}\big(M^A, R\big)$$

is an R-module isomorphism. This result, when $A = \mathrm{Map}(\Gamma, R)$ and Γ is a finite group, was proved in Proposition 2.2 of [CNET]. This proof can be used *mutatis mutandis* in this more general situation if, as in the situation considered in [CNET], the quotient M/M^A is torsion free. This is easily checked. We note that it suffices to prove the result when $M = A^D$. Let $f \in A^D$ and $d \in R$, $d \neq 0$ such that $df \in (A^D)^A$. It follows from the definition of $(A^D)^A$ that for any $g \in A^D$ then $g(df) = \varepsilon^D(g)(df)$. Since A^D is a projective R-module it is torsion free and thus $gf = \varepsilon^D(g)f$, which proves that $f \in (A^D)^A$. □

Remarks.

1. For any $x = \theta^D m$ and $y = \theta^D n$ of M^A it is easily verified that

$$q(x,y) = q\big(m, S^D\big(\theta^D\big)\theta^D n\big) = q\big(m, \varepsilon^D\big(\theta^D\big)y\big) = \varepsilon^D\big(\theta^D\big)q^A(x,y).$$

If A^D_K is not separable, then we know that $\varepsilon^D(x) = 0$ for any $x \in I(A^D_K)$, from Theorem 5.1.8 in [Sw]. Therefore, this situation makes clear that q^A

is not in general the restriction of q to M^A, since q^A is unimodular while the restriction of q to M^A is zero.

2. It is important to note that the form q^A depends upon the choice of a generator of $I(A^D)$. Taking $\theta'^D = \lambda\theta^D$ with $\lambda \in R^\times$ as a new generator of $I(A^D)$ provides us with a new symmetric form $q'^A = \lambda^{-1}q^A$ on M^A. If λ is a square of a unit of R, then the symmetric bundles (M^A, q^A) and (M^A, q'^A) are isometric. As we will see, at the end of Section 2, our future constructions will not depend upon this choice.

3. Twists of symmetric bundles

Recall that R is an integral domain with field of fractions K and that A is a Hopf R-order in the Hopf algebra A_K. The aim of this section is to define the *algebraic twist* of an A-equivariant symmetric bundle by a principal homogeneous space for A. As a first step we show, under certain assumptions on A, how to associate to a principal homogeneous space for A an A-equivariant projective symmetric bundle. The trace form is the key-tool of this construction.

We let A be a commutative Hopf algebra which is finite and flat over R. Let B be a commutative finite flat R-algebra, endowed with the structure of an A-comodule algebra

$$\alpha_B : B \to B \otimes_R A.$$

We suppose that $B^A = R$. We shall say that B is *a principal homogeneous space for A over R*, abbreviated to PHS, when

$$(Id \otimes 1, \alpha_B) : B \otimes_R B \simeq B \otimes_R A$$

is an isomorphism of B-algebras and left A^D-modules. We observe that A, endowed with the comultiplication map, provides an example of such a space.

Lemma 3.1. *Let A_K be a separable commutative Hopf K-algebra and let B_K be a principal homogeneous space for A_K. Let* Tr *denote the trace form on B_K. Then (B_K, Tr) is a projective A_K-equivariant symmetric bundle.*

Proof. Since B_K is a principal homogeneous space for A_K, we know that B_K is a projective A_K^D-module. Using the fact that B_K becomes isomorphic to A_K after a faithful base change, it follows by descent theory that B_K is separable and therefore that the trace is non-degenerate. Let q denote the trace form on B_K. We now want to show that q is an A_K-equivariant form. As in Proposition 2.3 we fix a finite extension K'/K such that $A_{K'}^D$ is isomorphic to $K'[\Gamma]$, where Γ is a finite group. In this case $A_{K'}^D$, as a K'-vector space, has a basis $\{\gamma, \gamma \in \Gamma\}$ consisting of group like elements. Since $B_{K'}$ is an $A_{K'}^D$-module algebra, one easily checks that every γ defines an automorphism of K'-algebras of $B_{K'}$ whose inverse is $S^D(\gamma)$. Therefore the trace form $q_{K'}$ of $B_{K'}$ is invariant under each $\gamma \in \Gamma$. Thus the A_K-equivariance of q follows from the A'_K-equivariance of $q_{K'}$. □

We now wish to generalize the above construction when working with the ring R in place of the field K. A key-role in this case is played by the codifferent of B.

3.1. The square root of the codifferent. The codifferent of B/R is defined by

$$\mathcal{D}^{-1}(B/R) = \big\{x \in B_K \mid \mathrm{Tr}(xb) \in R \ \forall b \in B\big\}.$$

For reason of simplicity $\mathcal{D}^{-1}(B/R)$ will be abbreviated by $\mathcal{D}^{-1}(B)$. In the case where R is a field then $\mathcal{D}^{-1}(B) = B$. It follows from the A_K-invariance of the trace form proved in Lemma 3.1 that $\mathcal{D}^{-1}(B)$ is an A^D-module. We start by studying the codifferent of A.

Proposition 3.2. *Let A be a commutative Hopf algebra and assume that A_K is separable. Let I be the set of integrals of A. Then*:

(i) *There exists a unique primitive idempotent e of A_K and a fractional ideal Λ of R such that*

$$I_K = Ke \quad \textit{and} \quad I = \Lambda e.$$

(ii) *We have the equality*:

$$\mathcal{D}^{-1}(A) = \Lambda^{-1} A.$$

Proof. We know from [Sw], Corollary 5.1.6, that I_K is a one dimensional K-vector space. Moreover, since A_K is a separable algebra, we deduce from [Sw], Theorem 5.1.8, that $A_K = I_K \oplus \mathrm{Ker}(\varepsilon)$. Let u be a basis of I_K. Since it is an integral, it follows that $u^2 = \varepsilon(u)u$. Therefore, replacing u by $u/\varepsilon(u)$, we obtain a new basis of I_K which is a non-trivial idempotent. We denote this idempotent by e. Since R is an integral domain, it follows that $\varepsilon(f) = 1$ for any idempotent f of I_K. We conclude that e is the unique idempotent of I_K. Let Λ be the fractional ideal of R consisting of elements $x \in K$ such that xe belongs to A. Then we have

$$I = I_K \cap A = \Lambda e.$$

We consider the left A_K^D-module structure on A_K^D defined by

$$\langle f * g, x\rangle = \big\langle g, S^D(f)x\big\rangle \quad \forall x \in A_K.$$

Since A_K is separable, the trace form is non-degenerate and induces an isomorphism of K-vector spaces

$$\Psi : A_K \to A_K^D = \mathrm{Hom}(A_K, K).$$

We note that

$$\big\langle \Psi(fa), x\big\rangle = \mathrm{Tr}(fax) = \mathrm{Tr}\big(aS^D(f)x\big) = \big\langle \Psi(a), S^D(f)x\big\rangle = \big\langle f * \Psi(a), x\big\rangle$$

for all $a, x \in A_K, f \in A_K^D$. Therefore Ψ is an isomorphism of A_K^D-modules. It follows from the definition of the codifferent that $\mathcal{D}^{-1}(A) = \Psi^{-1}(A^D)$. We now consider $\Psi(A)$. Since Ψ is an isomorphism of A_K^D-modules and since

$A = A^D I$ we obtain that $\Psi(A) = \Psi(A^D \Lambda e) = \Lambda A^D \Psi(e)$. Therefore we are reduced to determining $\Psi(e)$. Let x be an element of A_K. From the direct sum decomposition of A_K, it follows that x can be written as a sum $\lambda e + x'$ with $x' \in \operatorname{Ker}(\varepsilon)$ and $\lambda \in K$. Hence, we have

$$\big\langle \Psi(e), x \big\rangle = \operatorname{Tr}(ex) = \operatorname{Tr}\big(e\lambda + ex'\big).$$

We note that $ex' = 0$. Moreover, since e is a non-trivial idempotent whose K-span has dimension one, its trace is 1. Therefore, we have proved that $\langle \Psi(e), x \rangle = \lambda = \varepsilon(x)$ for all $x \in A_K$. We conclude that $\Psi(e) = \varepsilon$ which is the unit element of A_K^D. Therefore, we have proved that $\Psi(A) = \Lambda A^D$ and thus $\mathcal{D}^{-1}(A) = \Lambda^{-1} A$ as required. □

Remark. Observe that Λ is the R-ideal defined by

$$\Lambda = \varepsilon(I).$$

Corollary 3.3. *Assume that $I(A)$ is a free R-module. Then:*

(i) $I(A^D) = \Lambda^{-1} t$, *where t is the unique element of A_K^D such that $te = 1_{A_K}$.*
(ii) $\operatorname{Tr}(x) = tx$ *for any $x \in B_K$.*
(iii) $\mathcal{D}^{-1}(B) = \Lambda^{-1} B$.

Proof. Let $\lambda \in \Lambda$ be such that $\theta = \lambda e$ is a basis of $I(A)$. We note that $\lambda^{-1} t$ is the unique element $\theta^D \in A_K^D$ such that $\theta^D \theta = 1$. Since there exists such an element in A^D, we may conclude that $\theta^D \in A^D$. It follows from Lemma 2.2 that θ^D is an R-basis of $I(A^D)$ and thus (i) is proved. We now fix an extension K'/K as in Proposition 2.3 and we identify on the one hand the algebras $A_{K'}$ and $\operatorname{Map}(\Gamma, K')$ and on the other hand the algebras $A_{K'}^D$ and $K'[\Gamma]$. Since A_K is contained in $A_{K'}$ we observe that e is the unique idempotent in $\operatorname{Map}(\Gamma, K')$ such that $I_{K'} = K'e$. Therefore, as an element of $\operatorname{Map}(\Gamma, K')$, e is defined by $e(\gamma) = 1$ if $\gamma = 1$ and 0 otherwise. Let $\omega_\Gamma = \sum_{\gamma \in \Gamma} \gamma$. One can easily check that ω_Γ is the unique element in $K'[\Gamma]$ such that $\omega_\Gamma e = 1_{A_{K'}}$. Therefore, we deduce that $t = \omega_\Gamma$. We now have

$$\operatorname{Tr}_{B_K/K}(x) = \operatorname{Tr}_{B_{K'}/K'}(x) = \omega_\Gamma x = tx, \quad \forall x \in B_K$$

as required.

Recall that we have the commutative diagram

$$\begin{tikzcd}
B \otimes_R B \arrow[r, "\varphi"] \arrow[d] & B \otimes_R A \arrow[d] \\
B_K \otimes_K B_K \arrow[r, "\varphi_K"] & B_K \otimes_K A_K,
\end{tikzcd}$$

where φ (resp. φ_K) is an isomorphism of B (resp. B_K)-algebras and the vertical arrows are injections. Because B_K is finite and separable over K, the trace gives a non-degenerate form $\mathrm{Tr}_K : B_K \times B_K \to K$. This extends by $\otimes_K B_K$ to a non-degenerate pairing

$$\mathrm{Tr}_K : B_K \otimes_K B_K \times B_K \otimes_K B_K \to B_K.$$

The trace induces a pairing $\mathrm{Tr} : B \otimes_R B \times B \otimes_R B \to B$ and $\mathcal{D}^{-1}((B \otimes B)/B)$ is defined in the usual way by

$$\mathcal{D}^{-1}\big((B \otimes B)/B\big) = \big\{x \in B_K \otimes_K B_K \mid \mathrm{Tr}_K\big(x(B \otimes_R B)\big) \subset B\big\}.$$

By localization and choosing local self-dual bases, we get

$$\mathcal{D}^{-1}\big((B \otimes B)/B\big) = B \otimes \mathcal{D}^{-1}(B/R).$$

Let λ be a generator of Λ. By proceeding as before, we obtain the equality

$$\mathcal{D}^{-1}\big((B \otimes A)/B\big) = B \otimes \mathcal{D}^{-1}(A/R) = B \otimes \lambda^{-1} A.$$

Therefore

$$\varphi_K\big(B \otimes \lambda \mathcal{D}^{-1}(B/R)\big) = \varphi_K(B \otimes B) = B \otimes A$$

and so $B \otimes \lambda \mathcal{D}^{-1}(B/R) = B \otimes B$. Since B/R is faithfuly flat, we conclude that $\mathcal{D}^{-1}(B/R) = \lambda^{-1} B$ as required. □

We obtain as a corollary a result of Raynaud (see [R], Appendix, Proposition 9 and [T], Proposition 4.4).

Corollary 3.4. *We assume that A_K is separable of K-rank n and that $I(A)$ is R-free. Let θ (resp. θ^D) denote an integral of A (resp. A^D) such that $\theta^D \theta = 1$. Then $\varepsilon(\theta)\varepsilon^D(\theta^D) = n$. In particular if $\Lambda = \varepsilon(I)$ and $\Lambda^D = \varepsilon^D(I^D)$ then $\Lambda \Lambda^D = nR$.*

Proof. Let Tr denote the trace form on A_K. First, observe that $\mathrm{Tr}(\theta^D \theta) = n$. Moreover, since the trace is equivariant, it follows that

$$n = \mathrm{Tr}\big(\theta^D \theta\big) = \mathrm{Tr}\big(\theta . S^D\big(\theta^D\big) 1_A\big) = \varepsilon^D\big(\theta^D\big)\, \mathrm{Tr}(\theta).$$

Under our hypothesis, it follows from Proposition 3.2 that there exists $\lambda \in R$ such that

$$\Lambda = \lambda R \quad \text{and} \quad \theta = \lambda e.$$

It follows from the direct sum decomposition of A_K that $\mathrm{Tr}(e) = 1$. Since $\varepsilon(e) = 1$, we deduce from the previous equality that $\mathrm{Tr}(\theta) = \lambda = \varepsilon(\theta)$ and so that $\varepsilon^D(\theta^D)\varepsilon(\theta) = n$ and $\Lambda^D \Lambda = nR$. □

Remark. It can be shown that $\mathcal{D}(A)$ is the Fitting ideal of the module of differentials $\Omega^1_{A/R}$. It therefore follows from the lemma that, if n is a unit of R, then the module $\Omega^1_{A/R}$ is trivial. In this case the cover of schemes $(\mathrm{Spec}(B) \to \mathrm{Spec}(R))$ is étale for any principal homogeneous space B.

3.2. Twists of a form by a principal homogeneous space. The role played by the trace form and by the set of integrals leads us to consider Hopf algebras satisfying the following properties:

Definition 1. A finite and flat R-Hopf algebra A satisfies hypothesis $\mathbf{H}$ when A_K is a commutative separable K-algebra and the image under ε of the set of integrals of A is the square of a principal ideal of R.

When A satisfies $\mathbf{H}$ we denote by $\Lambda^{1/2}$ a principal ideal of R such that

$$\big(\Lambda^{1/2}\big)^2 = \Lambda = \varepsilon\big(I(A)\big).$$

Then, for any principal homogeneous space B of A, it follows from Corollary 3.3 that

$$\mathcal{D}^{-1/2}(B) = \Lambda^{-1/2}B$$

is a square root of $\mathcal{D}^{-1}(B)$ and that $(\mathcal{D}^{-1/2}(B), \mathrm{Tr})$ is a projective and A-equivariant symmetric bundle on R. Let us denote by $\lambda^{1/2}$ a generator of $\Lambda^{1/2}$, let θ be the generator λe of $I(A)$ and let θ^D be the unique element of A^D such that $\theta^D\theta = 1_A$. If we consider an A-equivariant symmetric bundle (M,q), it follows from Proposition 2.5 that $(\mathcal{D}^{-1/2}(B)\otimes_R M, \mathrm{Tr}\otimes q)$ is a projective A-equivariant symmetric bundle. Then, following the construction of Section 2.2, we can define the *twist of* (M,q) *by* B (associated to θ^D).

Definition 2. Let A be a Hopf R-algebra satisfying $\mathbf{H}$, let (M,q) be an A-equivariant symmetric bundle and let B be a principal homogeneous space of A. Define the algebraic twist of (M,q) by B as the R-symmetric bundle

$$(\tilde{M}_B, \tilde{q}_B) = \big(\mathcal{D}^{-1/2}(B)\otimes_R M, \mathrm{Tr}\otimes q\big)^A.$$

Remarks.

1. We observe that, since θ is defined up to the square of a unit of R, the same holds for θ^D. Therefore, as observed in Remark 2 of Section 2.2, the definition of $(\tilde{M}_B, \tilde{q}_B)$ is independent, up to isometry, of the choice of θ.
2. It follows from Proposition 2.7 that under hypothesis $\mathbf{H}$ we can attach to (M,q) an orthogonal representation $\rho: G = \mathrm{Spec}(A) \to \mathbf{O}(q)$. Following the general definition of [CCMT], Definition 6.4, we shall often refer to the twist of (M,q) by B as *the twist of* (M,q) *by* ρ *and* $X = \mathrm{Spec}(B)$. We will denote this twist as $(M_{\rho,X}, q_{\rho,X})$.
3. Suppose that $R = K$ is a field and that L/K is a Galois extension with Galois group Γ. Let (M,q) be the underlying symmetric bundle of an orthogonal representation $\rho: \Gamma \to \mathbf{O}(q)$. This is a situation where we can apply our previous construction. Let $A = \mathrm{Map}(\Gamma, K)$ be the Hopf algebra defining the constant group scheme associated to Γ. Since L is a principal homogeneous space for A, we can consider the twist of (M,q) by L

$$(\tilde{M}_L, \tilde{q}_L) = (L\otimes_K M, \mathrm{Tr}\otimes q)^A$$

as introduced in Definition 2. It follows from [F], Theorem 1 and [CNET], Proposition 2.5, that this new quadratic form coincides with the one introduced by Fröhlich in [F], Section 2.

4. Twists of a form and flat cohomology

Let S be the scheme $\mathrm{Spec}(R)$ and let G be the S-group scheme defined by the spectrum of an R-Hopf algebra A. To any R-linear map

$$\alpha_B : B \to B \otimes_R A,$$

which endows B with the structure of a comodule algebra over A, there corresponds a morphism of S-schemes

$$X \times_S G \to X.$$

In this correspondence the notion of PHS corresponds to the notion of a torsor for G over S.

Following Milne ([M], Chapter III, Section 4), we may associate to any flat covering $\mathcal{U} = (\mathcal{U}_i \to S)_{i \in I}$ a set of cohomology classes $\check{H}^1(\mathcal{U}, G)$; this is a set with a distinguished element. We define $\check{H}^1(S, G)$ to be the direct limit over all coverings $\mathcal{U}$ of $\check{H}^1(\mathcal{U}, G)$. From Theorem 4.3 and Proposition 4.6 in [M], it follows that there exists a one to one correspondence, $[X] \to c(X)$, between the isomorphism classes of G-torsors over S, that we denote by $H^1(S, G)$, and elements of $\check{H}^1(S, G)$ under which the class of the trivial torsor (the class of A) corresponds to the distinguished element of $\check{H}^1(S, G)$.

Let (M, q) denote an A-equivariant symmetric bundle and assume that A satisfies hypothesis **H**. As per Proposition 2.7 we can associate to (M, q) a morphism of group schemes $\rho : G \to \mathbf{O}(q)$. It is routine to check that ρ transforms 1-cocycles on G into 1-cocycles on $\mathbf{O}(q)$ and thereby induces a map ρ_* from $\check{H}^1(S, G)$ in $\check{H}^1(S, \mathbf{O}(q))$. The set $\check{H}^1(S, \mathbf{O}(q))$ classifies the set of isomorphism classes of twisted forms of (M, q) ([D-G], III, Section 5, n. 2). Therefore the class $\rho_*(c(X))$ defines, up to isometry, a unique symmetric bundle which we denote by $(M_{\rho(X)}, q_{\rho(X)})$. We now have at our disposal on the one hand the symmetric bundle $(M_{\rho(X)}, q_{\rho(X)})$, which has an abstract definition in terms of class of a cocycle in a flat cohomology set, and on the other hand the algebraic twist $(M_{\rho,X}, q_{\rho,X})$ given by a simple explicit formula (see Definition 2 in Section 3.2). The main goal of this section is to prove that the two bundles coincide.

THEOREM 4.1. *There exists an isometry of symmetric bundles*

$$(M_{\rho,X}, q_{\rho,X}) \simeq (M_{\rho(X)}, q_{\rho(X)}).$$

We keep the notation and the hypotheses of Section 3. We assume that A satisfies hypothesis **H**, and in particular that the image under ε of the set of integrals of A is the square of a principal ideal of R. We fix a generator $\lambda^{1/2}$ of this ideal. Since A_K is separable there exists a finite extension K'/K and a finite group Γ such that $A_{K'} = \mathrm{Map}(\Gamma, K')$ and $A^D_{K'} = K'[\Gamma]$. For the sake of notational simplicity we shall assume that $K' = K$; the general case can follow similarly. We let e be the element of A_K defined by $e(\gamma) = 1$ if $\gamma = 1$ and 0 otherwise and we denote by ω the element $\sum_{\gamma\in\Gamma} \gamma$ in $K[\Gamma]$. We have seen that $\theta = \lambda e$ (resp. $\theta^D = \lambda^{-1}\omega$) is an R-basis of $I(A)$ (resp. $I(A^D)$) and that we have the equalities

$$\theta^D\theta = 1_A, \qquad \theta\theta^D = 1_{A^D}, \qquad A = A^D\theta, \qquad A^D = A\theta^D.$$

4.1. Representative of a torsor. Let B be a PHS of A and again let $X = \mathrm{Spec}(B)$ be the associated G-torsor. It follows from the definition that the flat cover $\mathcal{U} = (X \to S)$ trivializes X. More precisely the isomorphism

$$\varphi = (Id \otimes 1, \alpha_B) : B \otimes_R B \to B \otimes_R A,$$

induces an isomorphism of S-schemes with G-action

$$\Phi = \mathrm{Spec}(\varphi) : X \times_S G \to X \times_X X.$$

Let p_1 (resp. p_2) denote the first (resp. second) projection map $X \times_S X \to X$. For $1 \le i \le 2$ the base change of Φ by p_i defines an isomorphism of schemes with G-action

$$\Phi_i : (X \times_S X) \times_S G \to (X \times_S X) \times_S X.$$

We know from p. 134 in [M] that $\Phi_1^{-1} \circ \Phi_2$ is a 1-cocycle representing $c(X)$. We wish to understand $\Phi_1^{-1} \circ \Phi_2$ in terms of $B \otimes_R B$-valued points of G.

Let q_1 (resp. q_2) denote the morphism of algebras $B \to B \otimes_R B$, defined by $(q_1 : x \to x \otimes 1)$ (resp. $q_2 : x \to 1 \otimes x$). Extending scalars by q_i for $1 \le i \le 2$, the map φ induces an isomorphism

$$\varphi_i : (B \otimes_R B) \otimes_R B \to (B \otimes_R B) \otimes_R A$$

of $B \otimes_R B$-algebras and A^D-modules. It is clear that $\Phi_1^{-1} \circ \Phi_2 = \mathrm{Spec}(\varphi_2 \circ \varphi_1^{-1})$.

Let C be the algebra $B \otimes_R B$. We recall the identifications of Section 2.2:

$$G(C) = \mathrm{Hom}_{\mathrm{alg},R}(A, C) = \mathrm{Hom}_{\mathrm{alg},C}(A_C, C).$$

We note that A_C is of course a C-algebra and an A_C-comodule. We write $\mathrm{Aut}(A_C)$ for the group of automorphisms of both C-algebras and A^D-comodules of A_C. We observe that $\varphi = \varphi_2 \circ \varphi_1^{-1}$ is an element of this group. For any element ψ of $\mathrm{Aut}(A_C)$ and $f \in G(C)$, we obtain a element of $G(C)$ by considering $f \circ \psi$.

Lemma 4.2. *The map*

$$\theta : \mathrm{Aut}(A_C) \to G(C), \quad \psi \to \varepsilon \circ \psi$$

is a group isomorphism.

Proof. Since any $\psi \in \mathrm{Aut}(A_C)$ is a morphism of comodules, it satisfies the equality

$$(\psi \otimes Id) \circ \Delta = \Delta \circ \psi.$$

This implies that for all $x \in A_C$,

$$\Delta\big(\psi(x)\big) = \sum_{(x)} \psi(x_{(0)}) \otimes x_{(1)},$$

where $\Delta(x) = \sum_{(x)} x_{(0)} \otimes x_{(1)}$ and so $\psi(x) = \sum_{(x)} \theta(\psi)(x_{(0)})x_{(1)}$. Using this last equality, it is easily verified that θ is a group homomorphism and is injective. Let us now consider an element $\alpha \in G(C)$. The C-endomorphism of A_C defined by

$$\psi(x) = \sum_{(x)} \alpha(x_{(0)})x_{(1)}$$

is a morphism of C-algebras and A_C-comodules such that $\theta(\psi) = \alpha$. This shows that θ is onto and completes the proof of the lemma. □

We deduce from this lemma that the map $\Psi = \mathrm{Spec}(\psi) \to \varepsilon \circ \psi$ is an isomorphism of groups from $\mathrm{Aut}(\mathrm{Spec}(C) \otimes_S G)$ onto $G(C)$. We identify these groups via this isomorphism. Under this identification, we conclude that $g = \varepsilon \circ \varphi$, where $\varphi = \varphi_2 \circ \varphi_1^{-1}$ is the element of $\mathrm{Aut}(A_C)$ introduced previously, is a 1-cocycle representative of $c(X)$ in $G(C)$.

Remark. As we have seen previously, for any $x \in A_C$, with $\Delta(x) = \sum_{(x)} x_{(0)} \otimes x_{(1)}$ we have the equality:

$$\varphi(x) = \sum (\varepsilon \circ \varphi)(x_{(0)})x_{(1)}.$$

In the case where $\Delta(x)$ is invariant under the twist map (which is the map induced by $c \otimes d \to d \otimes c$), this last equality can be written

$$\varphi(x) = (\varepsilon \circ \varphi)x,$$

where A_C is endowed with its structure of left A_C^D-module and where $\varepsilon \circ \varphi$ is considered as an element of A_C^D via the inclusion $G(C) \subset A_C^D$.

4.2. Proof of Theorem 4.1. Let (M, q) be an A-equivariant symmetric bundle and let B be a PHS of A. We consider the twist of (M, q) by B defined by

$$(M_{\rho,X}, q_{\rho,X}) = (\tilde{M}_B, \tilde{q}_B) = \big(\lambda^{-1/2} B \otimes_R M, \mathrm{Tr} \otimes q\big)^A.$$

The strategy for the proof of the theorem is to show that the flat covering $\mathcal{U} = (X \to S)$, which trivializes X as a G-torsor, likewise trivializes the symmetric bundle $(M_{\rho,X}, q_{\rho,X})$. With this in view we now construct an isometry of symmetric bundles

$$(M_B, q_B) \simeq (B \otimes_R \tilde{M}_B, \tilde{q}_{B,B}), \tag{4}$$

where $(\tilde{q}_{B,B})$ denotes the form $\tilde{q}_B$ extended to $B \otimes_R \tilde{M}_B$. This construction will be achieved via the next two lemmas. The results of Section 4.1 provide us with a representative of X in $\check{H}^1(\mathcal{U}, G)$. We will use the previous isometry to show that the image under ρ_* of this cocycle is a representative of the class of $(M_{\rho,X}, q_{\rho,X})$.

Lemma 4.3. *Let T be a finite flat R-algebra. Then:*

(i) *For any $f \in A_T^D$ and $m \in M_T$ one has*

$$\theta^D(f\theta \otimes m) = \theta^D\big(\theta \otimes S^D(f)m\big).$$

(ii) *The map $m \mapsto \theta^D(\lambda^{-1/2}\theta \otimes m)$ induces an isometry ν_T of symmetric bundles from $(T \otimes_R M, q_T)$ onto $(T \otimes_R \tilde{M}_A, \tilde{q}_{A,T})$ where $(\tilde{M}_A, \tilde{q}_A)$ is the symmetric bundle $(\lambda^{-1/2} A \otimes_R M, \mathrm{Tr} \otimes q)^A$.*

Proof. We first observe that it suffices to prove the lemma when $T = R$. The general case will follow by extension of scalars. Let f be an element of A^D. Since A^D is contained in $A_K^D = K[\Gamma]$ we write $f = \sum_{\gamma \in \Gamma} x_\gamma \gamma$ with $x_\gamma \in K$. Since A^D acts diagonally over $A \otimes_R M$ and since $\theta^D \gamma = \theta^D$, we obtain that for any $m \in M$ and $\gamma \in \Gamma$

$$\theta^D(f\theta \otimes m) = \sum_{\gamma \in \Gamma} \theta^D(x_\gamma \gamma\theta \otimes m) = \sum_{\gamma \in \Gamma} \theta^D\gamma\big(\theta \otimes x_\gamma \gamma^{-1} m\big) = \theta^D\big(\theta \otimes S^D(f)m\big),$$

as required.

Let $\nu : M \to \tilde{M}_A$ be the R-linear map defined by $m \mapsto \theta^D(\lambda^{-1/2}\theta \otimes m)$. We start by proving that ν is surjective. Let y be an element of $\tilde{M}_A$. We deduce from Lemma 2.4 the existence of a finite set of elements x_i of A and m_i of M such that $y = \sum_i \theta^D(\lambda^{-1/2} x_i \otimes m_i)$. Since θ is an A^D-basis of A, for an integer i, there exists an element f_i of A^D such that $x_i = f_i\theta$. Using (i) we deduce that

$$y = \sum_i \theta^D\big(f_i \lambda^{-1/2}\theta \otimes m_i\big) = \sum_i \theta^D\big(\lambda^{-1/2}\theta \otimes S^D(f_i)m_i\big) = \theta^D\big(\lambda^{-1/2}\theta \otimes x\big),$$

with $x = \sum_i S^D(f_i)m_i$. So we have found $x \in M$ such that $y = \nu(x)$.

Let us now consider $\tilde{\varepsilon} : A_K \otimes_K M_K \to M_K$ defined by $a \otimes m \mapsto \langle \varepsilon, a\rangle m$. Since the action of A_K^D is diagonal, for any $m \in A_K$ we have

$$\tilde{\varepsilon}\big(\theta^D(\theta \otimes m)\big) = (\alpha)m,$$

where $\Delta^D(\theta^D) = \sum \theta^D_{(0)} \otimes \theta^D_{(1)}$ and $\alpha = \sum \langle \varepsilon, \theta^D_{(0)}\theta)\rangle \theta^D_{(1)}$. We first observe that $\langle \varepsilon, \theta^D_{(0)}\theta)\rangle = \langle \theta^D_{(0)}, \theta\rangle$. Moreover, since A is commutative, we know that A^D is cocommutative. It follows from these facts that

$$\alpha = \sum \langle \theta^D_{(0)}, \theta\rangle \theta^D_{(1)} = \sum \langle \theta^D_{(1)}, \theta\rangle \theta^D_{(0)} = \theta\theta^D.$$

Since, as recalled at the beginning of this section, we know that $\theta\theta^D = 1_{A^D}$, then we have proved that

$$\tilde{\varepsilon}\big(\theta^D(\theta \otimes m)\big) = m, \quad \forall m \in M_K.$$

We conclude that ν is an isomorphism whose inverse is given by $\mu : x \mapsto \lambda^{1/2}\tilde{\varepsilon}(x)$. In order to complete the proof of the lemma, we must show that ν is an isometry. The proof consists of a verification by hand of the equality:

$$\tilde{q}_A\big(\theta^D\big(\lambda^{-1/2}\theta \otimes m\big), \theta^D\big(\lambda^{-1/2}\theta \otimes m'\big)\big) = q(m, m'), \quad \forall m, m' \in M. \qquad \square$$

Remark. As a consequence of the lemma, we observe that there is an isometry

$$(M, q) \simeq (\tilde{M}_A, \tilde{q}_A)$$

which proves Theorem 4.1 in the case when X is the trivial torsor.

We now return to the isomorphism $\varphi : B \otimes_R B \to B \otimes_R A$ introduced at the beginning of this section. This morphism induces an isomorphism

$$\tilde{\varphi} = (\varphi \otimes Id) : B \otimes_R \big(\lambda^{-1/2}B \otimes_R M\big) \to B \otimes_R \big(\lambda^{-1/2}A \otimes_R M\big)$$

of B and A^D-modules. Recall that A^D acts on the left-hand side (resp. the right-hand side) via its diagonal action on $(\lambda^{-1/2}B \otimes_R M)$ (resp. $(\lambda^{-1/2}A \otimes_R M)$). Therefore, taking fixed points by A^D, we see that $\tilde{\varphi}$ induces an isomorphism of B-modules

$$\tilde{\varphi} : B \otimes_R \tilde{M}_B \to B \otimes_R \tilde{M}_A.$$

Lemma 4.4. *The isomorphism $\tilde{\varphi}$ induces an isometry of symmetric bundles*

$$(B \otimes_R \tilde{M}_B, \tilde{q}_{B,B}) \simeq (B \otimes_R \tilde{M}_A, \tilde{q}_{A,B}).$$

Proof. This is an easy verification that we leave to the reader. $\square$

We can now complete the proof of the theorem. It follows from Lemmas 4.3 and 4.4 that

$$\tilde{\varphi}^{-1} \circ \nu_B : (B \otimes_R M, q_B) \to (B \otimes_R \tilde{M}_B, \tilde{q}_{B,B})$$

is an isometry. Let $C = B \otimes_R B$ and let $q_i : B \to C, 1 \leq i \leq 2$ be the morphisms as considered prior to Lemma 4.2 at the beginning of this section. For $1 \leq i \leq 2$ the map $\tilde{\varphi}^{-1} \circ \nu_B$ induces, by scalar extension, an isometry:

$$\tilde{\varphi}_i^{-1} \circ \nu_C : (C \otimes_R M, q_C) \to (C \otimes_R \tilde{M}_B, \tilde{q}_{B,C}).$$

This implies that $\sigma = (\tilde{\varphi}_1^{-1} \circ \nu_C)^{-1} \circ (\tilde{\varphi}_2^{-1} \circ \nu_C) = \nu_C^{-1} \circ (\tilde{\varphi}_1 \circ \tilde{\varphi}_2^{-1})\tilde{\nu}_C$ is a 1-cocycle representative of $(M_{\rho,X}, q_{\rho,X})$. Our goal is now to describe this map.

Let c (resp. m) be an element of C (resp. M). Since $\tilde{\varphi}_1 \circ \tilde{\varphi}_2^{-1}$ commutes with action of A^D, it follows from the definitions that

$$\big(\tilde{\varphi}_1 \circ \tilde{\varphi}_2^{-1}\big) \circ \nu_C(c \otimes m) = \theta^D\big(\big(\varphi_1 \circ \varphi_2^{-1}\big)\big(\lambda^{-1/2}\theta\big) \otimes (c \otimes m)\big).$$

It is easily checked that $\Delta(\theta) = \lambda\Delta(e)$ is invariant under the twist map. We then deduce from Remark, Section 4.2, that $(\varphi_1 \circ \varphi_2^{-1})(\lambda^{-1/2}\theta) = \lambda^{-1/2}(g^{-1}\theta)$, where g is the representative of $c(X)$ we constructed previously in Section 4.1. It now follows from Lemma 4.3 that

$$\begin{aligned}\theta^D\big((\varphi_1\circ\varphi_2^{-1})\big(\lambda^{-1/2}\theta\big)\otimes(c\otimes m)\big) &= \theta^D\big(\lambda^{-1/2}\big(g^{-1}\theta\big)\otimes(c\otimes m)\big)\\ &= \theta^D\big(\lambda^{-1/2}\theta\otimes g(c\otimes m)\big).\end{aligned}$$

This implies that $\sigma(c\otimes m)=\nu_C^{-1}(\theta^D(\lambda^{-1/2}\theta\otimes g(c\otimes m)))=g(c\otimes m)$. This tells us that $\rho(g)$ is a representative of $(M_{\rho,X},q_{\rho,X})$ and so completes the proof of the theorem.

5. Examples

5.1. The unit form. Let A be a commutative, finite and flat Hopf algebra over a principal ideal domain R. Let θ denote a generator of the module of integrals of A. We define the form κ on $A^D\times A^D$ by the equality:

$$\kappa(u,v)=\big\langle S^D(u)v,\theta\big\rangle$$

for all $u,v\in A^D$.

Proposition 5.1. *The following properties hold.*

(i) *The pair (A^D,κ) is an A-equivariant symmetric bundle.*

(ii) *If A satifies hypothesis* **H**, *then, for any principal homogeneous space B of A, the twist of (A^D,κ) by B coincides with the symmetric bundle $(\mathcal{D}^{-1/2}(B),\mathrm{Tr})$.*

Proof. The form κ is non-degenerate ([C], Corollary 3.5). Moreover, since we know from Proposition 2.3 that $S(\theta)=\theta$, we note that for all $u,v\in A^D$

$$\kappa(u,v)=\big\langle S^D(u)v,\theta\big\rangle=\big\langle S^D(u)v,S(\theta)\big\rangle=\big\langle S^D(v)u,\theta\big\rangle=\kappa(v,u)$$

so that the form is indeed symmetric. Finally, we observe that

$$\kappa(tu,v)=\big\langle S^D(tu)v,\theta\big\rangle=\big\langle S^D(u)S^D(t)v,\theta\big\rangle=\kappa\big(u,S^D(t)v\big).$$

We therefore conclude that the form is A-equivariant.

In order to prove (ii) we shall now assume that A satisfies **H**. In this case, we can provide a new description of (A^D,κ). From now on we use the notation of Section 3 and Corollary 3.3. We let θ (resp. θ^D) be the generator λe (resp. $\lambda^{-1}t$) of $I(A)$ (resp. $I^D(A)$), where λ is an R-basis of $\varepsilon(I(A))$. We consider the map $\varphi: u\mapsto\lambda^{-1/2}u\theta$ from A^D onto $\mathcal{D}^{-1/2}(A)$. We wish to show that this isomorphism of A^D-modules induces an isometry from (A^D,κ) into $(\mathcal{D}^{-1/2}(A),\mathrm{Tr})$. Hence, we need to show that for all $u,v\in A^D$

$$\kappa(u,v)=\mathrm{Tr}\big(\big(\lambda^{-1/2}u\theta\big)\big(\lambda^{-1/2}v\theta\big)\big).$$

It follows from the definitions that

$$\big\langle S^D(u)v,\theta\big\rangle=\lambda\big\langle S^D(u)v,e\big\rangle$$

while $\mathrm{Tr}((\lambda^{-1/2}u\theta)(\lambda^{-1/2}v\theta)) = \lambda t((ue)(ve))$. Writing $u = \sum_{\gamma\in\Gamma} u_\gamma\gamma$ and $v = \sum_{\delta\in\Gamma} v_\delta\delta$, we easily check that

$$\langle S^D(u)v, e\rangle = t\big((ue)(ve)\big) = \sum_{\gamma\in\Gamma} u_\gamma v_\gamma,$$

which is the required equality. Let B be a PHS for A. We wish to describe the twist of (A^D, κ) by B. From the very definition of the twist and from our previous observations, we obtain that

$$\begin{aligned}\big(\tilde{A}^D_B, \tilde{\kappa}_B\big) &\simeq \big(\mathcal{D}^{-1/2}(B) \otimes A^D, \mathrm{Tr} \otimes \kappa\big)^A \\ &\simeq \big(\mathcal{D}^{-1/2}(B) \otimes_R \mathcal{D}^{-1/2}(A), \mathrm{Tr} \otimes_R \mathrm{Tr}\big)^A.\end{aligned}$$

We now deduce from Lemma 4.3(ii) that

$$\big(\mathcal{D}^{-1/2}(B) \otimes_R \mathcal{D}^{-1/2}(A), \mathrm{Tr} \otimes_R \mathrm{Tr}\big)^A \simeq \big(\mathcal{D}^{-1/2}(B), \mathrm{Tr}\big).$$

This proves that $(\mathcal{D}^{-1/2}(B), \mathrm{Tr})$ is the twist of (A^D, κ) by B. □

Remarks.

1. If A satisfies **H**, then the integral θ used in the proof of the proposition has been chosen according to the stipulations of Section 3. It follows that (A^D, κ) is independent of this choice, up to isometry. We refer to (A^D, κ) as the *unit form of* A^D.
2. The Hopf algebra $A = \mathrm{Map}(\Gamma, R)$, with Γ a finite group, obviously satisfies **H**. In this situation, we choose for θ the integral of A defined by $\theta(g) = 1$ if g is the identity and 0 otherwise. We observe that A^D is the group algebra $R[\Gamma]$ and that the form κ is given on elements of Γ by

$$\kappa\big(\gamma, \gamma'\big) = \big\langle \gamma^{-1}\gamma', \theta\big\rangle = \delta_{\gamma,\gamma'}.$$

It follows from these equalities that $\{\gamma \in \Gamma\}$ is an orthonormal basis for κ. Therefore, the symmetric bundle (A^D, κ) is the usual *unit form of* Γ.
3. When G is generically constant, of odd order ($A_K = \mathrm{Map}(\Gamma, K)$, with Γ of odd order), we know from [BL], that after scalar extension to K, the forms become Γ-isometric. Therefore, we have the following isometries of equivariant symmetric bundles:

$$\big(\mathcal{D}^{-1/2}(B), \mathrm{Tr}\big) \otimes_R K \simeq \big(K[\Gamma], \kappa_K\big) \simeq \big(A^D, \kappa\big)_K.$$

This result leads us naturally to compare $(\mathcal{D}^{-1/2}(B), \mathrm{Tr})$ and (A^D, κ) both as R-symmetric bundles and also as A-equivariant symmetric bundles in the general situation.

5.2. An orthogonal representation of μ_n. Consider the R-algebra $A = (R[T]/(T^n - 1)) = R[t]$ with the following additional structure: a comultiplication $\Delta : A \to A \otimes_R A$ induced by $t \mapsto t \otimes t$, a counit ε induced by $t \mapsto 1$ and an antipode $S : A \to A$ induced by $t \mapsto t^{-1} = t^{n-1}$. This is then a Hopf R-algebra which represents the $\mathrm{Spec}(R)$-group scheme μ_n of nth roots of unity. Its dual $A^D = \mathrm{Hom}_R(R[t], R)$ represents the constant group scheme $\mathbf{Z}/n\mathbf{Z}$ over $\mathrm{Spec}(R)$.

We consider the symmetric bundle (V, q) consisting of the R-free module V, of rank 2, with basis $\{\varepsilon_1, \varepsilon_2\}$ and the symmetric bilinear form q defined by

$$q(\varepsilon_k, \varepsilon_k) = 0 \quad \text{for } 1 \leq k \leq 2 \text{ and } q(\varepsilon_1, \varepsilon_2) = 1/2.$$

We note that when R contains a square root of -1, then (V, q), is isometric to $(R^2, x^2 + y^2)$.

It is easy to check that the R-linear map defined by

$$\alpha(\varepsilon_1) = \varepsilon_1 \otimes t, \qquad \alpha(\varepsilon_2) = \varepsilon_2 \otimes t^{n-1}$$

induces an A-comodule structure on V and that (V, q) is an A-equivariant symmetric bundle. Note that the morphism of group schemes, $\rho : \mu_n \to \mathbf{O}(q)$ associated to this form is defined for any R-algebra C by the group homomorphism $\rho_C : \mu_n(C) \to O(q_C)$ where, for $\xi \in \mu_n(C)$, $\rho_C(\xi)$ is given on the basis $\{\varepsilon_1, \varepsilon_2\}$ by

$$\rho_C(\xi)(\varepsilon_1) = \xi\varepsilon_1, \qquad \rho_C(\xi)(\varepsilon_2) = \xi^{-1}\varepsilon_2.$$

When R contains a square root of -1, this is a representation of μ_n into $\mathbf{O}(2)$.

Our goal is now to study the twists of this form by torsors. We now assume that R is a discrete valuation ring of characteristic 0 and of residual characteristic p different from 2. We take $A = ((R[T]/(T^p - 1)) = R[t])$. For any unit $y \in R^\times$, we let B_y be the R-algebra $R[X]/(X^p - y) = R[x]$. The R-linear map $\alpha : B_y \to B_y \otimes A$ defined by $\alpha(x^k) = x^k \otimes t^k, 0 \leq k \leq p-1$, endows B_y with a structure of a A-comodule algebra. Let z be a pth root of y in an algebraic closure of the fraction field of R and let C be the algebra $R[z]$. The map $T \to zX$ induces an isomorphism of C-A comodule algebras from $C \otimes A$ onto $C \otimes B_y$. This proves that B_y is a PHS for A. Checking by hand we verify that

$$\Lambda = \varepsilon\big(I(A)\big) = pR.$$

We now assume that R *contains a square root of* p, denoted by $p^{1/2}$ so that A satisfies hypothesis $\mathbf{H}$. For any unit y of R the twist of (V, q) by B_y is the R-symmetric bundle

$$(V_y, q_y) = \big(\big(p^{-1/2}R[x] \otimes V\big)^A, (\mathrm{Tr} \otimes q)^A\big).$$

Proposition 5.2. *For any unit $y \in R$ there exists an isometry of R-symmetric bundles*:

$$(V, q) \simeq (V_y, q_y).$$

Proof. It suffices to check that the set

$$\{\varepsilon'_{1,y} = p^{-1/2}x^{p-1} \otimes \varepsilon_1, \varepsilon'_{2,y} = p^{-1/2}x \otimes \varepsilon_2\}$$

is a R-basis of V_y and that the R-linear map given by $(\varepsilon_1 \mapsto \varepsilon'_{1,y})$ and $(\varepsilon_2 \mapsto y^{-1}\varepsilon'_{2,y})$ induces an isometry from (V,q) onto (V_y,q_y). □

5.3. A dihedral representation. We construct an example of an orthogonal representation of a non-commutative group scheme which induces, by restriction to the generic fiber, a dihedral representation as defined in [F].

5.3.1. *The Hopf algebra.* Let D denote a dihedral group of order $2n$ with $n > 2$ and with generators and relations:

$$D = \langle \sigma, \tau \mid \sigma^n = 1 = \tau^2, \tau\sigma\tau = \sigma^{-1} \rangle.$$

R denotes an integral domain in which 2 is invertible. We let K denote the field of fractions of R and we suppose that $\mu_n \subset R$. We let H_K denote the group algebra $K[D]$, endowed with its structure of non-commutative Hopf algebra. For any character ϕ of $\langle\sigma\rangle$ we let e_ϕ be the idempotent $n^{-1}\sum_{\varsigma\in\langle\sigma\rangle}\phi(\varsigma)\varsigma^{-1}$ of $K\langle\sigma\rangle$. We consider the split maximal R-order $\mathcal{M}$ in the group algebra $K\langle\sigma\rangle$

$$\mathcal{M} = \bigoplus_{\phi} Re_\phi \supset R\langle\sigma\rangle,$$

where ϕ ranges over the abelian K-valued characters of the cyclic group $\langle\sigma\rangle$. Recall that $\mathcal{M}$ is an R-Hopf order in the group algebra $K\langle\sigma\rangle$ with

$$\Delta(e_\phi) = \sum_{\alpha,\beta\mid\alpha\beta=\phi} e_\alpha \otimes e_\beta.$$

We then let H denote the R-order in $K[D]$ given by the twisted group ring $\mathcal{M}\circ\langle\tau\rangle$; so that we may write

$$\mathcal{M}\circ\langle\tau\rangle = R\langle\tau\rangle \oplus'_\phi R\circ_\phi\langle\tau\rangle \quad \text{if } n \text{ is odd}$$

and

$$\mathcal{M}\circ\langle\tau\rangle = R\langle\tau\rangle \oplus Re_\theta\langle\tau\rangle \oplus'_\phi R\circ_\phi\langle\tau\rangle \quad \text{if } n \text{ is even},$$

where θ is the unique quadratic character of $\langle\sigma\rangle$ if n is even, where $\oplus'_\phi$ denotes the sum over the orbits of abelian characters ϕ of order greater than 2, modulo the action of the involution $\sigma \to \sigma^{-1}$ and where we have set

$$R\circ_\phi\langle\tau\rangle = (Re_\phi + Re_{\overline{\phi}})\circ\langle\tau\rangle \quad \text{with } \tau e_\phi = e_{\overline{\phi}}\tau.$$

LEMMA 5.3. *H is an R-Hopf order in H_K.*

Proof. Basically we need to show that $\Delta(H) \subset H \otimes H$. Since H is generated over$R$ by τ and the various e_ϕ, it will suffice to show that

$$\Delta(\tau) \in H \otimes H \quad \text{and} \quad \Delta(e_\phi) \in H \otimes H.$$

The first follows from the definition of Δ and the second from our previous equalities. □

Henceforth we identify $H_K^D = \mathrm{Map}(D, K)$; so that $\mathrm{Spec}(H_K^D)$ is the constant group scheme over $\mathrm{Spec}(K)$ associated to D. We then define A to be the R-dual

$$A = H^D = \mathrm{Hom}_R(H, R);$$

then $\mathrm{Spec}(A)$ is a non-constant (but generically constant) group scheme over $\mathrm{Spec}(R)$. We note that, since H is a finitely generated projective R-module, it follows that $A^D = (H^D)^D$ is naturally isomorphic to H. We will identify these Hopf algebras.

Lemma 5.4. *Since* 2 *is invertible in* R, *the modules of integrals for the Hopf orders* H *and* A *are*:

(i) $I(H) = 2R.e_D = n^{-1}R.\sum_{d \in D} d$;
(ii) $I(A) = Rn.l_0$ *where for* $d \in D$, $l_0(d) = 1$ *if* $d = 1_D$ *and* 0 *otherwise.*

Moreover, *for any principal homogeneous space* B *for* A, *we have the equality*:

$$\mathcal{D}_B = nB.$$

Proof. It follows from Corollary 3.4 that (i) and (ii) are equivalent. We shall prove (i). Let ϕ_0 be the trivial character of $\langle\sigma\rangle$. We observe that $\varepsilon(e_{\phi_0}) = 1$ while $\varepsilon(e_\phi) = 0\ \forall \phi \neq \phi_0$. Therefore, $x \in I(H)$ if and only if

$$e_\phi x = 0 \quad \forall \phi \neq \phi_0, \qquad e_{\phi_0} x = x \quad \text{and} \quad \tau x = x.$$

We deduce immediately from these equalities that $x \in 2Re_D$ as required. Let B be a PHS for A. It follows from (ii) and Corollary 3.3 that $\mathcal{D}_B = nB$. □

5.3.2. *The equivariant symmetric bundle.* We fix an abelian character χ of the cyclic group $\langle\sigma\rangle$ with order greater than 2, and we consider the quadratic R-module (M, q):

$$M = R\langle\sigma\rangle \circ \langle\tau\rangle.e_\chi = R.e_\chi + R.\tau e_\chi = R.e_\chi + R.e_{\overline{\chi}}\tau$$

endowed with the quadratic form

$$q(x, y) = \frac{1}{2}\,\mathrm{tr}(x.\tau.\overline{y}),$$

where $\mathrm{tr} : K[D] \to K$ denotes the usual trace map where for $d \in D$

$$\mathrm{tr}(d) = 2n \quad \text{if } d = 1_D \quad \text{and} \quad 0 \quad \text{otherwise.}$$

Lemma 5.5. (M, q) *is an* A*-equivariant symmetric bundle.*

Proof. It is immediate from the definition that M is an $H = A^D$-projective module. Note that

$$q(dx, dy) = \frac{1}{2}\operatorname{tr}\bigl(dx.\tau.\overline{y}d^{-1}\bigr) = \frac{1}{2}\operatorname{tr}(x.\tau.\overline{y}) = q(x, y)$$

so that q is indeed D-invariant. Of course we also have

$$q(e_\chi, e_{\overline{\chi}}.\tau) = \frac{1}{2}\operatorname{tr}\bigl(e_\chi \tau^2 e_\chi\bigr) = \frac{1}{2}\operatorname{tr}(e_\chi) = 1,$$
$$q(e_\chi, e_\chi) = 0 = q(e_{\overline{\chi}}.\tau, e_{\overline{\chi}}.\tau);$$

and so q is an R-perfect pairing on M, and in fact is seen to have discriminant -1. □

5.3.3. *Twists of the form.* Let B be a PHS for A over R. The structure map

$$\alpha_B : B \to B \otimes A$$

induces an isomorphism of B-algebras and H-modules

$$id \otimes \alpha_B : B \otimes_R B \simeq B \otimes_R A$$

(recall that H acts on each side via the right-hand factors). We put $C = \langle\sigma\rangle$ and set $E = B^C$.

Proposition 5.6. *E is a PHS for A^C and $\mathcal{D}_{A^C/R} = A^C$.*

Proof. Because B and A are R-flat we have the isomorphism induced by taking the C-fixed points:

$$\beta : B \otimes_R E \simeq B \otimes_R A^C.$$

We know that B is finite and flat and hence faithfully flat over R. Moreover it follows from the definitions that A^C is a finite and free R-module. This implies that $B \otimes_R A^C$ and thus $B \otimes_R E$ is flat over B and so that E is flat over R ([W], Chapter 13, Section 13.3). We have therefore shown that E is a commutative, finite and flat R-algebra.

Let $q : D \to \langle\tau\rangle$ be the quotient group homomorphism with kernel C. Because 2 is invertible in R, we know that $R\langle\tau\rangle$ is the unique maximal R-order in $K\langle\tau\rangle$; and so in particular we see that $\operatorname{Spec}(R\langle\tau\rangle)$ is a closed subgroup scheme of $\operatorname{Spec}(H)$. We recall the inclusions

$$A^C \subset A = \operatorname{Hom}_R(H, R) \subset A_K = \operatorname{Hom}_K\bigl(K[D], K\bigr).$$

The group D acts on A_K via the rule that for all $f \in A_K$, and for all $\gamma \in D$

$${}^\gamma f : \alpha \mapsto f\bigl(\gamma^{-1}\alpha\bigr).$$

It therefore follows that for any $f \in A$ and for any character ϕ of C we have:

$${}^\sigma f(e_\phi) = f\bigl(\sigma^{-1}e_\phi\bigr) = \phi(\sigma)^{-1} f(e_\phi) \quad \text{and}$$
$${}^\sigma f(e_\phi\tau) = f\bigl(\sigma^{-1}e_\phi\tau\bigr) = \phi(\sigma)^{-1} f(e_\phi\tau).$$

Therefore, by using the description of H above, we deduce that dually $\mathrm{Map}(\langle\tau\rangle, R)$ identifies as A^C and so $\mathrm{Spec}(A^C)$ identifies as a quotient group scheme of $\mathrm{Spec}(A)$.

We now observe that β induces an action map

$$\gamma : E \otimes_R E \to E \otimes_R A^C.$$

In order to show that γ is an isomorphism it suffices to prove that B is faithfully flat over E. One checks easily that A is free over A^C. Therefore, $B \otimes_R A$ is free over $B \otimes_R A^C$ and similarly $B \otimes_R B$ is free over $B \otimes_R E$. Using once again that B is faithfully flat over R, we deduce that B is flat over E. Since B is finite over E we conclude that it is faithfully flat over E and thus that γ is an isomorphism. We have proved that E is a PHS for A^C. Since by definition A^C is étale over R, then $\mathcal{D}_{A^C/R} = A^C$. □

We recall that $\mathcal{M}$ denotes the split maximal R-order in $K[C]$. If we let L denote the ring of fractions of E, then $\mathcal{M}_E = E \otimes_R \mathcal{M}$ is the split maximal order in $L[C]$. We consider the duals $\mathcal{N} = \mathrm{Hom}_R(\mathcal{M}, R)$ and $\mathcal{N}_E = \mathcal{N} \otimes_R E = \mathrm{Hom}_E(\mathcal{M}_E, E)$; by duality these are the minimal Hopf orders in $\mathrm{Map}(C, K)$ and $\mathrm{Map}(C, L)$, respectively. Then we have

$$\mathcal{D}_{\mathcal{N}/R} = n\mathcal{N} \quad \text{and} \quad \mathcal{D}_{\mathcal{N}_E/E} = n\mathcal{N}_E.$$

Proposition 5.7. *B is a PHS for $\mathcal{N}_E$ over E.*

Proof. The inclusion map $C \hookrightarrow D$ induces dual maps

$$\begin{tikzcd} \mathcal{M} \arrow[r, hook] \arrow[d] & H \arrow[d] \\ KC \arrow[r, hook] & KD \end{tikzcd}$$

$$\begin{tikzcd} A \arrow[r] \arrow[d] & \mathcal{N} \arrow[d] \\ \mathrm{Map}(D, K) \arrow[r] & \mathrm{Map}(C, K) \end{tikzcd}$$

and the isomorphism $Id \otimes \alpha_B$ induces a map

$$B \otimes_R B \to B \otimes_R A \to B \otimes_R \mathcal{N} \cong B \otimes_E E \otimes_R \mathcal{N} \cong B \otimes_E \mathcal{N}_E;$$

as $\mathcal{M}$ acts trivially on E, this map actually factors through $B \otimes_E B$, and so in summary we have produced the action map

$$B \otimes_E B \to B \otimes_E \mathcal{N}_E.$$

In order to show that this injective map is in fact an isomorphism, we shall show that their discriminants coincide. By the tower formula, we know that

$$\mathcal{D}_{B/E} = \mathcal{D}_{B/R}\mathcal{D}_{E/R}^{-1} = \mathcal{D}_{B/R} = nB;$$

here the second equality comes from Proposition 5.6 and the third equality comes from Lemma 5.4. Since we know that $\mathcal{D}_{\mathcal{N}_E/E} = n\mathcal{N}_E$ we conclude that the map is indeed an isomorphism. □

Next, we consider the ring E over the maximal order $R\langle\tau\rangle$. By the above, we may write E as a direct sum of two rank one free R-modules $E=E_+\oplus E_-$ where τ acts on $E_+=R$ trivially and on E_- by -1. Choosing a generator δ for E_- over R, we have an element of E with the property that $\delta^2\in R$; moreover, as E is a $\langle\tau\rangle$-torsor, we know that in fact $\delta^2\in R^\times$.

We now apply a somewhat similar analysis to B viewed initially as an $\mathcal{M}_E$-module. We assume R to be a local ring. We may then write $B=\bigoplus B_\chi$ with χ ranging over the abelian characters of $\langle\sigma\rangle$, and with each B_χ a free rank one R-module, with generator t_χ and with $t_\chi t_\phi$ divisible by $t_{\chi\phi}$ (see Section 2.e in [CEPT]); since B/E is an $\mathcal{N}_E$-torsor by Proposition 5.7 we can write:

$$B=E[X]\mathrm{mod}\big(X^n-\alpha^n\big)$$

for some $\alpha^n\in E^\times$, with $a=\alpha.{}^\tau\alpha\in R^\times$.

We now assume that A satisfies **H** which reduces to requiring that nR is the square of a principal ideal. For the sake of simplicity, we shall assume that n is a square of R when it is not a unit. We denote by $n^{1/2}$ a square root of n. Moreover, we choose χ as $\langle\sigma\rangle$-character of α. These preparations being in place, we can now determine the twist of (M,q) by B which is defined, according to Definition 2, by:

$$(\tilde{M}_B,\tilde{q}_B)=(cB\otimes_R M,\mathrm{Tr}\otimes q)^A,$$

where $c=1$ (resp. $n^{-1/2}$) if n is a unit (resp. otherwise).

Proposition 5.8. *We have the following equalities*:

(i) $\tilde{M}_B=R\varepsilon_1\oplus R\varepsilon_2$, *where we set*

$$\varepsilon_1=c\alpha^\tau\otimes e_\chi+c\alpha\otimes e_{\bar\chi}\tau\quad\textit{and}\quad\varepsilon_2=c\delta\alpha^\tau\otimes e_\chi-c\delta\otimes e_{\bar\chi}\tau.$$

(ii)

$$\tilde{q}_B(\varepsilon_1,\varepsilon_1)=2a,\qquad\tilde{q}_B(\varepsilon_2,\varepsilon_2)=-2a\delta^2,\qquad\tilde{q}_B(\varepsilon_1,\varepsilon_2)=0.$$

Proof. We recall from the definition that

$$\tilde{M}_B=(cB\otimes_R M)^A=\big\{z\in cB\otimes_R M\mid uz=\varepsilon^D(u)z\ \forall u\in A^D\big\}.$$

One easily checks from the definition of $A^D=H$ that

$$(cB\otimes_R M)^A=(cB\otimes_R M)^D.$$

We now observe that Propositions 5.6 and 5.7 provide us with a free R-basis of B. Moreover, we know the action of D on the elements of this basis. Hence, by a straightforward computation we obtain the equality:

$$(cB\otimes_R M)^C=R\big(c\alpha^\tau\otimes e_\chi\big)+R\big(c\delta\alpha^\tau\otimes e_\chi\big)+R(c\alpha\otimes e_{\bar\chi}\tau)+R(c\delta\alpha\otimes e_{\bar\chi}\tau).$$

It now suffices to take the C-fixed points of the right-hand side of the equality above to obtain (i). In order to prove (ii) we shall assume that n is not a unit;

the easier case where n is a unit is left to the reader. From the definitions, we obtain that

$$(\mathrm{Tr}\otimes q)(\varepsilon_1,\varepsilon_1)=2\,\mathrm{Tr}\big(n^{-1}\alpha\alpha^{\tau}\big)q(e_{\chi},e_{\bar{\chi}}\tau)=4a, \qquad (\mathrm{Tr}\otimes q)(\varepsilon_1,\varepsilon_2)=0$$

and

$$(\mathrm{Tr}\otimes q)(\varepsilon_2,\varepsilon_2)=-2\,\mathrm{Tr}\big(n^{-1}\delta^2\alpha\alpha^{\tau}\big)q(e_{\chi},e_{\bar{\chi}}\tau)=-4a\delta^2.$$

Finally, we have to compare the forms $\mathrm{Tr}\otimes q$ and $(\mathrm{Tr}\otimes q)^A$ on $\tilde{M}_B$. Using Lemmas 2.4 and 5.4, we note that $\tilde{M}_B=\theta^D M_B$, with $\theta^D=n^{-1}\sum_{u\in D}u$. Then, for any element m and n in M_B, we have:

$$\begin{aligned}(\mathrm{Tr}\otimes q)\big(\theta^D m,\theta^D n\big)&=n^{-1}\sum_{u\in D}(\mathrm{Tr}\otimes q)\big(um,\theta^D n\big)\\&=2(\mathrm{Tr}\otimes q)\big(m,\theta^D n\big)=2(\mathrm{Tr}\otimes q)^A\big(\theta^D m,\theta^D n\big).\end{aligned}$$

We conclude that $\tilde{q}_B=\frac{1}{2}(\mathrm{Tr}\otimes q)$ and so (ii) follows from the previous equalities. □

Remark. We observe that the discriminant of the form $\tilde{q}_B$ is equal to $-\delta^2$, up to a square. Therefore, if -1 is a square of R, since we know that δ^2 is not a square of R, we deduce that the discriminant of $\tilde{q}_B$ is not a square and thus that the forms q and $\tilde{q}_B$ are not isometric.

Acknowledgment. We would like to thank the referee for valuable comments.

References

[BL] E. Bayer-Fluckiger and H. W. Lenstra, *Forms in odd degree extensions and self-dual normal bases*, Amer. J. Math. **112** (1990), no. 3, 359–373. MR 1055648

[C] L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Survey and Monographs, vol. 80, Amer. Math. Soc., Providence, RI, 2000. MR 1767499

[CEPT] T. Chinburg, B. Erez, G. Pappas and M. J. Taylor, *Tame actions of group schemes: Integrals and slices*, Duke Math. J. **82** (1996), no. 2, 269–308. MR 1387229

[CNET] P. Cassou-Noguès, B. Erez and M. J. Taylor, *On Fröhlich twisted bundles*, Proceedings of the St. Petersburg Mathematical Society, vol. XI, Amer. Math. Soc. Transl. Ser. 2, vol. 218, Amer. Math. Soc., Providence, RI, 2006, pp. 87–100. MR 2284760

[CCMT] P. Cassou-Noguès, T. Chinburg, B. Morin and M. J. Taylor, *The classifying topos of a group scheme and invariants of symmetric bundles*, Proc. Lond. Math. Soc. (3) **109** (2014), no. 5, 1093–1136. MR 3283612

[D-G] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Avec un appendice Corps de classes local par Michiel Hazewinkel*, North-Holland, Amsterdam, 1970. MR 0302656

[F] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123. MR 0799658

[Kne] M. Knebusch, *Symmetric bilinear forms over algebraic varieties*, Conference on quadratic forms—1976 (G. Orzech, ed.), Queen's Papers in Pure and Appl. Math., vol. 46, Queen's University, Kingston, ON, 1977, pp. 103–283. MR 0498378

[Mc] S. Maclane, *Homology*, Die Grundlehren der Math. Wiss., vol. 114, Springer-Verlag, Berlin, 1967. MR 0349792

[M] J. S. Milne, *Etale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, NJ, 1980. MR 0559531

[P] B. Pareigis, *When Hopf algebras are Frobenius algebras*, J. Algebra **18** (1971), 588–596. MR 0280522

[R] M. Raynaud, *Schémas en groupes de type* $(p,\dots,p)$, Bull. Soc. Math. France **102** (1974), 241–280. MR 0419467

[S] H.-J. Schneider, *Cartan matrix of liftable finite group schemes*, Comm. Algebra **5** (1977), no. 8, 795–819. MR 0439857

[Se1] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), no. 4, 651–676. MR 0780081

[Sw] M. Sweedler, *Hopf algebras*, W.A. Benjamin, New York, 1969. MR 0252485

[T] M. Taylor, *Hopf orders and Galois module structure*, DMV Seminar, vol. 18, Birkhäuser, Basel, 1992. MR 1167451

[W] W. C. Waterhouse, *Introduction to affine group schemes*, Springer-Verlag, New York, 1979. MR 0547117

Philippe Cassou-Noguès, IMB, University of Bordeaux 1, 33405 Talence, France

E-mail address: Philippe.Cassou-Nogues@math.u-bordeaux1.fr

Ted Chinburg, Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104, USA

E-mail address: ted@math.upenn.edu

Baptiste Morin, IMB, University of Bordeaux 1, 33405 Talence, France

E-mail address: Baptiste.Morin@math.u-bordeaux1.fr

Martin J. Taylor, Merton College, Oxford OX1 4JD, UK

E-mail address: martin.taylor@merton.ox.ac.uk