

CUBIC STRUCTURES AND IDEAL CLASS GROUPS

GEORGIOS PAPPAS*

ABSTRACT. We establish a generalization of Breen’s theory of cubic structures on line bundles over group schemes. We study such “ n -cubic structures” inductively using multiextensions. As a result we obtain information on the set of isomorphism classes of line bundles with n -cubic structures over finite multiplicative group schemes over $\text{Spec}(\mathbf{Z})$ by relating this set to certain corresponding eigenspaces of ideal class groups of cyclotomic fields.

1. INTRODUCTION

Let \mathcal{L} be a line bundle over an abelian variety A . Consider the line bundle $\Theta_3(\mathcal{L})$ over the triple product $A \times \times A \times A$ whose fiber over the point (x, y, z) is

$$\Theta_3(\mathcal{L})_{(x,y,z)} := \mathcal{L}_{x+y+z} \otimes \mathcal{L}_{x+y}^{-1} \otimes \mathcal{L}_{y+z}^{-1} \otimes \mathcal{L}_{z+x}^{-1} \otimes \mathcal{L}_x \otimes \mathcal{L}_y \otimes \mathcal{L}_z \otimes \mathcal{L}_0^{-1}.$$

The classical theorem of the cube states that for any such \mathcal{L} , the line bundle $\Theta_3(\mathcal{L})$ is trivial. Since all regular functions on A are constants, any trivialization of $\Theta_3(\mathcal{L})$ satisfies certain additional compatibility conditions which were explained by L. Breen in [Br]. Breen studied the resulting structure in great detail and generality. In particular, he considered line bundles \mathcal{L} over a general commutative group scheme H : A trivialization of $\Theta_3(\mathcal{L})$ which satisfies certain conditions is called in [Br] a “cubic structure” on \mathcal{L} . (These conditions generalize the aforementioned compatibilities and so are satisfied automatically when H is an abelian variety). This notion of “cubic structure” is closely related to the notion of a biextension which was introduced previously by Mumford and Grothendieck. If $\xi : \mathcal{O}_{H \times H \times H} \xrightarrow{\sim} \Theta_3(\mathcal{L})$ is a cubic structure on \mathcal{L} , then the line bundle $\Theta_2(\mathcal{L})$ over $H \times H$ with fiber over (x, y) given by $\Theta_2(\mathcal{L})_{(x,y)} = \mathcal{L}_{x+y} \otimes \mathcal{L}_x^{-1} \otimes \mathcal{L}_y^{-1} \otimes \mathcal{L}_0$ supports the structure of a (symmetric) biextension. Conversely, if \mathcal{M} is a line bundle over $H \times H$ with a structure of a symmetric biextension, then the diagonal pull-back $\Delta^*(\mathcal{M})$ is a line bundle over H which supports a corresponding cubic structure.

In this paper, we study a generalization of the notion of cubic structure: For a line bundle \mathcal{L} over a commutative group scheme over H and $n \geq 2$, we consider trivializations ξ of the line bundle $\Theta_n(\mathcal{L})$ over $H^n = H \times \cdots \times H$ that satisfy appropriate “cubic” conditions (see Definition 3.1). We call such trivializations n -cubic structures on \mathcal{L} (for $n = 3$, we essentially recover the notion of [Br]). Our main results concern line bundles with n -cubic

Date: April 11, 2005.

* Supported by NSF Grants # DMS02-01140 and # DMS01-11298 (via the Institute for Advanced Study).

structures over finite multiplicative group schemes over \mathbf{Z} . Roughly speaking, we show that the set of isomorphism classes of line bundles with n -cubic structure (\mathcal{L}, ξ) over such group schemes is controlled by certain eigenspaces of ideal class groups of cyclotomic fields. As a corollary of classical results on the structure of these ideal class groups, we see that line bundles over finite multiplicative group schemes that support an n -cubic structure for some n are often trivial.

To state precisely some of our results we will need some additional notation. Recall that the k -th Bernoulli number B_k is defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!} .$$

Also, recall that by work of Borel ([Bo]), the Quillen K-groups $K_m(\mathbf{Z})$ are finite for even integers $m \geq 2$. For a prime p , and $a = p^k \cdot a' \in \mathbf{Z}_{>0}$ with $\gcd(a', p) = 1$, we set $\text{ord}_p(a) = p^k$. We set $h_p^+ = \#\text{Cl}(\mathbf{Q}(\zeta_p + \zeta_p^{-1}))$ and for $u \in \mathbf{Z}_{>0}$

$$e(u) = \begin{cases} 1 & , \text{ if } u = 1, \\ \text{numerator}(B_n/n) & , \text{ if } u \text{ is even,} \\ \prod_{p,p|h_p^+} \text{ord}_p(\#K_{2u-2}(\mathbf{Z})) & , \text{ if } u > 1 \text{ is odd.} \end{cases}$$

Let G be a finite abelian group and $n \geq 2$. We set $H = G_{\text{Spec}(\mathbf{Z})}^D = \text{Spec}(\mathbf{Z}[G])$ for the Cartier dual of the constant group scheme G .

Theorem 1.1. *The group of isomorphism classes (see §3.b (i)) of line bundles with n -cubic structure (\mathcal{L}, ξ) over $H = G_{\text{Spec}(\mathbf{Z})}^D$ is annihilated by*

$$M_{n-1} = M_{n-1}(G) = \prod_{k=1}^{n-1} \prod_{p,p|e(k)} \text{ord}_p(\#G) .$$

In particular, if \mathcal{L} is a line bundle over H which supports an n -cubic structure then we have $\mathcal{L}^{\otimes M_{n-1}} \simeq \mathcal{O}_H$.

Notice that since $B_2 = 1/6$, $B_4 = -1/30$ and $K_4(\mathbf{Z})$ is trivial ([Ro]), we have $M_{n-1}(G) = 1$ for $n \leq 5$ and all G . We also show (see Theorem 8.4 in the text):

Theorem 1.2. *Suppose \mathcal{L} is a line bundle over $H = G_{\text{Spec}(\mathbf{Z})}^D$ which supports an n -cubic structure. If the prime divisors of $\#G$ are bigger than or equal to n and satisfy Vandiver's conjecture, then the line bundle $\nu^*(\mathcal{L})$ which is obtained as the pull-back of \mathcal{L} by the normalization morphism $\nu : \tilde{H} \rightarrow H$ is trivial.*

Vandiver's conjecture (sometimes also attributed to Kummer) for the prime p is the statement that p does not divide the class number h_p^+ . This has been verified numerically for all $p < 12 \cdot 10^6$ [BCEM]. However, there is doubt about its truth in general (see [W], p. 158). By Rim's theorem ([Ri]) when $\#G = p$, ν^* gives an isomorphism between the Picard groups $\text{Pic}(\mu_p)$ and $\text{Pic}(\tilde{\mu}_p) \simeq \text{Cl}(\mathbf{Q}(\zeta_p))$. Hence, Theorem 1.2 implies the following: If the

line bundle \mathcal{L} over μ_p supports an n -cubic structure with $n \leq p$ and p satisfies Vandiver's conjecture, then \mathcal{L} is trivial.

The proofs of these results proceed via an inductive analysis of n -cubic structures. Our approach uses “ n -extensions” –this notion generalizes that of a biextension ($n = 2$) and already appears in [SGA7I]. To an n -cubic structure $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ we associate the structure of a “symmetric $n - 1$ -extension” $E(\mathcal{L}, \xi)$ on the line bundle $\Theta_{n-1}(\mathcal{L})$ over H^{n-1} . This generalizes the construction of the symmetric biextension on $\Theta_2(\mathcal{L})$ associated to the cubic structure (\mathcal{L}, ξ) which was described in the beginning of the introduction. We show that if $E(\mathcal{L}, \xi)$ is isomorphic to the trivial symmetric $n - 1$ -extension, then the n -cubic structure ξ on \mathcal{L} is obtained by an $n - 1$ -cubic structure ξ' on \mathcal{L} via a standard functorial procedure. Now consider the pull-back $\Delta^*(E(\mathcal{L}, \xi))$ via the diagonal $\Delta : H \rightarrow H^{n-1}$. Another key technical statement (Proposition 5.4) is that we can write

$$(1.1) \quad \mathcal{L}^{\otimes(n-1)!} = \Delta^*(E(\mathcal{L}, \xi)) \otimes \mathcal{L}^{\flat}$$

where \mathcal{L}^{\flat} has an $n - 1$ -cubic structure. These results allow us to inductively study n -cubic structures via (symmetric) n -extensions. For example, an inductive argument using (1.1) shows that we can write the $(n - 1)!! := (n - 1)!(n - 2)! \cdots 1!$ -th power of \mathcal{L} as a product of line bundles

$$(1.2) \quad \mathcal{L}^{\otimes(n-1)!!} = \bigotimes_{i=0}^{n-2} \delta(\mathcal{L}^{(i)})^{\otimes(n-i-2)!!} \otimes 0^* \mathcal{L}^{\otimes(n-1)!!}$$

where $\delta(\mathcal{L}^{(i)})$ is obtained via a diagonal pull-back from a line bundle over H^{n-i-1} that carries a structure of a symmetric $n - 1 - i$ -extension.

When $H = \mu_r$, with $r = p^m$ a prime power, the group of (symmetric) n -extensions over H can now be determined as follows: First we see that we can consider multiextensions of $\mathbf{Z}/r\mathbf{Z}$ -torsors over H^{n-1} instead. We then show that such multiextensions are given by families of unramified extensions of the fields $\mathbf{Q}(\zeta_{p^k})$ for $k \leq m$, which satisfy certain properties. Using class field theory one can see that these are described by appropriate eigenspaces of the p -primary part of the ideal class group $\text{Cl}(\mathbf{Q}(\zeta_{p^k}))$. Theorem 1.1 then follows from results on the relation of the orders of these eigenspaces with Bernoulli numbers and the orders of the Quillen K-groups $K_m(\mathbf{Z})$ (Herbrand's theorem, work of Soulé, Kurihara). To discuss Theorem 1.2 set $C(p^k) = \text{Cl}(\mathbf{Q}(\zeta_{p^k}))$ and use the superscript (j) to denote the eigenspace of $C(p^k)/p^k$, ${}_p C(p^k)$ (the p^k -torsion in $C(p^k)$) where $\text{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^*$ acts via the j -th power of the Teichmüller character $\omega : (\mathbf{Z}/p\mathbf{Z})^* \rightarrow \mathbf{Z}_p^*$. Recall the classical reflection homomorphism

$$R_k^{(j)} : \text{Hom}((C(p^k)/p^k)^{(1-j)}, p^{-k}\mathbf{Z}/\mathbf{Z}) \rightarrow ({}_p C(p^k))^{(j)}.$$

We show that the map which associates to the pair (\mathcal{L}, ξ) of a line bundle with n -cubic structure over μ_r the isomorphism class of $\nu^*(\mathcal{L})^{\otimes(n-1)!!}$ can be written as a composition of homomorphisms in which one of factors is the direct sum $\bigoplus_{j=1}^{n-1} \bigoplus_{k=1}^m R_k^{(j)}$. When p satisfies

Vandiver’s conjecture, the reflection homomorphisms are all trivial. This leads to the proof of Theorem 1.2.

Our study of cubic structures is motivated by the observation ([P]) that they play an important role in the theory of geometric Galois modules. The key link is the fact that the functor on line bundles given by the square of the determinant of cohomology along a projective flat morphism of relative dimension d is equipped with a $d + 2$ -cubic structure (of functors between strictly commutative Picard categories; see [Du]). This follows from [De] for $d = 1$ and was shown by Ducrot ([Du]) in general. Using this, Theorems 1.1 and 1.2 allow us to extend the results of [P] to higher dimensional varieties and are basic for understanding coherent fixed point formulas for finite abelian group actions on varieties over \mathbf{Z} (see [CPT]). These applications are treated in separate articles.

The author would like to thank T. Chinburg, M. Taylor, R. Kulkarni and L. Washington for useful conversations and the referee for helpful comments.

2. PICARD CATEGORIES AND TORSORS

2.a. A (commutative) *Picard category* is a non-empty category \mathcal{P} in which all morphisms are isomorphisms and which is equipped with an “addition” functor $+ : \mathcal{P} \times \mathcal{P} \rightarrow \mathcal{P}$, $(p_1, p_2) \mapsto p_1 + p_2$, associativity isomorphisms $\sigma_{p_1, p_2, p_3} : (p_1 + p_2) + p_3 \xrightarrow{\sim} p_1 + (p_2 + p_3)$, functorial in p_1, p_2, p_3 , and commutativity isomorphisms $\tau_{p_1, p_2} : p_1 + p_1 \xrightarrow{\sim} p_2 + p_1$ functorial in p_1, p_2 which satisfy the axioms described in [SGA4] XVIII, 1.4. If we have $\tau_{p, p} = \text{Id}_{p+p}$, for all objects p of \mathcal{P} then we say that the Picard category is “strictly commutative” (s.c.).

A commutative group defines a “discrete” s.c. Picard category: The objects are the elements of the group, the only morphisms are the identity morphisms and the addition is given by the group law. For a scheme S the category of invertible sheaves of \mathcal{O}_S -modules on S with morphisms isomorphisms of \mathcal{O}_S -modules and “addition” given by tensor product over \mathcal{O}_S is a s.c. Picard category which we will denote by $\text{PIC}(S)$ (see [De]).

2.b. Let $H \rightarrow S$ be a group scheme *flat and affine over S* . We refer to [DG] III for the notion of an H -torsor. Under our assumptions, this is given by a scheme $p : T \rightarrow S$ with right action of H and p affine faithfully flat such that the map $T \times_S H \rightarrow T \times_S T$ given by $(t, h) \mapsto (t \cdot h, t)$ is an isomorphism. If Y is an S -scheme we will occasionally use the expression “ $X \rightarrow Y$ is an H -torsor” to mean that $X \rightarrow Y$ is a torsor for the group scheme $H_Y := H \times_S Y \rightarrow Y$. If $\pi : X \rightarrow Y$ is an H -torsor, then π is affine and flat and identifies Y with the (categorical) quotient X/H . In fact, this quotient is *universal* in the sense that for every base change $S' \rightarrow S$, the natural morphism

$$(2.1) \quad (X \times_S S')/H \rightarrow (X/H) \times_S S'$$

is an isomorphism. If $H \rightarrow S$ is in addition of finite presentation then so is $\pi : X \rightarrow Y$.

For more details on the following the reader can refer to [DG] III §4. A morphism between two torsors $T_1 \rightarrow S, T_2 \rightarrow S$, is an S -morphism $f : T_1 \rightarrow T_2$ which commutes with the H -action; by descent such a morphism is necessarily an isomorphism. Assume now in addition that $H \rightarrow S$ is commutative; let $T_1 \rightarrow S, T_2 \rightarrow S$ be two H -torsors. We let the group scheme H act on the fiber product $T_1 \times_S T_2$ by $(t_1, t_2) \cdot h = (t_1 \cdot h, t_2 \cdot h^{-1})$. The quotient $(T_1 \times_S T_2)/H$ then gives an H -torsor over S (the action is via $(t_1, t_2) \cdot h = (t_1 \cdot h, t_2)$) which we will denote by $T_1 \cdot T_2$. We can see that there are canonical isomorphisms of H -torsors $T_1 \cdot (T_2 \cdot T_3) \simeq (T_1 \cdot T_2) \cdot T_3, T_1 \cdot T_2 \simeq T_2 \cdot T_1$; these give to the category of H -torsors over S the structure of a s.c Picard category.

Denote by \mathbf{G}_m the multiplicative group scheme over $\text{Spec}(\mathbf{Z})$. For a scheme S , there a natural additive functor equivalence between the s.c Picard category $\text{PIC}(S)$ of invertible \mathcal{O}_S -sheaves and the s.c Picard category of \mathbf{G}_{mS} -torsors over S given by $\mathcal{L} \rightarrow \underline{\text{Isom}}_{\mathcal{O}_S}(\mathcal{O}_S, \mathcal{L})$. (In what follows, for simplicity, we will denote the \mathbf{G}_{mS} -torsor associated to the invertible sheaf \mathcal{L} again by \mathcal{L}).

2.c. In what follows we let G be a finite commutative group. For a scheme S we will denote by G_S the constant group scheme $\sqcup_{g \in G} S$ given by G . Denote by G_S^D the Cartier dual group scheme of G_S ; by definition, this represents the sheaf of characters $\underline{\text{Hom}}(G_S, \mathbf{G}_{mS})$. When $S = \text{Spec}(\mathbf{Z})$ we will often abuse notation and simply write G instead of G_S . Let us recall that if $\pi : T \rightarrow S$ is a G -torsor over S then the morphism π is finite and étale ([D-G] III, §2, n° 6).

3. HYPERCUBIC STRUCTURES

3.a. Let $H \rightarrow S$ be a commutative S -group scheme. For $n \geq 1$, we will denote by $H^n := H \times \cdots \times H$ the n -fold fiber product over S (for simplicity, we will often omit the subscript S in the notation of the product). If I is a subset of the index set $\{1, \dots, n\}$, we will denote by m_I the morphism $H^n \rightarrow H$ given on points by $(h_1, \dots, h_n) \mapsto \sum_{i \in I} h_i$ (if $I = \emptyset$, $m_I(h_1, \dots, h_n) = 0$). When $I = \{i\}$, then m_I is the i -th projection $p_{i,H} : H^n \rightarrow H$. Recall that we identify the s.c. Picard category of invertible sheaves over an S -scheme T with the s.c. Picard category of \mathbf{G}_{mT} -torsors on T (see 2.b). [SGA4] XVIII 1.4.3 implies that the “tensor operations” we use in what follows to define invertible sheaves or \mathbf{G}_m -torsors give results that are well-defined up to coherent canonical isomorphism.

If \mathcal{L} is an invertible sheaf on H , then we set

$$(3.1) \quad \Theta_n(\mathcal{L}) = \bigotimes_{I \subset \{1, \dots, n\}} m_I^*(\mathcal{L})^{(-1)^{n-\#I}}$$

(an invertible sheaf on H^n). A permutation $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ induces a corresponding S -isomorphism $\sigma : H^n \rightarrow H^n$. Since $m_I \circ \sigma = m_{\sigma(I)}$ permuting the factors of 3.1 gives a canonical isomorphism

$$(3.2) \quad \mathfrak{P}_\sigma : \sigma^* \Theta_n(\mathcal{L}) \xrightarrow{\sim} \Theta_n(\mathcal{L}) .$$

Now suppose that $n \geq 2$ and consider the morphisms $A, B, C, D : H^{n+1} \rightarrow H^n$ given by

$$(3.3) \quad A(h_0, h_1, h_2, \dots, h_n) = (h_0 + h_1, h_2, \dots, h_n),$$

$$(3.4) \quad B(h_0, h_1, h_2, \dots, h_n) = (h_0, h_1, h_3, \dots, h_n),$$

$$(3.5) \quad C(h_0, h_1, h_2, \dots, h_n) = (h_0, h_1 + h_2, h_3, \dots, h_n),$$

$$(3.6) \quad D(h_0, h_1, h_2, \dots, h_n) = (h_1, h_2, h_3, \dots, h_n).$$

We can observe that there is a canonical isomorphism

$$(3.7) \quad \Omega : A^* \Theta_n(\mathcal{L}) \otimes B^* \Theta_n(\mathcal{L}) \xrightarrow{\sim} C^* \Theta_n(\mathcal{L}) \otimes D^* \Theta_n(\mathcal{L})$$

which is obtained by contracting duals and permuting factors (cf. [Br] §2 or [AHS] §2). (The order in which these operations are performed in the s.c. Picard category is of no consequence; the isomorphism remains the same. This can be viewed as a consequence of [SGA4] XVIII 1.4.3.)

Finally observe that if $(0, \dots, 0) : S \rightarrow H^n$ is the zero section, there is a canonical isomorphism

$$(3.8) \quad \mathfrak{A} : (0, \dots, 0)^* \Theta_n(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_S .$$

Definition 3.1. *Let $n \geq 2$. An n -cubic structure on the invertible sheaf \mathcal{L} over H is an isomorphism of invertible sheaves on H^n*

$$(3.9) \quad \xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$$

(i.e a choice of a global generator $\xi(1)$ of $\Theta_n(\mathcal{L})$) which satisfies the following conditions:

c0) It is “rigid”, i.e if $(0, \dots, 0) : S \rightarrow H^n$ is the zero section, then

$$\mathfrak{A}((0, \dots, 0)^*(\xi(1))) = 1 .$$

c1) It is “symmetric”, i.e for all $\sigma \in S_n$,

$$\mathfrak{P}_\sigma(\sigma^*(\xi(1))) = \xi(1) .$$

c2) It satisfies the “cocycle condition”

$$\Omega(A^*(\xi(1)) \otimes B^*(\xi(1))) = C^*(\xi(1)) \otimes D^*(\xi(1)) .$$

Remark 3.2. a) This definition also appears in [AHS] 2.39. For $n = 3$ it is a slight variant of Breen’s definition of a cubic structure ([Br] §2; see also Moret-Bailly [MB]). To explain this set

$$\Theta(\mathcal{L}) := \bigotimes_{\emptyset \neq I \subset \{1,2,3\}} m_I^*(\mathcal{L})^{(-1)^{3-\#I}} = \Theta_3(\mathcal{L}) \otimes m_\emptyset^* \mathcal{L}.$$

(Recall that $m_\emptyset : H^3 \rightarrow H$ is the zero homomorphism). There are isomorphisms analogous to (3.2) and (3.7) for $\Theta(\mathcal{L})$. According to Breen, a cubic structure on \mathcal{L} is a trivialization $t : \mathcal{O}_{H^3} \xrightarrow{\sim} \Theta(\mathcal{L})$ which respects these isomorphisms (i.e satisfies conditions analogous to (c1) and (c2)). On the other hand, (3.8) induces a canonical isomorphism

$$0^* \mathcal{L} \xrightarrow{\sim} (0, 0, 0)^* \Theta(\mathcal{L}).$$

Hence, t also induces a “rigidification” of \mathcal{L} , i.e an isomorphism $\mathcal{O}_S \xrightarrow{\sim} 0^*\mathcal{L}$ which we will denote by $r(t)$. For any invertible sheaf \mathcal{L} on H now set $\mathcal{L}^{\text{rig}} := \mathcal{L} \otimes p^*0^*\mathcal{L}^{-1}$, $p : H \rightarrow S$ the structure morphism. The invertible sheaf \mathcal{L}^{rig} is equipped with a canonical rigidification r_{can} and so there is a canonical isomorphism

$$\phi_{\text{can}} : \Theta_3(\mathcal{L}) \xrightarrow{\sim} \Theta(\mathcal{L}^{\text{rig}}).$$

One can now verify that $\xi \mapsto t(\xi) := \phi_{\text{can}} \cdot \xi$ gives a bijective correspondence between the set of 3-cubic structures ξ on \mathcal{L} in the sense above and the set of Breen’s cubic structures t on \mathcal{L}^{rig} which satisfy $r(t) = r_{\text{can}}$ (cf. [Br] §2.8 and [AHS] Remark 2.44).

b) In what follows, we will often denote various invertible sheaves by giving their fibers over a “general” point of the base. For example, we can denote $\Theta_3(\mathcal{L})$ as

$$\mathcal{L}_{x+y+z} \otimes \mathcal{L}_{x+y}^{-1} \otimes \mathcal{L}_{y+z}^{-1} \otimes \mathcal{L}_{z+x}^{-1} \otimes \mathcal{L}_x \otimes \mathcal{L}_y \otimes \mathcal{L}_z \otimes \mathcal{L}_0^{-1}.$$

(This gives the fiber of $\Theta_3(\mathcal{L})$ over the point (x, y, z) of H^3 .)

3.b. i) By definition, an isomorphism between the invertible sheaves with n -cubic structures (\mathcal{L}, ξ) and (\mathcal{L}', ξ') is an isomorphism $\phi : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ such that

$$\Theta_n(\phi) \cdot \xi = \xi' ,$$

where $\Theta_n(\phi) : \Theta_n(\mathcal{L}) \xrightarrow{\sim} \Theta_n(\mathcal{L}')$ is functorially induced from ϕ . If (\mathcal{L}, ξ) , (\mathcal{L}', ξ') are invertible sheaves with n -cubic structures we define their product

$$(\mathcal{L}, \xi) \cdot (\mathcal{L}', \xi') = (\mathcal{L} \otimes \mathcal{L}', \xi * \xi')$$

where $\xi * \xi'$ is the composition

$$\mathcal{O}_{H^n} = \mathcal{O}_{H^n} \otimes_{\mathcal{O}_{H^n}} \mathcal{O}_{H^n} \xrightarrow{\xi \otimes \xi'} \Theta_n(\mathcal{L}) \otimes_{\mathcal{O}_{H^n}} \Theta_n(\mathcal{L}') \xrightarrow{\alpha} \Theta_n(\mathcal{L} \otimes \mathcal{L}')$$

with α the standard natural isomorphism. We can see that the pairs (\mathcal{L}, ξ) give the objects of a s.c. Picard category $n\text{-CUB}(H, \mathbf{G}_m)$ with arrows given by isomorphisms as above and “addition” given by the above product. (This is similar to the corresponding statement for Breen’s cubic structures; see [Br] §2).

ii) Suppose that the invertible sheaf \mathcal{L} on H is trivial via $\psi : \mathcal{O}_H \xrightarrow{\sim} \mathcal{L}$. This then induces a trivialization

$$(3.10) \quad \Theta_n(\psi) : \mathcal{O}_{H^n} = \Theta_n(\mathcal{O}_H) \xrightarrow{\sim} \Theta_n(\mathcal{L}) .$$

A second trivialization $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ can now be given via the ratio of the generators

$$(3.11) \quad c = \xi(1)/\Theta_n(\psi)(1) \in \Gamma(H^n, \mathcal{O}_{H^n}^*) .$$

In this case, we can see that $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ gives an n -cubic structure on \mathcal{L} if and only if the element c satisfies:

$$\text{c0) } c(0, \dots, 0) = 1,$$

$$\text{c1) } c(h_{\sigma(1)}, \dots, h_{\sigma(n)}) = c(h_1, \dots, h_n), \text{ for all } \sigma \in S_n,$$

$$(c2) \quad c(h_0 + h_1, h_2, \dots, h_n)c(h_0, h_1, h_3, \dots, h_n) = c(h_0, h_1 + h_2, h_3, \dots, h_n)c(h_1, h_2, \dots, h_n).$$

(Here h_i , $0 \leq i \leq n$, range over all T -valued points of H , T any S -scheme. Also, for example, $c(h_1, h_2, \dots, h_n) \in \Gamma(T, \mathcal{O}_T^*)$ is obtained from c by pulling back along the morphism $T \rightarrow H^n$ given by (h_1, h_2, \dots, h_n)).

An inductive argument shows that if $c \in \Gamma(H^n, \mathcal{O}_{H^n}^*)$ satisfies (c0), (c1), (c2) above, then it also satisfies

$$(c0') \quad c(h_1, h_2, \dots, h_n) = 1, \text{ if at least one of the } h_i \text{ is } 0.$$

iii) Suppose that $S = \text{Spec}(R)$ and $H = G_S^D$, the Cartier dual of a finite abelian constant group scheme G . Then, $H = \text{Spec}(R[G])$, $H^n = \text{Spec}(R[G \times \dots \times G])$. If $T = \text{Spec}(R')$, then T -valued points $h_i : T \rightarrow H$ correspond to R' -valued characters $\chi_i : G \rightarrow R'^*$. Suppose now that R is local; then $R[G]$ is semi-local and any invertible sheaf \mathcal{L} on $H = \text{Spec}(R[G])$ is trivial. Hence, from (ii), we see that n -cubic structures on \mathcal{L} are given by units $c \in R[G^n]^*$ which satisfy

$$(c0) \quad (1 \otimes \dots \otimes 1)(c) = 1,$$

$$(c1) \quad (\chi_{\sigma(1)} \otimes \dots \otimes \chi_{\sigma(n)})(c) = (\chi_1 \otimes \dots \otimes \chi_n)(c),$$

$$(c2) \quad (\chi_0 \chi_1 \otimes \chi_2 \otimes \dots \otimes \chi_n)(c)(\chi_0 \otimes \chi_1 \otimes \chi_3 \otimes \dots \otimes \chi_n)(c) = \\ (\chi_0 \otimes \chi_1 \chi_2 \otimes \chi_3 \otimes \dots \otimes \chi_n)(c)(\chi_1 \otimes \chi_2 \otimes \dots \otimes \chi_n)(c) .$$

(In these relations $\chi_1 \otimes \dots \otimes \chi_n$ etc. are characters of G^n which are evaluated on the element c of $R[G^n]$).

As above if $c \in R[G^n]^*$ satisfies (c0), (c1), (c2) above (for all characters of G), then it also satisfies

$$(c0') \quad (\chi_1 \otimes \dots \otimes \chi_n)(c) = 1, \text{ if at least one of the characters } \chi_i \text{ is trivial.}$$

Definition 3.3. *An element c of $R[G^n]$ which satisfies (c0), (c1), (c2) above (for all characters of G) is called n -cubic.*

3.c. Suppose that A is an abelian group and $n \geq 1$. Denote by $I[A]$ the augmentation ideal of the group ring $\mathbf{Z}[A]$; by definition, this is the kernel of the ring homomorphism $\mathbf{Z}[A] \rightarrow \mathbf{Z}$; $\sum_a n_a[a] \mapsto \sum_a n_a$. Set

$$(3.12) \quad C_n(A) := \text{Sym}_{\mathbf{Z}[A]}^n I[A]$$

(the n -th symmetric power of the $\mathbf{Z}[A]$ -module $I[A]$; cf. [AHS] 2.3.1 where the reader is also referred to for more details). The abelian group $C_n(A)$ is the quotient of $\text{Sym}_{\mathbf{Z}}^n I[A]$ by all the relations of the form

$$([b + a_1] - [b]) \otimes ([a_2] - [0]) \otimes \dots \otimes ([a_n] - [0]) = \\ = ([a_1] - [0]) \otimes ([b + a_2] - [b]) \otimes \dots \otimes ([a_n] - [0])$$

with $a_1, \dots, a_n, b \in A$. After rearranging and reindexing, this relation can be expressed in terms of the generators $[a_1, \dots, a_n] := ([a_1] - [0]) \otimes \dots \otimes ([a_n] - [0])$ of $\text{Sym}_{\mathbf{Z}}^n I[A]$ as

$$\begin{aligned} [a_1, a_2, \dots, a_n] + [a_0, a_1 + a_2, a_3, \dots, a_n] &= \\ &= [a_0, a_1, a_3, \dots, a_n] + [a_0 + a_1, a_2, \dots, a_n]. \end{aligned}$$

Now suppose that $A = H(\text{Spec}(R'))$, the group of characters of the finite abelian group G with values in the R -algebra R' . We can see by the above that an n -cubic element $c \in R[G^n]^*$ gives a group homomorphism

$$(3.13) \quad \alpha(c) : C_n(A) \rightarrow R'^* ; \quad [\chi_1, \dots, \chi_n] \mapsto (\chi_1 \otimes \dots \otimes \chi_n)(c) .$$

In fact, every element $c \in R[G^n]^*$ which satisfies (c0') gives a group homomorphism

$$\bigotimes_{\mathbf{Z}}^n I[A] \rightarrow R'^* ; \quad ([\chi_1] - [1]) \otimes \dots \otimes ([\chi_n] - [1]) \mapsto (\chi_1 \otimes \dots \otimes \chi_n)(c) .$$

By the above, if this homomorphism factors through $C_n(A)$ (for all R -algebras R') then c is n -cubic.

4. MULTIEXTENSIONS

4.a. Suppose that J and H are two flat commutative group schemes over the scheme S . We will assume that $J \rightarrow S$ is affine. By [SGA7I] VII §1 giving a commutative group scheme extension E of H by J is equivalent to giving, for every S -scheme $U \rightarrow S$ and each U -point $a : U \rightarrow H$ over S , a J_U -torsor E_a with the following additional structure: These torsors should come together with isomorphisms

$$(4.1) \quad c_{a,a'} : E_a \cdot E_{a'} \xrightarrow{\sim} E_{a+a'}$$

which satisfy the commutativity and associativity conditions described by loc. cit. (1.1.4.1) and (1.2.1). Both the torsors and the above isomorphisms should be functorial in the S -scheme U .

4.b. We again refer the reader to [SGA7I] VII for the definition of J -biextensions of commutative group schemes. There is an obvious generalization of both the notions of extension and biextension: the notion of an n -extension of (H, \dots, H) by J . (Often, for simplicity, we will just say “ n -extension of H by J ”; for $n = 1$ this is an extension of commutative group schemes as above and for $n = 2$ a J -biextension of (H, H)). By definition (see loc. cit. Def. 2.1 for $n = 2$ and 2.10.2 in general) such an n -extension is a J -torsor E over H^n equipped with “compatible partial composition laws”. Giving an n -extension of (H, \dots, H) by J is equivalent to giving, for each S -scheme $U \rightarrow S$ and U -valued point (a_1, \dots, a_n) of H^n over S , a J -torsor $E_{(a_1, \dots, a_n)}$ over U with additional structure: These torsors should come together with isomorphisms ($i = 1, \dots, n$)

$$(4.2) \quad c_{a_1, \dots, a_i; a'_i, \dots, a_n}^i : E_{(a_1, \dots, a_i, \dots, a_n)} \cdot E_{(a_1, \dots, a'_i, \dots, a_n)} \xrightarrow{\sim} E_{(a_1, \dots, a_i + a'_i, \dots, a_n)}$$

which satisfy commutativity and associativity conditions. In addition, we require the compatibility between the isomorphisms for a pair $i \neq j$ described by the obvious generalization of [SGA7I] VII (2.1.1). Once again both the torsors and the isomorphisms should be functorial on the S -scheme U .

There is an obvious notion of isomorphism between n -extensions of H by J (it is given by an isomorphism of the corresponding torsors that respects the composition laws (4.2)). The n -extensions of H by J give the objects of a strictly commutative Picard category $n\text{-EXT}(H, J)$ with morphisms given by isomorphisms of n -extensions and a natural product which corresponds to the product of J -torsors. These facts are explained in detail in [SGA7I] Exp. VII §1 and §2 when $n = 1, 2$. The same constructions apply to the general case (see loc. cit. Remark 3.6.7). We will denote by $n\text{-Ext}^1(H, J)$ the commutative group of isomorphism classes of n -extensions of H by J and by $n\text{-Ext}^0(H, J)$ the commutative group of the endomorphisms of the identity object.

Note that sending the class of an n -extension to the class of the underlying J -torsor over H^n defines a group homomorphism

$$(4.3) \quad t : n\text{-Ext}^1(H, J) \rightarrow \mathbb{H}^1(H^n, J).$$

When $J = \mathbf{G}_m$, we can view this as a homomorphism

$$(4.4) \quad t : n\text{-Ext}^1(H, \mathbf{G}_m) \rightarrow \text{Pic}(H^n).$$

4.c. Suppose that E is an n -extension of H by J . If $\sigma \in S_n$ is a permutation, then we also denote by $\sigma : H^n \rightarrow H^n$ the corresponding automorphism. We can see that the pull-back J -torsor σ^*E also supports a canonical structure of an n -extension of H by J . Denote by Δ_n the diagonal homomorphism $H \rightarrow H^n$.

We will say that the n -extension E of H by J is *symmetric* if it comes together with isomorphisms of n -extensions

$$\Psi_\sigma : \sigma^*E \xrightarrow{\sim} E, \quad \text{for each } \sigma \in S_n,$$

which satisfy the following properties:

i) $\Delta_n^* \Psi_\sigma = i_\sigma$ where $i_\sigma : \Delta_n^* \sigma^*E \xrightarrow{\sim} \Delta_n^*E$ is the natural isomorphism of J -torsors obtained by $\sigma \cdot \Delta_n = \Delta_n$.

ii) For every pair $\sigma, \tau \in S_n$, the following diagram is commutative

$$\begin{array}{ccc} \sigma^*(\tau^*E) & \xrightarrow{\sigma^*\Psi_\tau} & \sigma^*E \\ \wr \downarrow & & \downarrow \Psi_\sigma \\ (\tau\sigma)^*E & \xrightarrow{\Psi_{\tau\sigma}} & E \end{array}$$

where the left vertical arrow is the natural isomorphism of J -torsors.

Notice that the trivial n -extension is naturally symmetric. When $n = 1$ every extension is symmetric with $\Psi_{\text{id}} = \text{id}$. By definition, an isomorphism between two symmetric n -extensions $(E, \{\Psi_\sigma\})$ and $(E', \{\Psi'_\sigma\})$ is an isomorphism $f : E \xrightarrow{\sim} E'$ of n -extensions such that for any $\sigma \in S_n$, we have $f \cdot \Psi_\sigma = \Psi'_\sigma \cdot \sigma^*f$.

5. DIFFERENCES AND POLYNOMIAL EXPANSIONS

In this section we assume that $S = \text{Spec}(R)$ and $H = G_S^D$, the Cartier dual of the finite *constant* group scheme given by the abelian group G . The constructions which we will describe below are certainly valid under less restrictive hypotheses. However, we are only going to need them under these assumptions and so we choose to explain them only in this case since then the presentation simplifies considerably. We consider the “ $n - 1$ -th symmetric difference” $\Theta_{n-1}(\mathcal{L})$ of the invertible sheaf with an n -cubic structure (\mathcal{L}, ξ) on H . We first show that $\Theta_{n-1}(\mathcal{L})$ is naturally equipped with the structure of an $n - 1$ -extension and then explain how we can recover a power of (\mathcal{L}, ξ) from such symmetric differences using a “polynomial expansion”.

5.a. Let $n \geq 2$. For $1 \leq i \leq n - 1$ consider the morphisms $A_i, B_i, C_i : H^n \rightarrow H^{n-1}$ given on points by

$$\begin{aligned} A_i(h_1, h_2, \dots, h_n) &= (h_1, \dots, \hat{h}_i, \dots, h_n), \\ B_i(h_1, h_2, \dots, h_n) &= (h_1, \dots, \hat{h}_{i+1}, \dots, h_n), \\ C_i(h_1, h_2, \dots, h_n) &= (h_1, \dots, h_i + h_{i+1}, \dots, h_n), \end{aligned}$$

where \hat{h}_j means “omit h_j ” and where in the last expression $h_i + h_{i+1}$ is placed in the i -th position. If \mathcal{L} is an invertible sheaf on H , we can see from the definitions that there is a canonical isomorphism

$$(5.1) \quad \Theta_n(\mathcal{L}) \xrightarrow{\sim} C_i^* \Theta_{n-1}(\mathcal{L}) \otimes A_i^* \Theta_{n-1}(\mathcal{L})^{-1} \otimes B_i^* \Theta_{n-1}(\mathcal{L})^{-1}.$$

Let now (\mathcal{L}, ξ) be an invertible sheaf with an n -cubic structure over H . We will show how we can associate to the pair (\mathcal{L}, ξ) an $n - 1$ -extension $E(\mathcal{L}, \xi)$ of H by \mathbf{G}_m . The corresponding \mathbf{G}_m -torsor on H^{n-1} is given by $\Theta_{n-1}(\mathcal{L})$. For $n = 3$ a similar construction is described in [Br] §2; the general case follows along the same lines. We sketch the argument below: By composing (5.1) with ξ we obtain an isomorphism

$$(5.2) \quad c^i : A_i^* \Theta_{n-1}(\mathcal{L}) \otimes B_i^* \Theta_{n-1}(\mathcal{L}) \xrightarrow{\sim} C_i^* \Theta_{n-1}(\mathcal{L})$$

of invertible sheaves on H^n . We can verify that these isomorphisms provide the partial composition laws (4.2) of an $n - 1$ -extension: To check that the c^i are commutative, associative and compatible with each other we can reduce to the case that R is local and \mathcal{L} is the trivial invertible sheaf on H (3.b (ii)-(iii)). Then the n -cubic structure ξ on \mathcal{L} is given by an n -cubic element $c \in R[G^n]^*$ and, by the above, the “composition law” c^i is given via multiplication by the element c . Hence, we are reduced to checking certain identities for c . These follow directly from properties (c1) and (c2) of 3.b (ii). More specifically, the commutativity, resp. associativity, property for c^i follows directly from property (c1), resp. (c2), for c . The compatibility between the partial composition laws c^i for various i also follows immediately from (c1) and (c2). As a result, the isomorphisms c^i , $1 \leq i \leq n - 1$, provide $\Theta_{n-1}(\mathcal{L})$ with the structure of an $n - 1$ -extension $E(\mathcal{L}, \xi)$. In fact, we can see that

the construction $(\mathcal{L}, \xi) \mapsto E(\mathcal{L}, \xi)$ is functorial and gives an additive functor

$$n\text{-CUB}(H, \mathbf{G}_m) \rightarrow (n-1)\text{-EXT}(H, \mathbf{G}_m) .$$

Actually, we can see that the $n-1$ -extension $E(\mathcal{L}, \xi)$ is symmetric (in the sense of the previous paragraph) with the symmetry isomorphisms Ψ_σ given by the isomorphisms \mathfrak{P}_σ of (3.2) ($\sigma \in S_{n-1}$). Indeed, it is easy to see that the isomorphisms \mathfrak{P}_σ of \mathbf{G}_m -torsors satisfy the conditions (i) and (ii) of 4.c and it remains to show that they actually give (iso)morphisms of $n-1$ -extensions. An argument as above now shows (by reducing to the case R local and \mathcal{L} trivial) that this follows from the definitions and property (c1).

5.b. In this paragraph, we assume that $n \geq 3$. Let \mathcal{L} be an invertible sheaf over H equipped with an isomorphism

$$\xi' : \mathcal{O}_{H^{n-1}} \xrightarrow{\sim} \Theta_{n-1}(\mathcal{L})$$

For simplicity, we set $A' = A_1$, $B' = B_1$, $C' = C_1$ for the morphisms $H^n \rightarrow H^{n-1}$ of 5.a. Recall the canonical isomorphism (5.1)

$$\Theta_n(\mathcal{L}) \xrightarrow{\sim} C'^* \Theta_{n-1}(\mathcal{L}) \otimes A'^* \Theta_{n-1}(\mathcal{L})^{-1} \otimes B'^* \Theta_{n-1}(\mathcal{L})^{-1} .$$

Define an isomorphism

$$(5.3) \quad \xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$$

by composing the inverse of (5.1) with the trivialization of

$$C'^* \Theta_{n-1}(\mathcal{L}) \otimes A'^* \Theta_{n-1}(\mathcal{L})^{-1} \otimes B'^* \Theta_{n-1}(\mathcal{L})^{-1}$$

induced by $\xi' : \mathcal{O}_{H^{n-1}} \xrightarrow{\sim} \Theta_{n-1}(\mathcal{L})$.

Lemma 5.1. *If (\mathcal{L}, ξ') is a line bundle with an $n-1$ -cubic structure on H , then ξ given by (5.3) gives an n -cubic structure on \mathcal{L} . In fact, the construction $(\mathcal{L}, \xi') \mapsto (\mathcal{L}, \xi)$ gives an additive functor*

$$(n-1)\text{-CUB}(H, \mathbf{G}_m) \rightarrow n\text{-CUB}(H, \mathbf{G}_m) .$$

PROOF. To show the first statement we have to show that the isomorphism (5.3) above satisfies the conditions (c0), (c1), (c2) of Definition 3.1 for an n -cubic structure. For this purpose, we may assume that R is local and that \mathcal{L} is the trivial invertible sheaf on H (see 3.b (ii)). Then the $n-1$ -cubic structure ξ' is given by an $n-1$ -cubic element $c' \in R[G^{n-1}]^* = \Gamma(H^{n-1}, \mathcal{O}_{H^{n-1}}^*)$ and we can see that ξ is given by $c \in R[G^n]^* = \Gamma(H^n, \mathcal{O}_{H^n}^*)$ which is defined by

$$(5.4) \quad c = C'^*(c')A'^*(c')^{-1}B'^*(c')^{-1} .$$

In other words, we have

$$(5.5) \quad c(h_1, h_2, \dots, h_n) = \\ = c'(h_1 + h_2, h_3, \dots, h_n)c'(h_1, h_3, \dots, h_n)^{-1}c'(h_2, h_3, \dots, h_n)^{-1}$$

for all points h_i , $1 \leq i \leq n$, of H . We now have to show that if c' satisfies (c0), (c1), (c2) of 3.b (ii) with n replaced by $n - 1$, then c satisfies (c0), (c1), (c2) for n : It is clear that c satisfies (c0) and that c is symmetric in the “variables” h_1, h_2 and in h_3, \dots, h_n separately. To show that c satisfies (c1) in general, it is enough to show that, in addition, we have

$$(5.6) \quad c(h_1, h_2, h_3, \dots, h_n) = c(h_1, h_3, h_2, \dots, h_n).$$

To explain this we may assume that $n = 3$ (the argument for $n > 3$ is essentially the same). By the cocycle condition (c2) for c' we obtain: $c'(h_2 + h_1, h_3)c'(h_1, h_3)^{-1} = c'(h_2, h_1 + h_3)c'(h_2, h_1)^{-1}$. By multiplying both sides with $c'(h_2, h_3)^{-1}$ and using the symmetry condition for c' we obtain (5.6) and this shows condition (c1) for c . The cocycle condition (c2) for c now follows directly from (5.5). This proves the first statement of the Lemma. To show the second statement we first observe that our construction is functorial. The rest follows from the definition of the product of multiextensions. \square

Lemma 5.2. *Suppose that (\mathcal{L}, ξ) is an invertible sheaf with an n -cubic structure over H which is such that the corresponding $n - 1$ -extension $E(\mathcal{L}, \xi)$ of 5.a is trivial as a symmetric multiextension. Then there is an $n - 1$ -cubic structure ξ' on \mathcal{L} which induces the n -cubic structure ξ by the procedure of Lemma 5.1. Conversely, if the n -cubic structure ξ is induced from an $n - 1$ -cubic structure ξ' by the procedure of Lemma 5.1 then $E(\mathcal{L}, \xi)$ is trivial as a symmetric multiextension.*

PROOF. (For $n = 3$ and general H this is essentially [Br] Prop. 2.11.) Suppose that $E(\mathcal{L}, \xi)$ is trivial as a symmetric $n - 1$ -extension. By definition, this means that there is an isomorphism

$$\xi' : \mathcal{O}_{H^{n-1}} \xrightarrow{\sim} E(\mathcal{L}, \xi) := \Theta_{n-1}(\mathcal{L})$$

which is compatible with the partial composition laws (4.2) and the symmetry isomorphisms

$$\mathfrak{P}_\tau : \tau^* \Theta_{n-1}(\mathcal{L}) \xrightarrow{\sim} \Theta_{n-1}(\mathcal{L})$$

for all $\tau \in S_{n-1}$. Recall that the composition laws on $E(\mathcal{L}, \xi)$ are given by (5.2). We can now see that the isomorphism ξ' is compatible with the composition law for $i = 1$ if and only if $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ is obtained from the isomorphism ξ' by the procedure described in the beginning of 5.b. We just have to show that the isomorphism ξ' defines an $n - 1$ -cubic structure. For this purpose, we may assume that R is local and that \mathcal{L} is the trivial invertible sheaf on H (see 3.b (ii)). As in the proof of the previous lemma, we see that the isomorphisms ξ, ξ' are given by elements $c \in R[G^n]^*$, $c' \in R[G^{n-1}]^*$ respectively which are related by (5.5). Since ξ is an n -cubic structure, c satisfies (c0), (c1) and (c2) of 3.b (ii). We would like to show that c' satisfies (c0), (c1) and (c2) with n replaced by $n - 1$. Property (c0) follows immediately from (5.5). Since ξ' is compatible with the symmetry isomorphisms c' satisfies (c1). It remains to show property (c2); the relevant equation can

be written

$$(5.7) \quad c'(h_1 + h_2, h_3, \dots, h_n) c'(h_2, h_3, \dots, h_n)^{-1} = \\ = c'(h_1, h_2 + h_3, \dots, h_n) c'(h_1, h_2, \dots, h_n)^{-1} .$$

This now follows from Property (c1) for c and (5.5). We will leave the converse to the reader. \square

Remark 5.3. Note that in the paragraph above we assumed that $n \geq 3$. Suppose now that $n = 2$. Then we have $\Theta_{n-1}(\mathcal{L}) = \Theta_1(\mathcal{L}) = \mathcal{L} \otimes 0^* \mathcal{L}^{-1}$. Hence, if $E(\mathcal{L}, \xi)$ is a trivial (1-)extension and $0^* \mathcal{L}$ a trivial invertible \mathcal{O}_H -sheaf then \mathcal{L} is also a trivial invertible \mathcal{O}_H -sheaf.

5.c. Let $n \geq 1$. Suppose that (\mathcal{L}, ξ) is an invertible sheaf with an $n + 1$ -cubic structure over H . If $\Delta_n : H \rightarrow H^n$ is the diagonal morphism, then we can consider the invertible sheaf $\delta(\mathcal{L}, \xi) := \Delta_n^* \Theta_n(\mathcal{L}) = \Delta_n^* E(\mathcal{L}, \xi)$ on H and set

$$(5.8) \quad \mathcal{L}^b := \mathcal{L}^{\otimes n!} \otimes \delta(\mathcal{L}, \xi)^{-1} .$$

Proposition 5.4. *Suppose that $n \geq 2$. Then the invertible sheaf \mathcal{L}^b defined above is equipped with a canonical n -cubic structure ξ^b .*

Remark 5.5. Notice that the invertible sheaf $\delta(\mathcal{L}, \xi)$ is always “rigid”, i.e equipped with an isomorphism $0^* \delta(\mathcal{L}, \xi) \simeq \mathcal{O}_H$. Hence, there is an isomorphism

$$0^* \mathcal{L}^b \simeq 0^* \mathcal{L}^{\otimes n!} .$$

Also notice that when $n = 1$, we have $\mathcal{L}^b = \mathcal{L} \otimes \delta(\mathcal{L}, \xi)^{-1} = \mathcal{L} \otimes \Theta_1(\mathcal{L})^{-1} = 0^* \mathcal{L}$.

Notice that successive application of Proposition 5.4, combined with the above remark, gives the following.

Corollary 5.6. (Polynomial expansion) *There is an isomorphism of invertible sheaves*

$$(5.9) \quad \mathcal{L}^{\otimes n!!} \simeq \bigotimes_{i=0}^{n-1} \delta(\mathcal{L}^{(i)}, \xi^{(i)})^{\otimes (n-i-1)!!} \otimes (0^* \mathcal{L})^{\otimes n!!}$$

where $(\mathcal{L}^{(0)}, \xi^{(0)}) := (\mathcal{L}, \xi)$, $(\mathcal{L}^{(i)}, \xi^{(i)}) := ((\mathcal{L}^{(i-1)})^b, (\xi^{(i-1)})^b)$ and $m!! = m!(m-1)! \cdots 2!$, $1!! = 0!! = 1$. In this tensor product, the sheaf $\delta(\mathcal{L}^{(i)}, \xi^{(i)})$, $0 \leq i \leq n-1$, is a pull-back $\Delta_{n-i}^*(E^{(n-i)})$ where $\Delta_{n-i} : H \rightarrow H^{n-i}$ is the diagonal and $E^{(n-i)}$ on H^{n-i} supports a (symmetric) $n-i$ -extension structure. In particular, for any $m \in \mathbf{Z}$ we have

$$(5.10) \quad m^*(\delta(\mathcal{L}^{(i)}, \xi^{(i)})) \simeq \delta(\mathcal{L}^{(i)}, \xi^{(i)})^{\otimes m^{n-i}} ,$$

where m^* denotes the pull back via multiplication by $m : H \rightarrow H$.

Remark 5.7. Suppose $n = 2$ and set $\mathcal{L}^{\text{rig}} = \mathcal{L} \otimes 0^* \mathcal{L}^{-1}$. Let us consider the pull-back of $\xi : \mathcal{O}_{H^3} \xrightarrow{\sim} \Theta_3(\mathcal{L})$ along $H \rightarrow H^3$; $x \mapsto (x, -x, x)$. This gives an isomorphism

$$(5.11) \quad \delta(\mathcal{L}, \xi) \simeq \mathcal{L}^{\text{rig}} \otimes (-1)^* \mathcal{L}^{\text{rig}} .$$

This in turn induces an isomorphism

$$(5.12) \quad \mathcal{L}^b \simeq \left[\mathcal{L} \otimes (-1)^* \mathcal{L}^{-1} \right] \otimes 0^* \mathcal{L}^{\otimes 2}.$$

The statement of Proposition 5.4 then amounts to the fact that $\mathcal{L} \otimes (-1)^* \mathcal{L}^{-1}$ has a canonical 2-cubic (“square”) structure. This is classical for line bundles on abelian varieties. For $n = 2$, the expansion of Corollary 5.6 is

$$\mathcal{L}^{\otimes 2} \simeq \left[\mathcal{L}^{\text{rig}} \otimes (-1)^* \mathcal{L}^{\text{rig}} \right] \otimes \left[\mathcal{L} \otimes (-1)^* \mathcal{L}^{-1} \right] \otimes (0^* \mathcal{L})^{\otimes 2}.$$

Notice that the identity (5.10) can be interpreted as saying that the term $\delta(\mathcal{L}^{(i)}, \xi^{(i)})$ in the expansion of Corollary 5.6 is of “degree $n - i$ ”. This somewhat justifies our use of the terminology “Polynomial expansion”.

PROOF OF 5.4. For simplicity, we set $E = E(\mathcal{L}, \xi)$, $\delta = \delta(\mathcal{L}, \xi)$. If R' is an R -algebra we consider $H(R') = H(\text{Spec}(R'))$; this is the group of characters of G with values in R' . Let $\chi_0, \chi_1, \dots, \chi_n$ be R' -valued characters of G . If S is a subset of $\{0, \dots, n\}$, we set $\chi_S = \prod_{i \in S} \chi_i$. (Here and below a product, resp. a tensor product, over the empty set is 1, resp. the trivial invertible sheaf.) By the definition, we have

$$(5.13) \quad \Theta_n(\delta)_{(\chi_1, \dots, \chi_n)} = \bigotimes_{S \subset \{1, \dots, n\}} E_{(\chi_S, \dots, \chi_S)}^{(-1)^{n-\#S}}.$$

Repeated application of the composition laws (4.2) now provide functorial isomorphisms

$$(5.14) \quad \bigotimes_{p: \{1, \dots, n\} \rightarrow S} E_{(\chi_{p(1)}, \dots, \chi_{p(n)})} \xrightarrow{\sim} E_{(\chi_S, \dots, \chi_S)}$$

(the tensor product runs over all maps $p: \{1, \dots, n\} \rightarrow S$). Observe that if $S \neq \{1, \dots, n\}$ we have

$$(5.15) \quad \sum_{S'; S \subset S' \subset \{1, \dots, n\}} (-1)^{n-\#S'} = 0.$$

This shows that in the tensor product

$$(5.16) \quad \bigotimes_{S \subset \{1, \dots, n\}} \bigotimes_{p: \{1, \dots, n\} \rightarrow S} E_{(\chi_{p(1)}, \dots, \chi_{p(n)})}^{(-1)^{n-\#S}}$$

the terms for which either $S \neq \{1, \dots, n\}$ or $S = \{1, \dots, n\}$ and p is not surjective contract (canonically). Therefore, we are left with

$$(5.17) \quad \bigotimes_{p: \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}} E_{(\chi_{p(1)}, \dots, \chi_{p(n)})}.$$

Hence, using the symmetry isomorphisms and (5.13) we can see that there is a canonical isomorphism

$$(5.18) \quad (E_{(\chi_1, \dots, \chi_n)})^{\otimes n!} \xrightarrow{\sim} \Theta_n(\delta)_{(\chi_1, \dots, \chi_n)}.$$

Since by definition $E = \Theta_n(\mathcal{L})$ we obtain from (5.18) a canonical isomorphism

$$(5.19) \quad \xi^b : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L}^b) = \Theta_n(\delta^{-1} \otimes \mathcal{L}^{\otimes n!}) \simeq \Theta_n(\delta) \otimes \Theta_n(\mathcal{L})^{\otimes n!}.$$

We will now show that the isomorphism (5.19) above satisfies the conditions (c0), (c1), (c2) of an n -cubic structure. For this purpose, we may assume that R is local and that \mathcal{L} is the trivial invertible sheaf on H (see 3.b (ii)-(iii)). Then all the invertible sheaves in the construction above are also trivial and the hypercubic structure ξ is given by an $n + 1$ -cubic element $c \in R[G^{n+1}]^*$. By unraveling the definition above we can now see that the isomorphism (5.19) is given as multiplication by

$$(5.20) \quad \prod_{S \subset \{1, \dots, n\}} (\chi_1 \otimes \dots \otimes \chi_n)(d_S^{-1})^{(-1)^{n-\#S}}$$

where $d_S \in R[G^n]^*$ and the term $(\chi_1 \otimes \dots \otimes \chi_n)(d_S)$ gives the isomorphism (5.14). (The element d_S gives the isomorphism (5.14) for χ_i , $i = 1, \dots, n$, the “universal” $R[G^n]$ -valued characters $G \rightarrow G^n \subset R[G^n]$, given by $\chi_i(g) = (g_j)_j$, with $g_j = g$ if $j = i$, $g_j = 1$ if $j \neq i$. Notice that if $\#S \leq 1$, then $d_S = 1$.) In fact, it is more convenient to consider the inverse of (5.14) and view that as the composition of several isomorphisms in which the arguments χ_S are unraveled one by one. Suppose that $S = \{i_1 < i_2 < \dots < i_m\} \neq \emptyset$. Then the first of these isomorphisms is

$$(5.21) \quad E_{(\chi_S, \dots, \chi_S)} \xrightarrow{\sim} \bigotimes_{k=1}^m E_{(\chi_{i_k}, \chi_S, \dots, \chi_S)} \cdot$$

By the definition of the composition law of the n -extension $E = E(\mathcal{L}, \xi)$ (see 5.a), this is described by the inverse of the element:

$$\begin{aligned} & (\chi_{i_1} \otimes \prod_{k>1} \chi_{i_k} \otimes \chi_S \otimes \dots \otimes \chi_S)(c) \cdot \\ & \cdot (\chi_{i_2} \otimes \prod_{k>2} \chi_{i_k} \otimes \chi_S \otimes \dots \otimes \chi_S)(c) \cdot \\ & \quad \vdots \\ & \cdot (\chi_{i_{m-1}} \otimes \chi_{i_m} \otimes \chi_S \otimes \dots \otimes \chi_S)(c). \end{aligned}$$

Using 3.c we see that we can write this as the value of the element

$$\left(\sum_{p=1}^{m-1} \{([\chi_{i_p}] - [1]) \otimes ([\prod_{k>p} \chi_{i_k}] - [1])\} \right) \otimes ([\chi_S] - [1]) \otimes \dots \otimes ([\chi_S] - [1])$$

of $C_{n+1}(H(R'))$ at c^{-1} . For simplicity, we set

$$(5.22) \quad A_S = \sum_{k=1}^m ([\chi_{i_k}] - [1]), \quad B_S = \sum_{p=1}^{m-1} \{([\chi_{i_p}] - [1]) \otimes ([\prod_{k>p} \chi_{i_k}] - [1])\} \cdot$$

Similarly, we can now see that the isomorphisms

$$(5.23) \quad E_{(\chi_{i_k}, \chi_S, \dots, \chi_S)} \xrightarrow{\sim} \bigotimes_{p=1}^m E_{(\chi_{i_k}, \chi_{i_p}, \chi_S, \dots, \chi_S)}$$

which give the next step in unraveling the inverse of (5.14) are described by evaluating at c^{-1} the element

$$(5.24) \quad ([\chi_{i_k}] - [1]) \otimes B_S \otimes ([\chi_S] - [1]) \otimes \cdots \otimes ([\chi_S] - [1]).$$

The combined effect (for $k = 1, \dots, m$) of all of these on the tensor product of (5.21) is given by evaluating at c^{-1} the element

$$(5.25) \quad A_S \otimes B_S \otimes (([\chi_S] - [1]))^{\otimes(n-2)}.$$

The next step is unraveling the first remaining χ_S in $E_{(\chi_{i_k}, \chi_{i_p}, \chi_S, \dots, \chi_S)}$. As above, we can see that this is given by the elements

$$(5.26) \quad ([\chi_{i_k}] - [1]) \otimes ([\chi_{i_p}] - [1]) \otimes B_S \otimes ([\chi_S] - [1])^{\otimes(n-3)}$$

with combined effect

$$(5.27) \quad A_S^{\otimes 2} \otimes B_S \otimes ([\chi_S] - [1])^{\otimes(n-3)}$$

and so on. Putting everything together we see that $(\chi_1 \otimes \cdots \otimes \chi_n)(d_S)$ is given by evaluating the element

$$(5.28) \quad \Psi_S(\chi_1, \dots, \chi_n) = \sum_{j=0}^{n-1} A_S^{\otimes j} \otimes B_S \otimes ([\chi_S] - [1])^{\otimes(n-j-1)}$$

of $C_{n+1}(H(R'))$ at c . Hence, the isomorphism (5.19) is given by an element $d \in R[G^n]^*$ which is such that

$$(5.29) \quad (\chi_1 \otimes \cdots \otimes \chi_n)(d) = \left(\sum_{\substack{S \subset \{1, \dots, n\} \\ S \neq \emptyset}} (-1)^{n-\#S} \Psi_S(\chi_1, \dots, \chi_n) \right) (c^{-1}).$$

For simplicity, set

$$(5.30) \quad \Phi(\chi_1, \dots, \chi_n) = \sum_{S \subset \{1, \dots, n\}} (-1)^{n-\#S} \Psi_S(\chi_1, \dots, \chi_n)$$

in $C_{n+1}(H(R'))$ (here by definition $\Psi_\emptyset = 0$). The proof of the proposition will follow if we show the following properties:

- f0) $\Phi(1, \dots, 1) = 0$,
- f1) $\Phi(\chi_{\sigma(1)}, \dots, \chi_{\sigma(n)}) = \Phi(\chi_1, \dots, \chi_n)$, for all $\sigma \in S_n$,
- f2) $\Phi(\chi_0 \chi_1, \chi_2, \dots, \chi_n) + \Phi(\chi_0, \chi_1, \chi_3, \dots, \chi_n) =$
 $= \Phi(\chi_0, \chi_1 \chi_2, \chi_3, \dots, \chi_n) + \Phi(\chi_1, \chi_2, \dots, \chi_n)$.

Property (f0) is obvious and it is enough to concentrate on (f1) and (f2). Let $F = \{\prod_{i=0}^n x_i^{k_i} \mid k_i \in \mathbf{Z}\}$ be the free abelian group generated by the symbols x_0, x_1, \dots, x_n and let us consider $C_k(F) := \text{Sym}_{\mathbf{Z}[F]}^k I[F]$, for $k \geq 1$. Recall that we denote by $I[F]^k$ the k -th power of the augmentation ideal $I[F]$ of the group ring $\mathbf{Z}[F]$.

Lemma 5.8. *The multiplication morphism $a_1 \otimes \cdots \otimes a_k \mapsto a_1 \cdots a_k$ induces an isomorphism*

$$C_k(F) = \text{Sym}_{\mathbf{Z}[F]}^k I[F] \xrightarrow{\sim} I[F]^k \subset \mathbf{Z}[F].$$

PROOF. In this case, $\mathbf{Z}[F] \simeq \mathbf{Z}[u_0, u_0^{-1}, \dots, u_n, u_n^{-1}]$ (the ring of Laurent polynomials in $n+1$ indeterminants) with $I[F]$ corresponding to the ideal $(u_0 - 1, \dots, u_n - 1)$. Consider the ideal $I = (v_0, \dots, v_n)$ in the polynomial ring $\mathbf{Z}[v] := \mathbf{Z}[v_0, \dots, v_n]$. Multiplication $\text{Sym}_{\mathbf{Z}[v]}^k I \rightarrow I^k$ gives an isomorphism and the desired statement follows from this fact by setting $v_i = u_i - 1$ and localizing. \square

Suppose that y_i , $1 \leq i \leq n$, are elements of F . The identities (5.28), (5.30) with χ_i replaced by y_i can be used to define elements $\Psi_S(y_1, \dots, y_n), \Phi(y_1, \dots, y_n) \in C_{n+1}(F)$. The group homomorphism $F \rightarrow H(R')$ given by $x_i \mapsto \chi_i$ induces a homomorphism $C_{n+1}(F) \rightarrow C_{n+1}(H(R'))$ which sends the elements $\Phi(x_1, \dots, x_n), \Phi(x_0 x_1, \dots, x_n)$, to $\Phi(\chi_1, \dots, \chi_n), \Phi(\chi_0 \chi_1, \dots, \chi_n)$ etc. Hence, it is enough to show

$$\begin{aligned} \text{g1)} \quad & \Phi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \Phi(x_1, \dots, x_n), \text{ for all } \sigma \in S_n, \\ \text{g2)} \quad & \Phi(x_0 x_1, x_2, \dots, x_n) + \Phi(x_0, x_1, x_3, \dots, x_n) = \\ & = \Phi(x_0, x_1 x_2, x_3, \dots, x_n) + \Phi(x_1, x_2, \dots, x_n). \end{aligned}$$

In what follows, we will identify $C_k(F)$ with $I[F]^k$ using the multiplication morphism of Lemma 5.8. Furthermore, we will eliminate the brackets from the notation of elements of the group ring $\mathbf{Z}[F]$.

As above, if $S = \{i_1 < \cdots < i_m\} \subset \{1, \dots, n\}$, we set

$$\begin{aligned} (5.31) \quad A_S &= A_S(y_1, \dots, y_n) = \sum_{k=1}^m y_{i_k} - m, \\ B_S &= B_S(y_1, \dots, y_n) = \sum_{p=1}^{m-1} \{(y_{i_p} - 1) \left(\prod_{k>p} y_{i_k} - 1 \right)\}, \end{aligned}$$

and also

$$(5.32) \quad P_S = P_S(y_1, \dots, y_n) = \prod_{k=1}^m y_{i_k} - 1.$$

Lemma 5.9. $\Psi_S(y_1, \dots, y_n) = P_S^n - A_S^n$.

PROOF. By the definition of $\Psi_S(y_1, \dots, y_n)$ we have

$$(5.33) \quad \Psi_S(\chi_1, \dots, \chi_n) = \sum_{j=0}^{n-1} A_S^j B_S P_S^{n-j-1} = B_S \cdot \left(\sum_{j=0}^{n-1} A_S^j P_S^{n-j-1} \right).$$

However, observe that by telescoping we find

$$(5.34) \quad \begin{aligned} B_S(y_1, \dots, y_n) &= \sum_{p=1}^{m-1} \left\{ (y_{i_p} - 1) \left(\prod_{k>p} y_{i_k} - 1 \right) \right\} = \\ &= \left(\prod_{k=1}^m y_{i_k} - 1 \right) - \left(\sum_{k=1}^m y_{i_k} - m \right) = P_S - A_S. \end{aligned}$$

The result now follows from the standard identity. \square

Lemma 5.9 and the definition of $\Phi(y_1, \dots, y_n)$ (cf. (5.30)) now imply

$$(5.35) \quad \Phi(y_1, \dots, y_n) = \sum_{S \subset \{1, \dots, n\}} (-1)^{n-\#S} \left(\left(\prod_{i \in S} y_i - 1 \right)^n - \left(\sum_{i \in S} y_i - \#S \right)^n \right).$$

Notice that (g1) now follows immediately. It remains to show (g2). To do that we will compare terms between the two sides of the equation (g2). Let us consider the left hand side of the equation. Using (5.35) above we can see that it is a sum:

$$Z + Y(x_0 x_1, x_2, \dots, x_n) + Y(x_0, x_1, x_3, \dots, x_n),$$

where we set

$$Y(y_1, \dots, y_n) = - \sum_{S \subset \{1, \dots, n\}} (-1)^{n-\#S} \left(\sum_{i \in S} (y_i - 1) \right)^n,$$

and where Z is a sum of terms which are either of the form $(-1)^{n-(\#T-1)} (\prod_{i \in T} x_i - 1)^n$ or of the form $(-1)^{n-\#T} (\prod_{i \in T} x_i - 1)^n$, for certain $T \subset \{0, 1, \dots, n\}$. More specifically, we can write

$$Z = 2\Sigma_1 + \Sigma_2 + \Sigma_3.$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{\{0,1,2\} \cap T = \emptyset} (-1)^{n-\#T} \left(\prod_{i \in T} x_i - 1 \right)^n, \\ \Sigma_2 &= \sum_{\{0,1,2\} \subset T} (-1)^{n-(\#T-1)} \left(\prod_{i \in T} x_i - 1 \right)^n, \\ \Sigma_3 &= \sum_{\#(T \cap \{0,1,2\})=1} (-1)^{n-\#T} \left(\prod_{i \in T} x_i - 1 \right)^n. \end{aligned}$$

(In these sums, T ranges over subsets of $\{0, 1, \dots, n\}$.) The rest of the terms cancel out since they appear twice but with different signs in $\Phi(x_0 x_1, x_2, \dots, x_n)$ and $\Phi(x_0, x_1, \dots, x_n)$.

Similarly, a careful look at the right hand side of (g2) reveals that it is equal to the sum

$$Z + Y(x_0, x_1 x_2, x_3, \dots, x_n) + Y(x_1, x_2, \dots, x_n).$$

Now observe that the identity

$$\sum_{S \subset \{1, \dots, n\}} (-1)^{n-\#S} \left(\sum_{i \in S} z_i \right)^n = n! z_1 z_2 \cdots z_n$$

gives

$$Y(y_1, \dots, y_n) = -n! \prod_{k=1}^n (y_k - 1).$$

Hence, by the above, we can now conclude that (g2) is equivalent to the identity

$$(5.36) \quad (x_0 x_1 - 1)(x_2 - 1) \cdots (x_n - 1) + (x_0 - 1)(x_1 - 1) \cdots (x_n - 1) = \\ = (x_0 - 1)(x_1 x_2 - 1) \cdots (x_n - 1) + (x_1 - 1)(x_2 - 1) \cdots (x_n - 1),$$

which is easily seen to be true. This concludes the proof of the identity (g2) and of Proposition 5.4. \square

6. MULTIEXTENSIONS AND ABELIAN SHEAVES

In the next few paragraphs, we will not distinguish in our notation between a commutative group scheme A over a scheme T and the sheaf of abelian groups on the site T_{fppf} which is given by the sections of A . We will use the derived category of the homotopy category of complexes of sheaves of abelian groups on T_{fppf} (recall that T_{fppf} is the site of T -schemes which are locally of finite presentation with the fppf topology). Otherwise, we continue with the notations and general set-up of §4. If $Y \rightarrow S$ is an object of S_{fppf} , we will denote by $\mathbf{Z}[Y]$ the abelian sheaf on the fppf site of S which is freely generated by the points of Y (see [SGA4] IV 11). If Y and Y' are two objects of S_{fppf} then there is a canonical isomorphism:

$$(6.1) \quad \mathbf{Z}[Y] \overset{\mathbf{L}}{\otimes} \mathbf{Z}[Y'] = \mathbf{Z}[Y] \otimes \mathbf{Z}[Y'] \simeq \mathbf{Z}[Y \times_S Y'].$$

The natural morphism of sheaves $Y \rightarrow \mathbf{Z}[Y]$ induces a canonical isomorphism ([SGA7I] VII 1.4):

$$(6.2) \quad \text{Ext}^1(\mathbf{Z}[Y], J) \xrightarrow{\sim} \mathbf{H}^1(Y, J_Y).$$

Now suppose that $H \rightarrow S$ is a commutative group scheme which is finite locally free over S . We will denote by $\epsilon_H : \mathbf{Z}[H] \rightarrow H$ the augmentation homomorphism. Then, under 6.2, the homomorphism $\text{Ext}^1(\epsilon_H, J)$ is identified with the natural homomorphism

$$(6.3) \quad \text{Ext}^1(H, J) \rightarrow \mathbf{H}^1(H, J).$$

Suppose F, F' are abelian sheaves (on S_{fppf}) and E a complex of abelian sheaves which is bounded above. Then there is a canonical spectral sequence

$$(6.4) \quad \text{Ext}^p(E, \underline{\text{Ext}}^q(F, F')) \Rightarrow \text{Ext}^{p+q}(E, \mathbf{R}\underline{\text{Hom}}(F, F'))$$

which induces an exact sequence:

$$(6.5) \quad 0 \rightarrow \text{Ext}^1(E, \underline{\text{Hom}}(F, F')) \rightarrow \text{Ext}^1(E, \mathbf{R}\underline{\text{Hom}}(F, F')) \rightarrow \text{Ext}^1(E, \underline{\text{Ext}}^1(F, F')).$$

There is also a canonical isomorphism:

$$(6.6) \quad \text{Ext}^p(E, \mathbf{R}\underline{\text{Hom}}(F, F')) \xrightarrow{\sim} \text{Ext}^p(E \overset{\mathbf{L}}{\otimes} F, F').$$

6.a. By [SGA7I] VII (2.5.4.1) and 3.6.7 (see also loc. cit. 3.6.4, 3.6.5 and the remarks in VIII §0.2) there are canonical isomorphisms

$$(6.7) \quad n\text{-Ext}^0(H, J) \xrightarrow{\sim} \text{Hom}(\underbrace{H \otimes \cdots \otimes H}_n, J),$$

$$(6.8) \quad n\text{-Ext}^1(H, J) \xrightarrow{\sim} \text{Ext}^1(\underbrace{H \otimes^{\mathbf{L}} \cdots \otimes^{\mathbf{L}} H}_n, J).$$

In the source of the second morphism $H \otimes^{\mathbf{L}} \cdots \otimes^{\mathbf{L}} H = ((H \otimes^{\mathbf{L}} \cdots \otimes^{\mathbf{L}} H) \otimes^{\mathbf{L}} H) \otimes^{\mathbf{L}} H$ is the complex, well-defined up to canonical isomorphism in the derived category, obtained by applying successively the derived tensor product functor.

When $J = \mathbf{G}_m$, the discussion in loc. cit. shows that the diagram

$$(6.9) \quad \begin{array}{ccc} n\text{-Ext}^1(H, \mathbf{G}_m) & \xrightarrow{\sim} & \text{Ext}^1(H \otimes^{\mathbf{L}} \cdots \otimes^{\mathbf{L}} H, \mathbf{G}_m) \\ \downarrow t & & \downarrow \\ \text{Pic}(H \times_S \cdots \times_S H) & \xrightarrow{\sim} & \text{Ext}^1(\mathbf{Z}[H] \otimes \cdots \otimes \mathbf{Z}[H], \mathbf{G}_m) \end{array}$$

commutes. Here the second vertical isomorphism is $\text{Ext}^1(\epsilon_H \otimes^{\mathbf{L}} \cdots \otimes^{\mathbf{L}} \epsilon_H, \mathbf{G}_m)$, and the lower horizontal isomorphism is given by (6.2) and (6.1).

6.b. We continue to assume that $H \rightarrow S$ is finite locally free. Once again, we denote by $H^D = \underline{\text{Hom}}(H, \mathbf{G}_m)$ the Cartier dual of H ; let $\{, \} : H^D \times H \rightarrow \mathbf{G}_m$ be the natural pairing. By [SGA7I] VIII Prop. 3.3.1, $\underline{\text{Ext}}^1(H^D, \mathbf{G}_m) = (0)$. Then, the exact sequence (6.5) gives an isomorphism

$$(6.10) \quad \text{Ext}^1(E, H^D) \xrightarrow{\sim} \text{Ext}^1(E, \mathbf{R}\underline{\text{Hom}}(H, \mathbf{G}_m)).$$

By composing (6.8) with (6.10) and (6.6) we obtain a canonical isomorphism

$$(6.11) \quad \text{Ext}^1(\underbrace{H \otimes^{\mathbf{L}} \cdots \otimes^{\mathbf{L}} H}_{n-1}, H^D) \xrightarrow{\sim} n\text{-Ext}^1(H, \mathbf{G}_m),$$

hence also

$$(6.12) \quad (n-1)\text{-Ext}^1(H, H^D) \xrightarrow{\sim} n\text{-Ext}^1(H, \mathbf{G}_m).$$

For $n = 1$, (6.11) amounts to an isomorphism

$$(6.13) \quad \text{H}^1(S, H^D) \simeq \text{Ext}^1(\mathbf{Z}, H^D) \xrightarrow{\sim} \text{Ext}^1(H, \mathbf{G}_m).$$

To describe the isomorphism (6.13), suppose we start with an H^D -torsor $Q \rightarrow S$ which, under (6.2), corresponds to the extension

$$0 \rightarrow H^D \rightarrow Q' \rightarrow \mathbf{Z} \rightarrow 0.$$

Tensoring with H gives an extension

$$0 \rightarrow H^D \otimes H \rightarrow Q' \otimes H \rightarrow H \rightarrow 0$$

which we can push out by $H^D \otimes H \rightarrow \mathbf{G}_m; a \otimes h \mapsto \{a, h\}$, to obtain an extension of H by \mathbf{G}_m . We can see that this push-out extension is isomorphic to

$$(6.14) \quad 1 \rightarrow \mathbf{G}_m \rightarrow (Q \times_S H \times_S \mathbf{G}_m)/H^D \rightarrow H \rightarrow 0.$$

Here the (representable) fppf sheaf in the middle is the quotient sheaf for the action of H^D on $Q \times_S H \times_S \mathbf{G}_m$ given by $(q, h, u) \cdot a = (q \cdot a, h, \{a, h\}^{-1}u)$ and has group structure given via descent by $(q, h, u) \cdot (q', h', u') = (q, hh', \{q^{-1}q', h'\}uu')$. The isomorphism (6.13) and the explicit extension (6.14) are discussed in detail in [Wa]; see Theorems 2 and 3.

(Notice that the fact that $H^1(S, H^D)$ is isomorphic to $\text{Ext}^1(H, \mathbf{G}_m)$ can also be obtained directly from the local-global spectral sequence $H^p(S, \underline{\text{Ext}}^q(H, \mathbf{G}_m)) \Rightarrow \text{Ext}^{p+q}(H, \mathbf{G}_m)$ by using $\underline{\text{Ext}}^1(H, \mathbf{G}_m) = (0)$.)

In fact, we can obtain a similar description for the map (6.12) (cf. [SGA7I] VIII (1.1.6) where the details of this construction for $n = 2$ are left to the reader): Suppose that $Q \rightarrow H^{n-1}$ is the $H_{H^{n-1}}^D$ -torsor supporting the structure of an $n - 1$ -extension of H by H^D . The construction (6.14) applied to $S = H^{n-1}$ provides us with an extension of $H_{H^{n-1}}$ by $\mathbf{G}_{mH^{n-1}}$. The underlying \mathbf{G}_{mH^n} -torsor over $H_{H^{n-1}} = H^n$ then supports a canonical structure of n -extension whose isomorphism class is the image of the class of Q under the map (6.12).

6.c. We continue to assume that $H \rightarrow S$ is finite locally free. For future use we observe that the following diagram is commutative:

$$(6.15) \quad \begin{array}{ccccc} n\text{-Ext}^1(H, \mathbf{G}_m) & \xrightarrow{t} & \text{Pic}(H^n) & \xrightarrow{\Delta_n^*} & \text{Pic}(H) \\ (6.12) \uparrow \wr & & & & \uparrow \Delta_2^* \\ (n-1)\text{-Ext}^1(H, H^D) & & & & \text{Pic}(H \times H) \\ (4.3) \downarrow t & & & & \uparrow t \\ H^1(H^{n-1}, H^D) & \xrightarrow{\Delta_{n-1}^*} & H^1(H, H^D) & \xrightarrow{(6.13) \sim} & \text{Ext}^1(H_H, \mathbf{G}_{mH}). \end{array}$$

This follows from the description of the maps (6.12), (6.13) in the previous paragraph.

6.d. Suppose now that $S = \text{Spec}(R)$ and $H = G_S^D = \text{Spec}(R[G])$ is the Cartier dual of the finite constant abelian group scheme G_S . Let $T \rightarrow S$ be an S -scheme; Suppose $q : Q \rightarrow T$ is a G -torsor; the construction (6.14) gives a corresponding extension of G_T^D by \mathbf{G}_{mT} . Suppose that $S' = \text{Spec}(R') \rightarrow S$ is another S -scheme and consider a character $\chi : G \rightarrow R'^*$; this corresponds to a point $S' \rightarrow G_S^D$ which we will still denote by χ . Now suppose that T' is an $S' \times_S T$ -scheme and consider the morphism $f : T' \rightarrow S' \times_S T \xrightarrow{(\chi, \text{id})} G_T^D = G_S^D \times_S T$. By pulling back the \mathbf{G}_{mT} -torsor underlying the extension (6.14) along $f : T' \rightarrow G_T^D$ we obtain

a $\mathbf{G}_{mT'}$ -torsor (i.e an invertible sheaf) \mathcal{L}_f^Q over T' . By definition, the class of \mathcal{L}_f^Q is the image of the class of Q under the composition

$$(6.16) \quad H^1(T, G) \xrightarrow{(6.13)} \text{Ext}^1(G_T^D, \mathbf{G}_{mT}) \rightarrow \text{Pic}(G_T^D) \xrightarrow{f^*} \text{Pic}(T').$$

Now recall (§2.c) that $q_*(\mathcal{O}_Q)$ is actually a coherent sheaf of $\mathcal{O}_T[G] = \mathcal{O}_T \otimes_R R[G]$ -modules; we may think of it as a coherent $\mathcal{O}_{G_T^D}$ -module which, as we can see using descent, is invertible.

Lemma 6.1. *Let G act on $q_*(\mathcal{O}_Q) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'}$ via $g \cdot (b \otimes t') = g \cdot b \otimes \chi(g)t'$. The sheaf of invariants $(q_*(\mathcal{O}_Q) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'})^G$ is an invertible sheaf of $\mathcal{O}_{T'}$ -modules and we have*

$$\mathcal{L}_f^Q \simeq (q_*(\mathcal{O}_Q) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'})^G.$$

PROOF. This is a special case of [Wa] Theorem 3. It also follows directly from the explicit description of the middle sheaf in the extension (6.14) as a quotient and the fact that in this case of free G -action taking quotient commutes with base change (see (2.1)). \square

Remark 6.2. Suppose that we take $T' = S' \times_S T$ and $f = (\chi, \text{id})$. For simplicity, we set $\mathcal{L}_\chi^Q := \mathcal{L}_{(\chi, \text{id})}^Q$. Then the fact that $\mathcal{L}_{(\chi, \text{id})}^Q$ is obtained from an extension (see (4.1)) implies that

$$(6.17) \quad \mathcal{L}_{\chi^a}^Q \simeq (\mathcal{L}_\chi^Q)^{\otimes a}$$

for any $a \in \mathbf{Z}$.

7. MULTIEXTENSIONS OF FINITE MULTIPLICATIVE GROUP SCHEMES

Suppose that $S = \text{Spec}(\mathbf{Z})$ and $H = G^D$, the Cartier dual of a finite abelian *constant* group scheme G . If $G \simeq \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$, then

$$(7.1) \quad H \simeq \mu_{n_1} \times \cdots \times \mu_{n_r}$$

where $\mu_k = \text{Spec}(\mathbf{Z}[x]/(x^k - 1))$ denotes the group scheme of k -th roots of unity over \mathbf{Z} . Our goal in this section is to understand the category of n -extensions of H by \mathbf{G}_m . The main result is Theorem 7.7.

7.a. Let us suppose that $n \geq 2$.

Lemma 7.1. *With the above notations and assumptions*

$$n\text{-Ext}^0(H, \mathbf{G}_m) = (\text{id}).$$

PROOF. We have ($n \geq 2$)

$$\text{Hom}(\underbrace{H \otimes \cdots \otimes H}_n, \mathbf{G}_m) \simeq \text{Hom}(\underbrace{H \otimes \cdots \otimes H}_{n-1}, H^D).$$

Each element of this last group is given by a morphism $H^{n-1} = H \times_S \cdots \times_S H \rightarrow H^D$. Since H^{n-1} is connected and $H^D \simeq G$ is constant any such morphism factors through the identity section; hence this group is trivial. The result now follows from (6.7). \square

Remark 7.2. a) Lemma 7.1 shows that for $n \geq 2$ the Picard category of n -extensions of H by \mathbf{G}_m is “discrete”, i.e there is at most one isomorphism between any two objects.

b) As a consequence of (a), any two symmetric n -extensions of H by \mathbf{G}_m which are isomorphic as n -extensions are also isomorphic as *symmetric* n -extensions. In particular, if an n -extension of H by \mathbf{G}_m is trivial as an n -extension then it is also trivial as a symmetric n -extension.

7.b. In what follows we will study the group $n\text{-Ext}^1(H, \mathbf{G}_m)$ of isomorphism classes of n -extensions of $H = G^D$ by \mathbf{G}_m . We begin by introducing some notations.

If C is an abelian group and $m \geq 1$ an integer, we will denote by C/m , resp. ${}_m C$, the cokernel, resp. kernel, of the map $C \rightarrow C$ given by multiplication by m . Set $\zeta_r = e^{2\pi i/r}$ and for simplicity denote by $C(r)$ the ideal class group $\text{Cl}(\mathbf{Q}(\zeta_r))$ of the cyclotomic field $\mathbf{Q}(\zeta_r)$. We will identify $(\mathbf{Z}/r\mathbf{Z})^*$ with the Galois group $\text{Gal}(\mathbf{Q}(\zeta_r)/\mathbf{Q})$ by sending $a \in (\mathbf{Z}/r\mathbf{Z})^*$ to σ_a defined by $\sigma_a(\zeta_r) = \zeta_r^a$. Now let p be a prime number; we will denote by v_p , resp. $|\cdot|_p$ the usual p -adic valuation, resp. p -adic absolute value. Consider the Teichmüller character $\omega : (\mathbf{Z}/p\mathbf{Z})^* \rightarrow \mathbf{Z}_p^*$ characterized by $a = \omega(a) \bmod p\mathbf{Z}_p$. For simplicity, set $\Delta = \text{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. We will view Δ as a direct factor of $\text{Gal}(\mathbf{Q}(\zeta_{p^k})/\mathbf{Q})$ for any $k \geq 1$. Suppose D is a $\mathbf{Z}[\Delta]$ -module which is annihilated by a power of p . For $i \in \mathbf{Z}$ we set

$$D^{(i)} = \{d \in D \mid \sigma_a(d) = \omega^i(a)d, \text{ for all } a \in (\mathbf{Z}/p\mathbf{Z})^*\}.$$

We have

$$D = \bigoplus_{0 \leq i \leq p-2} D^{(i)}.$$

We will consider the groups $\text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$, $k \geq 1$; these are naturally $\text{Gal}(\mathbf{Q}(\zeta_{p^k})/\mathbf{Q})$ -modules via

$$(7.2) \quad (\sigma_a(\phi))(c) = \phi(\sigma_a^{-1}(c)) \text{ for } \phi : C(p^k) \rightarrow p^{-k}\mathbf{Z}/\mathbf{Z}.$$

Note that the norm $C(p^k) \rightarrow C(p^{k-1})$ for the extension $\mathbf{Q}(\zeta_{p^k})/\mathbf{Q}(\zeta_{p^{k-1}})$ induces a homomorphism

$$N_{k-1} : \text{Hom}(C(p^{k-1}), p^{-(k-1)}\mathbf{Z}/\mathbf{Z}) \rightarrow \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}).$$

Definition 7.3. For $n \geq 1$, $m \geq 1$, let $\mathcal{C}(n; p^m)$ be the group of m -tuples

$$(f_k)_{1 \leq k \leq m}; \quad f_k \in \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$$

which satisfy

$$\begin{aligned} i) \quad & \sigma_a(f_k) = a^{n-1} f_k, \text{ for all } a \in (\mathbf{Z}/p^k)^*, \\ ii) \quad & N_{k-1}(f_{k-1}) = p^{n-1} f_k. \end{aligned}$$

Remark 7.4. Property (i) implies that

$$\begin{aligned} \mathcal{C}(n; p^m) &\subset \bigoplus_{1 \leq k \leq m} \text{Hom}(C(p^k), p^{-k} \mathbf{Z}/\mathbf{Z})^{(n-1)} = \\ &= \bigoplus_{1 \leq k \leq m} \text{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k} \mathbf{Z}/\mathbf{Z}). \end{aligned}$$

In particular, since $(C(p^k)/p^k)^{(0)} = (0)$ we obtain $\mathcal{C}(1; p^m) = (0)$.

One of the main results in this section is:

Proposition 7.5. *There is a natural injective homomorphism*

$$\psi_n : n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \rightarrow \bigoplus_{1 \leq k \leq m} \text{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k} \mathbf{Z}/\mathbf{Z})$$

with image the subgroup $\mathcal{C}(n; p^m)$.

Before we consider the proof we will discuss some consequences of this result. Observe that $\mathcal{C}(n; p) \simeq \text{Hom}(C(p), \mathbf{Z}/p)^{(n-1)}$. Hence, for $m = 1$ the result amounts to:

Corollary 7.6. *There are natural isomorphisms*

$$n\text{-Ext}^1(\mu_p, \mathbf{G}_m) \xrightarrow{\sim} \text{Hom}(C(p), \mathbf{Z}/p)^{(n-1)} \simeq \text{Hom}((C(p)/p)^{(1-n)}, \mathbf{Z}/p).$$

Recall the definition of the integer $e(n)$ from the Introduction. As we shall now see, Corollary 7.6 can now be used to obtain:

Theorem 7.7. *For every finite abelian group G , the group of isomorphism classes of n -extensions $n\text{-Ext}^1(G^D, \mathbf{G}_m)$ is annihilated by*

$$\prod_{p|e(n)} \text{ord}_p(\#G).$$

In particular, if $(\#G, e(n)) = 1$, then $n\text{-Ext}^1(G^D, \mathbf{G}_m) = (0)$.

PROOF. Using (6.8) we can see that the group $n\text{-Ext}^1(G^D, \mathbf{G}_m)$ is annihilated by the order $\#G$ and that it can be written as direct sum

$$\bigoplus_{p|\#G} n\text{-Ext}^1(G_p^D, \mathbf{G}_m)$$

where G_p is the p -Sylow subgroup of G . The desired result will now follow if we show that $p \nmid e(n)$ implies $n\text{-Ext}^1(G_p^D, \mathbf{G}_m) = (0)$. Using (6.8) again and employing the long exact cohomology sequence which is obtained by unraveling G_p^D into its “simple pieces” (each isomorphic to μ_p) we see that it is enough to show that $p \nmid e(n)$ implies that $n\text{-Ext}^1(\mu_p, \mathbf{G}_m) = (0)$. Corollary 7.6 then implies that it suffices to show that when $p \nmid e(n)$, we have $(C(p)/p)^{(1-n)} = (0)$. This now follows from well-known results on cyclotomic ideal class groups ([W], [Ku], [So]). For the convenience of the reader we sketch the argument (we can assume that p is odd). First of all, when $n \geq 2$ is even the result follows directly from Herbrand’s theorem ([W] Theorem 6.17) and Kummer’s congruences ([W] Cor. 5.14 and

Cor. 5.15). To deal with the case that n is odd, we will use the cohomology groups $H^i(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) := \varprojlim_m H_{\text{et}}^2(\mathbf{Z}[1/p], \mu_p^{\otimes m})$. By [Ku] Lemma 1.2 we have

$$H^2(\mathbf{Z}[1/p], \mu_p^{\otimes n}) \simeq (C(p)/p)^{(1-n)},$$

while since $H^3(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) = (0)$ we can see that

$$H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p \simeq H^2(\mathbf{Z}[1/p], \mu_p^{\otimes n}).$$

(See [So], [Ku] for more details.) For $n \geq 2$, there is a surjective Chern character ([DF]; see [So])

$$\text{ch} : K_{2n-2}(\mathbf{Z}) \rightarrow H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) .$$

Since $(C(p)/p)^{(0)} = (0)$ and $p \nmid h_p^+$ implies that $(C(p)/p)^{(1-n)} = (0)$ for $n > 1$ odd, these facts imply the result. \square

Remark 7.8. a) We have $B_2 = 1/6$, $B_4 = -1/30$ and $K_4(\mathbf{Z})$ is trivial (see [Ro]; in fact, for our purposes it suffices to know that $K_4(\mathbf{Z})$ has at most 6-power torsion. This is somewhat simpler and is shown in Soulé's addendum to [LS]). Hence, we see that Theorem 7.7 implies that for all finite abelian groups G

$$n\text{-Ext}^1(G^D, \mathbf{G}_m) = (0), \text{ for } n = 1, 2, 3, 4.$$

b) Note that [So] gives a doubly exponential bound on the order of $K_{2n-2}(\mathbf{Z})$ for $n > 1$ odd. However, according to the Kummer-Vandiver conjecture, $p \nmid h_p^+$. Assuming this we could replace in the statement of Theorem 7.7 $e(n)$ by $e'(n)$ given by $e'(n) = e(n)$ if n is even, $e'(n) = 1$ if n is odd. Actually when the prime divisors of $\#G$ satisfy the Kummer-Vandiver conjecture (which is true for all primes $< 12 \cdot 10^6$ by the computations of [BCEM]) we have

$$n\text{-Ext}^1(G^D, \mathbf{G}_m) = (0), \text{ for } 1 \leq n \leq 11.$$

Indeed, the first $e'(n)$ which is not equal to 1 is $e'(12) = 691$.

c) Note that the Quillen-Lichtenbaum conjecture, coupled with the argument in the proof of Theorem 7.7 above, implies that for $n > 1$ odd we have $e(n) = 2^a \cdot \#K_{2n-2}(\mathbf{Z})$ ($a \in \mathbf{Z}$).

Before we continue, we observe that Theorem 7.7 together with the results of the previous section imply Theorem 1.1 of the Introduction:

PROOF OF THEOREM 1.1. It follows by successive applications of Theorem 7.7, Lemma 5.1, Lemma 5.2 and Remark 5.3 (in view of Remark 7.2 (b) and the fact that $\text{Pic}(\mathbf{Z}) = (0)$). \square

This combined with Remark 7.8 (a) gives

Corollary 7.9. *Let G be a finite abelian group and $1 \leq n \leq 4$. If \mathcal{L} is an invertible sheaf on $H = G_{\text{Spec}(\mathbf{Z})}^D = \text{Spec}(\mathbf{Z}[G])$ which supports an $n+1$ -cubic structure then $\mathcal{L} \simeq \mathcal{O}_H$.*

PROOF OF PROPOSITION 7.5. Recall that we set $S = \text{Spec}(\mathbf{Z})$. When $n = 1$ the Proposition follows from (6.13), Remark 7.4 and the fact that $H^1(S, \mathbf{Z}/p^m) = (0)$. Now assume that $n \geq 2$ and let $r \geq 1$. Consider the homomorphisms

$$\delta_i : H^1(\mu_r^{n-1}, \mathbf{Z}/r) \rightarrow H^1(\mu_r^n, \mathbf{Z}/r), \quad 1 \leq i \leq n-1,$$

obtained as $m_i^* - p_i^* - q_i^*$ where

$$\begin{aligned} m_i : \mu_r^n &\rightarrow \mu_r^{n-1}; & (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_i x_{i+1}, \dots, x_n), \\ p_i : \mu_r^n &\rightarrow \mu_r^{n-1}; & (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_i, x_{i+2}, \dots, x_n), \\ q_i : \mu_r^n &\rightarrow \mu_r^{n-1}; & (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n). \end{aligned}$$

Lemma 7.10. *There is an exact sequence*

$$0 \rightarrow (n-1)\text{-Ext}^1(\mu_r, \mathbf{Z}/r) \xrightarrow{t} H^1(\mu_r^{n-1}, \mathbf{Z}/r) \xrightarrow{\oplus_i \delta_i} \bigoplus_{1 \leq i \leq n-1} H^1(\mu_r^n, \mathbf{Z}/r).$$

where t is the forgetful map.

PROOF. (Following a suggestion by the referee.) Let $L_\bullet := L_\bullet(\mu_r)$ be the canonical truncated flat resolution of the abelian sheaf μ_r described in [SGA7I] VII (3.5.1):

$$L_2 := \mathbf{Z}[\mu_r^2] \oplus \mathbf{Z}[\mu_r^3] \xrightarrow{d_1} L_1 := \mathbf{Z}[\mu_r^2] \xrightarrow{d_0} L_0 := \mathbf{Z}[\mu_r]$$

The augmentation $\epsilon : L_0 = \mathbf{Z}[\mu_r] \rightarrow \mu_r$ is given by $\epsilon(\sum_i n_i [a_i]) = a_i^{n_i}$. We can also replace L_\bullet by a “normalized” truncated flat resolution \bar{L}_\bullet in which each summand $\mathbf{Z}[\mu_r^k] = (\mathbf{Z}[\mu_r])^{\otimes k}$ in each L_i is replaced by its direct summand $(\mathbf{Z}[\mu_r]/\mathbf{Z}[1])^{\otimes k}$ (here 1 is the identity section and $\mathbf{Z}[\mu_r]/\mathbf{Z}[1] \simeq \mathbf{Z}[\mu_r - 1]$); in particular $\bar{L}_0 = \mathbf{Z}[\mu_r]/\mathbf{Z}[1]$. By (6.8) we can now use the total $n-1$ -fold tensor products $T_\bullet := L_\bullet \otimes \cdots \otimes L_\bullet$ and $\bar{T}_\bullet := \bar{L}_\bullet \otimes \cdots \otimes \bar{L}_\bullet$ to compute $(n-1)\text{-Ext}^1(\mu_r, \mathbf{Z}/r)$. Since the scheme μ_r^k is connected, we have $\text{Hom}(\bar{T}_i, \mathbf{Z}/r) = (0)$ for all i . By using $\text{Hom}(\bar{T}_2, \mathbf{Z}/r) = (0)$ in particular, we obtain $(n-1)\text{-Ext}^1(\mu_r, \mathbf{Z}/r) \simeq \text{Ext}^1([\bar{T}_1 \rightarrow \bar{T}_0], \mathbf{Z}/r)$. Using this, together with $\text{Hom}(\bar{T}_1, \mathbf{Z}/r) = (0)$, we obtain a short exact sequence:

$$(7.3) \quad 0 \rightarrow (n-1)\text{-Ext}^1(\mu_r, \mathbf{Z}/r) \rightarrow \text{Ext}^1(\bar{T}_0, \mathbf{Z}/r) \xrightarrow{\delta} \text{Ext}^1(\bar{T}_1, \mathbf{Z}/r).$$

Recall that by (6.2) $H^1(\mu_r^{n-1}, \mathbf{Z}/r) = \text{Ext}^1(T_0, \mathbf{Z}/r)$ and $\bigoplus_{i=1}^{n-1} H^1(\mu_r^n, \mathbf{Z}/r) = \text{Ext}^1(T_1, \mathbf{Z}/r)$. Now observe that the groups $\text{Ext}^1(\bar{T}_0, \mathbf{Z}/r)$ and $\text{Ext}^1(\bar{T}_1, \mathbf{Z}/r)$ are direct summands of $H^1(\mu_r^{n-1}, \mathbf{Z}/r)$ and $\bigoplus_{i=1}^{n-1} H^1(\mu_r^n, \mathbf{Z}/r)$ respectively; the complements are generated by the classes of \mathbf{Z}/r -torsors which are obtained by pull-back from projections $p_i^k : \mu_r^k \rightarrow \mu_r^{k-1}$, $1 \leq i \leq k$. It follows from the definition that δ is a direct summand of the homomorphism $\oplus_i \delta_i$ in the statement of the Lemma. It is not hard to see that $\ker(\delta) = \ker(\oplus_i \delta_i)$ and the result now follows. \square

We now continue with the proof of Proposition 7.5. Lemma 7.10 applied to $r = p^m$ and (6.12) implies that, for $n \geq 2$, it is enough to show there is a natural isomorphism

$$\mathcal{C}(n; p^m) \xrightarrow{\sim} \ker(H^1(\mu_{p^m}^{n-1}, \mathbf{Z}/p^m) \xrightarrow{\oplus_i \delta_i} \bigoplus_{1 \leq i \leq n-1} H^1(\mu_{p^m}^n, \mathbf{Z}/p^m)).$$

To identify the kernel above, we will follow a technique used by Mazur in [M] §2. For the convenience of the reader we repeat some of Mazur's arguments. Suppose that X and Y are any two schemes equipped with \mathbf{F}_p -valued points

$$(7.4) \quad X \leftarrow \text{Spec}(\mathbf{F}_p) \rightarrow Y.$$

We will use the symbol $X \vee Y$ to refer to any scheme theoretic union of X and Y along a subscheme which is a nilpotent extension of $\text{Spec}(\mathbf{F}_p)$. For $Y = S = \text{Spec}(\mathbf{Z})$ we set

$$\tilde{H}^1(X, \mathbf{Z}/p^m) = H^1(X \vee S, \mathbf{Z}/p^m)$$

(fppf or étale cohomology). There is an exact sequence

$$(7.5) \quad 0 \rightarrow \tilde{H}^1(X, \mathbf{Z}/p^m) \rightarrow H^1(X, \mathbf{Z}/p^m) \rightarrow H^1(\text{Spec}(\mathbf{F}_p), \mathbf{Z}/p^m)$$

obtained using the Mayer-Vietoris exact sequence for étale cohomology, the fact that $\text{Spec}(\mathbf{F}_p)$ is connected and that $H^1(S, \mathbf{Z}/p^m) = (0)$. Hence, $\tilde{H}^1(X, \mathbf{Z}/p^m)$ is independent of the exact scheme theoretic union of X and S used in the definition. A similar calculation, shows that for any diagram as in (7.4), we have

$$(7.6) \quad \tilde{H}^1(X \vee Y, \mathbf{Z}/p^m) = \tilde{H}^1(X, \mathbf{Z}/p^m) \oplus \tilde{H}^1(Y, \mathbf{Z}/p^m).$$

Now set $T_{p^k} = \text{Spec}(\mathbf{Z}[\zeta_{p^k}])$, $1 \leq k \leq m$; this is a closed subscheme of μ_{p^k} . Class-field theory gives a natural isomorphism

$$H^1(T_{p^k}, \mathbf{Z}/p^m) \xrightarrow{\sim} \text{Hom}(C(p^k), \mathbf{Z}/p^m).$$

Since the unique prime ideal of $\mathbf{Z}[\zeta_{p^k}]$ that lies above (p) is principal, by the exact sequence (7.5) and the definition of the Artin map, we have

$$(7.7) \quad \tilde{H}^1(T_{p^k}, \mathbf{Z}/p^m) = H^1(T_{p^k}, \mathbf{Z}/p^m) \xrightarrow{\sim} \text{Hom}(C(p^k), \mathbf{Z}/p^m).$$

Now observe that we have canonical identifications

$$(\mathbf{Z}/p^k)^* = \text{Aut}(\mu_{p^k}) = \text{Aut}(T_{p^k})$$

where $a \in (\mathbf{Z}/p^k)^*$ acts via the operation “raising to the a -th power” on μ_{p^k} . The isomorphism (7.7) is compatible with the action of $(\mathbf{Z}/p^k)^*$ by functoriality of cohomology on the one side and by (7.2) on the other. If $\pi_k : T_{p^k} \rightarrow T_{p^{k-1}}$ is the natural projection, there is a commutative diagram

$$(7.8) \quad \begin{array}{ccccc} \tilde{H}^1(T_{p^{k-1}}, \mathbf{Z}/p^m) & \xlongequal{\quad} & H^1(T_{p^{k-1}}, \mathbf{Z}/p^m) & \xrightarrow{\sim} & \text{Hom}(C(p^{k-1}), \mathbf{Z}/p^m) \\ \pi_k^* \downarrow & & \pi_k^* \downarrow & & \downarrow N_{k-1} \\ \tilde{H}^1(T_{p^k}, \mathbf{Z}/p^m) & \xlongequal{\quad} & H^1(T_{p^k}, \mathbf{Z}/p^m) & \xrightarrow{\sim} & \text{Hom}(C(p^k), \mathbf{Z}/p^m) \end{array}$$

with N_{k-1} induced by the norm. Now notice that $\mu_{p^s}^s$ for any $s \geq 1$, can be obtained as a wedge (in the sense of \vee defined above) of several copies of T_{p^k} , $1 \leq k \leq m$, with S . More precisely, $\mu_{p^s}^s$ is the wedge of S with

$$\bigvee_{1 \leq k \leq m} \left[\bigvee_{(a_1; \dots; a_s) \in \mathbf{P}^{s-1}(\mathbf{Z}/p^k)} T_{p^k} \right].$$

(Here \mathbf{P}^{s-1} denotes the projective space over \mathbf{Z} .) Using (7.6) we can deduce that

$$(7.9) \quad \mathbb{H}^1(\mu_{p^m}^s, \mathbf{Z}/p^m) = \bigoplus_{1 \leq k \leq m} \bigoplus_{(a_1; \dots; a_s) \in \mathbf{P}^{s-1}(\mathbf{Z}/p^k)} \tilde{\mathbb{H}}^1(T_{p^k}, \mathbf{Z}/p^m).$$

Notice that an element $(a_i) = (a_1, \dots, a_s) \in (p^{-k}\mathbf{Z}/\mathbf{Z})^s$ defines a group scheme homomorphism

$$(a_i) : \mu_{p^k} \rightarrow \mu_{p^m}^s ; \quad x \mapsto (x^{p^k a_1}, \dots, x^{p^k a_s})$$

and a scheme morphism

$$(a_i) : T_{p^k} \subset \mu_{p^k} \rightarrow \mu_{p^m}^s.$$

Since $\pi_k(x) = x^p$ we have a commutative diagram

$$(7.10) \quad \begin{array}{ccc} T_{p^k} & \xrightarrow{(pa_i)} & \mu_{p^m}^s \\ \pi_k \downarrow & & \parallel \\ T_{p^{k-1}} & \xrightarrow{(pa_i)} & \mu_{p^m}^s, \end{array}$$

where in the first, resp. second line, (pa_i) is considered as an element of $(p^{-k}\mathbf{Z}/\mathbf{Z})^s$, resp. of $(p^{-(k-1)}\mathbf{Z}/\mathbf{Z})^s$.

Set $U_{p^k}^s = (p^{-k}\mathbf{Z}/\mathbf{Z})^s - (p^{-k+1}\mathbf{Z}/\mathbf{Z})^s$; if (a_i) is in $U_{p^k}^s$ then the corresponding morphism is a closed immersion. Now consider the group of maps

$$\text{Maps}_{(\mathbf{Z}/p^k)^*}(U_{p^k}^s, \tilde{\mathbb{H}}^1(T_{p^k}, \mathbf{Z}/p^m))$$

which are compatible with the natural action of $(\mathbf{Z}/p^k)^*$ on domain and range. Note that $\mathbf{P}^{s-1}(\mathbf{Z}/p^k) \simeq (\mathbf{Z}/p^k)^* \setminus U_{p^k}^s$. We can define a homomorphism

$$(7.11) \quad \mathbb{H}^1(\mu_{p^m}^s, \mathbf{Z}/p^m) \rightarrow \bigoplus_{1 \leq k \leq m} \text{Maps}_{(\mathbf{Z}/p^k)^*}(U_{p^k}^s, \tilde{\mathbb{H}}^1(T_{p^k}, \mathbf{Z}/p^m))$$

by sending $h \in \mathbb{H}^1(\mu_{p^m}^s, \mathbf{Z}/p^m)$ to $(a_i) \mapsto (a_i)^* h$. Using (7.9) we see that (7.11) is an isomorphism. We can also consider the map

$$(7.12) \quad \mathbb{H}^1(\mu_{p^m}^s, \mathbf{Z}/p^m) \rightarrow \bigoplus_{1 \leq k \leq m} \text{Maps}_{(\mathbf{Z}/p^k)^*}((p^{-k}\mathbf{Z}/\mathbf{Z})^s, \tilde{\mathbb{H}}^1(T_{p^k}, \mathbf{Z}/p^m))$$

given by the same rule as the one above. The map (7.12) is injective and using (7.10) we can see that its image is the subgroup of all elements $(\phi_k)_{1 \leq k \leq m}$ which are such that $\phi_k((pa_i)) = \pi_k^* \phi_{k-1}((pa_i))$. Let us denote this subgroup by $F(s; p^m)$. By applying the above to $s = n - 1$, n we can conclude that there are commutative diagrams

$$(7.13) \quad \begin{array}{ccc} \mathbb{H}^1(\mu_{p^m}^{n-1}, \mathbf{Z}/p^m) & \xrightarrow{\delta_i} & \mathbb{H}^1(\mu_{p^m}^n, \mathbf{Z}/p^m) \\ (7.12)_{n-1} \downarrow & & \downarrow (7.12)_n \\ F(n-1; p^m) & \xrightarrow{\delta'_i} & F(n; p^m) \end{array}$$

where the k -th component of $\delta'_i((\phi_k)_{1 \leq k \leq m})$ is the map given by

$$(\dots, a_i, a_{i+1}, \dots) \mapsto \phi_k(\dots, a_i + a_{i+1}, \dots) - \phi_k(\dots, a_i, \dots) - \phi_k(\dots, a_{i+1}, \dots).$$

It now follows that the kernel of $\oplus_i \delta_i$ is isomorphic to the group of m -tuples $(\phi_k)_{1 \leq k \leq m}$ of multilinear maps

$$\phi_k : (p^{-k} \mathbf{Z}/\mathbf{Z})^{n-1} \rightarrow \tilde{\mathbf{H}}^1(T_{p^k}, \mathbf{Z}/p^m) = \text{Hom}(C(p^k), \mathbf{Z}/p^m)$$

which satisfy

$$\begin{aligned} i) \quad & \phi_k(ax_1, \dots, ax_{n-1}) = \sigma_a(\phi_k(x_1, \dots, x_{n-1})), \text{ for all } a \in (\mathbf{Z}/p^k)^*, \\ ii) \quad & \phi_k(px_1, \dots, px_{n-1}) = \pi_k^*(\phi_{k-1}(px_1, \dots, px_{n-1})). \end{aligned}$$

Note that a multilinear map $\phi_k : (p^{-k} \mathbf{Z}/\mathbf{Z})^{n-1} \rightarrow \text{Hom}(C(p^k), \mathbf{Z}/p^m)$ has image which is contained in ${}_p \text{Hom}(C(p^k), \mathbf{Z}/p^m) \simeq \text{Hom}(C(p^k), p^{-k} \mathbf{Z}/\mathbf{Z})$; such a map is uniquely determined by $f_k := \phi_k(p^{-k}, \dots, p^{-k}) \in \text{Hom}(C(p^k), p^{-k} \mathbf{Z}/\mathbf{Z})$. Using (7.8) and the multilinearity we see that conditions (i) and (ii) above translate to

$$\begin{aligned} i)' \quad & \sigma_a(f_k) = a^{n-1} f_k, \text{ for all } a \in (\mathbf{Z}/p^k)^*, \\ ii)' \quad & N_{k-1}(f_{k-1}) = p^{n-1} f_k. \end{aligned}$$

The proof of Proposition 7.5 now follows. \square

Remark 7.11. We can see from the proof that the injective homomorphism

$$(7.14) \quad \psi_n : n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \hookrightarrow \bigoplus_{1 \leq k \leq m} \text{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k} \mathbf{Z}/\mathbf{Z})$$

is obtained as follows: Consider the homomorphism

$$(7.15) \quad \psi'_n : n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \rightarrow \mathbf{H}^1(\mu_{p^m}, \mathbf{Z}/p^m),$$

defined as the composition

$$\begin{aligned} n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) & \rightarrow (n-1)\text{-Ext}^1(\mu_{p^m}, \mathbf{Z}/p^m) \xrightarrow{t} \\ & \xrightarrow{t} \mathbf{H}^1(\mu_{p^m}^{n-1}, \mathbf{Z}/p^m) \xrightarrow{\Delta_{n-1}^*} \mathbf{H}^1(\mu_{p^m}, \mathbf{Z}/p^m) \end{aligned}$$

where the first arrow is the inverse of (6.12), t is the forgetful map and Δ_{n-1}^* is the pull-back along the diagonal $\Delta_{n-1} : \mu_{p^m} \rightarrow \mu_{p^m}^{n-1}$. Then ψ_n is given by the composition of ψ'_n with the isomorphism

$$\mathbf{H}^1(\mu_{p^m}, \mathbf{Z}/p^m) \xrightarrow{\simeq} \bigoplus_{1 \leq k \leq m} \text{Hom}(C(p^k), p^{-m} \mathbf{Z}/\mathbf{Z})$$

obtained by (7.7) and (7.9). Indeed, the maps ϕ_k in the proof of the Proposition are determined by their image on the “diagonal” elements (p^{-k}, \dots, p^{-k}) .

8. REFLECTION HOMOMORPHISMS

In the next few paragraphs, we elaborate on the constructions of the previous section. We continue with the same assumptions and notations. In particular, we again write $T_{p^k} = \text{Spec}(\mathbf{Z}[\zeta_{p^k}])$ which we think of as a closed subscheme of μ_{p^k} . We will denote by $\widetilde{\mu_{p^m}} = \bigsqcup_{0 \leq k \leq m} T_{p^k}$ the normalization of the scheme μ_{p^m} and by $\nu : \widetilde{\mu_{p^m}} \rightarrow \mu_{p^m}$ the natural projection map. Our main goal is to express the composition

$$(8.1) \quad n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \xrightarrow{t} \text{Pic}(\mu_{p^m}^n) \xrightarrow{\Delta_n^*} \text{Pic}(\mu_{p^m}) \xrightarrow{\nu^*} \text{Pic}(\widetilde{\mu_{p^m}})$$

in terms of the classical “reflection homomorphisms” (see below). We do this in Corollary 8.2. We can then deduce some additional results on the pull-back $\nu^*\mathcal{L}$ of an invertible sheaf \mathcal{L} on μ_{p^m} with hypercubic structure.

8.a. Consider the homomorphism (6.16) described in 6.d

$$R_k : \mathbb{H}^1(T_{p^k}, \mathbf{Z}/p^k) \rightarrow {}_{p^k}\text{Pic}(T_{p^k}) ; \quad Q \mapsto \mathcal{L}_{f(\chi_0)}^Q$$

for $G = \mathbf{Z}/p^k$, $S' = T' = T = T_{p^k}$, $\chi_0 : T \hookrightarrow \mu_{p^k}$ the natural closed immersion which corresponds to the character $\chi_0 : \mathbf{Z}/p^k \rightarrow \mathbf{Z}[\zeta_{p^k}]^*$, $\chi_0(1) = \zeta_{p^k}$, and $f(\chi_0) : T' = T \rightarrow \mu_{p^k T}$ the morphism

$$f(\chi_0) : T \xrightarrow{\Delta} T \times_S T \xrightarrow{(\chi_0, \text{id})} \mu_{p^k T} = \mu_{p^k} \times T.$$

Using (7.7) (class field theory) and $C(p^k) = \text{Pic}(T_{p^k})$ we see that this amounts to a homomorphism

$$R_k : \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \rightarrow {}_{p^k}C(p^k).$$

If $Q \rightarrow T_{p^k}$ is a \mathbf{Z}/p^k -torsor there is an unramified Galois extension N of $\mathbf{Q}(\zeta_{p^k})$ with Galois group \mathbf{Z}/p^k and ring of integers \mathcal{O}_N such that the \mathbf{Z}/p^k -torsor Q is $Q = \text{Spec}(\mathcal{O}_N)$. Lemma 6.1 implies that $\mathcal{L}_{f(\chi_0)}^Q$ is isomorphic to the invertible sheaf which corresponds to the locally free rank 1 $\mathbf{Z}[\zeta_{p^k}]$ -module

$$(8.2) \quad L_{\chi_0}^Q := \{\xi \in \mathcal{O}_N \mid \sigma_a(\xi) = \chi_0^{-1}(a)\xi = \zeta_{p^k}^{-a}\xi, \text{ for all } a \in \mathbf{Z}/p^k\}.$$

Notice that $N/\mathbf{Q}(\zeta_{p^k})$ is a Kummer extension. Therefore, it can be obtained by adjoining the p^k -th root of an element $b \in \mathbf{Q}(\zeta_{p^k})^*$: $N = \mathbf{Q}(\zeta_{p^k})(\sqrt[p^k]{b})$. We can arrange so that the element $\sqrt[p^k]{b}$ gives a generic section of $\mathcal{L}_{f(\chi_0)}^Q$; the corresponding divisor of $\mathcal{L}_{f(\chi_0)}^Q$ is given by a fractional ideal I of $\mathbf{Q}(\zeta_{p^k})$ such that $I^{p^k} = (b)$. The class of $\mathcal{L}_{f(\chi_0)}^Q$ corresponds to the class (I) under the isomorphism $\text{Pic}(T_{p^k}) \simeq C(p^k)$. Using this we can see that R_k coincides with the classical “reflection homomorphism”

$$\text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \rightarrow {}_{p^k}C(p^k)$$

(see for example [W] §10.2 for the case $k = 1$; actually the reflection homomorphism defined there is the negative of the one above):

Now observe that the definition of $\mathcal{L}_{f(\chi_0)}^Q$ implies

$$a^*(\mathcal{L}_{f(\chi_0)}^Q) \simeq \mathcal{L}_{f(\chi_0^a)}^{a^*Q}, \quad a \in (\mathbf{Z}/p^k)^*,$$

where a^* denotes the pull-back by the Galois automorphism $a : T_{p^k} \rightarrow T_{p^k}$. Using Lemma 6.1 and (6.17) we see that this gives

$$(8.3) \quad a^*(\mathcal{L}_{f(\chi_0)}^Q) \simeq \mathcal{L}_{f(\chi_0^a)}^{a^*Q} \simeq (\mathcal{L}_{f(\chi_0)}^{a^*Q})^{\otimes a}.$$

The isomorphism (8.3) now implies that R_k “reflects” between odd and even eigenspaces, in fact it decomposes into a direct sum of

$$(8.4) \quad R_k^{(n)} : \text{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z}) = \\ = \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})^{(n-1)} \rightarrow ({}_{p^k}C(p^k))^{(n)}.$$

for $0 \leq n \leq p-2$ (cf. [W] §10.2).

8.b. For notational simplicity, we set $r = p^m$. Recall $\nu : \widetilde{\mu}_r \rightarrow \mu_r$ is the normalization morphism. Let us consider the homomorphism

$$(8.5) \quad \text{H}^1(\mu_r, \mathbf{Z}/r) \rightarrow \text{Pic}(\mu_r) \xrightarrow{\nu^*} \text{Pic}(\widetilde{\mu}_r) = \bigoplus_{1 \leq k \leq m} C(p^k)$$

where the first arrow is the composition

$$(8.6) \quad \text{H}^1(\mu_r, \mathbf{Z}/r) \xrightarrow{(6.13)} \text{Ext}^1(\mu_{r\mu_r}, \mathbf{G}_{m\mu_r}) \xrightarrow{t} \text{Pic}(\mu_r \times \mu_r) \xrightarrow{\Delta_2^*} \text{Pic}(\mu_r).$$

Recall that (7.7) and (7.9) give an isomorphism

$$(8.7) \quad \text{H}^1(\mu_r, \mathbf{Z}/r) \xrightarrow{\sim} \bigoplus_{1 \leq k \leq m} \text{Hom}(C(p^k), p^{-m}\mathbf{Z}/\mathbf{Z}).$$

Now let us restrict the map (8.5) to the subgroup of $\text{H}^1(\mu_r, \mathbf{Z}/r)$ that corresponds to

$$\bigoplus_{1 \leq k \leq m} \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$$

under (8.7). We obtain a homomorphism

$$(8.8) \quad R : \bigoplus_{1 \leq k \leq m} \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \rightarrow \bigoplus_{1 \leq k \leq m} C(p^k).$$

By unraveling the definition of R we see that the description of “reflection homomorphisms” in the above paragraph implies that

Proposition 8.1. *The homomorphism R is a direct sum $R = \bigoplus_{1 \leq k \leq m} R_k$ with*

$$R_k : \text{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \rightarrow {}_{p^k}C(p^k)$$

the “reflection homomorphism” as defined above. \square

We now obtain:

Corollary 8.2. *There is a commutative diagram*

$$\begin{array}{ccccccc}
 n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) & \xrightarrow{t} & \text{Pic}(\mu_{p^m}^n) & \xrightarrow{\Delta_n^*} & \text{Pic}(\mu_{p^m}) & \xrightarrow{\nu^*} & \text{Pic}(\widehat{\mu_{p^m}}) \\
 & & \psi_n \downarrow & & & & \cup \\
 \bigoplus_{1 \leq k \leq m} \text{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z}) & \xrightarrow{\bigoplus_{1 \leq k \leq m} R_k^{(n)}} & & & \bigoplus_{1 \leq k \leq m} ({}_{p^k}C(p^k))^{(n)}. & &
 \end{array}$$

PROOF. Recall that by Remark 7.11, the homomorphism ψ_n is given by the composition of $\psi'_n : n\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \rightarrow H^1(\mu_{p^m}, \mathbf{Z}/p^m)$ with the isomorphism (8.7). The result follows now from the definitions of the homomorphisms R and ψ'_n , Proposition 8.1, and the commutative diagram (6.15) for $H = \mu_{p^m}$: Indeed, we can observe that the composite homomorphism (8.6) essentially gives a half of the commutative diagram (6.15) for $H = \mu_{p^m}$. \square

Remark 8.3. If the prime p satisfies the Kummer-Vandiver conjecture, then the reflection maps $R_k^{(n)}$ are all trivial; indeed, either n or $1 - n$ is even and so either $({}_{p^k}C(p^k))^{(n)}$ or $(C(p^k)/p^k)^{(1-n)}$ is trivial ([W] Cor. 10.6). Then the composition $\nu^* \cdot \Delta_n^* \cdot t$ along the first row of the above diagram is also the trivial homomorphism.

8.c. We now combine the above to obtain an additional result about invertible sheaves with hypercubic structures over $H = \text{Spec}(\mathbf{Z}[G])$, for G any finite abelian group. For an integer $u \geq 1$ set

$$e'(u) = \begin{cases} 1 & , \text{ if } u \text{ is odd,} \\ \text{numerator}(B_u/u) & , \text{ if } u \text{ is even.} \end{cases}$$

(cf. Remark 7.8 (b)). Set

$$M'_n(G) = \prod_{u=1}^n \prod_{p|e'(u)} \text{ord}_p(\#G).$$

Theorem 8.4. *Assume that for all the prime divisors p of the order $\#G$, the eigenspaces $(\text{Cl}(\mathbf{Q}(\zeta_p))/p)^{(s)}$ for all even s in $[1, n] \cup [p - n, p - 1]$ are trivial. (This is true if p satisfies Vandiver's conjecture.) We denote by $\nu : \tilde{H} \rightarrow H$ the normalization morphism. Suppose that \mathcal{L} is an invertible sheaf on H which supports an $n + 1$ -cubic structure ξ and set $C = \text{GCD}(M'_n(G), n!)$. Then $\nu^* \mathcal{L}^{\otimes C} \simeq \mathcal{O}_{\tilde{H}}$. In particular, if in addition all the prime divisors of $\#G$ are $\geq n + 1$, then $\nu^* \mathcal{L} \simeq \mathcal{O}_{\tilde{H}}$.*

PROOF. Suppose that $G = G_{p_1} \times \cdots \times G_{p_k}$ is the decomposition of G into its p -Sylow subgroups. Set $H_{p_j} = (G_{p_j})^D = \text{Spec}(\mathbf{Z}[G_{p_j}])$ and let $\text{pr}_j : H \rightarrow H_{p_j}$ be the natural projection. If all the prime divisors p_j , $1 \leq j \leq k$, of $\#G$ satisfy the assumption of the

theorem then we have $\mathcal{L}^{\otimes M'_n(G)} \simeq \mathcal{O}_H$ by Theorem 1.1 and its proof (cf. Remark 7.8 (b)). On the other hand, Corollary 5.6 gives the “polynomial expansion”

$$\nu^* \mathcal{L}^{\otimes n!!} \simeq \bigotimes_{i=0}^{n-1} (\nu^* \Delta_{n-i}^* E(\mathcal{L}^{(i)}, \xi^{(i)}))^{\otimes (n-i-1)!!} \otimes \nu^* 0^* \mathcal{L}^{\otimes n!!}.$$

Here, the invertible sheaf $E(\mathcal{L}^{(i)}, \xi^{(i)})$ carries the structure of an $(n-i)$ -extension of H by \mathbf{G}_m . Notice that, since $\text{Pic}(\mathbf{Z}) = (0)$, $0^* \mathcal{L}$ is trivial. Our goal is to show that the invertible sheaves $\nu^* \Delta_{n-i}^* E(\mathcal{L}^{(i)}, \xi^{(i)})$, $0 \leq i \leq n-1$, are also trivial. This would imply that we have $\nu^* \mathcal{L}^{\otimes n!!} \simeq \mathcal{O}_{\tilde{H}}$ from which, given the above discussion, the result follows. Observe that (6.8) implies that there is an isomorphism of multiextensions

$$(8.9) \quad E(\mathcal{L}^{(i)}, \xi^{(i)}) \simeq \bigotimes_{j=1}^k (\text{pr}_j \times \cdots \times \text{pr}_j)^*(E_j^i),$$

where E_j^i is an $(n-i)$ -extension of H_{p_j} by \mathbf{G}_m . Using (8.9) we see that it is enough to prove that the invertible sheaves $\nu^* \Delta_{n-i}^*(E_j^i)$ are trivial, where now ν and Δ_{n-i} are the normalization and diagonal morphisms for the group scheme H_{p_j} . In fact, since the normalization \tilde{H}_{p_j} is the disjoint union of components corresponding to characters of G_{p_j} and these factor through prime power order cyclic quotients we can see that we can reduce to the case of a prime power order cyclic group. More precisely, it is enough to show the following statement: If E is an $(n-i)$ -extension of μ_{p^m} by \mathbf{G}_m , then the invertible sheaf $\nu^* \Delta_{n-i}^*(E)$ is trivial. Corollary 8.2 applied to $n-i$ implies that the composition

$$(8.10) \quad (n-i)\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \xrightarrow{t} \text{Pic}(\mu_{p^m}^{n-i}) \xrightarrow{\nu^* \Delta_{n-i}^*} \text{Pic}(\widetilde{\mu_{p^m}})$$

factors through the reflection homomorphisms. Hence, if p satisfies our assumption then the homomorphism (8.10) is trivial (Remark 8.3). Therefore, the invertible sheaves $\nu^* \Delta_{n-i}^*(E)$ are trivial. The result now follows. \square

8.d. Suppose that $G = \mathbf{Z}/p$ and that \mathcal{L} is an invertible sheaf on μ_p which supports an $n+1$ -cubic structure ξ with $p \geq n+1$. As above, Corollary 5.6 gives

$$\nu^* \mathcal{L}^{\otimes n!!} \simeq \bigotimes_{i=0}^{n-1} \nu^* (\Delta_{n-i}^* E(\mathcal{L}^{(i)}, \xi^{(i)}))^{\otimes (n-i-1)!!}.$$

Since, by Theorem 1.1, the invertible sheaf \mathcal{L} is p -power torsion and $\text{GCD}(p, n!!) = 1$, we can write

$$\nu^* \mathcal{L} \simeq \bigotimes_{i=0}^{n-1} \nu^* \Delta_{n-i}^* E'_{n-i},$$

where E'_{n-i} is an invertible sheaf on μ_p^{n-i} with a $(n-i)$ -extension structure. Let us denote by $t_j(\mathcal{L}, \xi)$ the image of E'_j under the homomorphism

$$\psi_j : j\text{-Ext}^1(\mu_p, \mathbf{G}_m) \rightarrow \text{Hom}((C(p)/p)^{(1-j)}, p^{-1}\mathbf{Z}/\mathbf{Z})$$

of Proposition 7.5 (In this case, ψ_j is an isomorphism; cf. Corollary 7.6). By [Ri], the pull back $\nu^* : \text{Pic}(\mu_p) \rightarrow \text{Pic}(\tilde{\mu}_p) = \text{Cl}(\mathbf{Q}(\zeta_p))$ is an isomorphism and we can use it to identify these class groups. Therefore, Corollary 8.2 and the above equality now implies that we can write

$$(8.11) \quad [\mathcal{L}] = \sum_{j=1}^n R^{(j)}(t_j(\mathcal{L}, \xi))$$

in $\text{Pic}(\mu_p) = \text{Cl}(\mathbf{Q}(\zeta_p))$ with $R^{(j)} = R_1^{(j)} : \text{Hom}((C(p)/p)^{(1-j)}, p^{-1}\mathbf{Z}/\mathbf{Z}) \rightarrow ({}_p C(p))^{(j)}$ the reflection homomorphism.

REFERENCES

- [AHS] M. Ando, M. J. Hopkins, N. P. Strickland: Elliptic spectra, the Witten genus and the theorem of the cube. *Invent. Math.* **146** (2001), no. 3, 595–687.
- [Bo] A. Borel: Stable real cohomology of arithmetic groups. *Ann. Sci. École Norm. Sup. (4)* **7** (1974), 235–272.
- [Br] L. Breen: *Fonctions thêta et théorème du cube*. Lecture Notes in Mathematics, Vol. 980. Springer-Verlag, Berlin-New York, 1983.
- [BCEM] J. Buhler, R. Crandall, R. Ernvall and T. Metsänkylä: Irregular primes and cyclotomic invariants to 12 million. *Computational algebra and number theory (Milwaukee, WI, 1996)*. *J. Symbolic Comput.* **31** (2001), no. 1-2, 89–96.
- [CPT] T. Chinburg, G. Pappas, M. J. Taylor: Cubic structures, equivariant Euler characteristics and modular forms. Preprint. ArXiv math.NT/0309327
- [DG] M. Demazure, P. Gabriel: *Groupes algébriques*. Masson et Cie, Paris; Amsterdam, North-Holland, 1970.
- [De] P. Deligne: Le déterminant de la cohomologie, in *Currents Trends in Arithmetical Algebraic Geometry*. Contemporary Mathematics, Vol. **67**, A.M.S. (1987).
- [DF] W. Dwyer, E. Friedlander: Algebraic and étale K -theory. *Trans. Amer. Math. Soc.* **292** (1985), no. 1, 247–280.
- [Du] F. Ducrot: Cube structures and intersection bundles. *J. Pure Appl. Algebra* **195** (2005), no. 1, 33–73.
- [Ku] M. Kurihara: Some remarks on conjectures about cyclotomic fields and K -groups of \mathbf{Z} . *Compositio Math.* **81** (1992), no. 2, 223–236.
- [L-MB] G. Laumon, L. Moret-Bailly: *Champs algébriques*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. 39. Springer-Verlag, Berlin, 2000.
- [LS] R. Lee, R. H. Szczarba: On the torsion in $K_4(\mathbf{Z})$ and $K_5(\mathbf{Z})$. *Duke Math. J.* **45** (1978), no. 1, 101–129; with an addendum by C. Soulé. 131–132.
- [M] B. Mazur: Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math. No.* **47**, (1977), 33–186 (1978).
- [MW] B. Mazur, A. Wiles: Class fields of abelian extensions of \mathbf{Q} . *Invent. Math.* **76** (1984), no. 2, 179–330.
- [MB] L. Moret-Bailly: *Pinceaux de variétés abéliennes*. Astérisque No. **129** (1985), 266 pp.
- [P] G. Pappas: Galois modules and the theorem of the cube. *Invent. Math.* **133** (1998), no. 1, 193–225.
- [Ri] D. S. Rim: Modules over finite groups. *Annals of Math.*, **69** (1959), 700–712.
- [Ro] J. Rognes: $K_4(\mathbf{Z})$ is the trivial group. *Topology* **39** (2000), no. 2, 267–281.

- [So] C. Soulé: Perfect forms and the Vandiver conjecture. *J. Reine Angew. Math.* **517** (1999), 209–221.
- [SGA4] *Théorie des topos et cohomologie étale des schémas*. Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat. Lecture Notes in Mathematics, Vol. 269, 270, 305. Springer-Verlag, Berlin-New York, 1972-73.
- [SGA7I] *Groupes de monodromie en géométrie algébrique. I*. Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin-New York, 1972.
- [W] L. Washington: *Introduction to cyclotomic fields*. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1982. xi+389 pp.
- [Wa] W. Waterhouse: Principal homogeneous spaces and group scheme extensions. *Trans. Amer. Math. Soc.* **153** (1971), 181–189.

SCHOOL OF MATH., INSTITUTE FOR ADVANCED STUDY, PRINCETON, NJ 08540, U.S.A.,
(Permanent address: Dept. of Mathematics, Michigan State Univ., East Lansing, MI 48824, U.S.A.)
E-mail address: `pappas@math.msu.edu`