COMPUTATIONS IN SYMMETRIC FUSION CATEGORIES IN CHARACTERISTIC p

PAVEL ETINGOF, VICTOR OSTRIK, SIDDHARTH VENKATESH

ABSTRACT. We study properties of symmetric fusion categories in characteristic p. In particular, we introduce the notion of a super Frobenius-Perron dimension of an object X of such a category, and derive an explicit formula for the Verlinde fiber functor $F(X)$ of X (defined by the second author) in terms of the usual and super Frobenius-Perron dimensions of X. We also compute the decomposition of symmetric powers of objects of the Verlinde category, generalizing a classical formula of Cayley and Sylvester for invariants of binary forms. Finally, we show that the Verlinde fiber functor is unique, and classify braided fusion categories of rank two and triangular semisimple Hopf algebras in any characteristic.

1. INTRODUCTION

Let $\mathbf{k}$ be an algebraically closed field of characteristic $p > 0$. Let $\mathcal{C}$ be a symmetric fusion category over $\mathbf{k}$. Then, according to the main result of [O], $\mathcal{C}$ admits a symmetric tensor functor $F : \mathcal{C} \to \mathrm{Ver}_p$ into the Verlinde category Ver_p (the quotient of $\mathrm{Rep}_{\mathbf{k}}(\mathbb{Z}/p\mathbb{Z})$ by negligible morphisms); we prove that this functor is unique. We derive an explicit formula for the decomposition of $F(X)$ into simple objects for each $X \in \mathcal{C}$; it turns out that this decomposition is completely determined by just two parameters — the Frobenius-Perron dimension $\mathrm{FPdim}(X)$ and the super Frobenius-Perron dimension $\mathrm{SFPdim}(X)$ which we introduce in this paper. We use this formula to find the decomposition of symmetric powers of objects in Ver_p, and in particular find the invariants in them — the "fusion" analog of the classical formula for polynomial invariants of binary forms. We also relate the super Frobenius-Perron dimension to the second Adams operation and to the p-adic dimension introduced in [EHO], and classify symmetric categorifications of fusion rings of rank 2. Finally, we classify triangular semisimple Hopf algebras in an arbitrary characteristic, generalizing the result of [EG] for characteristic zero, and classify braided fusion categories of rank two.

The paper is organized as follows. Section 2 contains preliminaries. In Section 3 we prove the uniqueness of the Verlinde fiber functor. In Section 4, we define the super Frobenius-Perron dimension of an object

of a symmetric fusion category, and give a formula for this dimension in terms of the second Adams operation; here we also classify braided fusion categories of rank two. In Section 5, we prove a decomposition formula for the Verlinde fiber functor of an object X of a symmetric fusion category in terms of the ordinary and super Frobenius-Peron dimensions of X, and use this formula to compute the transcendence degrees of the symmetric and exterior algebra of X. In Section 6, we use the formula of Section 5 to find the decomposition of symmetric powers of objects in the Verlinde category, and in particular give a formula for their invariants. In Section 7, we compute the p-adic dimensions of an object in a symmetric fusion category. Finally, in Section 8, we classify semisimple triangular Hopf algebras in any characteristic.

2. Preliminaries

Throughout the paper, $\mathbf{k}$ will denote an algebraically closed field. Unless specified otherwise, we will assume that the characteristic of $\mathbf{k}$ is $p > 0$.

By a symmetric tensor category over $\mathbf{k}$ (of any characteristic) we will mean an artinian rigid symmetric monoidal category in which the tensor product is compatible with the additive structure, and $\mathrm{End}(\mathbf{1}) = \mathbf{k}$ (see [EGNO], Definitions 4.1.1, 8.1.2). By a symmetric fusion category we mean a semisimple symmetric tensor category with finitely many simple objects.

2.1. **Verlinde categories.** Recall that the *Verlinde category* Ver_p is a symmetric fusion category over $\mathbf{k}$ obtained as the quotient of $\mathrm{Rep}_{\mathbf{k}}(\mathbb{Z}/p\mathbb{Z})$ by the tensor ideal of negligible morphisms, i.e. morphisms $f : X \to Y$ such that for any $g : Y \to X$ one has $\mathrm{Tr}(fg) = 0$ (see [O] for details). This category has $p - 1$ simple objects, $\mathbf{1} = L_1, \ldots, L_{p-1}$, such that

$$L_r \otimes L_s \cong \sum_{i=1}^{\min(r,s,p-r,p-s)} L_{|r-s|+2i-1}$$

(the Verlinde fusion rules).

Definition 2.1. We define Ver_p^+ to be the abelian subcategory of Ver_p generated by L_i for i odd, and define Ver_p^- to be the abelian subcategory of Ver_p generated by L_i for i even.

By the Verlinde fusion rules, Ver_p^+ is a fusion subcategory of Ver_p, and tensoring with L_{p-1} gives an equivalence of abelian categories $\mathrm{Ver}_p^+ \to$

Ver_p^- as long as $p > 2$. Since for $p > 2$ the symmetric fusion subcategory generated by L_1 and L_{p-1} is sVec, the category of supervector spaces over $\mathbf{k}$, we see that

$$\mathrm{Ver}_p = \mathrm{Ver}_p^+ \oplus \mathrm{Ver}_p^- \cong \mathrm{Ver}_p^+ \boxtimes \mathrm{sVec}, \ p > 2$$

(see [O, 3.3]).

Recall that for $r \in \mathbb{Z}$ and $z \in \mathbb{C}$,

$$[r]_z = \frac{z^r - z^{-r}}{z - z^{-1}}.$$

Let $q = e^{\pi i/p}$ be a primitive $2p$-th root of unity, and let $\mathrm{Gr}(\mathrm{Ver}_p)$ denote the Grothendieck ring of Ver_p. The following lemma is standard.

Lemma 2.2. $\mathrm{Gr}(\mathrm{Ver}_p)$ *has exactly* $p-1$ *distinct characters* $\chi_1, \ldots, \chi_{p-1}$, *where*

$$\chi_j(L_r) = [r]_{q^j}.$$

Proof. It is well known (and easy to show) that χ_j is a character. That these are all the distinct characters follows from the facts that $\mathrm{Gr}(\mathrm{Ver}_p) \otimes \mathbb{C}$ has dimension $p - 1$ and that distinct characters are linearly independent. $\qquad\square$

Note that the character χ_1 takes only positive values, and therefore coincides with the Frobenius-Perron dimension FPdim.

Let $K = \mathbb{Q}(q) \cap \mathbb{R}$. Then K is a Galois extension of $\mathbb{Q}$, with

$$\mathrm{Gal}(K/\mathbb{Q}) = \{g_0, \ldots, g_{\frac{p-3}{2}}\} \cong \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$$

for $p > 2$, where g_s is defined on $\mathbb{Q}(q)$ by sending q to q^{2s+1}; for $p = 2$, we have $K = \mathbb{Q}$.

Proposition 2.3. *The characters* χ_j *of* $\mathrm{Gr}(\mathrm{Ver}_p)$ *land in* K. *Moreover, for* $p > 2$ *and* $0 \leq s \leq \frac{p-3}{2}$ *we have*

$$\chi_{2s+1} = g_s \circ \chi_1, \ \ \chi_{p-2s-1} = g_s \circ \chi_{p-1}.$$

Proof. It is clear from Lemma 2.2 that all values of χ_j lie in $\mathbb{Q}(q)$ and are real, so the first statement follows. The second statement is obvious. $\qquad\square$

Recall that for any object X of a symmetric tensor category, we can define its symmetric powers $S^i X$ and exterior powers $\wedge^i X$ ([EHO], 2.1).

Proposition 2.4. *For every* $r > 1$, *we have* $S^i L_r = 0$ *if* $i + r > p$, *and for every* $r < p - 1$, *we have* $\wedge^i L_r = 0$ *if* $i > r$.

Proof. The first statement is proved in the proof of Proposition 3.1 of [Ven]. The second statement follows from the first one using the equality

$$\wedge^i L_r = L_{p-1}^{\otimes i} \otimes S^i(L_{p-1} \otimes L_r) = L_{p-1}^{\otimes i} \otimes S^i L_{p-r},$$

which holds since L_{p-1} generates a copy of sVec inside Ver_p. $\square$

2.2. **The Verlinde fiber functor.** Let $\mathcal{C}$ be any symmetric fusion category over $\mathbf{k}$. The following theorem is the main result of [O]:

Theorem 2.5. *([O]) There exists a symmetric tensor functor $F : \mathcal{C} \to \mathrm{Ver}_p$.*

We also have the following result, proved in Section 3.

Theorem 2.6. *A symmetric tensor functor $F : \mathcal{C} \to \mathrm{Ver}_p$ is unique up to a non-unique isomorphism of tensor functors.*

This theorem generalizes Theorem 3.2 of [DM] for functors with values in Vec and its extension to sVec discussed in Section 3 of [De], and its proof given below is based on similar ideas.

The functor F is called the *Verlinde fiber functor*, as it generalizes the fiber functor $\mathcal{C} \to$ sVec in characteristic zero, whose existence is a theorem of Deligne, [De] (see also [EGNO], Theorem 9.9.26).

The functor F is constructed as follows (see [O] for more details). First one constructs the *Frobenius functor* – a symmetric tensor functor Fr $: \mathcal{C} \to \mathcal{C}^{(1)} \boxtimes \mathrm{Ver}_p$, where $\mathcal{C}^{(1)}$ denotes the Frobenius twist of $\mathcal{C}$. Iterating this functor and taking tensor product in Ver_p, one obtains the n-th Frobenius functor $\mathrm{Fr}^n : \mathcal{C} \to \mathcal{C}^{(n)} \boxtimes \mathrm{Ver}_p$, where $\mathcal{C}^{(n)}$ is the n-th Frobenius twist of $\mathcal{C}$ (where $\mathrm{Fr}^1 = \mathrm{Fr}$). One then shows that for a sufficiently large n, Fr^n lands in $\mathcal{D} \boxtimes \mathrm{Ver}_p$, where $\mathcal{D} \subset \mathcal{C}^{(n)}$ is a nondegenerate fusion category. Then, using lifting theorems to characteristic zero (see [EGNO], Subsection 9.16) and Deligne's theorem in characteristic zero [De], one shows that there exists a symmetric tensor functor $\Phi : \mathcal{D} \to$ sVec. Then

$$(\Phi \boxtimes \mathrm{Id}) \circ \mathrm{Fr}^n : \mathcal{C} \to \mathrm{sVec} \boxtimes \mathrm{Ver}_p,$$

and we get F by composing this functor with the projection

$$\otimes : \mathrm{sVec} \boxtimes \mathrm{Ver}_p \to \mathrm{Ver}_p$$

Remark 2.7. In fact, it is shown in [O] that the functor Fr^n lands in $\mathcal{C}^{(n)} \boxtimes \mathrm{Ver}_p^+$, so that Φ lands in sVec $\boxtimes \mathrm{Ver}_p^+$.

Corollary 2.8. *If $\mathcal{C}$ is a symmetric fusion category over $\mathbf{k}$, then for any $X \in \mathcal{C}$, the Frobenius-Perron dimension $\mathrm{FPdim}(X)$ belongs to $\mathbb{Z}[q] \cap K$.*

Proof. By Theorem 2.5, we have the Verlinde fiber functor $F : \mathcal{C} \to$ Ver_p. This functor preserves FPdim. Thus, for $X \in \mathcal{C}$

$$\text{FPdim}(X) = \text{FPdim}(F(X)) = \chi_1(F(X)) \in \mathbb{Z}[q].$$

Also, $\text{FPdim}(X) \in \mathbb{R}$, which implies the statement. $\qquad\square$

2.3. **p-adic dimensions.** Let $\mathcal{C}$ be a symmetric tensor category over $\mathbf{k}$. Let $X \in \mathcal{C}$. Then to X one can attach its categorical dimension $\dim(X) \in \mathbf{k}$, and it is shown in [EGNO], Exercise 9.9.9(ii) that in fact $\dim(X) \in \mathbb{F}_p \subset \mathbf{k}$ (see also [EHO], Lemma 2.2).

Further, it is shown in [EHO] that $\dim(X)$ is the reduction modulo p of a richer invariant of X which takes values in $\mathbb{Z}_p$, called the p-adic dimension of X. In fact, there are two such invariants: the symmetric p-adic dimension $\text{Dim}_+(X)$ and the exterior p-adic dimension $\text{Dim}_-(X)$.

Namely, let $d = d_0 + pd_1 + p^2 d_2 + \dots$ be a p-adic integer (where d_i are the digits of d). We can define the power series over $\mathbb{F}_p$,

$$(1+z)^d := (1+z)^{d_0}(1+z^p)^{d_1}(1+z^{p^2})^{d_2}\dots$$

Definition 2.9. ([EHO]) We say that the symmetric p-adic dimension $\text{Dim}_+(X)$ of X is d if

$$\sum_j \dim(S^j X) z^j = (1-z)^{-d},$$

and say that the exterior p-adic dimension $\text{Dim}_-(X)$ of X is d if

$$\sum_j \dim(\wedge^j X) z^j = (1+z)^d.$$

Theorem 2.10. ([EHO]) *The p-adic dimensions $\text{Dim}_+(X)$, $\text{Dim}_-(X)$ exist and are unique for any X.*

3. Uniqueness of the Verlinde fiber functor

The goal of this Section is to give a proof of Theorem 2.6.

3.1. **Commutative algebras in Ver_p.**

Lemma 3.1. *Let X be an object of Ver_p with $\text{Hom}(\mathbf{1}, X) = 0$. Then there exists N such that $S^n X = 0$ for all $n \geq N$.*

Proof. We proceed by induction in the length of X. Then the base of induction is given by Proposition 2.4 and the induction step follows from the decomposition

$$S^n(X \oplus Y) = \bigoplus_{i=0}^{n} S^i X \otimes S^{n-i} Y.$$

$\square$

Now let A be a unital commutative associative algebra in the category Ver_p, see e.g. [EGNO, Section 8.8]. Let $m_n : A^{\otimes n} \to A$ be the multiplication morphism (so $m_1 = \mathrm{id}_A$, $m_2 = m$ is the multiplication in A, and $m_n = m \circ (m_{n-1} \otimes \mathrm{id}_A)$ for $n \geq 2$). There is a unique decomposition $A = A_0 \oplus A_1$ where A_0 is a multiple of $\mathbf{1}$ and $\mathrm{Hom}(\mathbf{1}, A_1) = 0$.

Lemma 3.2. *There exists N such that the restriction of m_n to $A_1^{\otimes n}$ equals zero for $n \geq N$.*

Proof. Since A is commutative, the restriction of m_n to $A_1^{\otimes n}$ factors through the canonical map $A_1^{\otimes n} \to S^n A_1$. The result follows from Lemma 3.1. $\square$

Let J be the image of multiplication morphism $m : A \otimes A_1 \to A$. Then J is an ideal in A (note that since A is commutative, there is no difference between left, right and two-sided ideals in A). The ideal J is nilpotent:

Lemma 3.3. *There exists N such that the restriction of m_n to $J^{\otimes n}$ equals zero for $n \geq N$.*

Proof. Since A is associative, the image of m_n restricted to $J^{\otimes n}$ equals the image of m_{2n} restricted to $(A \otimes A_1) \otimes \ldots \otimes (A \otimes A_1)$. Since A is commutative, this is the same as image of $m_{2n} = m \circ (m_n \otimes m_n)$ restricted to $A^{\otimes n} \otimes A_1^{\otimes n}$. The result follows from Lemma 3.2. $\square$

The unit object $\mathbf{1} \in \mathrm{Ver}_p$ has an obvious structure of unital, asociative, commutative algebra.

Proposition 3.4. *Let $A \in \mathrm{Ver}_p$ be a unital, associative, commutative algebra. Then there exists a unital algebra homomorphism $A \to \mathbf{1}$.*

Proof. Since A is unital, the ideal J contains A_1. By Lemma 3.3 this ideal is proper: $J \neq A$. Thus A/J is a nonzero unital, associative, commutative algebra contained in subcategory $\mathrm{Vec} \subset \mathrm{Ver}_p$ generated by the unit object. Thus by Hilbert's Nullstellensatz there exists a unital homomorphism $A/J \to \mathbf{1}$. The result follows. $\square$

3.2. **Fiber functors and commutative algebras.** Let $\mathcal{C}$ be a symmetric fusion category and let $F : \mathcal{C} \to \mathrm{Ver}_p$ be a symmetric tensor functor. Let $I : \mathrm{Ver}_p \to \mathcal{C}$ be the right adjoint of F (it exists since the categories $\mathcal{C}$ and Ver_p are finite semisimple).

Proposition 3.5. *(cf. [DMNO, Lemma 3.5])*
(i) The object $A := I(\mathbf{1}) \in \mathcal{C}$ has a natural structure of unital, associative, commutative algebra in $\mathcal{C}$.

(ii) The functor I induces a tensor equivalence $\tilde{I} : F(\mathcal{C}) \simeq \mathcal{C}_A$ of the image $F(\mathcal{C})$ of F in Ver_p (i.e., the fusion subcategory generated by objects of the form $F(X)$) with the category $\mathcal{C}_A$ of right $A-$modules in $\mathcal{C}$.

(iii) The functor $\tilde{I} \circ F : \mathcal{C} \to \mathcal{C}_A$ is naturally isomorphic to the functor $F_A =? \otimes A$ as a tensor functor.

Proof. Part (i) follows from Lemma 3.5 of [DMNO], see [DMNO, Remark 3.7]. The functor F makes Ver_p into a module category over $\mathcal{C}$, see e.g. [EGNO, Example 7.4.7]. It follows from definitions that the functor I identifies with the internal Hom functor $\underline{\mathrm{Hom}}(\mathbf{1}, ?)$. Thus the fact that I induces an equivalence $\tilde{I}$ follows from [EGNO, Corollary 7.10.5 (ii)]. Also using [EGNO, (7.25)] we get a canonical isomorphism of functors in part (iii). Now one defines tensor structure on the functor $\tilde{I}$ as in the proof of Theorem 3.1 of [ENO]; it follows immediately from definitions that the isomorphism of functors in (iii) respects this tensor structure. $\square$

Note that Proposition 3.5 (ii) implies that $A = \tilde{I}(\mathbf{1})$ is a simple $A-$module. Equivalently we have

Corollary 3.6. *The algebra A has no nontrivial ideals.*

Let $\tilde{F} : \mathcal{C}_A \to \mathrm{Ver}_p$ denote the composition of $\tilde{I}^{-1}$ with the embedding functor $F(\mathcal{C}) \to \mathrm{Ver}_p$. Note that functor $\tilde{F}$ is injective (that is, fully faithful). Then Proposition 3.5 (iii) implies

Corollary 3.7. *The functor F is isomorphic to the composition $\tilde{F} \circ F_A$ as a tensor functor.*

3.3. **Autoequivalences of** Ver_p**.** The following result contains a special case of Theorem 2.6 when $\mathcal{C} = \mathrm{Ver}_p$.

Lemma 3.8. *Any tensor autoequivalence of Ver_p (not necessarily preserving the braiding) is isomorphic to the identity functor as a tensor functor.*

Proof. It was proved in [O, 4.3.2] that the category Ver_p is equivalent to the semisimple quotient of the category of tilting modules over $SL(2)$. The result follows from the universal property of the category of tilting modules over $SL(2)$, see [O1, Theorem 2.4] (this is equivalent to the description of tilting modules over $SL(2)$ as the idempotent completion of the Temperley-Lieb category). $\square$

Corollary 3.9. *Let $\mathcal{A}$ be a fusion category and let G_1, G_2 be two injective tensor functors $\mathcal{A} \to \mathrm{Ver}_p$. Then G_1 and G_2 are isomorphic as tensor functors.*

Proof. The classification of fusion subcategories of Ver_p (see [O, Proposition 3.3]) implies that the images $G_1(\mathcal{A}) \subset \mathrm{Ver}_p$ and $G_2(\mathcal{A})$ are the same. Thus there exists a tensor autoequivalence R of $\mathcal{A}$ such that $G_2 \simeq G_1 \circ R$. Again by the classification of fusion subcategories of Ver_p there exists a fusion subcategory $\mathcal{B} \subset \mathrm{Ver}_p$ such that $\mathrm{Ver}_p = G_1(\mathcal{A}) \boxtimes \mathcal{B}$. Thus the autoequivalence R extends to autoequivalence of Ver_p as $R \boxtimes \mathrm{id}$. Then Lemma 3.8 implies that $R \simeq \mathrm{id}$ and we are done. $\qquad\square$

3.4. **Proof of Theorem 2.6.** Let F_1 and F_2 be two symmetric tensor functors $\mathcal{C} \to \mathrm{Ver}_p$. Let I_1, I_2 be right adjoint functors and let $A_1 = I_1(\mathbf{1}), A_2 = I_2(\mathbf{1})$ be the corresponding commutative algebras, see Section 3.2. Then $F_2(A_1)$ is a unital, associative, commutative algebra in Ver_p. Thus by Proposition 3.4 there exists a unital algebra homomorphism $F_2(A_1) \to \mathbf{1}$. Thus we have a unital algebra homomorphism $\tilde{I}_2(F_2(A_1)) \to \tilde{I}_2(\mathbf{1}) = A_2$, or $A_1 \otimes A_2 \to A_2$, see Proposition 3.5 (iii). Composing this with the homomorphism $A_1 = A_1 \otimes \mathbf{1} \to A_1 \otimes A_2$ we get a unital (and hence non-zero) homomorphism $A_1 \to A_2$. By Corollary 3.6, this homomorphism is injective. By symmetry we have an injective homomorphism $A_2 \to A_1$. It follows that the algebras A_1 and A_2 are isomorphic.

We choose an isomorphism and set $A = A_1 \simeq A_2$. By Corollary 3.7 the functors $F_i, i = 1, 2$ are isomorphic to $\tilde{F}_i \circ F_A$ where $\tilde{F}_i$ are injective tensor functors $\mathcal{C}_A \to \mathrm{Ver}_p$. By Corollary 3.9 the functors $\tilde{F}_1$ and $\tilde{F}_2$ are isomorphic. Hence F_1 and F_2 are isomorphic and the proof is complete.

4. Super Frobenius-Perron Dimension

4.1. **Definition of** SFPdim**.** Let $\mathcal{C}$ be a symmetric fusion category over $\mathbf{k}$, and $F : \mathcal{C} \to \mathrm{Ver}_p$ be the Verlinde fiber functor. For any $X \in \mathcal{C}$ we can write

$$F(X) = F(X)^+ \oplus F(X)^-$$

where $F(X)^+ \in \mathrm{Ver}_p^+$ and $F(X)^- \in \mathrm{Ver}_p^-$.

Definition 4.1. Let

$$d_+(X) := \mathrm{FPdim}(F(X)^+), \quad d_-(X) := \mathrm{FPdim}(F(X)^-),$$

Define the super Frobenius-Perron dimension of X as

$$\mathrm{SFPdim}(X) := d_+(X) - d_-(X).$$

Remark 4.2. 1. Note that this definition makes sense in characteristic zero, if we replace Ver_p with sVec, and F with the usual fiber functor; in this case, we recover the standard notion of superdimension of a supervector space. Also, if $\mathcal{C} = $ sVec and F is the natural embedding of sVec into Ver_p as the subcategory generated by L_1 and L_{p-1}, then

SFPdim also agrees with the usual notion of superdimension. In particular, SFPdim = FPdim in characteristic 2 and coincides with the usual superdimension in characteristic 3.

2. Below we will give another definition of SFPdim which does not use F.

3. It follows from the definition that $\mathrm{SFPdim}(X) = \mathrm{SFPdim}(F(X))$.

Lemma 4.3. *(i)* SFPdim *is a character of the Grothendieck ring of $\mathcal{C}$.*
(ii) For $\mathcal{C} = \mathrm{Ver}_p$ and $F = \mathrm{id}$, we have SFPdim $= \chi_{p-1}$. *Thus,* $\mathrm{SFPdim}(X) = \chi_{p-1}(F(X))$.

Proof. Using the equivalence

$$\mathrm{Ver}_p \cong \mathrm{Ver}_p^+ \boxtimes \mathrm{sVec},$$

for $\mathcal{C} = \mathrm{Ver}_p$ and $F = \mathrm{id}$ we can write SFPdim as $\mathrm{FPdim} \boxtimes \mathrm{sdim}$, where sdim denotes the superdimension of a supervector space. Since FPdim and sdim are characters of the Grothendieck rings of Ver_p^+ and sVec respectively, SFPdim is a character of the Grothendieck ring of Ver_p. Moreover, we have $\mathrm{SFPdim}(L_2) = -\mathrm{FPdim}(L_2) = -q - q^{-1} = q^{p-1} + q^{-p+1} = \chi_{p-1}(L_2)$, which implies that SFPdim $= \chi_{p-1}$ (as L_2 generates the Grothendieck ring of Ver_p). Now the general case follows from the facts that $\mathrm{SFPdim}(X) = \mathrm{SPdim}(F(X))$ and that F induces a homomorphism of Grothendieck rings. $\qquad\square$

4.2. **The second Adams operation and** SFPdim. Let char$\mathbf{k} \neq 2$. For a symmetric tensor category $\mathcal{C}$ over $\mathbf{k}$, the second Adams operation Ψ^2 is defined on the Grothendieck ring of $\mathcal{C}$ as

$$\Psi^2(X) = S^2 X - \wedge^2 X,$$

the difference between the symmetric and exterior squares.

Lemma 4.4. Ψ^2 *is a ring homomorphism* $\mathrm{Gr}(\mathcal{C}) \to \mathrm{Gr}(\mathcal{C})$.

Proof. We have $S^2(X \oplus Y) = S^2 X \oplus X \otimes Y \oplus S^2 Y$ and $\wedge^2(X \oplus Y) = \wedge^2 X \oplus X \otimes Y \oplus \wedge^2 Y$, which implies that Ψ^2 is a group homomorphism.

We have $S^2(X \otimes Y) = S^2 X \otimes S^2 Y \oplus \wedge^2 X \otimes \wedge^2 Y$ and $\wedge^2(X \otimes Y) = S^2 X \otimes \wedge^2 Y \oplus \wedge^2 X \otimes S^2 Y$, which implies that Ψ^2 is multiplicative. $\qquad\square$

Now we give another definition of SFPdim which does not use the functor F.

Proposition 4.5. *Let $\mathcal{C}$ be a fusion category over $\mathbf{k}$, and $X \in \mathcal{C}$. Then,*

(1) $$\mathrm{SFPdim}(X) = g(\mathrm{FPdim}(\Psi^2(X)))$$

where $g : \mathbb{Q}(q) \to \mathbb{Q}(q)$ is the Galois automorphism defined by sending q^2 to $-q$ (note that $\mathbb{Q}(q) = \mathbb{Q}(q^2)$).

Proof. Let F be the Verlinde fiber functor $\mathcal{C} \to \text{Ver}_p$. Then $\text{SFPdim}(X) = \text{SFPdim}(F(X))$. Also, since F preserves the symmetric structure and the FP-dimension, $g(\text{FPdim}(\Psi^2(X))) = g(\text{FPdim}(\Psi^2(F(X))))$. Hence, without loss of generality, we can assume that $\mathcal{C} = \text{Ver}_p$ and $F = \text{id}$.

By Lemma 4.4 and Lemma 4.3, both sides of (1) are characters on the complexified Grothendieck ring of Ver_p. Hence, as L_2 tensor generates Ver_p, it suffices to check the equality on L_2. In this case, if $p \geq 5$, the LHS is by definition $-q - q^{-1}$ and the RHS of (1) is

$$g(\text{FPdim}(L_3 - L_1)) = g([3]_q - 1) = g(q^2 + q^{-2}) = -q - q^{-1},$$

as desired. For $p = 3$, on both sides of (1) we have -1 (here g is the identity and $L_3 = 0$). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

4.3. Symmetric and braided categorifications of fusion rings of rank 2.
Here is an application of the second Adams operation. Let R_n be the fusion ring of rank 2 with basis $1, X$ and relation $X^2 = nX + 1$, where $n \geq 0$.

Proposition 4.6. *Let $n \geq 1$. There is a symmetric fusion category $\mathcal{C}$ with Grothendieck ring R_n only if $n = 1$ and $\text{char}\mathbf{k} = 5$, and in this case $\mathcal{C} = \text{Ver}_5^+$.*

Proof. If $\text{char}\mathbf{k} = 2$ then there is a Verlinde fiber functor $F : \mathcal{C} \to \text{Vec}$, so $\text{FPdim}(X)$ must be an integer, i.e. the equation $x^2 = nx + 1$ should have integer solutions, which is impossible. So we may assume that $\text{char}\mathbf{k} \neq 2$. We have a homomorphism $\Psi^2 : R_n \to R_n$, so $\Psi^2(X) = X$ or $\Psi^2(X) = n - X$. But the multiplicity of 1 in $\Psi^2(X)$ is 1 or -1, as either $S^2 X$ or $\wedge^2 X$ contains a copy of the unit object $\mathbf{1}$ (but not both). So $n = 1$ and $\text{FPdim}(X) = \frac{1+\sqrt{5}}{2}$. Also, $\mathcal{C}$ must be a degenerate category (otherwise, it would lift to a symmetric category in characteristic zero by [EGNO], Subsection 9.16, and hence would have had integer FP dimensions, see [EGNO], Theorem 9.9.26), so $\text{char}\mathbf{k} = 5$ (as $\dim(\mathcal{C}) = \frac{5\pm\sqrt{5}}{2}$, which vanishes only in characteristic 5). Thus we have a Verlinde fiber functor $\mathcal{C} \to \text{Ver}_5$, which is easily seen to be an equivalence onto Ver_5^+. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Note that Proposition 4.6 completely classifies symmetric categorifications of fusion rings of rank 2, as the problem of categorification of the ring R_0 is trivial (since X is invertible).

The main result of [O2] states that in characteristic zero there is no fusion categories with Grothendieck ring R_n, $n \geq 2$. It is an open question whether this is true in positive characteristic. However we have the following

Proposition 4.7. *There is no braided fusion categories $\mathcal{C}$ over $\mathbf{k}$ with Grothendieck ring R_n, $n \geq 2$.*

Proof. For the sake of contradiction assume that $\mathcal{C}$ is a braided fusion category with $\mathrm{Gr}(\mathcal{C}) = R_n$, $n \geq 2$. Then the same argument as in proof of [O2, Corollary 2.2] shows that $\mathcal{C}$ is spherical. The lifting theory (see [EGNO, 9.16]) shows that $\mathcal{C}$ must be degenerate, that is $1 + d^2 = 0$ where $d \in \mathbf{k}$ is the dimension of the object X (as by the result of [O2], there is no categorifications of R_n in characteristic zero). Since $d^2 = 1 + nd$, this is equivalent to $nd = -2$. Moreover by [O, Proposition 2.9] the ring $\mathrm{Gr}(\mathcal{C}) \otimes \mathbf{k}$ must not be semisimple, so $X \mapsto d$ is a unique homomorphism $R_n \to \mathbf{k}$. Thus $\frac{s_{X,X}}{d} = d$ where $s_{X,X}$ is the entry of $S-$matrix of $\mathcal{C}$, see [EGNO, Proposition 8.3.11]. By [EGNO, Proposition 8.13.8] we have $s_{X,X} = \theta^{-2}(1 + \theta n d)$ where θ is the twist of the object X, see [EGNO, Definition 8.10.1]. Thus

$$\frac{s_{X,X}}{d} = d \Leftrightarrow \theta^{-2}(1 + \theta n d) = d^2 \Leftrightarrow \theta^{-2}(1 - 2\theta) = -1 \Leftrightarrow \theta = 1.$$

It follows (see [EGNO, Definition 8.10.1]) that the category $\mathcal{C}$ is symmetric, and the result follows from Proposition 4.6. □

Remark 4.8. The argument in the proof of Proposition 4.7 works also in the case $n = 1$, showing that if $\mathcal{C}$ is degenerate then it must be symmetric, and hence by Proposition 4.6 has to be equivalent to Ver_5^+ with $\mathrm{char}\mathbf{k} = 5$. Another option for $n = 1$ is that $\mathcal{C}$ is nondegenerate; then by lifting theory ([EGNO, 9.16]) it is a reduction modulo $p = \mathrm{char}\mathbf{k}$ of a Yang-Lee category YL_+ or YL_- in characteristic zero ([EGNO, Exercise 9.4.6]), and each can be taken with two different braidings (inverse to each other). Thus we have four choices for each characteristic $p \neq 5$ (which are distinct since lifting is faithful).

Also, the case $n = 0$ is easy since X is invertible. Namely, in this case, if $p = 2$, then $\mathcal{C} = \mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}$ ($\mathbb{Z}/2\mathbb{Z}$-graded vector spaces), and the only possible braiding is trivial. On the other hand, for $p > 2$ the classification is the same as in characteristic zero, namely by quadratic forms on $\mathbb{Z}/2\mathbb{Z}$, which are labeled by solutions of the equation $\theta^4 = 1$ in $\mathbf{k}$ ([EGNO, 8.2]). Thus, we have obtained a full classification of braided fusion categories with two simple objects over a field of any characteristic.

5. Decomposition of the Verlinde fiber functor of an object of a symmetric fusion category

5.1. **The decomposition formulas.** Let $\mathcal{C}$ be a symmetric fusion category over $\mathbf{k}$ and let $F : \mathcal{C} \to \mathrm{Ver}_p$ be the Verlinde fiber functor. Let

$X \in \mathcal{C}$. Our goal in this section is to compute the decomposition of $F(X)$ into the simples of Ver_p in terms of $\mathrm{FPdim}(X)$ and $\mathrm{SFPdim}(X)$. Let

$$F(X) = \bigoplus_{r=1}^{p-1} a_r L_r.$$

If $p = 2$ then $a_1 = \mathrm{FPdim}(X)$, so assume that $p > 2$.

Let $\mathrm{Tr} : K \to \mathbb{Q}$ be the trace map, given by $\mathrm{Tr}(x) = \sum_{s=0}^{\frac{p-3}{2}} g_s(x)$. For example, for r not divisible by p, we have

(2) $$\mathrm{Tr}(q^r + q^{-r}) = (-1)^{r-1}.$$

Theorem 5.1. *For $p > 2$ we have*

$$a_r = \frac{1}{2p} \mathrm{Tr}\left((q^{-r} - q^r)(q - q^{-1})(\mathrm{FPdim}(X) - (-1)^r \mathrm{SFPdim}(X))\right).$$

In other words, for r odd, we have

$$a_r = \frac{1}{p} \mathrm{Tr}((q^{-r} - q^r)(q - q^{-1})d_+(X))$$

and for r even, we have

$$a_r = \frac{1}{p} \mathrm{Tr}((q^{-r} - q^r)(q - q^{-1})d_-(X)).$$

Proof. Applying $g_s \circ \mathrm{FPdim}$ and $g_s \circ \mathrm{SFPdim}$ to the decomposition of $F(X)$, we get, for each $s = 0, \ldots, \frac{p-3}{2}$:

$$g_s(\mathrm{FPdim}(X)) = \sum_{r=1}^{p-1} a_r [r]_{q^{2s+1}}$$

and

$$g_s(\mathrm{SFPdim}(X)) = \sum_{r=1}^{p-1} (-1)^{r-1} a_r [r]_{q^{2s+1}}.$$

Clearing denominators, we get

$$g_s((q - q^{-1})\,\mathrm{FPdim}(X)) = \sum_{r=1}^{p-1} a_r (q^{(2s+1)r} - q^{-(2s+1)r})$$

and

$$g_s((q - q^{-1})\mathrm{SFPdim}(X)) = \sum_{r=1}^{p-1} (-1)^{r-1} a_r (q^{(2s+1)r} - q^{-(2s+1)r}).$$

12

Let us extend the sequence a_r to all integer r by setting $a_r = -a_{-r} = a_{r+2p}$ (in particular, $a_r = 0$ if r is divisible by p). Then we can rewrite the above sums as summations over $\mathbb{Z}/2p\mathbb{Z}$:

$$g_s((q - q^{-1})\,\mathrm{FPdim}(X)) = \pm \sum_{r \in \mathbb{Z}/2p\mathbb{Z}} a_r q^{\pm(2s+1)r}$$

and

$$-g_s((q - q^{-1})\mathrm{SFPdim}(X)) = \pm \sum_{r \in \mathbb{Z}/2p\mathbb{Z}} a_r q^{\pm(p+2s+1)r}.$$

Now taking the inverse Fourier transform on the group $\mathbb{Z}/2p\mathbb{Z}$ gives the desired result. $\qquad\square$

5.2. **Transcendence degrees.** Let X be an object of a fusion category $\mathcal{C}$ over $\mathbf{k}$. Recall from [Ven] that the algebra of invariants $(SX)^{\mathrm{inv}}$ (which is an ordinary commutative $\mathbf{k}$-algebra) is finitely generated. Let $\mathrm{Trd}_+(X)$ be the transcendence degree of this algebra, i.e. the largest number of algebraically independent elements. Similarly, let $\mathrm{Trd}_-(X)$ be the transcendence degree of $(\wedge X)^{\mathrm{inv}}_{\mathrm{even}}$ (the largest number of even algebraically independent elements). It is shown in [Ven] that $\mathrm{Trd}_+(X) = d$ if and only if SX is a finitely generated module over $\mathbf{k}[z_1, ..., z_d] \subset (SX)^{\mathrm{inv}}$, and likewise $\mathrm{Trd}_-(X) = d$ if and only if $\wedge X$ is a finitely generated module over $\mathbf{k}[z_1, ..., z_d] \subset (\wedge X)^{\mathrm{inv}}_{\mathrm{even}}$. This implies that $\mathrm{Trd}_\pm(X)$ are preserved under symmetric tensor functors between fusion categories.

It follows from Proposition 2.4 that $\mathrm{Trd}_+(L_i) = 0$ if $2 \le i \le p - 1$ and $\mathrm{Trd}_-(L_i) = 0$ if $1 \le i \le p - 2$, while $\mathrm{Trd}_+(L_1) = \mathrm{Trd}_-(L_{p-1}) = 1$. Therefore, we have

Proposition 5.2. *(i) One has* $\mathrm{Trd}_+(X) = a_1$ *and* $\mathrm{Trd}_-(X) = a_{p-1}$.
(ii) One has

$$\mathrm{Trd}_+(X) = \frac{1}{p}\mathrm{Tr}(|q - q^{-1}|^2 d_+(X)),$$

and

$$\mathrm{Trd}_-(X) = \frac{1}{p}\mathrm{Tr}(|q - q^{-1}|^2 d_-(X)).$$

Proof. (i) is immediate from the above, and (ii) follows from (i) and Theorem 5.1 by plugging in $r = 1, p - 1$. $\qquad\square$

6. DECOMPOSITION OF SYMMETRIC POWERS OF SIMPLE OBJECTS IN Ver_p

We will now apply Theorem 5.1 to compute the decomposition into simples of $S^i L_m$, the symmetric powers of the simple object $L_m \in \mathrm{Ver}_p$,

for each $2 \leq m \leq p-1$ and $0 \leq i \leq p-m$ (note that by Proposition 2.4, we have $S^i L_m = 0$ if $i > p - m$). To do so, we need to compute the FPdim and SFPdim of $S^i L_m$.

As before, we assume that $p > 2$. Let

$$\binom{n}{m}_z := \frac{\prod_{j=1}^m (z^{n-j+1} - z^{-n+j-1})}{\prod_{j=1}^m (z^j - z^{-j})}$$

be the symmetrized Gauss polynomial (the z-binomial coefficient).

Proposition 6.1. *(i) For $2 \leq m \leq p-1$ and $0 \leq i \leq p-m$,*

$$\mathrm{FPdim}(S^i L_m) = \binom{i+m-1}{m-1}_q,$$

(ii) One has $\mathrm{SFPdim}(S^i L_m) = (-1)^{i(m-1)} \mathrm{FPdim}(S^i L_m)$.

Proof. (i) Let $\mathrm{Ver}_p(SL_m)$ be the Verlinde category attached to the group SL_m (see [O], 4.3.2, 4.3.3 and references therein). The $\mathbb{Z}_+$-basis of $\mathrm{Gr}(\mathrm{Ver}_p(SL_m))$ is $\{V_\lambda\}$, where λ runs through dominant integral weights for SL_m such that $(\lambda + \rho, \theta) < p$, and we have a character of this ring given by

$$(3) \qquad V_\lambda \mapsto \dim_q V_\lambda = \prod_{\alpha > 0} \frac{[(\lambda + \rho, \alpha)]_q}{[(\rho, \alpha)]_q},$$

where α runs through positive roots, θ is the maximal root, and ρ the half-sum of the positive roots (the q-deformed Weyl dimension formula, see [BK], 3.3). It is easy to see that all these values are positive.

Let $V = V_{\omega_1}$, where ω_1 is the first fundamental weight, i.e., V is the tautological object. Then $S^i V = V_{i\omega_1}$ for $i \leq p-m$. So, by (3), $\dim_q S^i V = \binom{i+m-1}{m-1}_q$. Hence $\mathrm{FPdim}(S^i V) = \binom{i+m-1}{m-1}_q$.

We have the Verlinde fiber functor $F : \mathrm{Ver}_p(SL_m) \to \mathrm{Ver}_p(SL_2)$, and $F(V) = L_m$. Hence $F(S^i V) = S^i L_m$, and the statement follows.

(ii) It is clear that $S^i L_m$ is in Ver_p^+ if $i(m-1)$ is even and is in Ver_p^- otherwise, which implies the statement. $\qquad\square$

Let $S^i L_m = \oplus_{r=1}^{p-1} a_r L_r$.

Corollary 6.2. *If $i(m-1) - r$ is odd, then*

$$a_r = \frac{1}{p} \mathrm{Tr}\left((q^{-r} - q^r)(q - q^{-1}) \binom{i+m-1}{m-1}_q \right),$$

and if $i(m-1) - r$ is even, then $a_r = 0$. In particular,

$$(4) \qquad \dim_{\mathbf{k}}(S^i L_m)^{\mathrm{inv}} = \frac{1}{p} \mathrm{Tr}\left(|q - q^{-1}|^2 \binom{i+m-1}{m-1}_q \right).$$

14

Proof. This follows from Proposition 6.1 and Theorem 5.1. □

These formulas can be written more combinatorially using that for any Laurent polynomial $f(z)$ with integer coefficients such that $f(z) = f(z^{-1})$, we have

$$2\mathrm{Tr} f(q) = \tau(f),$$

where

$$\tau(\sum_{j\in\mathbb{Z}} b_j z^j) = p\sum_{j\in\mathbb{Z}}(-1)^j b_{pj} - \sum_{j\in\mathbb{Z}}(-1)^j b_j = p\sum_{j\in\mathbb{Z}}(-1)^j b_{pj} - f(-1),$$

which follows from (2). For instance, from (4) we have

$$(5) \qquad \dim_{\mathbf{k}}(S^i L_m)^{\mathrm{inv}} = \sum_{j\in\mathbb{Z}}(-1)^j b_{pj},$$

where

$$\sum_{j\in\mathbb{Z}} b_j z^j = -\frac{1}{2}(z - z^{-1})^2 \binom{i+m-1}{m-1}_z.$$

More generally, we have

$$a_r = \sum_{j\in\mathbb{Z}}(-1)^j b_{pj,r},$$

where

$$\sum_{j\in\mathbb{Z}} b_{j,r} z^j = \frac{1}{2}(z^{-r} - z^r)(z - z^{-1})\binom{i+m-1}{m-1}_z.$$

Remark 6.3. Since $\mathrm{Ver}_p = \mathrm{Ver}_p(SL_2)$, formula (5) may be viewed as a "fusion" analog of the classical Cayley-Sylvester formula for the number $N(i,m)$ of linearly independent invariants of degree i of a binary form of degree m, which says that $N(i,m) = b_0$ (see [S]). Indeed, this formula is recovered from (5) as $p \to \infty$.

Remark 6.4. Let G be a simply connected simple algebraic group over $\mathbf{k}$ (for simplicity assumed of type ADE), h the Coxeter number of G, and $p > h$. Let $\mathrm{Ver}_p(G)$ be the Verlinde category corresponding to G (see [O], 4.3.2, 4.3.3). The simple objects of $\mathrm{Ver}_p(G)$ are highest weight modules V_λ, where $(\lambda+\rho, \theta) < p$. Using a similar method to the above, we can compute the decomposition of $F(V_\lambda)$. Namely, similarly to the SL_m case, $\mathrm{FPdim}(V_\lambda) = \dim_q(V_\lambda)$, given by formula (3) (this is a character and all its values are positive). Also, for each λ, $F(V_\lambda)$ is in Ver_p^+ or Ver_p^- depending on whether the element $-1 = \exp(2\pi i h_\rho) \in SL_2^{\mathrm{principal}} \subset G$ acts by 1 or -1 on V_λ in characteristic zero (see [O],

15

4.3.3). In other words, we have $\text{SFPdim}(V_\lambda) = (-1)^{(\lambda,\rho)}\,\text{FPdim}(V_\lambda)$. Thus we get $F(V_\lambda) = \sum_r a_r L_r$, where

$$a_r = \frac{1}{p}\text{Tr}\left((q^{-r} - q^r)(q - q^{-1})\prod_{\alpha>0}\frac{[(\lambda + \rho, \alpha)]_q}{[(\rho, \alpha)]_q}\right)$$

7. p-ADIC DIMENSIONS IN A FUSION CATEGORY

The following proposition relates the p-adic dimensions with the super Frobenius Perron dimension.

Proposition 7.1. *One has*

$$\text{SFPdim}(X) = (\text{Dim}_+ \boxtimes \text{FPdim})(\text{Fr}^n(X)) = (\text{Dim}_- \boxtimes \text{FPdim})(\text{Fr}^n(X)).$$

where n is such that $\text{Fr}^n : \mathcal{C} \to \mathcal{D} \boxtimes \text{Ver}_p^+$, with $\mathcal{D} \subset \mathcal{C}^{(n)}$ nondegenerate (see Subsection 2.2).

Proof. Since $\mathcal{D}$ is a nondegenerate fusion category, it admits a super fiber functor, and thus both p-adic dimensions in $\mathcal{D}$ coincide with the usual superdimension. This implies the statement. $\square$

Theorem 7.2. *(i) $\text{Dim}_+(L_r)$ equals 1 if $r = 1$ and $r - p$ if $r > 1$. $\text{Dim}_-(L_r)$ equals r if $r < p - 1$, and -1 if $r = p - 1$.*

(ii) The p-adic dimensions of any object X of a fusion category are as follows: if $F(X) = \sum_{r=1}^{p-1} a_r L_r$ then

$$\text{Dim}_+(X) = a_1 + \sum_{i>1}(i - p)a_i, \ \ \text{Dim}_-(X) = \sum_{i<p-1} ia_i - a_{p-1}.$$

Proof. (i) Let $r > 1$. By Proposition 2.4, $(1 - z)^{-\text{Dim}_+(L_r)}$ is a polynomial of degree $\leq p - r$. Thus, $-\text{Dim}_+(L_r)$ is an integer between 0 and $p - r$. Since $\text{Dim}_+(L_r)$ must equal $\dim L_r = r$ modulo p, we conclude that $\text{Dim}_+(L_r) = r - p$.

Let $r < p - 1$. By Proposition 2.4, $(1 + z)^{\text{Dim}_-(L_r)}$ is a polynomial of degree $\leq r$. Thus, $\text{Dim}_-(L_r)$ is an integer between 0 and r. Since $\text{Dim}_-(L_r)$ must equal $\dim L_r = r$ modulo p, we conclude that $\text{Dim}_-(L_r) = r$.

The remaining cases $r = 1, p - 1$ are easy, as the corresponding objects are invertible.

(ii) is immediate from (i). $\square$

Corollary 7.3. *One has*

$$\text{length}F(X) = \text{Trd}_+(X) + \text{Trd}_-(X) + \frac{\text{Dim}_-(X) - \text{Dim}_+(X)}{p}.$$

Proof. This follows from Theorem 7.2(ii), using that $\text{length}F(X) = \sum_i a_i$. $\square$

8. CLASSIFICATION OF TRIANGULAR SEMISIMPLE HOPF ALGEBRAS IN POSITIVE CHARACTERISTIC

The following theorem classifies traingular semisimple Hopf algebras in any characteristic, generalizing Theorem 2.2 of [EG] in characteristic zero.

For a finite group scheme G over $\mathbf{k}$, let $\mathbf{k}G$ denote the dual Hopf algebra $O(G)^*$ to the function algebra $O(G)$ of G.

Theorem 8.1. *Let H be a finite dimensional triangular semisimple Hopf algebra over a field $\mathbf{k}$ of any characteristic (see* [EGNO], *Chapter 5). Then there exists a semisimple finite group scheme G over $\mathbf{k}$, a central element $\varepsilon \in G(\mathbf{k})$ of order ≤ 2 (with $\varepsilon = 1$ if $p = 2$) and a twist $J \in \mathbf{k}G \otimes \mathbf{k}G$ such that $H = \mathbf{k}G^J$ as a Hopf algebra, and the universal R-matrix of H is $R = J_{21}^{-1}R_0J$, where $R_0 = 1 \otimes 1$ if $p = 2$ and $R_0 = \frac{1}{2}(1 \otimes 1 + 1 \otimes \varepsilon + \varepsilon \otimes 1 - \varepsilon \otimes \varepsilon)$ otherwise.*

Note that this classification is completely explicit. Namely, by Nagata's theorem ([DG], IV, 3.6), $G = \Gamma \ltimes A$, where Γ is a finite group of order coprime to p and A is the dual group scheme to a finite abelian p-group P; in other words, we have $\mathbf{k}G = \mathbf{k}\Gamma \ltimes O(P)$. Moreover, the twists J for G are classified in terms of subgroup schemes of G and 2-cocycles on them in [Ge], Proposition 6.3. Namely, a twist corresponds to a nondegenerate class $\psi \in H^2(G', \mathbb{G}_m)$, where G' is a group subscheme of G. It is easy to see that G' is conjugate to $\Gamma' \ltimes A'$, where $\Gamma' \subset \Gamma$ and $A' \subset A$ is Γ'-invariant. Now the Hochschild-Serre spectral sequence (for group schemes) implies that ψ is pulled back from Γ' (as the cohomology $H^i(A', \mathbb{G}_m)$ vanishes for $i > 0$, so the pullback map $H^i(\Gamma, \mathbf{k}^\times) = H^i(\Gamma, \mathbb{G}_m) \to H^i(G, \mathbb{G}_m)$ is an isomorphism). Since ψ is nondegenerate, this implies that $A' = 1$, i.e., the twist J comes from $\mathbf{k}\Gamma \otimes \mathbf{k}\Gamma$, i.e. corresponds to a subgroup of central type $\Gamma' \subset \Gamma$.

Proof. We may assume that char$\mathbf{k} = p > 0$. For $p = 2$, this is immediate from [O] (see [O], Corollary 1.6), so let us assume that $p > 2$. The category Rep H is a symmetric fusion category. Let $F : \text{Rep } H \to \text{Ver}_p$ be the Verlinde fiber functor. Since Rep H is integral (i.e., has integer FP dimensions), F lands in sVec $\subset \text{Ver}_p$, as this is the largest integral subcategory of Ver_p. Thus, as in [O], 1.3, Rep $H = \text{Rep}(G, \varepsilon)$, the category of representations of G on superspaces on which ε acts by parity, where G is a semisimple finite supergroup scheme over $\mathbf{k}$ and $\varepsilon \in G(\mathbf{k})$ is an element of order ≤ 2 acting on $O(G)$ by the parity automorphism. (For a general theory of affine algebraic supergroup schemes we refer the reader to [Ma].)

It remains to show that G is in fact an ordinary group scheme. This is shown in [Ma] (see Corollary 43 and Theorem 45); here we provide an alternative proof. We will need the following two lemmas.

Lemma 8.2. *If M is a subsupergroup scheme of G containing ε, then $\mathrm{Rep}(M, \varepsilon)$ is semisimple.*

Proof. Recall that if $\mathcal{C}$ is a fusion category and $\Phi : \mathcal{C} \to \mathcal{D}$ is a surjective tensor functor ([EGNO], 6.3) to a finite tensor category, then $\mathcal{D}$ is also fusion. Indeed, $\mathcal{D}$ is an exact $\mathcal{C}$-module ([EGNO], Example 7.5.6), hence semisimple. Now take $\mathcal{C} = \mathrm{Rep}(G, \varepsilon)$ and $\mathcal{D} = \mathrm{Rep}(M, \varepsilon)$, and take Φ to be the restriction functor. $\square$

Now let G_+ be the even part of G (i.e., $O(G_+) = O(G)/I$, where I is the ideal generated by the odd elements, which is automatically a Hopf ideal), and G_+^0 its connected component of the identity. By Lemma 8.2, $\mathrm{Rep}(G_+^0)$ is semisimple. Thus, by Nagata's theorem ([DG], IV, 3.6), G_+^0 is abelian.

Let $\mathrm{Lie}(G) = \mathfrak{g}_+ \oplus \mathfrak{g}_-$ be the Lie algebra of G, decomposed into the even and odd parts. Let G^0 be the connected component of the identity in G.

Lemma 8.3. *The action of G_+^0 on $\mathfrak{g}_-$ is trivial. In other words, G_+^0 is central in G^0.*

Proof. Let $x \in \mathfrak{g}_-$ be an eigenvector, on which G_+^0 acts by a character χ. We claim that $[x, x] \neq 0$. Indeed, assume the contrary, and let N be the supergroup scheme generated by ε and $\exp(\mathbf{k}x)$. Then we have a surjective restriction functor $\mathrm{Rep}(G, \varepsilon) \to \mathrm{Rep}(N, \varepsilon)$, so $\mathrm{Rep}(N, \varepsilon)$ is semisimple by Lemma 8.2, which is a contradiction.

Now, G_+^0 acts on $[x, x]$ by χ^2. But $[x, x] \in \mathfrak{g}_+$, hence $\chi^2 = 1$, as G_+^0 is abelian.

But χ has order which is a power of p, so $\chi = 1$. Thus, Lemma 8.3 follows from Lemma 8.2 (which implies that the action of G_+^0 on $\mathfrak{g}_-$ is semisimple). $\square$

We see that we have a central extension of supergroup schemes

$$1 \to G_+^0 \to G^0 \to \exp(\mathfrak{g}_-) \to 1,$$

where $\exp(\mathfrak{g}_-) = \mathrm{Spec} \wedge \mathfrak{g}_-$ (purely odd abelian supergroup scheme). Let P be the supergroup scheme generated by ε and G^0, and Q be the supergroup scheme generated by ε and $\exp(\mathfrak{g}_-)$. Thus the category $\mathrm{Rep}(Q, \varepsilon)$ is a tensor subcategory of $\mathrm{Rep}(P, \varepsilon)$. But the category $\mathrm{Rep}(P, \varepsilon)$ is semisimple by Lemma 8.2. Hence, $\mathrm{Rep}(Q, \varepsilon)$ is semisimple. This can only hold if $\mathfrak{g}_-$ is zero. Thus, we have $G^0 = G_+^0$, hence $G = G_+$, as desired. $\square$

References

[BK] B. Bakalov, A. Kirillov Jr., Lectures on tensor categories and and modular functors, AMS, 2001.

[DMNO] A. Davydov, M. Müger, D. Nikshych, V. Ostrik, The Witt group of non-degenerate braided fusion categories, J. für die reine und angewandte Mathematik, **677** (2013), pp. 135—177.

[DG] M. Demazure, P. Gabriel, Groupes algébriques, tome I, Paris, 1970.

[DM] P. Deligne, J. S. Milne, Tannakian categories, Lecture Notes in Mathematics 900, 1982, http://www.jmilne.org/math/xnotes/tc.pdf

[De] P. Deligne, Catégories tensorielles, Mosc. Math. J., 2002, Volume 2, Number 2, Pages 227—248.

[EG] P. Etingof and S. Gelaki, Some properties of finite-dimensional semisimple Hopf algebras, Mathematical Research Letters 5 (1998), 191—197.

[EGNO] P. Etingof, S. Gelaki, D. Nikshych, V. Ostrik, Tensor categories, AMS, Providence, 2015.

[EHO] P. Etingof, N. Harman, V. Ostrik, p-adic dimensions in symmetric tensor categories in characteristic p, arXiv:1510.04339.

[ENO] P. Etingof, D. Nikshych, V. Ostrik, Weakly group-theoretical and solvable fusion categories, Adv. Math. **226** (2011), no. 1, pp. 176—205.

[Ge] S. Gelaki, Module categories over affine group schemes. Quantum Topol. 6 (2015), no. 1, 1—37, arXiv:/1209.1155.

[Ma] A. Masuoka, Harish-Chandra pairs for algebraic affine supergroup schemes over an arbitrary field, Transf. Groups, v. 17, issue 4, 2012, pp. 1085—1121, arXiv:1111.2387.

[O] V. Ostrik, On symmetric fusion categories in positive characteristic, arXiv:1503.01492.

[O1] V. Ostrik, Module categories over representations of $SL_q(2)$ in the non-semisimple case, Geom. Funct. Anal. **17** (2008), no. 6, p. 2005—2017.

[O2] V. Ostrik, Fusion categories of rank 2, Math. Res. Lett. **10** (2003), no. 2—3, pp. 177—183.

[S] T.A. Springer, Invariant Theory, Lecture Notes in Mathematics, vol. 585, Springer-Verlag (1977)

[Ven] S. Venkatesh, Hilbert Basis Theorem and Finite Generation of Invariants in Symmetric Fusion Categories in Positive Characteristic, arXiv:1507.05142, to appear in IMRN.

ETINGOF: DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139, USA

  E-mail address: etingof@math.mit.edu

OSTRIK: DEPARTMENT OF MATHEMATICS UNIVERSITY OF OREGON EUGENE, OR 97403, USA

  E-mail address: vostrik@math.uoregon.edu

VENKATESH: DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139, USA

  E-mail address: sidnv@mit.edu