Descent and Forms of Tensor Categories

DESCENT AND FORMS OF TENSOR CATEGORIES

PAVEL ETINGOF AND SHLOMO GELAKI

Abstract. We develop a theory of descent and forms of tensor categories over arbitrary fields. We describe the general scheme of classification of such forms using algebraic and homotopical language, and give examples of explicit classification of forms. We also discuss the problem of categorification of weak fusion rings, and for the simplest families of such rings, determine which ones are categorifiable.

1. Introduction

The goal of this paper is to give an exposition of the theory of forms of tensor categories over arbitrary fields, providing a categorical counterpart of the classical theory of forms of algebraic structures (such as associative algebras, Lie algebras, Hopf algebras, algebraic varieties, etc.). We provide a classification of forms both in the algebraic language and in the homotopical language, using the theory of higher groupoids, similarly to [ENO2]. Ideologically, this is not really new, since it is an application of the general ideology of descent theory. The point of this paper is to work out the classification of forms more or less explicitly in the setting of tensor categories, and to discuss examples of this classification for specific tensor categories. In particular, we show that even in the simplest cases, such classification problems reduce to interesting questions in number theory, such as the classification of constructible regular polygons (i.e., Fermat primes), the Merkurjev-Suslin theorem, and global class field theory.

The organization of the paper is as follows. In Section 2, we recall the classical theory of forms of algebraic structures (i.e., the theory of descent), and reformulate it in the homotopical language. In Section 3, we explain a generalization of this theory to semisimple abelian categories and then to semisimple tensor categories. Finally, in Section 4, we discuss the theory of categorification of weak unital based rings by rigid tensor categories over arbitrary fields.

Date: February 7, 2012.

Key words and phrases. descent, forms, categories.

Acknowledgments. We are grateful to V. Ostrik for useful discussions, in particular for suggesting Theorem 4.10. The research of the first author was partially supported by the NSF grant DMS-1000113. The second author was supported by The Israel Science Foundation (grant No. 317/09). Both authors were supported by BSF grant No. 2008164.

2. Forms of algebraic structures

In this section we give an exposition of the well known theory of forms of algebraic structures.

2.1. **Definition of a form.** Let K be a field, and let L be an extension field of K. Let C be an algebraic structure defined over L (associative algebra, Lie algebra, Hopf algebra, algebraic variety, etc.).

Definition 2.1. A *form* of C over K (or a *descent* of C to K) is an algebraic structure $\overline{C}$ defined over K, of the same type as C, together with an $L-$linear isomorphism $\xi : \overline{C} \otimes_K L \to C$.

An *isomorphism* of two forms $(\overline{C}_1, \xi_1)$, $(\overline{C}_2, \xi_2)$ is an isomorphism $\theta : \overline{C}_1 \to \overline{C}_2$ not necessarily respecting ξ_1, ξ_2. A *framed isomorphism* is an isomorphism θ such that $\xi_2 \circ \theta = \xi_1$.

2.2. **The first condition.** Let us recall necessary and sufficient conditions for the existence of a form of C over K. For simplicity let us assume that L is a *finite Galois extension* of K (the case of infinite Galois extensions is similar, and the general case can be reduced to the case of a Galois extension). Let $\Gamma := \mathrm{Gal}(L/K)$ be the Galois group of L over K.

For any $g \in \Gamma$, let ${}^gC$ denote the algebraic structure obtained from C by twisting its $L-$structure by means of g. This operation is a functor: any morphism $\beta : C \to D$ gives rise to a morphism $g(\beta) : {}^gC \to {}^gD$, which set-theoretically is the same as β (its only difference from β is that its source and target have been twisted by g).

Let us call a pair (g, φ) consisting of $g \in \Gamma$ and an isomorphism $\varphi : {}^gC \to C$, a *twisted automorphism* of C, and let $\mathrm{Aut}_K(C)$ be the group of all twisted automorphisms of C. We have a group homomorphism $\psi : \mathrm{Aut}_K(C) \to \Gamma$ whose kernel is the group $\mathrm{Aut}(C)$ of automorphisms of C. Clearly, if a form of C over K exists then ψ must be surjective, i.e., there is a short exact sequence of groups

$$1 \to \mathrm{Aut}(C) \to \mathrm{Aut}_K(C) \xrightarrow{\psi} \Gamma \to 1. \tag{1}$$

Equivalently, in topological terms, there is a fibration

$$\begin{array}{c} B\mathrm{Aut}_K(C) \\ \Big\downarrow{\scriptstyle B\mathrm{Aut}(C)} \\ B\Gamma \end{array} \tag{2}$$

where BG denotes the classifying space of a group G.

2.3. **The second condition.** Moreover, if a form of C over K exists, we must be able to choose a set of representatives

$$\varphi := \{\varphi_g \in \psi^{-1}(g) \mid g \in \Gamma\}$$

such that the conditions

$$\varphi_{gh} = \varphi_g \circ g(\varphi_h),\ g, h \in \Gamma, \tag{3}$$

are satisfied, that is, the extension in (1) must split. Equivalently, the fibration in (2) must have a section σ_φ.

2.4. **Sufficiency of the two conditions.** It turns out that this is also sufficient. Namely, we have the following standard result.

Proposition 2.2. *A form of C over K exists if and only if the extension in (1) splits, i.e., if and only if the fibration in (2) has a section.* □

For example, if C is an (associative, Lie, Hopf, etc.) algebra A over L and the extension in (1) splits via φ then the set of fixed points $\overline{A} := \{a \in A \mid \varphi_g(a) = a, \forall g \in \Gamma\}$ is a form of A over K. Conversely, it is easy to see that any form canonically defines a splitting.

Example 2.3. Suppose that $\mathrm{Aut}(C)$ is an abelian group. In this case, extension (1) yields an action of Γ on $\mathrm{Aut}(C)$, and the obstruction to the existence of a form of C over K lies in $H^2(\Gamma, \mathrm{Aut}(C))$. Indeed, suppose ψ is surjective, and pick a collection of pre-images $\varphi_g \in \psi^{-1}(g)$ for $g \in \Gamma$. Then we have

$$\varphi_{gh} = \alpha(g, h) \circ \varphi_g \circ g(\varphi_h),$$

where $\alpha : \Gamma \times \Gamma \to \mathrm{Aut}(C)$, and it easy to check that α is a $2-$cocycle: $\alpha \in Z^2(\Gamma, \mathrm{Aut}(C))$. Moreover, φ_g can be corrected to satisfy (3) if and only if this cocycle is a coboundary. Thus the obstruction to the existence of a form is the class $[\alpha] \in H^2(\Gamma, \mathrm{Aut}(C))$.

2.5. **Classification of forms.** Let us now recall the classification of forms of C over K. For this purpose, assume that a form exists. Let us fix one such form, call it $\overline{C}$, and classify all the forms of C over K (which in this situation are also called *twisted forms* of $\overline{C}$).

As explained above, forms of C over K correspond to splittings of extension (1) (i.e., homotopy classes of sections of fibration (2)). So, if we choose such a splitting φ (which, in particular, defines an action of Γ on $\mathrm{Aut}(C)$) then for any other splitting φ', we have $\varphi'_g = \lambda_g \circ \varphi_g$, $g \in \Gamma$, for some function $\lambda : \Gamma \to \mathrm{Aut}(C)$, $g \mapsto \lambda_g$.

The following proposition is standard.

Proposition 2.4. *The following hold:*

(i) φ' is a splitting if and only if $\lambda \in Z^1(\Gamma, \mathrm{Aut}(C))$ (i.e., λ is a $1-$cocycle).

(ii) $\lambda_1, \lambda_2 \in Z^1(\Gamma, \mathrm{Aut}(C))$ determine the same form up to a framed isomorphism if and only if they define the same cohomology class in $H^1(\Gamma, \mathrm{Aut}(C))$. □

Corollary 2.5. *The framed isomorphism classes of twisted forms of $\overline{C}$ over K are in a natural bijection with the set $H^1(\Gamma, \mathrm{Aut}(C))$, and the unframed isomorphism classes of twisted forms are in a natural bijection with orbits of the group $\mathrm{Aut}(C)^\Gamma = \mathrm{Aut}(\overline{C})$ on $H^1(\Gamma, \mathrm{Aut}(C))$.* □

Remark 2.6. If the group $\mathrm{Aut}(C)$ is abelian, the action of Γ on $\mathrm{Aut}(C)$ is defined a priori, and the above discussion shows that the set of isomorphism (or framed isomorphism) classes of forms of C over K is naturally a (possibly empty) torsor T over the group $H^1(\Gamma, \mathrm{Aut}(C))$, which is trivialized once we choose a form $\overline{C} \in T$.

3. Forms of categories

3.1. **Definition of a form.** Let K be a field (which for simplicity we will assume to be perfect), and let L be a field extension of K.

Let $\overline{\mathcal{C}}$ be a semisimple abelian category over K with finite-dimensional Hom$-$spaces. Then one can define a semisimple abelian category $\mathcal{C} := \overline{\mathcal{C}} \otimes_K L$, which is the Karoubian envelope of the category obtained from $\overline{\mathcal{C}}$ by extending scalars from K to L in the spaces of morphisms (for example, if G is a finite group, then $\mathrm{Rep}_K(G) \otimes_K L = \mathrm{Rep}_L(G)$). Note that under this operation, simple objects of $\overline{\mathcal{C}}$ may cease to be simple, and decompose into several simple pieces (in particular, $\mathcal{C}$ may have more simple objects than $\overline{\mathcal{C}}$). Also note that this operation respects the structures of a tensor category, braided tensor category, etc.

Let us say that a semisimple abelian category $\overline{\mathcal{C}}$ over K is *split* if for any simple object $X \in \overline{\mathcal{C}}$, one has $\mathrm{End}(X) = K$. If $\overline{\mathcal{C}}$ is split, then extension of scalars reduces just to tensoring up with L, and taking the Karoubian envelope is not needed.

Let $\mathcal{C}$ be a semisimple $L-$linear category with finite-dimensional Hom$-$spaces (possibly with extra structure, e.g., tensor, braided, etc.). In this section, we develop a theory of forms of such categories, categorifying the results of the previous section. [1]

Definition 3.1. A *form* of $\mathcal{C}$ over K (or a *descent* of $\mathcal{C}$ to K) is a category $\overline{\mathcal{C}}$ defined over K, of the same type as $\mathcal{C}$, together with an $L-$linear equivalence $\Xi : \overline{\mathcal{C}} \otimes_K L \to \mathcal{C}$.

An *equivalence* of two forms $(\overline{\mathcal{C}}_1, \Xi_1)$, $(\overline{\mathcal{C}}_2, \Xi_2)$ of $\mathcal{C}$ over K is an equivalence $\Theta : \overline{\mathcal{C}}_1 \to \overline{\mathcal{C}}_2$ not necessarily respecting Ξ_1, Ξ_2. A *framed equivalence* is an equivalence Θ together with an isomorphism of functors $\Xi_2 \circ \Theta \cong \Xi_1$. We will say that an equivalence admits a framing if it can be upgraded to a framed equivalence.

The necessary and sufficient conditions for the existence of a form of $\mathcal{C}$ over K are similar to the case of algebraic structures. Namely, as before, let us assume for simplicity that L is a finite Galois extension of K, and let $\Gamma := \mathrm{Gal}(L/K)$ be the Galois group of L over K.

3.2. **The first condition.** Let $\mathcal{C}$ be an $L-$linear category (abelian, tensor, braided, etc.). For any $g \in \Gamma$, let ${}^g\mathcal{C}$ denote the category obtained from $\mathcal{C}$ by twisting its $L-$structure by means of g. This operation is a $2-$functor.

Let us call a pair (g, Φ) consisting of $g \in \Gamma$ and an equivalence $\Phi : {}^g\mathcal{C} \to \mathcal{C}$, a *twisted auto-equivalence* of $\mathcal{C}$, and let $\underline{\mathrm{Aut}}_K(\mathcal{C})$ be the categorical $(1-)$group (or gr-category) of all twisted auto-equivalences of $\mathcal{C}$.

Remark 3.2. There is an (equivalent) approach in which one considers an auto-equivalence $\Phi_g : \mathcal{C} \to \mathcal{C}$, which is *semi-linear relative to* g (see e.g. [DM, p.158]). A similar approach can be taken in the algebraic setting of Section 2, as well.

The reason we prefer to use twisted auto-equivalences is that it exhibits more clearly why the cohomology classes we get as obstructions

[1] Although for simplicity we work with semisimple categories, our constructions can be generalized to the non-semisimple case, using an appropriate notion of extension of scalars for linear categories (see e.g. [DM, p. 155]). Also, the condition that K is perfect can be dropped without any changes if we work with absolutely semisimple categories, i.e., categories in which endomorphism algebras of simple objects are separable (which means semisimple after any field extension).

or freedoms are with twisted coefficients (i.e., with coefficients in a non-trivial module).

We have a categorical group homomorphism $\Psi : \underline{\mathrm{Aut}}_K(\mathcal{C}) \to \Gamma$ (where Γ is the usual Galois group regarded as a categorical group) whose kernel is the categorical group $\underline{\mathrm{Aut}}(\mathcal{C})$ of auto-equivalences of $\mathcal{C}$. Clearly, if a form of $\mathcal{C}$ over K exists then Ψ must be surjective, i.e., there is a short exact sequence of categorical groups

$$1 \to \underline{\mathrm{Aut}}(\mathcal{C}) \to \underline{\mathrm{Aut}}_K(\mathcal{C}) \xrightarrow{\Psi} \Gamma \to 1. \tag{4}$$

Equivalently, in topological terms, there is a fibration

$$\begin{array}{c} B\underline{\mathrm{Aut}}_K(\mathcal{C}) \\ \Big\downarrow {\scriptstyle B\underline{\mathrm{Aut}}(\mathcal{C})} \\ B\Gamma. \end{array} \tag{5}$$

Here $B\mathcal{G}$ denotes the classifying space of a categorical group $\mathcal{G}$. Recall that this space is $2-$type, i.e., it has two non-trivial homotopy groups $\pi_1 = G := \mathrm{Ob}(\mathcal{G})$ and $\pi_2 = A := \mathrm{Aut}(\mathbf{1})$, and its structure is determined by an action of G on A and an element of $H^3(G, A)$.

Example 3.3. Let $L := \mathbb{C}$, let p be a prime of the form $4k-1$, and let $\mathcal{C} := \mathrm{Vec}^{\omega}_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{C})$ be the category of $\mathbb{Z}/p\mathbb{Z}-$graded complex vector spaces with a non-trivial $3-$cocycle ω. Let $K := \mathbb{R}$, and let $g \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ be the complex conjugation. Then ${}^g\mathcal{C} = \mathrm{Vec}^{\omega^{-1}}_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{C})$, which is not equivalent to $\mathcal{C}$, since -1 is a quadratic non-residue modulo p. Hence $\mathcal{C}$ is not defined over $\mathbb{R}$.

3.3. **The second condition.** Moreover, if a form exists, we must be able to choose a set of representatives

$$\Phi := \{\Phi_g \in \Psi^{-1}(g) \mid g \in \Gamma\}$$

such that the conditions

$$\Phi_{gh} \cong \Phi_g \circ g(\Phi_h),\ g, h \in \Gamma, \tag{6}$$

are satisfied. That is, the extension in (4) must split at the level of ordinary groups. Equivalently, the fibration in (5) must have a section over the $2-$skeleton of the base.

Example 3.4. Let us keep the setting of Example 3.3, except that p is a prime of the form $4k+1$. Let $m \in \mathbb{Z}/p\mathbb{Z}$ be such that $m^2 = -1$. Then we have an equivalence $\Phi_g : {}^g\mathcal{C} \to \mathcal{C}$ such that $\Phi_g(X_1) = X_m$ (where $X_0 := \mathbf{1}, \dots, X_{p-1}$ are the simple objects of $\mathcal{C}$). So the square of this functor is not the identity on simple objects, i.e., equation (6) is not satisfied (for any choice of m and Φ). This implies that $\mathcal{C}$ still

does not have a real form, even though it is equivalent to its complex conjugate category.

3.4. **The third condition (vanishing of $o_\Phi(\mathcal{C}) \in H^3(\Gamma, \mathrm{Aut}(\mathrm{Id}_\mathcal{C}))$).** Unlike the case of algebraic structures, the first two conditions are not sufficient, and there is another obstruction that must vanish in order for a form to exist. Namely, suppose that exact sequence (4) splits at the level of ordinary groups. Then we can choose functorial isomorphisms

$$J_{g,h} : \Phi_g \circ g(\Phi_h) \to \Phi_{gh},\ g, h \in \Gamma.$$

Thus, we obtain two functorial isomorphisms

$$\Phi_g \circ g(\Phi_h) \circ gh(\Phi_k) \to \Phi_{ghk},\ g, h, k \in \Gamma,$$

namely, $J_{gh,k} \circ J_{g,h}$ and $J_{g,hk} \circ g(J_{h,k})$. If there exists a form, there should be a choice of $J_{g,h}$ such that these two functorial isomorphisms are equal. However, we may consider the element

$$\omega = \omega_\Phi = \{\omega_{g,h,k} \in \mathrm{Aut}(\Phi_{ghk}) \cong \mathrm{Aut}(Id_\mathcal{C}) \mid g, h, k \in \Gamma\}$$

such that

$$\omega_{g,h,k} \circ J_{gh,k} \circ J_{g,h} = J_{g,hk} \circ g(J_{h,k}).$$

It is easy to see that the splitting of exact sequence (4) at the level of ordinary groups gives a homomorphism $\Gamma \to \mathrm{Aut}_K(\mathcal{C})$, and hence an action of Γ on $\mathrm{Aut}(\mathrm{Id}_\mathcal{C})$. Moreover, it is readily seen that ω is a $3-$cocycle for this action: $\omega \in Z^3(\Gamma, \mathrm{Aut}(\mathrm{Id}_\mathcal{C}))$. Finally, changing $J_{g,h}$ corresponds to changing ω by a coboundary. Thus the last obstruction to existence of a form of $\mathcal{C}$ over K is the class $o_\Phi(\mathcal{C})$ of $\omega = \omega_\Phi$ in $H^3(\Gamma, \mathrm{Aut}(\mathrm{Id}_\mathcal{C}))$; a form exists if and only if this obstruction vanishes. Topologically speaking, this condition is equivalent to the condition that the section σ_Φ of fibration (5) over the $2-$skeleton of $B\Gamma$ defined by Φ lifts to the $3-$skeleton. This is equivalent to the condition that σ_Φ lifts to the entire $B\Gamma$, since any section of (5) over the $3-$skeleton of $B\Gamma$ extends canonically (up to homotopy) to the entire base (as $B\underline{\mathrm{Aut}}(\mathcal{C})$ has only two non-trivial homotopy groups).

Summarizing, we obtain the following proposition.

Proposition 3.5. *A form of $\mathcal{C}$ over K exists if and only if extension (4) splits as an extension of categorical groups, i.e., if and only if the fibration in (5) has a section.*

Proof. The "only if" part is clear from the above discussion. To prove the "if" part, let $\mathcal{C}$ be a semisimple category over L, and assume that extension (4) splits via (Φ, J). In this case, define a $\Gamma-$stable object of

$\mathcal{C}$ to be an object $X \in \mathcal{C}$ together with an isomorphism $\alpha_g : \Phi_g(X) \to X$ for each $g \in \Gamma$, such that

$$\alpha_{gh} \circ J_{g,h}|_X = \alpha_g \circ \Phi_g(\alpha_h).$$

(Note that simple objects may fail to admit a $\Gamma-$stable structure since they may be non-trivially permuted by Γ.) Given two $\Gamma-$stable objects X, Y, the $L-$space $\mathrm{Hom}(X, Y)$ has a natural action of Γ defined by α_g. Define the category $\overline{\mathcal{C}}$ of $\Gamma-$stable objects of $\mathcal{C}$ with

$$\mathrm{Hom}_{\overline{\mathcal{C}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)^{\Gamma}.$$

Then there is a canonical equivalence $\overline{\mathcal{C}} \otimes_K L \to \mathcal{C}$, so $\overline{\mathcal{C}}$ is a form of $\mathcal{C}$ over K. Indeed, since J satisfies the $2-$cocycle condition, one can show that any object $Y \in \mathcal{C}$ is a direct summand in a $\Gamma-$stable object of $\mathcal{C}$. □

Example 3.6. (*Minimal field of definition.*) Keep the setting of Example 3.3, with an arbitrary odd prime p. We would like to determine the minimal field of definition of the category $\mathcal{C} := \mathrm{Vec}^{\omega}_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{C})$. Clearly, this category is defined over the cyclotomic field $L := \mathbb{Q}(\zeta)$, where $\zeta := e^{2\pi i/p}$. So we would like to find the minimal subfield $K \subseteq L$ over which this category has a form. By the main theorem of Galois theory, such subfields K correspond to subgroups $\Gamma \subseteq \mathbb{F}_p^{\times} = \mathrm{Gal}(L/\mathbb{Q})$, so we are looking for the largest possible subgroup Γ. Note that by Examples 3.3, 3.4, K cannot be a real field, and hence Γ is of odd order (as it cannot contain -1, i.e., complex conjugation). So if we write p as $p = 2^m r + 1$, where r is odd, then the largest Γ can be is the group $\Gamma := \mathbb{Z}/r\mathbb{Z} = (\mathbb{F}_p^{\times})^{2^m}$.

Let us show that this group in fact works, i.e., there is a form of $\mathcal{C}$ over the corresponding field K (which has degree 2^m over $\mathbb{Q}$). To see this, note that since r is odd, we have a square root homomorphism $s : \Gamma \to \Gamma$. Now, for $g \in \Gamma$, let $\Phi_g : {}^g\mathcal{C} \to \mathcal{C}$ be defined on objects by $\Phi_g(X_1) = X_{s(g)}$. This can be extended to a tensor functor (since raising to power a in $\mathbb{F}_p$ acts on ω by a^{-2}). Moreover, it is easy to see that the functors Φ_g satisfy the $1-$cocycle condition, and the obstruction $o_\Phi(\mathcal{C})$ must vanish since it lies in $H^3(\Gamma, \mathbb{Z}/p\mathbb{Z}) = 0$. Thus, there is a form $\overline{\mathcal{C}}$ of $\mathcal{C}$ over K (which is in fact unique since $H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}) = 0$). The simple objects of $\overline{\mathcal{C}}$ are $Y_0 := \mathbf{1}$ and $Y_1, \dots, Y_{2^m}$ (of Frobenius-Perron dimension r).

We see that the initial field of definition L is minimal only very rarely. This happens if $r = 1$ (i.e., the form $\overline{\mathcal{C}}$ is split), which is equivalent to the condition that p is a Fermat prime, i.e., a prime of the form $2^{2^n} + 1$

(there are only five such primes known, namely, 3, 5, 17, 257, and 65537).

Also, note that if $p = 4k-1$ then $m = 1$, and thus $\mathcal{C}$ is defined over the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. The corresponding form $\overline{\mathcal{C}}$ has three simple objects $\mathbf{1}, X, X^*$, with $\mathrm{FPdim} X = \frac{p-1}{2} = 2k-1$, and fusion rules

$$X \otimes X = (k-1)X \oplus kX^* \tag{7}$$

and

$$X \otimes X^* = X^* \otimes X = (2k-1)\mathbf{1} \oplus (k-1)(X \oplus X^*).$$

Similar analysis applies to the situation when $\mathcal{C} := \mathrm{Vec}^{\omega}_{\mathbb{Z}/n\mathbb{Z}}(\mathbb{C})$, where ω is a generator of $H^3(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^\times)$, where $n > 1$ is a positive integer, not necessarily a prime. In this case, the a priori field of definition is $L := \mathbb{Q}(e^{2\pi i/n})$, with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$, of order $\varphi(n)$. We write $\varphi(n) = 2^m r$, where r is odd. Then the minimal field of definition K is of degree 2^m over $\mathbb{Q}$, and the group $\Gamma = \mathrm{Gal}(L/K)$, of order r, is the group of elements of odd order in $(\mathbb{Z}/n\mathbb{Z})^\times$. So we have

Proposition 3.7. *The minimal field of definition of $\mathcal{C} := Vec^{\omega}_{\mathbb{Z}/n\mathbb{Z}}(\mathbb{C})$ is L (i.e., $\Gamma = 1$) if and only if the regular $n-$gon can be constructed by compass and ruler, i.e., if and only if n is a Gauss number, $n = 2^s q$, where q is a product of distinct Fermat primes.* □

3.5. **Classification of forms.** Let us now describe the classification of forms of $\mathcal{C}$ over K in the case when they do exist. For this purpose, fix one such form, call it $\overline{\mathcal{C}}$, and classify all the forms of $\mathcal{C}$ over K (which in this situation are also called *twisted forms* of $\overline{\mathcal{C}}$).

As explained above, forms of $\mathcal{C}$ over K correspond to splittings of extension (4) (i.e., homotopy classes of sections of fibration (5)) together with collections of isomorphisms $J = (J_{g,h})$. So, if we choose such a splitting Φ of the extension of ordinary groups (which, in particular, defines an action of Γ on $\mathrm{Aut}(\mathcal{C})$) then for any other splitting Φ', we have $\Phi'_g = \Lambda_g \circ \Phi_g$, $g \in \Gamma$, for some $1-$cocycle $\Lambda = \Lambda_\Phi : \Gamma \to \mathrm{Aut}(\mathcal{C})$, $g \mapsto \Lambda_g$, and conversely, any $1-$cocycle defines a splitting. Moreover, two $1-$cocycles define equivalent splittings if and only if they are in the same cohomology class.

Furthermore, it is easy to show that the obstruction $o_{\Phi'}(\mathcal{C})$ is the pullback of the canonical class $o(\mathcal{C}) \in H^3(\mathrm{Aut}_K(\mathcal{C}), \mathrm{Aut}(\mathrm{Id}_\mathcal{C}))$ (defining the associativity isomorphism in $\underline{\mathrm{Aut}}_K(\mathcal{C})$) under the homomorphism $\gamma_\Lambda : \Gamma \to \mathrm{Aut}_K(\mathcal{C})$ defined by Λ.

Thus, we obtain the following proposition.

Proposition 3.8. *The following hold:*

(i) An element $\Lambda \in Z^1(\Gamma, \mathrm{Aut}(\mathcal{C}))$ gives rise to a twisted form of $\overline{\mathcal{C}}$ if and only if $\gamma_\Lambda^* o(\mathcal{C}) = 0$; this condition depends only on the class $[\Lambda] \in H^1(\Gamma, \mathrm{Aut}(\mathcal{C}))$.

(ii) If the condition of (i) is satisfied then framed equivalence classes of twisted forms of $\overline{\mathcal{C}}$ corresponding to Λ are parameterized by a torsor over $H^2(\Gamma, \mathrm{Aut}(Id_{\mathcal{C}}))$.

(iii) Unframed equivalence classes of twisted forms correspond to orbits of $\mathrm{Aut}(\mathcal{C})^\Gamma = \mathrm{Aut}(\overline{\mathcal{C}})$ on the data of (i),(ii).

Proof. For a given Φ', choices of J' up to equivalence are parameterized by a torsor over $H^2(\Gamma, \mathrm{Aut}(Id_{\mathcal{C}}))$. □

3.6. **Forms of semisimple abelian categories.**

Example 3.9. Let $\mathcal{C} := \mathrm{Vec}(L)$ be the abelian $L-$linear category of finite-dimensional vector spaces over L. Let $\overline{\mathcal{C}} := \mathrm{Vec}(K)$. We have $\mathrm{Aut}(\mathcal{C}) = 1$, so there is a unique choice of Φ. The obstruction $o_\Phi(\mathcal{C})$ vanishes since there is a form of $\mathcal{C}$ (namely, $\overline{\mathcal{C}}$). Therefore, the twisted forms of $\overline{\mathcal{C}}$ are classified by $H^2(\Gamma, \mathrm{Aut}(\mathrm{Id}_{\mathcal{C}})) = H^2(\Gamma, L^\times)$, which is the relative Brauer group $\mathrm{Br}(L/K)$. Indeed, for any $a \in \mathrm{Br}(L/K)$, there is a division algebra D_a over K with trivial center (which splits over L), and the form of $\mathcal{C}$ corresponding to a is just the $K-$linear category of finite-dimensional left vector spaces over D_a.

Example 3.10. Let $\mathcal{C} := \mathrm{Vec}(L)^n$ be the direct sum of n copies of the category $\mathrm{Vec}(L)$. Let $\overline{\mathcal{C}} := \mathrm{Vec}(K)^n$. We have $\mathrm{Aut}(\mathcal{C}) = S_n$, with a trivial action of Γ. Thus, choices of Φ correspond to homomorphisms $\Phi : \Gamma \to S_n$, i.e., commutative semisimple $K-$algebras R of dimension n with a splitting over L. The obstruction $o_\Phi(\mathcal{C})$ vanishes for all Φ, since for any R we have a form $\overline{\mathcal{C}}_R$ of $\mathcal{C}$ over K, which is the category of finite-dimensional $R-$modules. So all the forms corresponding to Φ are parameterized by $H^2(\Gamma, (L^\times)^n)$, where the action of Γ corresponds to Φ.

The algebra R is a direct sum of field extensions of K:

$$R = K_1 \oplus \cdots \oplus K_m.$$

These extensions correspond to orbits of Γ on the set $\{1, ..., n\}$. Thus it suffices to consider the case when there is just one orbit; the general case is obtained by taking the direct sum. In the case of one orbit, R is a field extension of K of degree n, and Γ acts transitively on $(L^\times)^n$. By the Shapiro Lemma, $H^2(\Gamma, (L^\times)^n) = H^2(\Gamma_1, L^\times)$, where Γ_1 is the stabilizer of $1 \in \{1, ..., n\}$. But Γ_1 is the Galois group of L over R, so we get that the twisted forms are parameterized by the relative Brauer group $\mathrm{Br}(L/R)$. Indeed, given $a \in \mathrm{Br}(L/R)$, let D_a

be the corresponding division algebra with center R; then the form corresponding to R is the $K-$linear category of finite-dimensional left vector spaces over D_a.

3.7. **Forms of tensor categories.** Let us now pass to tensor categories.

Example 3.11. Let $\overline{K}$ be the algebraic closure of K, and let $\mathcal{C} := \mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}(\overline{K})$ be the tensor category of $\mathbb{Z}/2\mathbb{Z}-$graded $\overline{K}-$vector spaces. Let $\overline{\mathcal{C}} := \mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}(K)$. Then $\mathrm{Aut}(\mathcal{C}) = 1$, so there is a unique choice of Φ, the obstruction $o_\Phi(\mathcal{C})$ vanishes, and twisted forms are classified by $H^2(\Gamma, \mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C})) = H^2(\Gamma, \mathbb{Z}/2\mathbb{Z})$.

Let μ_n denote the group of roots of unity of order n in $\overline{K}$, regarded as a $\Gamma-$module. Recall that $H^2(\Gamma, \mu_n)$ is the group $\mathrm{Br}_n(K) := \mathrm{Ker}\,(n|_{\mathrm{Br}(K)})$ of $n-$torsion in the Brauer group of K. Indeed, we have a short exact sequence of $\Gamma-$modules

$$1 \to \mu_n \to \overline{K}^\times \xrightarrow{n} \overline{K}^\times \to 1,$$

which yields an exact sequence

$$H^1(\Gamma, \overline{K}^\times) \to H^2(\Gamma, \mu_n) \to H^2(\Gamma, \overline{K}^\times) \to H^2(\Gamma, \overline{K}^\times).$$

Since by Hilbert theorem 90, $H^1(\Gamma, \overline{K}^\times) = 0$, the claim follows.

So the forms of the tensor category $\mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}(\overline{K})$ over K are classified by the group $\mathrm{Br}_2(K)$ of elements of order ≤ 2 in the Brauer group $\mathrm{Br}(K)$ (which is $H^2(\Gamma, \mathbb{Z}/2\mathbb{Z})$).

For example, if $K = \mathbb{R}$ then $\Gamma = \mathbb{Z}/2\mathbb{Z}$ and $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, so there is one non-trivial form. Its simple objects are the unit object $\mathbf{1}$ and an object X satisfying $X \otimes X = 4 \cdot \mathbf{1}$, with $\mathrm{End}(\mathbf{1}) = \mathbb{R}$ and $\mathrm{End}(X) = \mathbb{H}$ (the algebra of quaternions).

Similar analysis applies to the category $\mathrm{Vec}^\omega_{\mathbb{Z}/2\mathbb{Z}}(\overline{K})$ with a non-trivial associator (over a field of characteristic different from 2). Its forms over K are parameterized by $\mathrm{Br}_2(K)$, and for $K = \mathbb{R}$ there is one trivial and one non-trivial form.

Example 3.12. Here is an example where $o_\Phi(\mathcal{C}) \neq 0$.

For a finite group G, let $\mathrm{Out}(G)$ denote the group of outer automorphisms of G, and let $Z(G)$ be the center of G. Let H be another finite group, and let $\phi : H \to \mathrm{Out}(G)$ be a homomorphism; then H acts naturally on $Z(G)$. It is well known that there is a canonical Eilenberg-MacLane class $E \in H^3(H, Z(G))$ corresponding to ϕ, which is not always trivial.

Indeed, here is an example, pointed out to us by David Benson. Take $G := \mathrm{SL}(2, \mathbb{F}_9)$ (it is a double cover of the alternating group

$A_6 = \mathrm{PSL}(2, \mathbb{F}_9)$) and let $H := \mathbb{Z}/2\mathbb{Z}$. Then $Z(G) = \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Out}(G) = \mathrm{Out}(A_6) = (\mathbb{Z}/2\mathbb{Z})^2$. Consider the map $\phi : H \to \mathrm{Out}(G)$ for which the corresponding extension of $\mathbb{Z}/2\mathbb{Z}$ by A_6 is the Mathieu group M_{10} (i.e., the image of the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$ under ϕ is the outer automorphism defined by the composition of conjugation by a matrix whose determinant is a non-square with the Frobenius automorphism). Then it is easy to show that there is no extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathrm{SL}(2, \mathbb{F}_9)$ implementing ϕ, so the Eilenberg-MacLane class $E \in H^3(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ is non-trivial.

Let $L := \overline{K}$, let G be a finite group as above, and let $\mathcal{C} := \mathrm{Rep}_{\overline{K}}(G)$ be the tensor category of representations of G. In this case, we have a natural homomorphism $\zeta : \mathrm{Aut}(G) \to \mathrm{Aut}(\mathcal{C})$ which factors through $\mathrm{Out}(G)$ and lands in $\mathrm{Aut}(\mathcal{C})^\Gamma$. So any homomorphism $\eta : \Gamma \to \mathrm{Out}(G)$ gives rise to a homomorphism $\Gamma \to \mathrm{Aut}(\mathcal{C})^\Gamma \subseteq \mathrm{Aut}(\mathcal{C})$ (which is also a $1-$cocycle), and hence to a homomorphism $\Phi : \Gamma \to \mathrm{Aut}_K(\mathcal{C})$. Also, we have $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}) = Z(G)$. Thus, $o_\Phi(\mathcal{C}) \in H^3(\Gamma, Z(G))$, and one can show that $o_\Phi(\mathcal{C}) = \eta^*(E)$. For any G and $H \subset \mathrm{Out}(G)$, one can find K, L and η such that the image of η is H, which gives a desired example.

Note that if $o_\Phi(\mathcal{C}) = 0$ then forms obtained from Φ are parameterized by a torsor over $H^2(\Gamma, Z(G))$. Also note that if η factors through $\mathrm{Aut}(G)$ then $o_\Phi(\mathcal{C}) = 0$ and moreover the torsor parameterizing forms is canonically trivial. The point 0 of this torsor corresponds to the form of the (algebraic) group G defined by η.

Example 3.13. Let $\mathcal{C}$ be a split semisimple tensor category over L, and let $\overline{\mathcal{C}}$ be a form of $\mathcal{C}$ over K. Let us say that a twisted form of $\overline{\mathcal{C}}$ is *quasi-trivial* if the corresponding $1-$cocycle Λ is trivial. It follows from the above that quasi-trivial forms (up to framed equivalence) are classified by $H^2(\Gamma, \mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}))$. Let us compute this group in the case $L = \overline{K}$. Let $U_\mathcal{C}$ be the universal grading group of $\mathcal{C}$ ([GN]), i.e., the group such that $\mathcal{C}$ is $U_\mathcal{C}-$graded, and any faithful grading of $\mathcal{C}$ comes from a quotient of $U_\mathcal{C}$ (for example, if $\mathcal{C} := \mathrm{Vec}_G(L)$, then $U_\mathcal{C} = G$). Then $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}) = \mathrm{Hom}(U_\mathcal{C}, \overline{K}^\times)$ as a $\Gamma-$module. So if $(U_\mathcal{C})_{\mathrm{ab}} = \bigoplus_{j=1}^N \mathbb{Z}/n_j\mathbb{Z}$, then by the above discussion we get that quasi-trivial twisted forms of $\overline{\mathcal{C}}$ are parameterized by

$$\bigoplus_{j=1}^N \mathrm{Br}_{n_j}(K).$$

For instance, for Tambara-Yamagami categories [TY], $U_\mathcal{C} = \mathbb{Z}/2\mathbb{Z}$, so quasi-trivial forms are parameterized by $\mathrm{Br}_2(K)$. This is a generalization of Example 3.11.

3.8. **Split forms.** It is an interesting question whether a given split semisimple tensor category $\mathcal{C}$ over L has a split form over a given subfield $K \subseteq L$ (see [MoS, Section 2.1] for a discussion of this question). In particular, if G is a finite group, it is an interesting question to determine a minimal number field K over which there is a split form of the category $\mathrm{Rep}(G)$ of representations of G; e.g., for which G can we take $K = \mathbb{Q}$?

We note that, as pointed out in [MoS, Section 2.1], the irrationality of characters of G does not imply that $\mathrm{Rep}(G)$ has no split form over $\mathbb{Q}$: e.g., if G is abelian then $\mathrm{Rep}(G) = \mathrm{Vec}_{G^\vee}$ and hence has a split form over $\mathbb{Q}$. However, if the action of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on irreducible representations of G does not come from outer automorphisms of G, then the minimal field K must be larger than $\mathbb{Q}$. This happens for most finite simple groups of Lie type, since the outer automorphism groups of these groups are very small, while Galois orbits of representations increase with the corresponding prime p.

3.9. **Forms of braided and symmetric categories.** The theory of forms of braided and symmetric tensor categories $\mathcal{C}$ is completely parallel to the theory of forms of usual tensor categories. The only change is that the categorical group of tensor auto-equivalences of $\mathcal{C}$ needs to be replaced by the categorical group of braided (respectively, symmetric) auto-equivalences. This group is a subgroup of all auto-equivalences at the level of π_1, and has the same π_2 (which is the group of tensor automorphisms of the identity functor).

As an example consider forms of the nondegenerate braided categories $\mathcal{C} := \mathrm{Vec}_{\mathbb{Z}/p\mathbb{Z}}$ where p is an odd prime (see [DGNO]). It is well known that braidings on this category correspond to quadratic forms on $\mathbb{Z}/p\mathbb{Z}$. Suppose we are given such a form β, which is nondegenerate. Then $\mathcal{C}$ is defined and split over the cyclotomic field $L := \mathbb{Q}(\zeta)$, $\zeta := e^{2\pi i/p}$, and one can ask what is the minimal field of definition K. Since the braiding is defined by a quadratic form, the answer is the same as in Example 3.6: we have to write $p-1$ as $2^m r$, where r is odd, and K is the fixed field of the subgroup $\mathbb{Z}/r\mathbb{Z} \subseteq \mathbb{F}_p^\times$ (of degree 2^m). So we have that $K = L$ if $r = 1$, i.e., if p is a Fermat prime, and $K = \mathbb{Q}(\sqrt{-p})$ if $p = 4k-1$.

4. Categorification of weak unital based rings

4.1. Definition of weak unital based rings.

Definition 4.1. A *weak unital based ring* is a ring R with $\mathbb{Z}-$basis b_i, $i \in I$, containing the unit element 1, whose structure constants

N_{ij}^k (defined by $b_i b_j = \sum_k N_{ij}^k b_k$) are non-negative integers, with an involution $* : I \to I$ defining an anti-involution of R, such that the coefficient of 1 in $b_i b_j$ is zero if $i \neq j^*$ and positive if $i = j^*$. A *weak fusion ring* is a weak unital based ring of finite rank. A *unital based ring* (respectively, *fusion ring*) is a weak unital based ring (respectively, weak fusion ring) such that the coefficient of 1 in $b_i b_{i^*}$ equals 1.

It is well known that the Grothendieck ring of a semisimple rigid tensor category (respectively, fusion category) over an algebraically closed field K is a unital based ring (respectively, a fusion ring) (see e.g. [ENO1]). Similarly, we have the following proposition.

Proposition 4.2. *The Grothendieck ring of a semisimple rigid tensor category (respectively, fusion category) over a general (perfect) field K is a weak unital based ring (respectively, a weak fusion ring).*

Proof. The properties of a weak unital based ring are obvious, except for the property of the coefficient of 1 in $b_i b_j$, which follows from Schur's lemma. □

This gives rise to the problem of categorification of weak unital based rings, and in particular weak fusion rings, i.e., finding a rigid tensor category whose Grothendieck ring is a given weak unital based ring. This problem is discussed in the following subsection.

4.2. **Categorification of weak fusion rings.** Let us now discuss the classification problem of categorifications of given weak fusion rings.

4.2.1. *The rings R_m.* We start by considering the simplest non-trivial weak fusion rings R_m, with basis $\mathbf{1}$ and X, and fusion rules

$$X^2 = m\mathbf{1},\ X^* = X,$$

where m is a positive integer.

Recall that the categorifications of R_1 over an algebraically closed field K are $\mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}(K)$, and also $\mathrm{Vec}^{\omega}_{\mathbb{Z}/2\mathbb{Z}}(K)$ if $\mathrm{char}(K) \neq 2$ (where ω is the non-trivial element of $H^3(\mathbb{Z}/2\mathbb{Z}, K^\times) = \mathbb{Z}/2\mathbb{Z}$).

The classification of categorifications of R_m over any perfect field K of characteristic $\neq 2$ is given by the following theorem.

Theorem 4.3. *Let K be a perfect field of characteristic $\neq 2$.*

(i) Categorifications $\mathcal{D}_Q^{\pm}$ of R_m over K are parameterized by a central division algebra Q over K of dimension m such that $Q = Q^{op}$, and a choice of sign.

(ii) Categorifications $\mathcal{D}_Q^{\pm}$ of R_4 over K are parameterized by a choice of a quaternion division algebra Q over K (i.e. a division algebra

$Q_{a,b}$ with generators x, y and relations $xy = -yx, x^2 = a, y^2 = b$, for $a, b \in K$), as well as a choice of sign.

(iii) If R_m admits a categorification over K then $m = 4^n$ for some non-negative integer n.

(iv) Any categorification $\mathcal{D}$ of R_{4^n} over K is a subcategory in a category of the form $\mathcal{D}^{\pm}_{Q_1} \boxtimes \mathcal{D}^{+}_{Q_2} \boxtimes \cdots \boxtimes \mathcal{D}^{+}_{Q_N}$, where Q_i are quaternion division algebras.

(v) If K is a number field or $K = \mathbb{R}$ then R_m is categorifiable over K if and only if $m = 1$ or $m = 4$.

(vi) R_{4^n} is categorifiable over $K := \mathbb{C}(a_1, ..., a_n, b_1, ..., b_n)$.

Proof. Let $\overline{\mathcal{C}}$ be a categorification of R_m, and let $\mathcal{C} := \overline{\mathcal{C}} \otimes_K \overline{K}$. Then $\Gamma := \mathrm{Gal}(\overline{K}/K)$ acts by automorphisms of the Grothendieck ring $\mathrm{Gr}(\mathcal{C})$ as a unital based ring, and $X \in \overline{\mathcal{C}}$ decomposes in $\mathcal{C}$ as $(\bigoplus_{Z \in O} Z)^{\ell}$, where O is the $\Gamma-$orbit of simple objects corresponding to X, and ℓ is a positive integer. Since $X \otimes X = m\mathbf{1}$, the orbit O consists of a single element Z, and Z is invertible, with $Z \otimes Z = \mathbf{1}$. So we see that $m = \ell^2$, and $\mathcal{C} = \mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}(\overline{K})$ or $\mathcal{C} = \mathrm{Vec}^{\omega}_{\mathbb{Z}/2\mathbb{Z}}(\overline{K})$. Thus, $\overline{\mathcal{C}}$ is a form over K of one of these two categories, so it is determined by a choice of sign ($+$ in the first case and $-$ in the second case) as well as a central division algebra $Q \in \mathrm{Br}_2(K)$ over K, namely, $Q = \mathrm{End}(X)$. So we see that $\dim Q = \ell^2$. This implies (i) and (ii), since in the later case we have $m = 4$, so Q is a quaternion division algebra.

Statement (iii) follows from the following theorem of Brauer.

Theorem 4.4. *(see* [GS]*) The dimension of a central division algebra over K and its order in the Brauer group* $\mathrm{Br}(K)$ *have the same prime factors.*

Statement (iv) follows from the following theorem of Merkurjev.

Theorem 4.5. [M] *Any element of order* 2 *in* $\mathrm{Br}(K)$ *is represented by a tensor product of quaternion algebras over K.*

Statement (v) follows from a well known result of global class field theory (see [AT, p.105], [E, Theorem 3.6]) saying that any element of order 2 in $\mathrm{Br}(K)$ for fields K as in (v) is represented by a quaternion algebra (i.e., taking the tensor product is not necessary).

Finally, to prove (vi), we take the category corresponding to the division algebra $Q := \otimes_{i=1}^{n} Q_{a_i,b_i}$ over K, which is a division algebra of dimension 4^n. □

4.2.2. *The rings $R_{p,r}$.* Theorem 4.3 can be generalized to the setting involving the $p-$torsion in the Brauer group for primes $p > 2$. Namely,

for any prime p define the weak fusion ring $R_{p,r}$ with basis $\mathbf{1}$ and X_i, $i \in \mathbb{F}_p^\times$, and relations

$$X_i^* = X_{-i},\ X_iX_j = rX_{i+j} \text{ for } i+j \neq 0,\ X_iX_{-i} = r^2\mathbf{1}.$$

Thus, $R_{2,r} = R_{r^2}$. Then we have the following result.

Theorem 4.6. *Let K be a perfect field which contains a primitive $p-$th root of unity ζ (so in particular $\mathrm{char}K \neq p$).*

(i) Categorifications $\mathcal{D}_Q^\omega$ of $R_{p,r}$ over K are parameterized by a central division algebra Q over K of dimension r^2 such that $Q^{\otimes p} = \mathrm{Mat}_{r^p}(K)$ and a choice of $\omega \in H^3(\mathbb{Z}/p\mathbb{Z}, \overline{K}^\times) = \mathbb{Z}/p\mathbb{Z}$.

(ii) Categorifications $\mathcal{D}_Q^\omega$ of $R_{p,p}$ over K are parameterized by a choice of a cyclic division algebra Q over K (i.e., an algebra $Q_{a,b,p}$ with generators x, y and relations $xy = \zeta yx, x^p = a, y^p = b$, for $a, b \in K$), as well as a choice of $\omega \in H^3(\mathbb{Z}/p\mathbb{Z}, \overline{K}^\times) = \mathbb{Z}/p\mathbb{Z}$.

(iii) If $R_{p,r}$ admits a categorification over K then $r = p^n$ for some non-negative integer n.

(iv) Any categorification $\mathcal{D}$ of R_{p,p^n} over K is a subcategory in a category of the form $\mathcal{D}_{Q_1}^\omega \boxtimes \mathcal{D}_{Q_2}^1 \boxtimes \cdots \boxtimes \mathcal{D}_{Q_N}^1$, where Q_i are cyclic algebras of dimension p^2.

(v) If K is a number field then $R_{p,r}$ is categorifiable over K if and only if $r = 1$ or $r = p$.

(vi) R_{p,p^n} is categorifiable over $K := \mathbb{C}(a_1, ..., a_n, b_1, ..., b_n)$.

Proof. The proof is parallel to the proof of Theorem 4.3. Let $\overline{\mathcal{C}}$ be a categorification of $R_{r,p}$, and let $\mathcal{C} := \overline{\mathcal{C}} \otimes_K \overline{K}$. Then $\Gamma := \mathrm{Gal}(\overline{K}/K)$ acts by automorphisms of $\mathrm{Gr}(\mathcal{C})$, and $X := X_1 \in \overline{\mathcal{C}}$ decomposes in $\mathcal{C}$ as $(\bigoplus_{Z \in O} Z)^\ell$, where O is the $\Gamma-$orbit of simple objects corresponding to X, and ℓ is a positive integer. Since $X \otimes X^* = r^2\mathbf{1}$, the orbit O consists of a single element Z, and Z is invertible, with $Z \otimes Z^* = \mathbf{1}$. So we see that $\ell = r$, and $\mathcal{C} = \mathrm{Vec}_{\mathbb{Z}/p\mathbb{Z}}^\omega(\overline{K})$ for some $\omega \in H^3(\mathbb{Z}/p\mathbb{Z}, \overline{K}^\times) = \mathbb{Z}/p\mathbb{Z}$. Thus, $\overline{\mathcal{C}}$ is a form of one of these categories over K, so it is determined by a choice of ω as well as a central division algebra $Q \in \mathrm{Br}_p(K)$ over K, namely, $Q = \mathrm{End}(X)$. So we see that $\dim Q = r^2$. This implies (i).

To prove (ii), note that Q is a central division algebra of dimension p^2 over K, so by the Albert-Brauer-Hasse-Noether theorem [BHN], [AH], it is a cyclic algebra.

Statement (iii) follows from Brauer's theorem (Theorem 4.4).

Statement (iv) follows from the theorem of Merkurjev and Suslin:

Theorem 4.7. *([MeS]) Any element of order p in $\mathrm{Br}(K)$ is represented by a tensor product of cyclic division algebras of dimension p^2 over K.*

Statement (v) follows from a well known result of global class field theory (see [AT, p.105], [E, Theorem 3.6]) saying that any element of order p in $\mathrm{Br}(K)$ for fields K as in (v) is represented by a cyclic algebra of dimension p^2 (i.e., taking the tensor product is not necessary).

Finally, to prove (vi), we take the category corresponding to the division algebra $Q := \otimes_{i=1}^n Q_{a_i,b_i,p}$ over K, which is a division algebra of dimension p^{2n}. □

4.2.3. *The rings S_k.* For a positive integer k define the weak fusion ring S_k with basis $\mathbf{1}, X$ and relations

$$X^2 = k\mathbf{1} + (k-1)X,\ X^* = X.$$

Let us classify categorifications $\overline{\mathcal{C}}$ of this ring over a field K, say, of characteristic zero. We have $\mathrm{FPdim}(X) = k$. Passing to the algebraic closure, we get $X = (\bigoplus_{i\in O} X_i)^\ell$, where O is a Galois group orbit. Now, it is clear that $\mathrm{FPdim}(X_i) = 1$ (otherwise we would not be able to write a decomposition for $X_i \otimes X_i^*$), so we get $k = \ell|O|$. Also, from the equation for $XX^* = X^2$ we get $\ell^2|O| = k$, which implies that $\ell = 1$, $|O| = k$. So $\mathcal{C} := \overline{\mathcal{C}} \otimes_K \overline{K}$ is the category $\mathrm{Vec}_G^\omega(\overline{K})$ for some group G and 3−cocycle $\omega \in H^3(G, \overline{K}^\times)$.

The absolute Galois group Γ of K acts on G and has two orbits, namely $\{1\}$ and O. This means that all elements of G other than 1 have the same order, which then has to be a prime p, such that $k + 1 = p^n$ for some positive integer n. Moreover, if G were non-abelian then the Galois group would have to preserve its non-trivial proper subgroup (the center), which is impossible because we have just two orbits. Thus G must be abelian, hence a vector space V over $\mathbb{F}_p$, and we have a homomorphism $\Phi : \Gamma \to \mathrm{GL}(V)$ such that Γ acts transitively on non-zero vectors, i.e., the image $\overline{\Gamma}$ of Γ in $\mathrm{GL}(V)$ is a transitive finite linear group.

On the other hand, if we have any surjective homomorphism $\Phi : \Gamma \to \mathrm{GL}(V)$ then for $\omega = 1$ we obtain a categorification of S_k over an appropriate field K (the category of representations of the twisted form of the algebraic group V^* defined by the homomorphism Φ). Thus, we obtain the following proposition, which is somewhat similar to [EGO, Corollary 7.4].

Proposition 4.8. *The weak fusion ring S_k is categorifiable over a suitable field if and only if $k + 1$ is a prime power.* □

For example, for $k \le 10$, S_k is categorifiable except for $k = 5, 9$.

The problem of explicit classification of categorifications of S_k for $k = p^n - 1$ is rather tricky. For simplicity consider the case when

$p > 3$, and K contains a primitive root of unity of order p. In this case, $H^3(V, \overline{K}^\times) = S^2V^* \oplus \wedge^3 V^*$ as a $\Gamma-$module. Clearly, ω must be $\Gamma-$invariant. Since $\overline{\Gamma}$ is transitive, ω cannot have a non-zero component q_ω in S^2V^*, since the level sets of $q_\omega(v,v)$ are invariant under Γ. So we have $\omega \in (\wedge^3 V^*)^\Gamma$, and each such ω will give rise to a categorification. Apart from the case of vanishing ω, if $m = 3d$, we have the example $\Gamma = \mathrm{SL}_3(\mathbb{F}_q)$, where $q = p^d$. In this case, we can take $\omega(v,w,u) = \psi(v \wedge w \wedge u)$, where $v, w, u \in \mathbb{F}_q^3$, and $\psi : \mathbb{F}_q \to \mathbb{F}_p$ is any non-zero linear function. The full classification of categorifications can be obtained by using the known classification of transitive finite linear groups (see e.g. [BH]); we will not do it here.

4.2.4. *The rings T_k.* Now, consider the fusion ring T_k defined by (7), where k is a non-negative integer. Let us classify categorifications $\overline{\mathcal{C}}$ of this ring over a field K, say, of characteristic zero. We have $\mathrm{FPdim}(X) = 2k-1$. Passing to the algebraic closure, we get $X = (\bigoplus_{i \in O} X_i)^\ell$, where O is a Galois group orbit. Now, it is clear that $\mathrm{FPdim}(X_i) = 1$ (otherwise we would not be able to write a decomposition for $X_i \otimes X_i^*$), so we get $2k-1 = \ell|O|$. Also, from the equation for $X \otimes X^*$ we get $\ell^2|O| = 2k-1$, which implies that $\ell = 1$, $|O| = 2k-1$. So $\mathcal{C} := \overline{\mathcal{C}} \otimes_K \overline{K}$ is the category $\mathrm{Vec}_G^\omega(\overline{K})$ for some group G and $3-$cocycle $\omega \in H^3(G, \overline{K}^\times)$.

The absolute Galois group Γ of K acts on G and has three orbits, namely $\{1\}$, O, and O^{-1}. This means that all elements of G other than 1 have the same order, which then has to be an (odd) prime p, such that $4k-1 = p^{2n+1}$ for some non-negative integer n. Moreover, if G were non-abelian then the Galois group would have to preserve its non-trivial proper subgroup (the center), which is impossible because we have just three orbits. Thus G must be abelian, hence a vector space V of dimension $2n+1$ over $\mathbb{F}_p$, and we have a homomorphism $\Phi : \Gamma \to \mathrm{GL}(V)$.

Now, for any such p, n, we can take $V = \mathbb{F}_q$, where $q = p^{2n+1}$, and $\Gamma = (\mathbb{F}_q^\times)^2$. Since $p = 4l-1$, and q is an odd power of p, we get that -1 is a non-square in $\mathbb{F}_q$, so Γ satisfies the above condition, and we get a categorification with trivial ω. Thus, we obtain the following proposition.

Proposition 4.9. *The weak fusion ring T_k is categorifiable over a suitable field if and only if $4k-1$ is an (odd) power of a prime.* □

For example, for $k \leq 10$, S_k is categorifiable except for $k = 4, 9, 10$.

4.2.5. *Weak fusion rings of rank* 2. Here is a generalization of the results of Subsection 4.2.3 to general weak fusion rings of rank 2, proposed by V. Ostrik (based on an argument by Josiah Thornton).

For a positive integer a and a nonnegative integer b define the weak fusion ring $S_{a,b}$ with basis $\mathbf{1}, X$ and relations

$$X^2 = a\mathbf{1} + bX,\ X^* = X.$$

Theorem 4.10. *The weak fusion ring $S_{a,b}$ is categorifiable over a suitable field of characteristic zero if and only if either $a = b = 1$ or there is a prime p and integers $m \geq 0, n \geq 1$ such that $a = p^{2m}(p^n - 1)$ and $b = p^m(p^n - 2)$.*

Note that in the case $b = 0$ (i.e., $p = 2$, $n = 1$) Theorem 4.10 reduces to the result of Subsection 4.2.1 (in characteristic 0), and in the case $a = b+1$ (i.e., $m = 0$) Theorem 4.10 reduces to the result of Subsection 4.2.3.

Proof. Let $\overline{\mathcal{C}}$ be a categorification of $S_{a,b}$ over a field K of characteristic zero. Passing to the algebraic closure, we get $X = (\bigoplus_{i\in O} X_i)^\ell$, where O is a Galois group orbit. Consider two cases.

Case 1. $|O| = 1$. Then $\mathcal{C} := \overline{\mathcal{C}} \otimes_K \overline{K}$ has two simple objects, $\mathbf{1}$ and Y, and $Y \otimes Y = \mathbf{1} \oplus rY$. By a theorem of Ostrik [O], $r = 0$ or $r = 1$. If $r = 0$, and $X = \ell Y$, then $b = 0$ and $a = \ell^2$, so the Theorem follows from Theorem 4.3 (namely, $p = 2$, $n = 1$, and m is arbitrary).

If $r = 1$, then $\mathcal{C}$ is the Yang-Lee category or its Galois conjugate. Let us show that any form $\overline{\mathcal{C}}$ of this category is split. [2] First of all, any field of definition of a Yang-Lee category must contain $\sqrt{5}$, since it occurs in the Müger's squared norm of the nontrivial object Y. Next, it is explained in [O] that the Yang-Lee category is defined as a split category over $\mathbb{Q}(\sqrt{5})$. Finally, this category has no nontrivial tensor auto-equivalences or tensor automorphisms of the identity functor, so by the theory of forms of tensor categories, the split form has no nontrivial twists, as desired.

Case 2. $|O| > 1$. In this case we use the argument due to J. Thornton [Th]. Namely, we claim that $\mathrm{FPdim}(X_i) = 1$. To see this,

[2] Here is another proof of this fact. Suppose we have a non-split form with simple objects $\mathbf{1}, X$ and $\mathrm{End}(X) = D$, a central division algebra of dimension s^2 over a ground field K (where $s > 1$). Then extension of scalars turns X into sY, so the fusion rule for this form is $X^2 = s^2\mathbf{1} + sX$, and $X^* = X$. Thus we have $D^{op} \cong D$, and $D \otimes D$ (which sits inside $\mathrm{End}(X \otimes X)$) injects into $\mathrm{End}(s^2\mathbf{1} \oplus sY) = \mathrm{Mat}_{s^2}(K) \oplus \mathrm{Mat}_s(D)$. But since $D^{op} \cong D$, $D \otimes D \cong \mathrm{Mat}_{s^2}(K)$, and there is no homomorphisms from $\mathrm{Mat}_{s^2}(K)$ to $\mathrm{Mat}_s(D)$ (since the former contains nilpotent elements of nilpotency degree $> s$). This is a contradiction. Thus, $\overline{\mathcal{C}}$ is split and we have $a = b = 1$.

note first that since X_i are permuted by the Galois group, $\mathrm{FPdim}(X_i) = d$ is independent of i. Next, if $i \neq j$ (which is possible since $|O| > 1$) then $X_i \otimes X_j^*$ is a direct sum of X_k, so d is an integer. Finally, $X_i \otimes X_i^*$ is $\mathbf{1}$ plus a sum of X_k, so $d^2 - 1$ is divisible by d, hence $d = 1$.

So $\mathrm{FPdim}(X) = \ell|O|$, and we get

$$(\ell|O|)^2 = a + b\ell|O|.$$

Also, from the relation $XX^* = X^2$ we get $a = \ell^2|O|$, which gives $b = \ell(|O| - 1)$.

Now, consider the group V formed by the objects X_i and the unit object $X_0 = \mathbf{1}$. Since V consists of two Galois orbits, it is a vector space over $\mathbb{F}_p$ for some prime p. Thus, $|O| = p^n - 1$ for some $n \geq 1$.

It remains to determine ℓ. To this end, let Γ be the Galois group of $\overline{K}$ over K (which acts on V), and let Γ' be the stabilizer of some $0 \neq i \in V$. Let $L := \overline{K}^{\Gamma'}$. Then L is a finite extension of K, and $\overline{\mathcal{C}} \otimes_K L$ has simple objects Y_i labeled by $i \in V$ (with $Y_0 = \mathbf{1}$ and $Y_i^* = Y_{-i}$), and one has $Y_i \otimes Y_j = \ell Y_{i+j}$ if $i \neq -j$, $Y_i \otimes Y_{-i} = \ell^2\mathbf{1}$. Let $D_i := \mathrm{End}(Y_i)$. Then D_i has dimension ℓ^2 and it defines an element of order p in the Brauer group $\mathrm{Br}(L)$. So by Brauer's theorem (Theorem 4.4), D_i has dimension p^{2m} for some nonnegative integer m. This implies that $\ell = p^m$ for some $m \geq 0$, and thus a, b are as required.

Conversely, if $a = p^{2m}(p^n - 1)$ and $b = p^m(p^n - 2)$, then the ring $S_{a,b}$ admits a categorification. In showing this, we may (and will) assume that $m > 0$, since the case $m = 0$ is considered in Subsection 4.2.3. Namely, take the category $\mathcal{C} := \mathrm{Vec}_{\mathbb{F}_q}$, where $q = p^n$. Assume that the field K is such that the Galois group $\Gamma = \mathrm{Gal}(\overline{K}/K)$ has a normal subgroup Γ' with $\Gamma/\Gamma' = \mathbb{F}_q^\times$, and let $L \subseteq \overline{K}$ be the fixed field of this subgroup (it is a cyclic Galois extension of K of degree $p^n - 1$). So we can make Γ act on $\mathbb{F}_q$ by multiplications so that Γ' acts trivially. We have a form $\overline{\mathcal{C}}'$ of $\mathcal{C}$ over K defined by this action, which is split over L (namely, the category of representations of the twisted form of the additive group of $\mathbb{F}_q$ corresponding to the action of Γ on $\mathbb{F}_q$); this form categorifies the ring S_k with $k = p^n - 1$. Now, this form can be twisted by an element η of

$$H^2(\Gamma, \mathrm{Hom}(\mathbb{F}_q, \mu_p)) = H^2(\Gamma', \mathrm{Hom}(\mathbb{F}_q, \mu_p))^{\Gamma/\Gamma'} = \mathrm{Hom}(\mathbb{F}_q, \mathrm{Br}_p(L))^{\mathbb{F}_q^\times},$$

where the action of $\mathbb{F}_q^\times$ on $\mathrm{Br}_p(L)$ is through the isomorphism of $\mathbb{F}_q^\times$ with Γ/Γ'.

Now we would like to choose a suitable field K. We will take $L := \mathbb{C}(a_{ijk}, b_{ijk})$, where $i = 1, \dots, m$, $j = 1, \dots, p^n - 1$ and $k = 1, \dots, n$. Then we can make the group $\mathbb{F}_q^\times$ act on L by cyclic permutations of

j, and define K to be the subfield of invariants. Then K, L have the required properties. Define D_{jk} to be the division algebra over L given by the formula

$$D_{jk} := \otimes_{i=1}^{n} D_{ijk},$$

where D_{ijk} is generated by x_{ijk} and y_{ijk} with

$$x_{ijk}^p = a_{ijk},\ y_{ijk}^p = b_{ijk},\ x_{ijk}y_{ijk} = \zeta y_{ijk}x_{ijk},$$

where ζ is a primitive $p-$th root of unity. Let E be the subgroup in $\mathrm{Br}_p(L)$ generated by D_{jk}, $j = 1, \dots, p^n - 1$, $k = 1, \dots, n$. Since D_{jk} are linearly independent vectors in $\mathrm{Br}_p(L)$, the space E is isomorphic to the space of matrices over $\mathbb{Z}/p\mathbb{Z}$, of size n by $p^n - 1$, with $\mathbb{F}_q^\times = \mathbb{Z}/(p^n-1)\mathbb{Z}$ acting by cyclic permutations of columns. Thus,

$$\mathrm{Hom}(\mathbb{F}_q, E)^{\mathbb{F}_q^\times} = \mathrm{Hom}(\mathbb{F}_q, (\mathbb{Z}/p\mathbb{Z})^n) \subseteq \mathrm{Hom}(\mathbb{F}_q, \mathrm{Br}_p(L))^{\mathbb{F}_q^\times}.$$

Take a nondegenerate element η from this group (i.e., defining an isomorphism $\mathbb{F}_q \to (\mathbb{Z}/p\mathbb{Z})^n$). Then the twist $\overline{\mathcal{C}}$ of $\overline{\mathcal{C}}'$ by η is a categorification of $S_{a,b}$, as desired. □

Remark 4.11. The assumption of characteristic zero is needed here because Ostrik's classification [O] of fusion categories of rank 2 is unknown in positive characteristic. All the other arguments in this subsection can be extended to positive characteristic.

References

[AH] A.A. Albert and H. Hasse, A determination of all normal division algebras over an algebraic number field, *Trans. Amer. Math. Soc.*, **34** (1932).

[AT] E. Artin and J. Tate, Class field theory, Addison-Wesley, New York, 1968.

[BH] N. Blackburn and B. Huppert, Finite groups III, *Grundlehren der Mathematischen Wissenschaften*, **243**, Berlin-New York, Springer-Verlag, 1982.

[BHN] R. Brauer, H. Hasse and E. Noether, Beweis eines Hauptsatzes in der Theorie der Algebren, *J. Reine Angew. Math.*, **167** (1932) 399–404.

[DGNO] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, *On braided fusion categories I*, *Selecta Mathematica New Series*, **16** (2010), 1–119.

[DM] P. Deligne and J. Milne, Tannakian Categories, *Lecture Notes in Mathematics*, **900** (1982) 101–228.

[E] K. Eisenträger, The theorem of Honda and Tate, http://www.math.psu.edu/eisentra/

[EGO] P. Etingof, S. Gelaki and V. Ostrik, Classification of fusion categories of dimension pq, *International Mathematics Research Notices*, **57** (2004), 3041–3056.

[ENO1] P. Etingof, D. Nikshych, V. Ostrik, On fusion categories, *Ann. of Math.* **162** (2005), 581–642.

[ENO2] P. Etingof, D. Nikshych and V. Ostrik, Fusion categories and homotopy theory. With an appendix by Ehud Meir. *Quantum Topol.* **1** (2010), no. 3, 209-273.

[GN] S. Gelaki and D. Nikshych, Nilpotent fusion categories, *Advances in Mathematics* **217** (2008) 1053–1071.

[GS] Ph. Gille, T. Szamuely, Central Simple Algebras and Galois Cohomology, *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, 2006.

[M] M. Merkurjev, K_2 of fields and the Brauer group. *Proc. Boulder Conference on $K-$theory*, (1983).

[MeS] M. Merkurjev and A. Suslin, $K-$cohomology of Severi-Brauer varieties and norm residue homomorphism, *Izv. Akad. Nauk SSSR* **46**, (1982) 1011–1046.

[MoS] S. Morrison and N. Snyder, Non-cyclotomic fusion categories, arXiv:1002.0168.

[O] V. Ostrik, Fusion categories of rank 2, *Math. Res. Lett.* **10** (2003), 177–183.

[TY] D. Tambara and S. Yamagami, Tensor categories with fusion rules of self-duality for finite abelian groups, *J. Algebra* **209** (1998), no. 2, 692–707.

[Th] J. Thornton, On braided near-group categories, *preprint* (to appear).

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

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

Department of Mathematics, Technion-Israel Institute of Technology, Haifa 32000, Israel

E-mail address: gelaki@math.technion.ac.il