ON PRIME FACTORIZATIONS IN MODULAR CATEGORIES

YILONG WANG

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G, and let $\mathrm{N}_{\mathbb{Q}}^{K}$ be the norm map. In other words, for any $x \in K$, we have

$$\mathrm{N}_{\mathbb{Q}}^{K}(x) = \prod_{\sigma \in G} \sigma(x).$$

Note that $\mathrm{N}_{\mathbb{Q}}^{K}(\mathcal{O}) \subset \mathbb{Z}$. Let $\mathcal{O}$ be the ring of integers in K. For any prime ideal $\mathfrak{p} \subset \mathcal{O}$, and for any prime number $p \in \mathbb{Z}$, we say that $\mathfrak{p}$ *lies above* $p\mathbb{Z}$ if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. If $\mathfrak{p}$ lies above $p\mathbb{Z}$, then $\mathfrak{p} \supset p\mathcal{O}$. We call the largest integer e such that $\mathfrak{p}^e \supset p\mathcal{O}$ the *ramification index* of $\mathfrak{p}$ over $p\mathbb{Z}$. It is clear that if $\mathfrak{p}$ lies above $p\mathbb{Z}$, then $e \geq 1$.

Let $\alpha \in \mathcal{O}$ be a d-number per Ostrik [Ost09]. In particular, for any $\sigma \in G$, we have

$$\sigma(\alpha\mathcal{O}) = \alpha\mathcal{O}.$$

Recall that $\mathcal{O}$ is a Dedekind domain.

Theorem 1. *A prime number $p \in \mathbb{Z}$ divides $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$ if, and only if, all of the prime ideals in $\mathcal{O}$ lying above $p\mathbb{Z}$ are prime factors of $\alpha\mathcal{O}$.*

Proof. Firstly, suppose that p divides $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$. We have $p\mathbb{Z} \supset \mathrm{N}_{\mathbb{Q}}^{K}(\alpha)\mathbb{Z}$. For any $\mathfrak{p} \subset \mathcal{O}$ lying above $p\mathbb{Z}$, let e be the ramification index of $\mathfrak{p}$ over $p\mathcal{O}$, we have

$$p\mathcal{O} = \left(\prod_{\sigma \in G} \sigma(\mathfrak{p})\right)^e$$

as K is a Galois extension of $\mathbb{Q}$ ([Lan94, p. 26, Corollary 2], see Appendix for reference). Therefore, we have

$$\mathfrak{p} \supset \left(\prod_{\sigma \in G} \sigma(\mathfrak{p})\right)^e = p\mathcal{O} \supset \mathrm{N}_{\mathbb{Q}}^{K}(\alpha)\mathcal{O} = \left(\prod_{\sigma \in G} \sigma(\alpha)\right)\mathcal{O} = \left(\prod_{\sigma \in G} \sigma(\alpha\mathcal{O})\right) = \alpha\mathcal{O}.$$

Conversely, assume that all of the prime ideals in $\mathcal{O}$ lying above $p\mathbb{Z}$ are prime factors of $\alpha\mathcal{O}$. Let $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal lying above $p\mathbb{Z}$. By assumption, we have $\mathfrak{p} \supset \alpha\mathcal{O}$. By a similar argument as above, we have

$$p\mathcal{O} = \left(\prod_{\sigma \in G} \sigma(\mathfrak{p})\right)^e \supset \left(\prod_{\sigma \in G} \sigma(\alpha\mathcal{O})\right)^e = \left(\prod_{\sigma \in G} \sigma(\alpha)\right)^e \mathcal{O} = \left(\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)^e\right)\mathcal{O}.$$

Therefore, we have

$$p\mathbb{Z} = p\mathcal{O} \cap \mathbb{Z} \supset \left(\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)^e\right)\mathcal{O} \cap \mathbb{Z} = \left(\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)^e\right)\mathbb{Z}$$

since both p and $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$ are integers. In other words, p divides $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)^e$. Therefore, p divides $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$. □

Let $\mathcal{C}$ be modular category of global dimension $\mathcal{D}^2$. Let $n := \mathrm{FSexp}(\mathcal{C}) = \mathrm{ord}(T)$ be the Frobenius-Schur exponent of $\mathcal{C}$. By definition, $n \in \mathbb{Z}$ is a d-number, and according to [Ost09, Corollary 1.4], $\mathcal{D}^2$ is a d-number. Note that $\mathbb{Q}(\mathcal{D}^2)$ is a Galois extension of $\mathbb{Q}$ as $\mathcal{D}^2$ is contained in the cyclotomic field $\mathbb{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$ (see, for example, [EGNO15, Chapter 8]).

Applying Theorem 1 to the field $K := \mathbb{Q}(\mathcal{D}^2)$ and the corresponding ring of integer $\mathcal{O}$, we have the following theorem.

Theorem 2. *$\mathcal{D}^2\mathcal{O}$ and $n\mathcal{O}$ have the same set of prime ideal factors in $\mathcal{O}$ if, and only if, $\mathrm{N}_{\mathbb{Q}}^{K}(\mathcal{D}^2)$ and n have the same set of prime factors in $\mathbb{Z}$.* □

Acknowledgment. The author thanks Professor Richard Ng for helping the author tailor the proof.

Appendix

For our readers' convenience, we record [Lan94, p. 26, Corollary 2] here. Let A be a Dedekind domain, and let K be its quotient field. Let L be a finite separable extension of K, and let B be the integral closure of A. Let $\mathfrak{P} \subset B$ be a prime ideal lying above a prime ideal $\mathfrak{p} \subset A$. Let $e_{\mathfrak{P}}$ be the corresponding ramification index, and let $f_{\mathfrak{P}}$ be the residue class degree of the finite field extension $[B/\mathfrak{P} : A/\mathfrak{p}]$.

Proposition 1. *Assume that L is Galois over K. Then all the $e_{\mathfrak{P}}$ are equal to the same number e, all the $f_{\mathfrak{P}}$ are equal to the same number f, and if*

$$\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

then

$$efr = [L : K].$$

References

[EGNO15] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik. *Tensor categories*, volume 205 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2015.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Ost09] Victor Ostrik. On formal codegrees of fusion categories. *Math. Res. Lett.*, 16(5):895–901, 2009.