DEEP CONGRUENCES + THE BRAUER-NESBITT THEOREM

SAMUELE ANNI, ALEXANDRU GHITZA, AND ANNA MEDVEDOVSKY

Abstract. We prove that mod-p congruences between polynomials in $\mathbb{Z}_p[X]$ are equivalent to deeper mod-$p^{1+v_p(n)}$ congruences between the n^{th} power-sum functions of their roots. We give two proofs, one combinatorial and one algebraic. This result generalizes to torsion-free $\mathbb{Z}_{(p)}$-algebras modulo divided-power ideals. As a direct consequence, we obtain a refinement of the Brauer-Nesbitt theorem for finite free $\mathbb{Z}_p$-modules with an action of a single linear operator, with applications to the study of Hecke modules of mod-p modular forms.

See also note below on a simpler proof of the result.

1. Introduction

1.1. **The basic module-theoretic question.** Let p be a prime. For a finite free $\mathbb{Z}_p$-module M with an action of a linear operator T, how much information does one need to know about the traces of $\mathbb{Z}_p[T]$ acting on M to know the structure of the semisimplification of $M \otimes \mathbb{F}_p$ as an $\mathbb{F}_p[T]$-module?

Certainly knowing $\mathrm{tr}(T^n|M)$ for enough n as an element of $\mathbb{Z}_p$ is plenty: the Brauer-Nesbitt theorem — or in this one-parameter case, even simply linear independence of characters (see Appendix) — tell us that these traces determine $(M \otimes \mathbb{Q}_p)^{\text{ss}}$, so that they determine the multiset of eigenvalues of T on M in characteristic zero, and hence in characteristic p. But this very precise characteristic-zero information is much more than we need: we merely want to understand M modulo p.

On the other hand, knowing all the $\mathrm{tr}(T^n|M)$ modulo p is not enough to determine $M \otimes \mathbb{F}_p$. Indeed, if M has rank p and T acts on M as multiplication by a scalar α in $\mathbb{Z}_p$ then for every $n \geq 0$ we have $\mathrm{tr}(T^n|M) = p\alpha^n \equiv 0 \bmod p$, and we cannot recover $\alpha \bmod p$ from this trace data.

Since knowing $\mathrm{tr}(T^n|M)$ in $\mathbb{Z}_p$ is too much and knowing $\mathrm{tr}(T^n|M)$ modulo p is not enough, one can ask for some kind of in-between criterion depending on $\mathrm{tr}(T^n|M)$ modulo *powers* of p. This is the purpose of the present text: we precisely describe the exact depth of the p-adic congruence that the $\mathrm{tr}(T^n|M)$ must satisfy in order to pin down $M \otimes \mathbb{F}_p$ up to semisimplification, and nothing more. In particular, we prove the following theorem.

Theorem A (see Theorem 6.1)**.** *Let M and N be two finite free $\mathbb{Z}_p$-modules of the same rank d, each with an action of an operator T. Then $\overline{M}^{\text{ss}} \simeq \overline{N}^{\text{ss}}$ as $\mathbb{F}_p[T]$-modules if and only if for every n with $1 \leq n \leq d$ we have* $\mathrm{tr}(T^n|M) \equiv \mathrm{tr}(T^n|N) \mod pn$.

Here $\overline{M}$ and $\overline{N}$ are the $\mathbb{F}_p[T]$-modules $M \otimes \mathbb{F}_p$ and $N \otimes \mathbb{F}_p$, respectively, and $\overline{M}^{\text{ss}}$ and $\overline{N}^{\text{ss}}$ refers to their semisimplification. We highlight a few observations.

Date: August 23, 2023.

2020 *Mathematics Subject Classification.* 05E05 (primary), 05E40, 05E10, 11F33, 11P83, 11T99, 20C99.

Key words and phrases. mod-p and p-power congruences between symmetric functions, Brauer-Nesbitt theorem, linear independence of characters, divided-power ideals.

The research of Samuele Anni is partially funded by the Melodia ANR-20-CE40-0013 project.

Anna Medvedovsky was partially supported by NSF postdoctoral research fellowship DMS-1703834.

- Since every prime except p is a $\mathbb{Z}_p$-unit, congruence modulo pn is the same as congruence modulo $p^{1+v_p(n)}$, where $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0}$ is the p-adic valuation normalized so that $v_p(p) = 1$.
- Theorem A completely resolves our example with $T = \alpha$ acting on $M = \mathbb{Z}_p^{\oplus p}$: knowing $\mathrm{tr}(T^p|M) = p\alpha^p$ modulo p^2 is tantamount to knowing α^p modulo p, which in turn determines α modulo p uniquely. Yet this information is not enough to pin down α in $\mathbb{Z}_p$.
- The "only if" direction of Theorem A is trivial when all the eigenvalues of M and N are in $\mathbb{Z}_p$. Indeed, $\overline{M}^{\mathrm{ss}} \simeq \overline{N}^{\mathrm{ss}}$ implies that eigenvalues of M and N pair by mod-p congruence. But the $(p^k)^{\mathrm{th}}$ powers of two mod-p-congruent elements of $\mathbb{Z}_p$ are congruent modulo p^{k+1} (see Lemma 3.7); the deeper congruence claim follows. Thus the heart of Theorem A is the "if" direction.
- Theorem A generalizes to p-adic fields that are not too ramified: see Theorem 6.1.

In this text we present *two* proofs of Theorem A. One approach, taken in section 6, is algebraic: isomorphisms between semisimplified $\mathbb{F}_p[T]$-modules are the same as equalities between multiplicities of eigenvalues in $\bar{\mathbb{F}}_p$. We establish successive mod-p^n congruences between these multiplicities by using an enhanced trace version of the Brauer-Nesbitt theorem, equivalent to linear independence of characters in our setting (Appendix). The second proof, combinatorial in nature, follows from the slightly more general Theorem B, described in the next subsection.

NB. After the creation of this document, an anonymous referee suggested a much simpler proof of Theorem A than those we present here; see subsection 3.4. We still believe that our notion of p-equivalence for partitions, and in particular Proposition C (the proof of which given here is due to Ira Gessel), as well as the observation in Proposition 2.1 (which we have not seen in the literature), has something to offer.

1.2. **The combinatorial perspective.** Viewing Theorem A as a combinatorial statement about deep congruences between power-sum symmetric functions implying simple congruences between corresponding elementary symmetric functions permits more generality. Let A be a torsion-free $\mathbb{Z}_{(p)}$-algebra; for the purposes of this introduction only, we also assume that A is a domain. Let $\mathfrak{a} \subset A$ be a *divided-power ideal* — see subsection 2.2 for details and discussion, but in short, we must have $a^p \in p\mathfrak{a}$ for any $a \in \mathfrak{a}$. For a monic polynomial $P \in A[X]$, write $\overline{P}$ for the image of P in $(A/\mathfrak{a})[X]$ and $\mathsf{p}_n(P)$ for the n^{th} power-sum symmetric function of the roots of P — see Notation in subsection 3.2 for more and for the nondomain case. The following combinatorial theorem is a generalization of Theorem A.

Theorem B (see Theorem 2.7)**.** *Let P, Q be monic polynomials in $A[X]$. Then*

$$\overline{P} = \overline{Q} \text{ in } (A/\mathfrak{a})[X] \iff \mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \text{ modulo } n\mathfrak{a} \qquad \text{for } 1 \leq n \leq \max\{\deg P, \deg Q\}.$$

In particular, here we do not require P and Q to be of the same degree; nor do we require $\mathfrak{a}$ to be prime (nor indeed A to be a domain).

The proof of Theorem B uses combinatorial theory of symmetric functions, specifically, formulas that express elementary symmetric functions in terms of power-sum functions and vice versa. Both directions of these formulas are sums indexed by partitions; for the "if" direction, we introduce a new equivalence relation called *p-equivalence* on the space of partitions to break up the sum: see subsection 5.1 for exact definitions — but, for example, partitions $(6,2)$, $(3,3,2)$, $(6,1,1)$, and $(3,3,1,1)$ are all 2-equivalent. The raison d'être result of p-equivalence is the following proposition.

Proposition C (see Proposition 5.4).
Fix a partition λ of an integer n. Write C_λ for the set of partitions of n that are p-equivalent to λ. Then the symmetric function $\mathsf{g}_\lambda := \sum_{\mu \in C_\lambda} \frac{(-1)^\mu}{z_\mu} \mathsf{p}_\mu$ has coefficients in $\mathbb{Z}_{(p)}$.

Here $(-1)^\mu$ is the sign in S_n of any permutation σ with cycle structure μ, and $n!/z_\mu$ is the size of the S_n-conjugacy class of such a σ (subsection 3.1); the symmetric function p_μ is the product of power-sum functions associated to the parts of μ (subsection 3.2). For context, the elementary symmetric function e_n is the sum of the g_λ as λ runs through a set of representatives of the p-equivalence classes (see subsection 5.2 for details).

The elegant proof of Proposition C that we present in subsection 5.3, which relies on the p-integrality of the Artin-Hasse series, is due to Ira Gessel. We hope that the p-equivalence relation may be of independent interest in the study of partitions.

1.3. **A generalization to virtual modules.** The final result that we highlight in this introduction is a corollary of Theorem A, a generalization to virtual modules.

Corollary 1.1. *Let M_1, M_2, N_1, N_2 be free $\mathbb{Z}_p$-modules of finite rank, each with an action of an operator T. Suppose we have fixed T-equivariant embeddings $\iota_1 : \overline{N_1} \hookrightarrow \overline{M_1}$ and $\iota_2 : \overline{N_2} \hookrightarrow \overline{M_2}$ and consider the quotients*

$$W_1 := \overline{M_1}/\iota_1(\overline{N_1}), \qquad W_2 := \overline{M_2}/\iota_2(\overline{N_2}).$$

Then $W_1^{\mathrm{ss}} \simeq W_2^{\mathrm{ss}}$ as $\mathbb{F}_p[T]$-modules if and only if for every $n \geq 0$ we have

$$v_p\big(\operatorname{tr}(T^n|M_1) - \operatorname{tr}(T^n|N_1) - \operatorname{tr}(T^n|M_2) + \operatorname{tr}(T^n|N_2)\big) \geq 1 + v_p(n).$$

The essential point is that we do not assume that there are embeddings $N_i \hookrightarrow M_i$ over $\mathbb{Z}_p$, but only after base change to $\mathbb{F}_p$. Corollary 1.1 is the form of the result that we use in a separate work to study the Hecke modules structure on certain quotients of spaces of mod-p modular forms. This is the motivating application of the present work, which we describe briefly below.

1.4. **Motivating application to modular forms.** For N prime to p and $k \geq 2$, write $M_k(Np, \mathbb{Z}_p)$ for the space of classical modular forms of weight k and level Np, viewed via the q-expansion map as a finite free $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p[\![q]\!]$. Let $M_k(Np, \mathbb{F}_p)$ denote the image of $M_k(Np, \mathbb{Z}_p)$ in $\mathbb{F}_p[\![q]\!]$. For $k \geq 4$, multiplication by the level-p and weight-2 Eisenstein form $E_{2,p}$, normalized to be in $1 + p\mathbb{Z}_p[\![q]\!]$, induces an embedding $M_{k-2}(Np, \mathbb{F}_p) \hookrightarrow M_k(Np, \mathbb{F}_p)$; let

$$W_k(Np) := M_k(Np, \mathbb{F}_p)/M_{k-2}(Np, \mathbb{F}_p)$$

denote the quotient. In our forthcoming paper we use Corollary 1.1 to prove that, for $p \geq 5$,

$$W_k(Np)^{\mathrm{ss}}[1] \simeq W_{k+2}(Np)^{\mathrm{ss}} \tag{1.4.1}$$

as modules for the Hecke algebra generated by the action of Hecke operators T_m for m prime to Np (this is the *anemic* or *shallow* Hecke algebra). With some interpretive work, (1.4.1) may also be deduced from the $\overline{\rho}$-dimension-counting formulas of Bergdall and Pollack, obtained from the Ash-Stevens filtrations of mod-p modular symbol spaces [BP, section 6]. Our forthcoming paper thus recovers the Bergdall-Pollack $\overline{\rho}$-dimension-counting formulas, but we also refine the isomorphism in (1.4.1) for the action of the Atkin-Lehner operator at p, about which purely-characteristic-p Ash-Stevens says nothing. That refinement, finally, is the heart of our forthcoming paper and the main motivation for the present work. Our techniques should be readily adaptable to $p = 2$ and 3.

Leitfaden. Sections 2 to 5 are devoted to the proof of Theorem B. In section 2, we state Theorem 2.7, the most general version of Theorem B, after a detailed discussion of the divided-power property of an ideal. In section 3 we collect and at times slightly extend a number of well-known results about symmetric functions, p-valuations of multinomial coefficients, and the p-integrality of the Artin-Hasse exponential series. We do include complete proofs, both for completeness and because we hope that the motivating application will lure readers less familiar with combinatorics. In sections 4 and 5 we prove the two directions of Theorem 2.7; in particular, section 5 is the heart of our main work here. In section 6, we return to the module-theoretic Theorem A, and give two proofs, one relying on Theorem A and the other completely independent. In the same section we also prove Corollary 1.1.

Acknowledgements. First and foremost we thank Ira Gessel, both for his beautiful proof of Proposition 5.4 and for allowing us to use it here. We are also grateful to Preston Wake, who patiently and generously listened to an error-riddled half-baked early presentation on our motivating application and both pushed and helped us to articulate the precise conditions on the ring A in the present Theorem 2.7. We thank John Bergdall for helpful comments. Finally we are grateful to the the Max-Planck-Institut für Mathematik in Bonn, whose generous hospitality allowed us to begin collaborating in 2018 and nurtured the third-named author during the Summer 2021 pandemic reprieve. Much of the work on this article was completed under soft lockdown conditions; the third-named author thanks her husband and their nanny for countless hours of childcare support.

Contents

2. Statement of the main theorem

2.1. **A bit of symmetric function notation.** For any ring B and monic polynomial $P \in B[X]$ of degree d, let $\mathsf{e}_n(P)$ be the X^{d-n}-coefficient of P scaled by $(-1)^n$. If B is a domain, then P determines d roots $\alpha_1, \ldots, \alpha_d$ in some integral extension of B, and $\mathsf{e}_n(P)$ is the n^{th} elementary symmetric function in the α_i: namely,

$$\mathsf{e}_n(P) = \sum_{1 \le i_1 < i_2 < \cdots < i_n \le d} \alpha_{i_1} \cdots \alpha_{i_n}.$$

Also if B is a domain, write $\mathsf{p}_n(P)$ for the n^{th} power-sum function of the roots of P: that is, $\mathsf{p}_n(P) := \sum_{i=1}^{d} \alpha_i^n$. For a general B, use Newton's identities [Mac, I.2.11′] to express p_n as an integer polynomial in $\mathsf{e}_1, \ldots, \mathsf{e}_d$ to compute $\mathsf{p}_n(P)$, or see subsection 3.2 below.

2.2. **Divided-power ideals in torsion-free $\mathbb{Z}_{(p)}$-algebras.** Fix a torsion-free $\mathbb{Z}_{(p)}$-algebra[(i)] A; in particular, A embeds into $A[\frac{1}{p}] = A \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q}$. We say that an ideal $\mathfrak{a}$ of A *satisfies the divided-power property at* some $k \geq 1$ if $a \in \mathfrak{a}$ implies that $a^k/k!$ is also in $\mathfrak{a}$. Since A is $\mathbb{Z}$-torsion free and a $\mathbb{Z}_{(p)}$-algebra, this last condition may be reformulated: indeed, we have

$$\frac{a^k}{k!} \text{ is in } \mathfrak{a} \iff a^k \text{ is in } k!\mathfrak{a} \iff a^k \text{ is in } p^{v_p(k!)}\mathfrak{a}.$$

An ideal $\mathfrak{a}$ that satisfies the divided power property for all $k \geq 1$ will be called a *divided-power ideal*. This concept plays a key role in the theory of crystalline cohomology, where $\mathfrak{a}$ satisfying the above condition exactly means that the maps $\gamma_k \colon \mathfrak{a} \to A$ given by $\gamma_k(a) = \frac{a^k}{k!}$ define a *divided-power structure* on $\mathfrak{a}$ [BO, §3].

In a torsion-free $\mathbb{Z}_{(p)}$-algebra, satisfying the divided-power property at p only is equivalent to being a divided-power ideal, as the following proposition shows.

Proposition 2.1. *For an ideal $\mathfrak{b}$ in a commutative ring B, the following are equivalent*

(a) *For all $n \in \mathbb{Z}^+$ and all $a \in \mathfrak{b}$, we have $a^n \in p^{v_p(n!)}\mathfrak{b}$.*

(b) *For all $a \in \mathfrak{b}$ we have $a^p \in p\mathfrak{b}$.*

Proof. The implication (a) $\implies$ (b) is immediate given that $v_p(p!) = 1$. Suppose now that (b) is satisfied. First we show that (a) is true for $n = p^k$ by induction on k. The case $k = 0$ is trivial and $k = 1$ is exactly (b). Suppose now (a) is true for $n = p^k$ for some $k \geq 1$. Note that

$$v_p(p^{k+1}!) = p^k + p^{k-1} + \cdots + 1 = p v_p(p^k!) + 1.$$

For any $a \in \mathfrak{b}$, there exists a $b \in \mathfrak{b}$ so that $a^{p^k} = p^{v_p(p^k!)}b$. Therefore

$$a^{p^{k+1}} = (a^{p^k})^p = \left(p^{v_p(p^k!)}b\right)^p = p^{p v_p(p^k!)}b^p.$$

Since $b \in \mathfrak{b}$, by the (b) assumption we have $b^p \in p\mathfrak{b}$. Therefore

$$a^{p^{k+1}} \in p^{p v_p(p^k!)+1}\mathfrak{b} = p^{v_p(p^{k+1}!)}\mathfrak{b},$$

as desired.

Now for general $n \geq 1$, write n in base p as $n = n_k p^k + \cdots + n_1 p + n_0$, with $n_i \in \{0, \ldots, p-1\}$ for $i = 0, \ldots, k$. Fix $a \in \mathfrak{b}$ again. Since we've shown that for every i we have $a^{p^i} \in p^{v_p(p^i!)}\mathfrak{b}$, we have $a^{n_i p^i} \in p^{n_i v_p(p^i!)}\mathfrak{b}$, so that $a^n \in p^{\sum_{i=0}^k n_i v_p(p^i!)}\mathfrak{b}$. The desired statement follows by observing that

$$\sum_{i=0}^{k} n_i v_p(p^i!) = \sum_{i=0}^{k} n_i \frac{p^i - 1}{p - 1} = \frac{n - \sum_{i=0}^k n_i}{p - 1} = v_p(n!),$$

where the last equality follows from a refinement of Legendre's formula on valuations of $n!$ (for a convenient exposition of this refinement, see [Rom]). $\square$

Corollary 2.2. *The ideal $\mathfrak{a} \subset A$ is a divided-power ideal if and only if $a^p \in p\mathfrak{a}$ for every $a \in \mathfrak{a}$.*

In fact, it suffices to check the condition of Corollary 2.2 on generators.

Proposition 2.3. *Let $S \subseteq A$ be a subset. Then the ideal $\mathfrak{a}$ generated by S is a divided-power ideal if and only if $a^p \in p\mathfrak{a}$ for every $a \in S$.*

(i) Recall that $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ is the subring of rationals that can be expressed as $\frac{a}{b}$ where $p \nmid b$.

Proof. It suffices to show that for $a_1, a_2 \in S$, $b_1, b_2 \in A$, if a_1^p and a_2^p are both in $p\mathfrak{a}$, then so is $(b_1a_1 + b_2a_2)^p$. We expand

$$(b_1a_1 + b_2a_2)^p = b_1^p a_1^p + \sum_{k=1}^{p-1} \binom{p}{k} b_1^k a_1^k b_2^{p-k} a_2^{p-k} + b_2^p a_2^p.$$

The first and last terms are in $p\mathfrak{a}$ by assumption on a_1, a_2; the middle terms because $p \mid \binom{p}{k}$. □

Corollary 2.4. *If $\mathfrak{a} \subset A$ is a divided-power ideal, then so is $\mathfrak{a}\mathfrak{b}$ for any ideal $\mathfrak{b} \subseteq A$.*

Proof. For $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ we have $(ab)^p = a^p b^p \in (p\mathfrak{a})b^p \subseteq p(\mathfrak{a}\mathfrak{b})$. Now use Proposition 2.3. □

2.3. **Divided-power ideals in p-adic DVRs.** Write $v_p : \mathbb{Q}_p \to \mathbb{Z}$ for the usual p-adic valuation, normalized so that $v_p(p) = 1$. Let $\mathcal{O}$ be the ring of integers in a finite extension of $\mathbb{Q}_p$, so that v_p extends uniquely to $\mathcal{O}$. Then $\mathcal{O}$ is a torsion-free $\mathbb{Z}_{(p)}$-algebra and a complete DVR, so we will refer to such an $\mathcal{O}$ as a *p-adic DVR*. Any results for p-adic DVRs below also hold for localizations of rings of integers of number fields at prime ideals above p — these are local torsion-free $\mathbb{Z}_{(p)}$-algebras whose completions are p-adic DVRs in the sense above, with completion establishing a one-to-one correspondence of ideals preserving the divided-power property.

Lemma 2.5. *An ideal $\mathfrak{a}$ of a p-adic DVR is a divided-power ideal if and only if $v_p(\mathfrak{a}) \geq \frac{1}{p-1}$.*

Proof. Let $a \in \mathfrak{a}$ be a generator, so that $v_p(a) = v_p(\mathfrak{a})$. By Proposition 2.3, the ideal $\mathfrak{a}$ is a divided-power ideal if and only if $a^p \in p\mathfrak{a}$, which happens in our p-adic DVR setting if and only if

$$pv_p(a) = v_p(a^p) \geq v_p(p\mathfrak{a}) = 1 + v_p(a);$$

in other words, if and only if $v_p(a) \geq \frac{1}{p-1}$. □

Corollary 2.6. *Let $\mathfrak{m}$ be the maximal ideal of a p-adic DVR $\mathcal{O}$. Let e be the ramification degree of $\mathfrak{m}$ over p. Then $\mathfrak{m}$ is a divided-power ideal of $\mathcal{O}$ if and only if $e \leq p - 1$. In particular, (p) is a divided-power ideal of $\mathbb{Z}_p$.*

Proof. Immediate from Lemma 2.5 as $v_p(\mathfrak{m}) = \frac{1}{e}$ in this setting. □

2.4. **Statement of the main theorem.** We are ready to state the fullest version of Theorem B.

Theorem 2.7. *Let A be a torsion-free $\mathbb{Z}_{(p)}$-algebra and $\mathfrak{a}$ a divided-power ideal, and let P, Q be monic polynomials in $A[X]$. Then the following are equivalent:*

(a) $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ *for every $n \geq 1$;*

(b) $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ *for every n with $1 \leq n \leq \max\{\deg P, \deg Q\}$;*

(c) $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \bmod n\mathfrak{a}$ *for every $n \geq 1$;*

(d) $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \bmod n\mathfrak{a}$ *for every n with $1 \leq n \leq \max\{\deg P, \deg Q\}$.*

Remark 2.8. We do not require $\deg P = \deg Q$ here. In fact, since the statement $\deg P = \deg Q$ is the same as the congruence

$$\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \mod n\mathfrak{a} \text{ for } n = 0,$$

we may if we like replace $n \geq 1$ with $n \geq 0$ in (c) and (d) at the price of adding the condition $\deg P = \deg Q$ in (a) and (b). In this case, we may add a fifth equivalent statement to Theorem 2.7:

(e) $\overline{P} = \overline{Q}$ in $(A/\mathfrak{a})[X]$. △

Example 2.9. Let $p = 2$ and $A = \mathbb{Z}_p$; let $P = X^2 + X + 3$ and $Q = X^4 + 3X^3 + 5X^2 + 2X + 6$. From matching up coefficients (or from the fact that $Q = (X^2 + 2X)P - (4X - 6)$), it's clear that $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q)$ modulo 2 for every $n \geq 1$. In the following table, the last two columns illustrate Theorem 2.7: for $n \geq 1$ we have $v_2\big(\mathsf{p}_n(Q) - \mathsf{p}_n(P)\big) \geq 1 + v_2(n)$.

n	$\mathsf{e}_n(P)$	$\mathsf{e}_n(Q)$	$\mathsf{p}_n(P)$	$\mathsf{p}_n(Q)$	$v_2\big(\mathsf{p}_n(Q) - \mathsf{p}_n(P)\big)$	$1 + v_2(n)$
0	1	1	2	4	2	∞
1	-1	-3	-1	-3	1	1
2	3	5	-5	-1	2	2
3	0	-2	8	12	2	1
4	0	6	7	-49	3	3
5	0	0	-31	107	1	1
6	0	0	10	-94	3	2
7	0	0	83	-227	1	1
8	0	0	-113	1231	6	4
9	0	0	-136	-3012	2	1
10	0	0	475	3899	5	2
11	0	0	-67	2263	1	1
12	0	0	-1358	-27646	4	3
13	0	0	1559	81897	1	1
14	0	0	2515	-135381	3	2
15	0	0	-7192	38372	2	1
16	0	0	-353	563871	10	5

△

We now give a skeleton proof of Theorem 2.7. Technical details are postponed to sections 4 and 5.

Proof of Theorem 2.7. We clearly have (c) $\implies$ (d) and (a) $\implies$ (b); moreover since $\mathsf{e}_n(P) = 0$ for $n > \deg P$ we have (b) $\implies$ (a) as well, so that (a) $\iff$ (b).

We show that (a) $\implies$ (c) and (b) $\implies$ (d) by proving the following (see section 4).

Proposition 2.10. *Fix $N \geq 1$.*
If $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q)$ mod $\mathfrak{a}$ for all $1 \leq n \leq N$, then $\mathsf{p}_N(P) \equiv \mathsf{p}_N(Q)$ mod $N\mathfrak{a}$.

We then show that (c) $\implies$ (a) and (d) $\implies$ (b) by proving the following (see section 5).

Proposition 2.11. *Fix $N \geq 1$.*
If $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q)$ mod $n\mathfrak{a}$ for all $1 \leq n \leq N$, then $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q)$ mod $\mathfrak{a}$ for all $1 \leq n \leq N$.

Since we have shown that (a) $\iff$ (c) $\implies$ (d) $\iff$ (b) $\iff$ (a), we have a cycle and in particular deduce the equivalence of (c) and (d). □

The divided-power property of the ideal $\mathfrak{a}$ is crucial to both directions of Theorem 2.7. We illustrate this point by giving two counterexamples in the absence of this property. In both Example 2.12 and Example 2.13 below, let $\mathcal{O}$ be the valuation ring of the field $\mathbb{Q}_p(\alpha)$ where $\alpha = p^{\frac{1}{p}}$. Then the maximal ideal $\mathfrak{m}$ of $\mathcal{O}$ is not a divided-power ideal (Corollary 2.6), having ramification degree p. In both cases, P and Q have the same degree p, so statements (a) and (b) of Theorem 2.7 are equivalent to the equality $\overline{P} = \overline{Q}$ in $\mathbb{F}_p[X]$.

Example 2.12. Consider $P = X^p - \alpha X^{p-1}$ and $Q = X^p$. Then P and Q, and hence their roots and their elementary symmetric functions are congruent modulo $\mathfrak{m}$. But $\mathsf{p}_p(P) = \alpha^p = p$ has p-valuation 1, and is not congruent to $\mathsf{p}_p(Q) = 0$ modulo $p\mathfrak{m}$, which has valuation $1 + \frac{1}{p}$. Thus statements (a) and (b) of Theorem 2.7 hold but (c) and (d) do not. △

Example 2.13. Consider $P = \big(X - (\alpha + p - 1)\big)\big(X + 1\big)^{p-1}$ and $Q = X^p$. Then P and Q are *not* congruent modulo $\mathfrak{m}$: indeed, the roots of P are units in $\mathcal{O}$ whereas Q has only zero as a root with multiplicity. But we show that $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) = 0 \mod n\mathfrak{m}$ for $1 \leq n \leq p$. Indeed, for any $n \geq 1$,

$$\begin{aligned} \mathsf{p}_n(P) &= \big(\alpha + (p-1)\big)^n + (p-1)(-1)^n \\ &= \alpha^n + \sum_{i=1}^{n-1} \binom{n}{i} \alpha^i (p-1)^{n-i} + (p-1)^n + (p-1)(-1)^n \\ &= (\text{terms divisible by } \alpha) + (p-1)^n + (p-1)(-1)^n. \end{aligned} \tag{2.4.1}$$

Since $(p-1)^n + (p-1)(-1)^n \equiv (-1)^n - (-1)^n = 0$ modulo $p = \alpha^p$, we have $\mathsf{p}_n(P) \equiv 0$ modulo $\mathfrak{m}$.

If further $n = p$, then the summation term in (2.4.1) is divisible by $p\alpha = \alpha^{p+1}$, and the rest of the terms are $\alpha^p + (p-1)^p + (p-1)(-1)^p$. If p is odd, then

$$\alpha^p + (p-1)^p + (p-1)(-1)^p = p + (p-1)^p - (p-1) = (p-1)^p - (-1) \equiv 0 \mod p^2,$$

where the last congruence holds because $p - 1 \equiv -1 \mod p$, so that their p^{th} powers are congruent modulo p^2 (see also Lemma 3.7 below). And if $p = 2$ then

$$p + (p-1)^p + (p-1)(-1)^p = 2 + (-1)^2 + (1)(-1)^2 = 4.$$

In either case, $\mathsf{p}_p(P)$ is a sum of a term in $\mathfrak{m}^{p+1}$ and a term in $\mathfrak{m}^{2p}$, so $\mathsf{p}_p(P) \in p\mathfrak{m}$, as required. Thus statement (d) of Theorem 2.7 holds but (a) and (b) do not. One can show analogously that (c) also does not hold, as $v_p\big(\mathsf{p}_{2p}(P)\big) = 1$. △

Questions. • Is there a direct proof of (d) $\implies$ (c) in Theorem 2.7? The divided-power property or a similar assumption must play a role, as Example 2.13 above satisfies (d) but not (c).

• Although in Theorem 2.7 statement (d) does not imply (a) or (b) without the divided-power assumption (again, see Example 2.13 above), is it possible that (c) does? △

The next three sections are devoted to the proof of Theorem 2.7.

3. Combinatorial preliminaries

3.1. **Partitions.** A *partition* λ of an integer $n \geq 0$, denoted $\lambda \vdash n$, is a (finite or infinite) ordered tuple $(\lambda_1, \lambda_2, \ldots)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ and $\sum_{i \geq 1} \lambda_i = n$. If the partition is infinite, only finitely many of the *parts* λ_i are nonzero. The number of nonzero parts of λ is exactly the cardinality of $\{i \geq 1 : \lambda_i > 0\}$. There is a unique partition of 0, namely $\varnothing \vdash 0$, the *empty* partition. The following four definitions are standard.

- The *weight* $|\lambda|$ of a partition $\lambda = (\lambda_1, \lambda_2, \ldots)$ is the number being partitioned: $|\lambda| := \sum_{i \geq 1} \lambda_i$.
- For $a \geq 1$, let $r_a(\lambda)$ be the number of times that a appears as a part in λ.
- For $\lambda \vdash n$, let $(-1)^\lambda$ be the sign of a permutation in S_n with cycle structure λ. In other words, if $\lambda = (\lambda_1, \ldots, \lambda_k)$ with $\lambda_k > 0$, then $(-1)^\lambda = (-1)^{\sum_i (\lambda_i - 1)}$.

- For $\lambda \vdash n$, let $z_\lambda := \prod_{a\geq 1} a^{r_a(\lambda)} r_a(\lambda)!$ be the order of the centralizer in S_n of any permutation of cycle structure λ, so that $n!/z_\lambda$ is the number of permutations of n with cycle structure λ. Accordingly, $z_\varnothing = 1$.

For $n \geq 0$, let $\mathcal{P}_n$ be the set of partitions of n, and let $\mathcal{P} := \bigcup_{n\geq 0} \mathcal{P}_n$ be the set of all partitions, graded by weight. We can multiply two partitions as follows: for $\lambda \vdash n$ and $\mu \vdash m$, let $\lambda\mu$ be the partition of $m+n$ whose parts are the union of the parts of λ and μ. This operation gives $\mathcal{P}$ the structure of a free abelian monoid on the set $\{(n) : n \in \mathbb{N}\}$ of partitions consisting of a single part. In particular, for any partition $\lambda \vdash n$ and any $k \geq 0$, we may consider the partition $\lambda^k \vdash kn$.

Definition. Let p be a prime and $\lambda := (\lambda_1, \lambda_2, \ldots)$ a partition of $n \geq 0$. Define the *p-valuation of* λ by $v_p(\lambda) := \min_i\{v_p(\lambda_i)\}$. Note that $v_p(\lambda)$ is the greatest integer with the property that we can express λ as a $(p^v)^{\text{th}}$ power: $\lambda = \mu^{p^v}$, where $\mu = (\lambda_1/p^v, \lambda_2/p^v, \ldots)$. Of course $v_p(\varnothing) = \infty$. △

3.2. **Ring of symmetric functions.** Let Λ_d be the ring of symmetric polynomials in d variables $x_1, x_2, \ldots, x_d$ with integer coefficients: that is, Λ_d consists of the S_d-invariants of $\mathbb{Z}[x_1, \ldots, x_d]$, where the symmetric group S_d acts by permuting the variables. Then Λ_d is a ring graded by degree: $\Lambda_d = \bigoplus_{n\geq 0} \Lambda_d^n$, where $\Lambda_d^n \subseteq \Lambda_d$ are the homogeneous symmetric polynomials in $x_1, \ldots, x_d$ of degree n. For any $d \geq d'$ we have a graded map $\Lambda_d \twoheadrightarrow \Lambda_{d'}$ mapping x_i to x_i for $i \leq d'$ and sending x_i with $i > d'$ to zero. This forms a compatible system of graded rings, and we take the so-called graded inverse limit to form the ring of symmetric functions: that is, $\Lambda^n := \varprojlim_d \Lambda_d^n$ and $\Lambda := \bigoplus_{n\geq 0} \Lambda^n$. This somewhat fussy construction guarantees that every symmetric function in Λ has finite degree. For any ring A, let $\Lambda_A := \Lambda \otimes_{\mathbb{Z}} A$.

We now recall the definitions of some special symmetric functions and some general constructions.

- **Elementary symmetric functions:** For $n \geq 0$, let $\mathsf{e}_{n,d} \in \Lambda_d^n$ be the n^{th} *elementary symmetric polynomial*:

$$\mathsf{e}_{n,d} = \sum_{1\leq i_1 < i_2 < \cdots i_n \leq d} x_{i_1} \cdots x_{i_n},$$

  and let $\mathsf{e}_n := \varprojlim_d \mathsf{e}_{n,d} \in \Lambda^n$ be the n^{th} elementary symmetric function. In particular $\mathsf{e}_0 = \mathsf{e}_{0,d} = 1$. One can check — for example, see [Mac, I.2.4] — that

$$\Lambda = \mathbb{Z}[\mathsf{e}_1, \mathsf{e}_2, \ldots]. \tag{3.2.1}$$

- **Power-sum symmetric functions:** Similarly, for $n \geq 0$, let $\mathsf{p}_{n,d} := \sum_{i=1}^d x_i^n \in \Lambda_d^n$ be the n^{th} *power-sum polynomial*. For $n \geq 1$ we also let $\mathsf{p}_n := \varprojlim_d \mathsf{p}_{n,d} \in \Lambda^n$ be the n^{th} *power-sum function*. Note that $\mathsf{p}_{0,d} = d$, so that these do not interpolate and p_0 is not defined as an element of $\Lambda^0 = \mathbb{Z}$. One can check that $\Lambda_{\mathbb{Q}} = \mathbb{Q}[\mathsf{p}_1, \mathsf{p}_2, \ldots]$; see, for example, [Mac, I.2.12].
- **Symmetric function depending on partition:** We use the following standard notation: given a family of symmetric function $\{f_n\}_{n\geq 1}$ — for example, elementary or power-sum symmetric functions — and a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, let $f_\lambda := f_{\lambda_1} f_{\lambda_2} \cdots f_{\lambda_k}$. In other words, we view f as a map $(n) \mapsto f_n$ and extend it to a map of multiplicative monoids $\mathcal{P} \to \Lambda$. Note that $f_\varnothing = 1$. In particular, although p_0 is undefined, we do have $\mathsf{p}_\varnothing = \mathsf{e}_\varnothing = \mathsf{e}_0 = 1$. We can also use the notation f_λ for any tuple λ, not necessarily a partition. One can check that $\{e_\lambda\}_{\lambda \vdash n}$ is a $\mathbb{Z}$-basis for Λ^n and $\{\mathsf{p}_\lambda\}_{\lambda\vdash n}$ is a $\mathbb{Q}$-basis for $\Lambda_{\mathbb{Q}}^n$.

Building on these, we introduce notation for a symmetric function evaluated at a polynomial.

Notation. For a polynomial $Q = X^d + a_1 X^{d-1} + \cdots + a_d \in A[X]$ and $n \geq 0$, denote by

$$\mathsf{e}_n(Q) := \begin{cases} 1 & \text{if } n = 0 \\ (-1)^n a_n & \text{if } 1 \leq n \leq d \\ 0 & \text{if } n > d. \end{cases}$$

More generally, for any symmetric function f and any monic polynomial $Q \in A[X]$, let $f(Q) \in A$ be defined as follows: first use (3.2.1) to write f as a polynomial in the e_n and let $f(Q)$ be the result of plugging $\mathsf{e}_n(Q)$ for e_n into that polynomial. If A is a domain, this is equivalent to plugging in to f the roots of Q with multiplicity for the first $\deg Q$-many xs, and zeros for the rest. We extend this definition to p_0, which is not a priori a symmetric function, by letting $\mathsf{p}_0(Q) := \deg Q$. With this definition, the sequence $\{\mathsf{p}_n(Q)\}_{n \geq 0}$ satisfies an A-linear recurrence of order $\deg Q$, closely related to Newton's identities (see, for example, [Mac, I.2.11′]). △

3.3. **Combinatorial lemmas.** Here we collect standard facts relating generating functions of various symmetric functions: see, for example, [Mac, I.2]. For a set of positive integers $S \subseteq \mathbb{N}$, let

$$\mathsf{P}_S(t) := \sum_{s \in S} (-1)^{s-1} \frac{\mathsf{p}_s}{s} t^s \tag{3.3.1}$$

be the weighted and signed power-sum generating function. Also set $\mathsf{P}(t) := \mathsf{P}_{\mathbb{N}}(t)$. On one hand, we can interpret the exponential of $\mathsf{P}_S(t)$ as a weighted sum of power-sum functions for partitions with parts restricted to S. The following proposition is standard for $S = \mathbb{N}$; this formulation we learned from Gessel.

Proposition 3.1. *Let $S \subseteq \mathbb{N}$ be a set of positive integers. Then* $\exp \mathsf{P}_S(t) = \sum_{n=0}^{\infty} \sum_{\substack{\lambda \vdash n \\ \text{parts in } S}} (-1)^{\lambda} \frac{\mathsf{p}_\lambda}{z_\lambda} t^n.$

Proof.

$$\begin{aligned} \exp \mathsf{P}_S(t) &= \exp\left(\sum_{s \in S} (-1)^{s-1} \frac{\mathsf{p}_s}{s} t^s\right) = \prod_{s \in S} \exp\left((-1)^{s-1} \frac{\mathsf{p}_s}{s} t^s\right) \\ &= \prod_{s \in S} \sum_{r_s = 0}^{\infty} \frac{1}{r_s!} (-1)^{r_s(s-1)} \frac{\mathsf{p}_s^{r_s}}{s^{r_s}} t^{s r_s} = \sum_{(r_s) \in \mathbb{N}^S} (-1)^{\sum_s r_s(s-1)} \frac{\prod_s \mathsf{p}_s^{r_s}}{\prod_s r_s! s^{r_s}} t^{\sum_s s r_s} \\ &= \sum_{\lambda \text{ has parts in } S} (-1)^{\lambda} \frac{\mathsf{p}_\lambda}{z_\lambda} t^{|\lambda|}. \end{aligned}$$

Here the sum in the penultimate line is over tuples of nonnegative integers r_s indexed by elements of S only finitely many of which are nonzero, and in the last line such a tuple is interpreted as a partition λ all of whose parts are in S, with part s appearing r_s times. □

On the other hand, for $S = \mathbb{N}$ we can reinterpret $\exp \mathsf{P}_S(t)$ as the generating function for the elementary symmetric functions. Let

$$\mathsf{E}(t) := \sum_{k \geq 0} \mathsf{e}_k t^k = \prod_{i=1}^{\infty} (1 + x_i t).$$

The remaining statements of this section are completely standard.

Proposition 3.2. $\mathsf{E}(t) = \exp \mathsf{P}(t)$.

Proof. We show that $\log \mathsf{E}(t) = \mathsf{P}(t)$:

$$\log \mathsf{E}(t) := \log \prod_{i=1}^{\infty}(1+x_it) = \sum_{i=1}^{\infty} \log(1+x_it) = \sum_{i=1}^{\infty}\sum_{n=1}^{\infty}(-1)^{n-1}\frac{(x_it)^n}{n}$$
$$= \sum_{n=1}^{\infty}(-1)^{n-1}\frac{t^n}{n}\sum_{i=1}^{\infty}x_i^n = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{\mathsf{p}_n}{n}t^n = \mathsf{P}(t). \qquad \square$$

Proposition 3.2 allows us to express e_n as a $\mathbb{Q}$-linear combination of the p_λ for $\lambda \vdash n$, and, conversely, p_n as a $\mathbb{Z}$-linear combination of e_λ over $\lambda \vdash n$: see Corollary 3.3 and Corollary 3.4.

Corollary 3.3 (Expressing e_n in terms of p_λ)**.** *For all $n \geq 0$, we have*

$$\mathsf{e}_n = \sum_{\lambda \vdash n}(-1)^{\lambda}\frac{\mathsf{p}_\lambda}{z_\lambda}. \tag{3.3.2}$$

For example, $\mathsf{e}_2 = \frac{\mathsf{p}_1^2-\mathsf{p}_2}{2}$ and $\mathsf{e}_3 = \frac{\mathsf{p}_1^3-3\mathsf{p}_1\mathsf{p}_2+2\mathsf{p}_3}{6}$.

Proof. Combining Proposition 3.2 with Proposition 3.1 for $S = \mathbb{N}$ yields $\sum_{\lambda}(-1)^{\lambda}\frac{\mathsf{p}_\lambda}{z_\lambda}t^{|\lambda|} = \sum_{n=0}^{\infty}\mathsf{e}_nt^n$. The statement follows from considering the coefficients of t^n on each side. $\square$

Corollary 3.4 (Expressing p_n in terms of e_λ)**.** *For $n \geq 1$, we have*

$$\mathsf{p}_n = (-1)^n\, n\sum_{\lambda \vdash n}\frac{(-1)^m}{m}\binom{m}{r_1(\lambda), r_2(\lambda), \dots}\mathsf{e}_\lambda, \tag{3.3.3}$$

where $m := r_1(\lambda) + r_2(\lambda) + \dots$ is the number of nonzero parts of the partition λ.

Proof. From Proposition 3.2 we have

$$\sum_{n=0}^{\infty}(-1)^{n-1}\frac{\mathsf{p}_n}{n}t^n = \mathsf{P}(t) = \log \mathsf{E}(t) = \log\left(1+\sum_{k=1}^{\infty}\mathsf{e}_kt^k\right) = \sum_{m=1}^{\infty}\frac{(-1)^{m-1}}{m}\left(\sum_{k=1}^{\infty}\mathsf{e}_kt^k\right)^m$$
$$= \sum_{m=1}^{\infty}\frac{(-1)^{m-1}}{m}\sum_{1\leq k_1,\dots,k_m}\mathsf{e}_{k_1}\cdots\mathsf{e}_{k_m}t^{k_1+\dots+k_m},$$

where the last sum is over m-tuples $(k_1, \dots, k_m)$ of positive integers. We can interpret such a tuple as a (badly ordered) partition λ of $\sum k_i$ into m parts, with $r_a(\lambda)$ of the k_is equal to a and $m = \sum_a r_a(\lambda)$. Moreover, each such partition λ will arise from exactly $\binom{m}{r_1(\lambda), r_2(\lambda), \dots}$ such m-tuples. Equating coefficients of t^n on each side, we obtain, as desired,

$$\mathsf{p}_n = (-1)^{n-1}\, n\sum_{m\geq 1}\sum_{\substack{\lambda\vdash n \\ \text{with } m \text{ parts}}}\frac{(-1)^{m-1}}{m}\binom{m}{r_1(\lambda), r_2(\lambda), \dots}\mathsf{e}_\lambda. \qquad \square$$

3.4. **A simple proof of Theorem A.** The anonymous referee of an earlier version of this paper suggested a simpler proof of Theorem A, which builds on the above discussion of the generating functions P and E.

Let M, N be free $\mathbb{Z}_p$-modules of rank d, each endowed with an action of an operator T. Writing $\mathsf{p}_n(M)$ and $\mathsf{e}_n(M)$ for the n^{th} power-sum and elementary symmetric function of the eigenvalues of T on M, with the corresponding generating functions

$$\mathsf{P}(M,t) := \sum_{n\geq 1}(-1)^{n-1}\frac{\mathsf{p}_n(M)}{n}t^n \in \mathbb{Q}_p[\![t]\!] \quad \text{and} \quad \mathsf{E}(M,t) := \sum_{n\geq 0}\mathsf{e}_n(M)t^n \in \mathbb{Z}_p[t],$$

we note that we still have $\mathsf{P}(M,t) = \log \mathsf{E}(M,t)$ as in Proposition 3.2, so that we may proceed as follows:

$$\begin{aligned}
\overline{M}^{\text{ss}} \simeq \overline{N}^{\text{ss}} &\iff \text{for all } 1 \leq n \leq d \text{ we have } \mathsf{e}_n(M) \equiv \mathsf{e}_n(N) \mod p \\
&\iff \mathsf{E}(M,t) \equiv \mathsf{E}(N,t) \mod p\mathbb{Z}_p[t] \\
&\iff \mathsf{E}(M,t) = \mathsf{E}(N,t)S(t) \text{ for some } S(t) \in 1 + tp\mathbb{Z}_p[\![t]\!] \\
&\iff \log \mathsf{E}(M,t) = \log E(N,t) + \log S(t) \\
&\iff \mathsf{P}(M,t) = \mathsf{P}(N,t) + R(t) \text{ for some } R(t) \in tp\mathbb{Z}_p[\![t]\!] \\
&\iff \text{for all } n \geq 1 \text{ we have } \mathsf{p}_n(M) \equiv \mathsf{p}_n(N) \mod np \\
&\iff \text{for all } n \geq 1 \text{ we have } \operatorname{tr}(T^n|M) \equiv \operatorname{tr}(T^n|N) \mod np.
\end{aligned}$$

Note that we used the fact that log maps $1 + tp\mathbb{Z}_p[\![t]\!]$ onto $tp\mathbb{Z}_p[\![t]\!]$.

The argument generalizes to the setting of Theorem B, with $\mathbb{Z}_p$ and p, respectively, replaced by torsion-free $\mathbb{Z}_{(p)}$-algebra A and a divided-power ideal $\mathfrak{a}$ (see subsection 2.2 for definitions), and the assumption $\operatorname{rank} M = \operatorname{rank} N$ relaxed.

3.5. **p-valuation lemmas.** Here we collect a few lemmas about p-valuations. First, in light of the expression in Corollary 3.4 and our end goal, we need a formula for the p-valuation of multinomial coefficients. Let $r_1, \ldots, r_k$ be nonnegative integers, write $m = r_1 + \cdots r_k$, and let p be any prime. The following statement is due to Kummer for $k = 2$; see, for example [Rom]. The generalization to any k is immediate through the formula

$$\binom{r_1 + \cdots + r_k}{r_1, \ldots, r_k} = \binom{r_1 + \cdots + r_k}{r_1}\binom{r_2 + \cdots + r_k}{r_2}\cdots\binom{r_{k-1} + r_k}{r_{k-1}}$$

expressing multinomial coefficients in terms of binomial coefficients.

Theorem 3.5 (Kummer, 1852)**.** *The p-valuation of the multinomial coefficient $\binom{m}{r_1,\ldots,r_k}$ is the sum of the carry digits when the addition $r_1 + \cdots + r_k$ is performed in base p.*

Corollary 3.6. *For any i, we have $v_p(r_i) \geq v_p(m) - v_p\left(\binom{m}{r_1, \ldots r_k}\right)$.*

Proof. Any end zero of m base p not corresponding to an end zero of r_i base p contributes to a carry digit of the base-p computation $r_1 + \cdots + r_k = m$. Therefore, $v_p\left(\binom{m}{r_1,\ldots r_k}\right) \geq v_p(m) - v_p(r_i)$. ☐

The second statement we need (Corollary 3.8 below) is a partition version of the standard observation that the depth of the p-adic congruence of two integers increases upon taking p^{th} powers.

Recall that A is a torsion-free $\mathbb{Z}_{(p)}$-algebra and $\mathfrak{a} \subset A$ is an ideal with a divided power structure.

Lemma 3.7. *Suppose $x \equiv y \bmod \mathfrak{a}$ for some $x, y \in A$. Then*

(a) for all $m \geq 0$ we have $x^{p^m} \equiv y^{p^m} \bmod p^m\mathfrak{a}$; more generally

(b) for all $n \geq 0$ we have $x^n \equiv y^n \bmod n\mathfrak{a}$.

Proof. Since A is a $\mathbb{Z}_{(p)}$-algebra, the ideal $n\mathfrak{a}$ is the same as the ideal $p^{v_p(n)}\mathfrak{a}$. Thus it suffices to prove the first statement. For $m = 1$, write $y = x + a$ with $a \in \mathfrak{a}$. Then

$$y^p - x^p = (x+a)^p - x^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-i} a^i.$$

We show that each of the terms on the right-hand side is in $p\mathfrak{a}$. This is clear for each term in the summation because for $0 < i < p$ we have both $p \mid \binom{p}{i}$ and $a^i \in \mathfrak{a}$. Corollary 2.2 tells us that $a^p \in p\mathfrak{a}$. To prove the statement for $m > 1$ we proceed by induction using Corollary 2.4. ☐

Corollary 3.8. *Let $P, Q \in A[X]$ be two polynomials, and let $\{f_n\}_{n\geq 1}$ be a family of symmetric functions. If $f_n(P) \equiv f_n(Q)$ modulo $\mathfrak{a}$ for all n, then for every partition λ*

$$f_\lambda(P) \equiv f_\lambda(Q) \pmod{p^{v_p(\lambda)}\mathfrak{a}}.$$

Proof. Let $v = v_p(\lambda)$. By the definition of p-valuation of a partition (subsection 3.1) there exists a partition μ so that $\lambda = \mu^{p^v}$. Therefore

$$f_\lambda(P) = f_{\mu^{p^v}}(P) = f_\mu(P)^{p^v} \equiv_{p^v\mathfrak{a}} f_\mu(Q)^{p^v} = f_{\mu^{p^v}}(Q) = f_\lambda(Q),$$

where the middle congruence modulo $p^v\mathfrak{a}$ holds by Lemma 3.7. ☐

3.6. **Artin-Hasse exponential series.** We briefly recall the Artin-Hasse exponential series

$$F(z) = \exp\left(\sum_{j=0}^{\infty} \frac{z^{p^j}}{p^j}\right) = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots + \frac{z^{p-1}}{(p-1)!} + \frac{\left(\frac{(p-1)!+1}{p}\right) z^p}{(p-1)!} + \cdots, \tag{3.6.1}$$

here viewed merely as a formal power series, a priori in $\mathbb{Q}[\![z]\!]$. In subsection 5.3 we will make use of the fact that $F(z)$ is actually p-integral (Corollary 3.11); here we briefly review this well-known result. We follow the convenient expository notes [Lur] of Jacob Lurie.

Proposition 3.9. *We have $F(z) = \prod_{p \nmid d} \left(1 - z^d\right)^{-\frac{\mu(d)}{d}}$.*

Here μ is the Möbius function, the multiplicative arithmetic function taking squarefree products of primes $p_1 \dots p_k$ to $(-1)^k$ and other positive integers to 0, and satisfying the property

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{3.6.2}$$

Before giving the proof of Proposition 3.9, we need a lemma:

Lemma 3.10. *For prime p we have* $\displaystyle\sum_{d \mid n,\, p \nmid d} \mu(d) = \begin{cases} 1 & \textit{if } n \textit{ is a power of } p \\ 0 & \textit{otherwise.} \end{cases}$

Proof. Quite generally if $f(n)$ is a multiplicative arithmetic function, then the function

$$\phi(n) := \sum_{d|n,\, p\nmid d} f(n)$$

is also multiplicative. Indeed, say a divisor d of n is *p-deprived* if $p \nmid n$. Then assuming $\gcd(m,n) = 1$, each p-deprived divisor of mn is uniquely a product of a p-deprived divisor of m and a p-deprived divisor of n, which are, in turn, relatively prime to each other. The multiplicativity of f then allows the factorization $\phi(mn) = \phi(m)\phi(n)$.

Now for the claim. Since μ is multiplicative, it suffices to check the claim for n a power of p and n relatively to p. In the former case the claim is immediate; in the latter it follows from (3.6.2). $\square$

Proof of Proposition 3.9. We have

$$\begin{aligned}
\log \prod_{p\nmid d} \left(1 - z^d\right)^{-\frac{\mu(d)}{d}} &= \sum_{p\nmid d} \frac{\mu(d)}{d} \log \frac{1}{1-z^d} &&= \sum_{p\nmid d} \frac{\mu(d)}{d} \sum_{k\geq 1} \frac{z^{dk}}{k} \\
&= \sum_{n\geq 1} \frac{z^n}{n} \sum_{d|n,\, p\nmid d} \mu(d) &&= \sum_{n=p^j,\, j\geq 0} \frac{z^n}{n},
\end{aligned}$$

where the last equality follows from Lemma 3.10. The claim follows. $\square$

Corollary 3.11. *The Artin-Hasse exponential series $F(z)$ is in $\mathbb{Z}_{(p)}[\![z]\!]$.*

Proof. The coefficients of $(1-z^d)^{\pm 1/d}$ in the expression in Proposition 3.9 are algebraically generated by binomial coefficients $\binom{1/d}{k}$, all in $\mathbb{Z}[\frac{1}{d}]$. Since all the d are prime to p, the claim follows. $\square$

4. Proof of Proposition 2.10: e_n congruent implies p_n deeply congruent

Here we prove Proposition 2.10. The proof uses the combinatorial expression from Corollary 3.4 for p_n in terms of e_λ.

Proof of Proposition 2.10. Let $P, Q \in A[X]$ be monic polynomials, fix $N \geq 1$, and suppose that $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q)$ modulo $\mathfrak{a}$ for all n with $1 \leq n \leq N$. We seek to show that $\mathsf{p}_N(P) - \mathsf{p}_N(Q)$ is in $N\mathfrak{a}$.

From Corollary 3.4 we have

$$\mathsf{p}_N(P) - \mathsf{p}_N(Q) = (-1)^N N \sum_{m\geq 1} \sum_{\substack{\lambda\vdash N \\ \text{with } m \text{ parts}}} \frac{(-1)^m}{m} \binom{m}{r_1(\lambda), r_2(\lambda), \dots} \big(\mathsf{e}_\lambda(P) - \mathsf{e}_\lambda(Q)\big).$$

Corollary 3.8 for $f = \mathsf{e}$ tells us that our assumptions on the e_n imply that $\mathsf{e}_\lambda(P) - \mathsf{e}_\lambda(Q) \in p^{v_p(\lambda)}\mathfrak{a}$ for each relevant λ. Therefore it suffices to show that for every $\lambda \vdash N$ with m parts,

$$v_p(N) - v_p(m) + v_p\left(\binom{m}{r_1(\lambda), r_2(\lambda), \dots}\right) + v_p(\lambda) \geq v_p(N),$$

or, equivalently, canceling $v_p(N)$ and using the definition of $v_p(\lambda)$, that for every i,

$$-v_p(m) + v_p\left(\binom{m}{r_1(\lambda), r_2(\lambda), \dots}\right) + v_p\big(r_i(\lambda)\big) \geq 0.$$

But this is exactly Corollary 3.6. $\square$

Incidentally, although we know from the fact that the e_λ are a $\mathbb{Z}$-basis for Λ in (3.3.3) that $\frac{n}{m}\binom{m}{r_1,r_2,\dots}$ is always integral — here of course $r_1, r_2, \dots$ is a sequence of nonnegative integers almost all zero, $m = \sum r_i$ and $n = \sum i r_i$ — it is not a priori obvious. But this integrality does follow from Corollary 3.6.

5. Proof of Proposition 2.11: p_n deeply congruent implies e_n congruent

Here we give the first, combinatorial, proof of the "if" direction of Theorem 2.7: we show that if the power sums of roots satisfy deep congruences, then elementary symmetric functions of the roots are (simply) congruent.

5.1. ***p*-Equivalent partitions.** We introduce an equivalence relation on the set $\mathcal{P}_n$ of partitions of an integer $n \geq 0$.

Definitions. • If λ and μ are in $\mathcal{P}_n$, we say that μ is a *p-splitting* of λ if λ contains an instance of the part pu for some $u \geq 1$, and μ is obtained from λ by replacing pu with p copies of part u. In other words, for every $u \in \mathbb{N}$, the partition $(u)^p$ is a p-splitting of (pu), and if μ is a p-splitting of λ, then $\mu\nu$ is a p-splitting of $\lambda\nu$.
• Let *p-equivalence*, written $\sim_p$, be the equivalence relation generated by the p-splitting relation. For $\lambda \vdash n$, let $C_\lambda = \{\mu \vdash n : \mu \sim_p \lambda\}$ be the p-equivalence class of λ.
• Call a partition λ of n *p-deprived* if none of its parts are divisible by p. The empty partition $\varnothing$ is a p-deprived partition of 0 for every p. Write $\lambda \vdash^{(p)} n$ for a p-deprived partition λ of n. △

Example 5.1. Let $u \geq 1$ be prime to p and let $r \geq 0$. Then the partition $(u)^r$ is p-deprived and
$$C_{(u)^r} = \left\{\lambda \vdash ur \colon \lambda \text{ has parts in } \{up^j \colon j \geq 0\}\right\}. \qquad \triangle$$

Every p-equivalence class has a unique p-deprived partition representative. We therefore have, for every $n \geq 0$, the following disjoint union:

$$\mathcal{P}_n = \{\lambda \vdash n\} = \bigsqcup_{\lambda \vdash^{(p)} n} C_\lambda. \tag{5.1.1}$$

5.2. **The contribution to e_n from a single p-equivalence class.** Fix $n \geq 0$ and $\lambda \vdash n$. Let

$$\mathsf{g}_\lambda := \sum_{\mu \sim_p \lambda} (-1)^\mu \frac{\mathsf{p}_\mu}{z_\mu}, \tag{5.2.1}$$

so that in particular $\mathsf{g}_\varnothing = 1$. In other words, g_λ is the piece of the expression for e_n from (3.3.2) that comes from all the partitions that are p-equivalent to λ. Because of (5.1.1), for any $n \geq 0$,

$$\mathsf{e}_n = \sum_{\lambda \vdash^{(p)} n} \mathsf{g}_\lambda. \tag{5.2.2}$$

To show that $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ in Proposition 2.11, it will therefore suffice to establish that $\mathsf{g}_\lambda(P) \equiv \mathsf{g}_\lambda(Q) \bmod \mathfrak{a}$ for every $\lambda \vdash^{(p)} n$. But in fact we can break these up further:

Lemma 5.2. *Suppose $\lambda \vdash^{(p)} n$, $\mu \vdash^{(p)} m$ are partitions of $n, m \geq 0$ with no common parts. Then*
$$\mathsf{g}_{\lambda\mu} = \mathsf{g}_\lambda \mathsf{g}_\mu.$$
Thus for $\lambda \vdash^{(p)} n$,
$$\mathsf{g}_\lambda = \prod_{u \geq 1,\ p \nmid u} \mathsf{g}_{(u)^{r_u(\lambda)}}.$$

Proof. Any two partitions λ and μ, disjoint or not, satisfy $\mathsf{p}_{\lambda\mu} = \mathsf{p}_\lambda \mathsf{p}_\mu$ and $(-1)^{\lambda\mu} = (-1)^\lambda(-1)^\mu$. If λ and μ have no parts in common, then $z_{\lambda\mu} = z_\lambda z_\mu$. And finally if both λ and μ additionally have only prime-to-p parts, then every $\nu \sim_p \lambda\mu$ factors uniquely as $\nu = \nu_\lambda \nu_\mu$ with $\nu_\lambda \sim_p \lambda$ and $\nu_\mu \sim_p \mu$. The claim follows by the distributive property. ☐

Therefore rather than showing that $\mathsf{g}_\lambda(P) \equiv_{\mathfrak{a}} \mathsf{g}_\lambda(Q)$ for every $\lambda \vdash^{(p)} n$, it suffices to show that

$$\mathsf{g}_{(u)^r}(P) \equiv_{\mathfrak{a}} \mathsf{g}_{(u)^r}(Q) \tag{5.2.3}$$

for every $ur \leq n$ where $r \geq 0$ and $u \geq 1$ is prime to p. We prove this in subsection 5.4 after establishing a p-integrality result for the symmetric function g_λ.

5.3. **p-integrality of g_λ.** First note that the signs $(-1)^\mu$ in the definition of g_λ are the same for every $\mu \sim_p \lambda$ for odd p. In other words,

Lemma 5.3. *If p is odd, then* $\mathsf{g}_\lambda = (-1)^\lambda \displaystyle\sum_{\mu \sim_p \lambda} \frac{\mathsf{p}_\mu}{z_\mu}$.

Proof. If p is odd, then for any $u \geq 1$ and $j \geq 0$, the parity of (up^j) is the same as the parity of (u) to the p^j power:

$$(-1)^{(up^j)} = (-1)^{up^j - 1} = (-1)^{u-1} = (-1)^{p^j(u-1)} = (-1)^{(u)^{p^j}}.$$

Then extend multiplicatively. ☐

From the definition in (5.2.1) it's clear that g_λ is in $\Lambda_{\mathbb{Q}}$. However, one can show that g_λ is p-integral as a symmetric function.

Proposition 5.4. *For any partition $\lambda \vdash n \geq 0$, we have g_λ in $\Lambda_{\mathbb{Z}_{(p)}}$.*

The following elegant argument is due to Gessel.

Proof. Since every equivalence class C_λ has a unique representative with prime-to-p parts, it suffices to consider g_λ for $\lambda \vdash^{(p)} n$. By Lemma 5.2, it suffices to show that for any u prime to p and any $r \geq 0$, we have $\mathsf{g}_{(u)^r} \in \Lambda_{\mathbb{Z}_{(p)}}$. Equivalently, it suffices to show that for any u prime to p, the generating function

$$G_u(t) := \sum_{r=0}^{\infty} \mathsf{g}_{(u)^r} t^{ur} \tag{5.3.1}$$

for the sequence $\{g_{(u)^r}\}_{r \geq 0}$ is in $\Lambda_{\mathbb{Z}_{(p)}}[\![t]\!]$. Recall that $F(z) = \exp\left(\sum_{j=0}^{\infty} \frac{z^{p^j}}{p^j}\right) \in \mathbb{Z}_{(p)}[\![z]\!]$ is the Artin-Hasse exponential series (Corollary 3.11).

For p odd, let $\varepsilon_u = (-1)^{u-1} \in \{\pm 1\}$ be the sign of (up^j) for $j \geq 0$ (Lemma 5.3). Then

$$\begin{aligned} G_u(t) &= \exp\left(\sum_{j=0}^{\infty} \frac{\varepsilon_u \mathsf{p}_{up^j}}{up^j} t^{up^j}\right) = \exp\left(\frac{\varepsilon_u}{u} \sum_{j=0}^{\infty} t^{up^j} \frac{(x_1^{up^j} + x_2^{up^j} + \cdots)}{p^j}\right) \\ &= F(x_1^u t^u)^{\varepsilon_u/u} F(x_2^u t^u)^{\varepsilon_u/u} \cdots, \end{aligned} \tag{5.3.2}$$

where the first equality is Proposition 3.1 for the set $S = \{up^j : j \geq 0\}$ (see Example 5.1). Since $F(x_i^u t^u)$ has coefficients in $\mathbb{Z}_{(p)}$ and constant coefficient 1, and since binomial coefficients $\binom{\varepsilon_u/u}{m}$ are in $\mathbb{Z}[\frac{1}{u}] \subset \mathbb{Z}_{(p)}$, each $F(x_i^u t^u)^{\varepsilon_u/u}$ is in $\mathbb{Z}_{(p)}[\![x_i, t]\!]$, so that $G_u(t)$ is in $\mathbb{Z}_{(p)}[\![t, x_1, x_2, \ldots]\!]$. We already know it to be in $\Lambda_{\mathbb{Q}}[\![t]\!]$, so we conclude that $G_u(t) \in \Lambda_{\mathbb{Z}_{(p)}}[\![t]\!]$, as desired.

It remains to consider $p = 2$. In this case, the sign of (up^j) is -1 unless $j = 0$, in which case it is 1 as u is odd. Therefore, for $p = 2$,

$$G_u(t) = \exp\left(\frac{2t^u \mathsf{p}_u}{u} - \sum_{j=0}^{\infty} \frac{t^{up^j}}{up^j} \mathsf{p}_{up^j}\right) = \left(\sum_{k=0}^{\infty} \frac{2^k}{u^k k!} \mathsf{p}_u^k\, t^{uk}\right) F(x_1^u t^u)^{-1/u} F(x_2^u t^u)^{-1/u} \cdots . \tag{5.3.3}$$

To conclude that $G_u(t) \in \Lambda_{\mathbb{Z}_{(p)}}[\![t]\!]$ for $p = 2$, we note that

$$v_2(k!) = \left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{k}{2^2} \right\rfloor + \cdots < \sum_{i=1}^{\infty} \frac{k}{2^i} = k = v_2(2^k), \tag{5.3.4}$$

so that the first factor in (5.3.3) is in $\Lambda_{\mathbb{Z}_{(p)}}[\![t]\!]$; the rest of the expression is as in (5.3.2). □

5.4. **Proof of Proposition 2.11.** Recall that we assume that $\mathsf{p}_n(P) - \mathsf{p}_n(Q) \in n\mathfrak{a}$ for all n with $1 \le n \le N$; we aim to show that $\mathsf{e}_n(P) - \mathsf{e}_n(Q) \in \mathfrak{a}$ for n in the same range. We use the results of subsection 5.2 to make some reductions: by (5.2.2), it suffices to show that $\mathsf{g}_\lambda(P) - \mathsf{g}_\lambda(Q) \in \mathfrak{a}$ for $\lambda \vdash^{(p)} n$ if $1 \le n \le N$; by (5.2.3) it suffices to prove that $\mathsf{g}_{(u)^r}(P) - \mathsf{g}_{(u)^r}(Q) \in \mathfrak{a}$ for all u prime to p and all r with $ur \le N$. As in (5.3.1), write

$$G_u(P)(t) := \sum_{r=0}^{\infty} \mathsf{g}_{(u)^r}(P)\, t^{ur} \tag{5.4.1}$$

and the same for Q. By Proposition 5.4 we know that $G_u(P)(t)$ and $G_u(Q)(t)$ are in $A[\![t]\!]$; to prove the current proposition it suffices to show that

$$G_u(P)(t) - G_u(Q)(t) \in \mathfrak{a}[\![t]\!] + (t^{N+1})$$

under the assumption that $\mathsf{p}_{up^j}(P) - \mathsf{p}_{up^j}(Q) = p^j a_j$ for some $a_j \in \mathfrak{a}$ for every j with $up^j \le N$. Let J be the maximum such j. We work modulo t^{N+1}. Assume again for now that p is odd, and again set $\varepsilon_u = (-1)^{u-1}$. Then as in (5.3.2) we have

$$\begin{aligned} G_u(P)(t) - G_u(Q)(t) &= \exp\Big(\sum_{j=0}^{\infty} \varepsilon_u \frac{\mathsf{p}_{up^j}(P)}{up^j}\, t^{up^j}\Big) - G_u(Q)(t) \\ &\equiv \exp\Big(\sum_{j=0}^{J} \varepsilon_u \frac{\mathsf{p}_{up^j}(Q) + p^j a_j}{up^j}\, t^{up^j}\Big) - G_u(Q)(t) \mod t^{N+1}. \end{aligned} \tag{5.4.2}$$

Since the exponential of a sum is the product of corresponding exponentials, we may rewrite (5.4.2):

$$\begin{aligned}
G_u(P)(t) - G_u(Q)(t) &\equiv \exp\Big(\sum_{j=0}^{J} \varepsilon_u \frac{\mathsf{p}_{up^j}(Q)}{up^j}\, t^{up^j}\Big) \exp\Big(\sum_{j=0}^{J} \frac{\varepsilon_u a_j t^{up^j}}{u}\Big) - G_u(Q)(t) \quad \bmod t^{N+1} \\
&\equiv \exp\Big(\sum_{j=0}^{\infty} \varepsilon_u \frac{\mathsf{p}_{up^j}(Q)}{up^j}\, t^{up^j}\Big) \exp\Big(\sum_{j=0}^{J} \frac{\varepsilon_u a_j t^{up^j}}{u}\Big) - G_u(Q)(t) \quad \bmod t^{N+1} \\
&= G_u(Q)(t)\bigg(\exp\Big(\sum_{j=0}^{J} \frac{\varepsilon_u a_j t^{up^j}}{u}\Big) - 1\bigg) \;=\; G_u(Q)(t)\bigg(\prod_{j=0}^{J} \exp\Big(\frac{\varepsilon_u a_j}{u}\, t^{up^j}\Big) - 1\bigg) \\
&= G_u(Q)(t)\bigg(\prod_{j=0}^{J} \Big(1 + \sum_{k=1}^{\infty} \frac{\varepsilon_u^k a_j^k\, t^{kup^j}}{u^k k!}\Big) - 1\bigg). \qquad (5.4.3)
\end{aligned}$$

By assumption, $\mathfrak{a}$ is a divided-power ideal (subsection 2.2), so that $a_j^k/k! \in \mathfrak{a}$ for every $k \geq 1$. Moreover $u^{-k} \in \mathbb{Z}_{(p)}$ since u is prime to p. Therefore, for each j, the expression

$$\sum_{k=1}^{\infty} \frac{\varepsilon_u^k a_j^k\, t^{kup^j}}{u^k k!} \text{ is in } \mathfrak{a}[\![t]\!];$$

and hence the same is true for all of

$$\prod_{j=0}^{J} \Big(1 + \sum_{k=1}^{\infty} \frac{\varepsilon_u^k a_j^k\, t^{kup^j}}{u^k k!}\Big) - 1.$$

Finally, since $G_u(Q)(t) \in A[\![t]\!]$ as already recalled (Proposition 5.4), we know that last expression of (5.4.3), and thus $G_u(P)(t) - G_u(Q)(t)$, is in $\mathfrak{a}[\![t]\!]$ modulo t^{N+1}, as required.

For $p = 2$, use (5.3.3) in place of (5.3.2), so that the analogue of (5.4.3) is

$$G_u(P)(t) - G_u(Q)(t) \equiv G_u(Q)(t)\bigg(\exp\Big(\frac{2t^u a_0}{u}\Big) \exp\Big(\sum_{j=0}^{J} \frac{-a_j t^{up^j}}{u}\Big) - 1\bigg) \quad \bmod t^{N+1}.$$

But the additional term $\exp\big(\frac{2t^u a_0}{u}\big)$ is in $1 + \mathfrak{a}[\![t]\!]$ for the same reason as $\exp\big(\sum_{j=0}^{J} \frac{-a_j t^{up^j}}{u}\big)$. Therefore Proposition 2.11 is proved for all primes p. $\square$

6. The module-theoretic perspective

In the case where A, in addition to being a torsion-free $\mathbb{Z}_{(p)}$-algebra, is a domain and the divided-power ideal $\mathfrak{a}$ is maximal, we can interpret a monic polynomial in $A[T]$ as the characteristic polynomial for the action of a linear operator T on a free A-module and the n^{th} power sum of its roots as the trace of T^n on that module. Theorem 2.7 then becomes a statement about congruences between traces of T^n implying isomorphisms between semisimplified $(A/\mathfrak{a})[T]$-modules.

We focus on the case where $A = \mathcal{O}$ is a p-adic DVR and $\mathfrak{a} = \mathfrak{m}$ is its maximal ideal to state the following representation-theoretic version of Theorem 2.7; Theorem A is a special case.

Theorem 6.1. *Let $\mathcal{O}$ be a p-adic DVR with maximal ideal $\mathfrak{m}$ of ramification degree $e \leq p - 1$ and residue field $\mathbb{F}$. If M and N are $\mathcal{O}[T]$-modules, finite and free of the same rank d as $\mathcal{O}$-modules, then $(M \otimes \mathbb{F})^{\mathrm{ss}} \simeq (N \otimes \mathbb{F})^{\mathrm{ss}}$ as $\mathbb{F}[T]$-modules if and only if for all n with $1 \leq n \leq d$ we have*

$$\operatorname{tr}(T^n|M) \equiv \operatorname{tr}(T^n|N) \pmod{n\mathfrak{m}}. \qquad (6.0.1)$$

We give two proofs of Theorem 6.1 in this section. The first may well be already clear to the reader, but we include it for completeness.

First proof of Theorem 6.1. Let P (respectively, Q) in $\mathcal{O}[T]$ be the characteristic polynomial of the action of T on M (respectively, on N). Let $\alpha_1, \ldots, \alpha_d$ (respectively, $\beta_1, \ldots, \beta_d$) be the roots of P (respectively, Q) in some p-adic DVR $\mathcal{O}'$ extending $\mathcal{O}$. With this notation, as detailed in Remark 2.8, Theorem 2.7 under the assumption $\deg P = \deg Q$ tells us that $\bar{P} = \bar{Q}$ in $\mathbb{F}[X]$ if and only if $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \mod n\mathfrak{m}$ for all $1 \le n \le d$. The latter condition is equivalent to (6.0.1), since $\mathrm{tr}(T^n|M) = \alpha_1^n + \cdots + \alpha_d^n = \mathsf{p}_n(P)$, and similarly $\mathrm{tr}(T^n|N) = \mathsf{p}_n(Q)$. The former condition $\bar{P} = \bar{Q}$ is equivalent to $\bar{P}$ and $\bar{Q}$ having the same multiset of roots with multiplicity in some extension of $\mathbb{F}$. But the roots of $\bar{P}$ (respectively, $\bar{Q}$) are the reductions $\bar{\alpha}_1, \ldots, \bar{\alpha}_d$ (respectively, $\bar{\beta}_1, \ldots, \bar{\beta}_d$) modulo the maximal ideal $\mathfrak{m}'$ of $\mathcal{O}'$ of $\alpha_1, \ldots, \alpha_d$ (respectively, $\beta_1, \ldots, \beta_d$). In other words, (6.0.1) is equivalent to the statement that, up to reordering, we have equalities in $\mathbb{F}'$

$$\bar{\alpha}_1 = \bar{\beta}_1,\ \bar{\alpha}_2 = \bar{\beta}_2,\ \ldots,\ \bar{\alpha}_d = \bar{\beta}_d. \tag{6.0.2}$$

But the $\bar{\alpha}_i$ (respectively, $\bar{\beta}_j$) are the eigenvalues of T acting on $M \otimes \mathbb{F}$ (respectively $N \otimes \mathbb{F}$), so that the matching in (6.0.2) is exactly equivalent to the up-to-semisimplification isomorphism $(M \otimes \mathbb{F})^{\mathrm{ss}} \equiv (N \otimes \mathbb{F})^{\mathrm{ss}}$. □

The second proof of Theorem 6.1 will be given in two parts. The "only if" direction, which is a special case of Proposition 2.10, is straightforward if a little tedious, and given in subsection 6.1. The "if" direction, a special case of Proposition 2.11, is more interesting: the proof, given in subsection 6.2, relies on either a version of the Brauer-Nesbitt theorem for representations of the one-parameter algebra $\mathbb{F}[T]$ or on linear independence of characters (see Appendix for details).

6.1. **Second proof of "only if" direction of Theorem 6.1.** Here we prove the straightforward direction of Theorem 6.1. Namely, we show the following.

Proposition 6.2. *Let $\mathcal{O}$ be a p-adic DVR with maximal ideal $\mathfrak{m}$ of ramification degree $e \le p-1$ and residue field $\mathbb{F}$. Suppose P and Q are monic degree-d polynomials in $\mathcal{O}[X]$; let $\alpha_1, \ldots, \alpha_d$ be the roots of P and $\beta_1, \ldots, \beta_d$ the roots of Q, all in some p-adic DVR extending $\mathcal{O}$. If $\bar{P} = \bar{Q}$ in $\mathbb{F}[X]$, then for all $n \ge 1$ we have*

$$\alpha_1^n + \cdots + \alpha_d^n \equiv \beta_1^n + \cdots + \beta_d^n \mod n\mathfrak{m}. \tag{6.1.1}$$

Proof. Let $\mathcal{O}'$ be a p-adic DVR extending $\mathcal{O}$ containing all the roots of P and Q, and let $\mathfrak{m}'$ be the maximal ideal of $\mathcal{O}'$. As in the first proof of Theorem 6.1, the equation $\bar{P} = \bar{Q}$ implies that, up to reordering, we have $\alpha_i \equiv \beta_i$ modulo $\mathfrak{m}'$ for each i. If we knew that $\mathfrak{m}'$ is a divided-power ideal of $\mathcal{O}'$ in its own right (for example, if $\mathcal{O}' = \mathcal{O}$) then (6.1.1) would follow immediately from Lemma 3.7: modulo-$\mathfrak{m}'$ congruences $\alpha_i \equiv \beta_i$ would imply the modulo $n\mathfrak{m}'$-congruence $\alpha_i^n \equiv \beta_i^n$, and the fact that $n\mathfrak{m}' \cap \mathcal{O} = n\mathfrak{m}$ would complete the proof. Instead we complete the argument with Lemma 6.3 below, which generalizes Lemma 3.7. □

Lemma 6.3. *Let $(\mathcal{O}, \mathfrak{m}, \mathbb{F})$ be a p-adic DVR with $\mathfrak{m}$ a divided-power ideal. Suppose P, Q are monic polynomials in $\mathcal{O}[X]$ with $\bar{P} = \bar{Q}$ in $\mathbb{F}[X]$. Then $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q)$ modulo $n\mathfrak{m}$ for every $n \ge 1$.*

Lemma 6.3 follows from Proposition 6.4 below once we introduce the notation. For $n \ge 0$, let $P_n \in \mathcal{O}[X]$ denote the degree-d monic polynomial whose roots are $\alpha_1^n, \ldots, \alpha_d^n$, so that

$$P_n = (X - \alpha_1^n) \cdots (X - \alpha_d^n).$$

It is now clear that $\mathsf{p}_n(P) = \mathsf{e}_1(P_n)$, and Lemma 6.3 is a direct consequence of the following.

Proposition 6.4. *Let $(\mathcal{O}, \mathfrak{m}, \mathbb{F})$ be a p-adic DVR with $\mathfrak{m}$ a divided-power ideal. Suppose P, Q are monic polynomials in $\mathcal{O}[X]$ with $\overline{P} = \overline{Q}$ in $\mathbb{F}[X]$. Then for any $n \geq 1$ and any symmetric function $f \in \Lambda$, we have $f(P_n) \equiv f(Q_n) \mod n\mathfrak{m}$.*

The proof of Proposition 6.4 is straightforward if tedious; it occupies the remainder of subsection 6.1.

Proof. Let d be the common degree of P and Q. Observe that establishing the claim for any $f \in \Lambda$ is equivalent to establishing it for $f = \mathsf{e}_1, \ldots, \mathsf{e}_d$: see (3.2.1). And the case $n = 1$ follows from the assumptions on P, Q.

We prove the claim for $n = p^k$ by induction on k. The base case $k = 0$ is the case $n = 1$, already established. Now suppose for some $k \geq 0$ we know that, whenever P, Q are monic polynomials in $\mathcal{O}[X]$ with $\overline{P} = \overline{Q}$, we have $f(P_{p^k}) \equiv f(Q_{p^k})$ modulo $p^k\mathfrak{m}$ for any symmetric function $f \in \Lambda$. We aim to show that this statement is true for $k+1$ as well. So let P, Q be such a pair of polynomials (monic with $\overline{P} = \overline{Q}$), and let $\alpha_1, \ldots, \alpha_d$ and $\beta_1, \ldots, \beta_d$ be roots of P and Q, respectively, in an extension of $\mathcal{O}$. Fix i with $1 \leq i \leq d$. By the inductive hypothesis on P, Q, we have $\mathsf{e}_i(P_{p^k}) \equiv \mathsf{e}_i(Q_{p^k})$ modulo $p^k\mathfrak{m}$. Lemma 3.7 and Corollary 2.4 imply that

$$\mathsf{e}_i(P_{p^k})^p \equiv \mathsf{e}_i(Q_{p^k})^p \mod p^{k+1}\mathfrak{m}. \tag{6.1.2}$$

For compactness of notation we write $\mathsf{e}_i(P_{p^k}) = \sum_{\underline{j} \in E_i} (\alpha_{\underline{j}})^{p^k}$, where E_i is the set of i-tuples of indices $\underline{j} = (j_1, \ldots, j_i)$ with $1 \leq j_1 < \cdots < j_i \leq d$, and $\alpha_{\underline{j}}$ is shorthand for $\alpha_{j_1} \cdots \alpha_{j_i}$. This allows us to expand the left-hand side of (6.1.2) as

$$\begin{aligned}
\mathsf{e}_i(P_{p^k})^p = \left(\sum_{\underline{j} \in E_i} (\alpha_{\underline{j}})^{p^k} \right)^p &= \sum_{\underline{j} \in E_i} (\alpha_{\underline{j}})^{p^{k+1}} + \sum_{\underline{s} \in D_{p,i}} \binom{p}{\underline{s}} (\alpha^{\underline{s}})^{p^k} \\
&= \mathsf{e}_i(P_{p^{k+1}}) + \sum_{\underline{s} \in D_{p,i}} \binom{p}{\underline{s}} (\alpha^{\underline{s}})^{p^k},
\end{aligned}$$

where $D_{p,i}$ is the set of $|E_i|$-tuples of indices $\underline{s} = (s_{\underline{j}} : \underline{j} \in E_i)$ with $0 \leq s_{\underline{j}} \leq p-1$ for each $\underline{j}$ satisfying $\sum_{\underline{j} \in E_i} s_{\underline{j}} = p$; and $\alpha^{\underline{s}}$ is shorthand for $\prod_{\underline{j} \in E_i} \alpha_{\underline{j}}^{s_{\underline{j}}}$. The analogous formula is true for the right-hand side of (6.1.2) as well:

$$\mathsf{e}_i(Q_{p^k})^p = \mathsf{e}_i(Q_{p^{k+1}}) + \sum_{\underline{s} \in D_{p,i}} \binom{p}{\underline{s}} (\beta^{\underline{s}})^{p^k},$$

so that $\mathsf{e}_i(P_{p^{k+1}}) \equiv \mathsf{e}_i(Q_{p^{k+1}})$ modulo $p^{k+1}\mathfrak{m}$ if and only if

$$\sum_{\underline{s} \in D_{p,i}} \binom{p}{\underline{s}} (\alpha^{\underline{s}})^{p^k} \equiv \sum_{\underline{s} \in D_{p,i}} \binom{p}{\underline{s}} (\beta^{\underline{s}})^{p^k} \mod p^{k+1}\mathfrak{m}. \tag{6.1.3}$$

To establish (6.1.3), we break up each sum into symmetric functions of the $\alpha_i^{p^k}$ or $\beta_i^{p^k}$ with the same multinomial coefficient. The symmetric group S_d acts on E_i by permuting the indices: for $\underline{j} = (j_1, \ldots, j_i)$ we define $\sigma(\underline{j})$ to be the tuple $\big(\sigma(j_1), \ldots, \sigma(j_i)\big)$ reordered to land in E_i. Permutations of E_i in turn permute $D_{p,i}$: for $\sigma \in S_d$ and $\underline{s} = (s_{\underline{j}} : \underline{j} \in E_i) \in D_{p,i}$, we set $\sigma(\underline{s}) := (s_{\sigma(\underline{j})} : \underline{j} \in E_i)$. Clearly, $\binom{p}{\underline{s}} = \binom{p}{\sigma(\underline{s})}$, so we can group terms in the same orbit of the action together. Moreover, each multinomial coefficient $\binom{p}{\underline{s}}$ is (exactly) divisible by p (Corollary 3.6). It thus suffices to prove that for each S_d-orbit $\mathcal{R} \subseteq D_{p,i}$ of this action, we have

$$\sum_{\underline{s}\in\mathcal{R}} (\alpha^{\underline{s}})^{p^k} \equiv \sum_{\underline{s}\in\mathcal{R}} (\beta^{\underline{s}})^{p^k} \mod p^k\mathfrak{m}. \tag{6.1.4}$$

But (6.1.4) follows from the inductive hypothesis. Indeed, any symmetric function of $\{\alpha^{\underline{s}} : \underline{s} \in \mathcal{R}\}$ is also symmetric in $\{\alpha_1, \dots, \alpha_d\}$, so that in particular corresponding symmetric functions of $\{\alpha^{\underline{s}} : \underline{s} \in \mathcal{R}\}$ and of $\{\beta^{\underline{s}} : \underline{s} \in \mathcal{R}\}$ will be congruent modulo $\mathfrak{m}$. By the inductive hypothesis, corresponding symmetric functions in $\{(\alpha^{\underline{s}})^{p^k} : \underline{s} \in \mathcal{R}\})$ and in $\{(\beta^{\underline{s}})^{p^k} : \underline{s} \in \mathcal{R}\})$ are then congruent modulo $p^k\mathfrak{m}$, as desired. This completes the induction: we have established that $\mathsf{e}_i(P_{p^k}) \equiv \mathsf{e}_i(Q_{p^k})$ modulo $p^k\mathfrak{m}$ for any $1 \le i \le d$ and any $k \ge 0$; the claim for any symmetric function $f \in \Lambda$ follows.

Finally, to prove the case of general n, write $n = up^k$ with $p \nmid u$. Fix i with $1 \le i \le d$. By what we have already shown, $\mathsf{e}_i(P_{p^k}) \equiv \mathsf{e}_i(Q_{p^k})$ modulo $p^k\mathfrak{m}$. Raising both sides to the u^{th} power we obtain $\mathsf{e}_i(P_{p^k})^u \equiv \mathsf{e}_i(Q_{p^k})^u \mod p^k\mathfrak{m}$. As in the inductive proof above, we expain the left-hand side (the right-hand side is similar)

$$\mathsf{e}_i(P_{p^k})^u = \Big(\sum_{\underline{j}\in E_i} (\alpha_{\underline{j}})^{p^k}\Big)^u = \mathsf{e}_i(P_n) + \sum_{\underline{s}\in D_{u,i}} \binom{u}{\underline{s}} (\alpha^{\underline{s}})^{p^k},$$

so that the claim is once again equivalent to establishing

$$\sum_{\underline{s}\in D_{u,i}} \binom{u}{\underline{s}} (\alpha^{\underline{s}})^{p^k} \equiv \sum_{\underline{s}\in D_{u,i}} \binom{u}{\underline{s}} (\beta^{\underline{s}})^{p^k} \mod p^k\mathfrak{m}. \tag{6.1.5}$$

The details are similar to the inductive proof above and left to the reader. □

6.2. **Second proof of "if" direction of Theorem 6.1.** Here we prove the more interesting direction of Theorem 6.1. Namely, we show the following.

Proposition 6.5. *Let $\mathcal{O}$ be a p-adic DVR with maximal ideal $\mathfrak{m}$ of ramification degree $e \le p-1$ and residue field $\mathbb{F}$. Suppose P and Q are monic degree-d polynomials in $\mathcal{O}[X]$; let $\alpha_1, \dots, \alpha_d$ be the roots of P and $\beta_1, \dots, \beta_d$ the roots of Q, all in the p-adic DVR $\mathcal{O}'$ extending $\mathcal{O}$; let $\mathfrak{m}'$ be the maximal ideal of $\mathcal{O}'$. Suppose for each $n \ge 1$ we have*

$$\alpha_1^n + \cdots + \alpha_d^n \equiv \beta_1^n + \cdots + \beta_d^n \mod n\mathfrak{m}. \tag{6.2.1}$$

Then up to reordering we have $\alpha_i \equiv \beta_i \mod \mathfrak{m}'$ for each $1 \le i \le d$.

Proof. For the proof, write α for the multiset $\alpha_1, \dots, \alpha_d$ and similarly for β. For $x \in \mathbb{F}'$, write $m(x, \alpha)$ for the cardinality of the set $\{i : \alpha_i \equiv x \mod \mathfrak{m}'\}$, and the same for $m(x, \beta)$. For our goal it suffices to show that $m(x, \alpha) = m(x, \beta)$ for all $x \in \mathbb{F}'$: indeed, this proves that

$$\bar{P} = \prod_{x\in\mathbb{F}'} (X - x)^{m(x,\alpha)} = \prod_{x\in\mathbb{F}'} (X - x)^{m(x,\beta)} = \bar{Q}$$

in $\mathbb{F}'[X]$, and hence in $\mathbb{F}[X]$.

We now proceed as follows: first we alter the α_i, in a Galois-equivariant way, so that if two of them are congruent modulo $\mathfrak{m}'$, then they are equal; we do the same for the β_j. Then we prove, by induction on s, that $m(x, \alpha) \equiv m(x, \beta)$ modulo p^s.

Step 1: Adjust α and β to take values in $t(\mathbb{F}')$. Recall that the mod-$\mathfrak{m}'$ reduction map $(\mathcal{O}')^\times \twoheadrightarrow (\mathbb{F}')^\times$ is a group homomorphism with a canonical section $t : (\mathbb{F}')^\times \to (\mathcal{O}')^\times$, called the *Teichmüller lift*. We extend t to all of $\mathbb{F}'$ by mapping 0 to 0. In particular t is Galois-equivariant, in the sense that $t(\bar{\tau}(x)) = \tau(t(x))$ for any $\tau \in \mathrm{Aut}(\mathcal{O}'/\mathcal{O})$ mapping modulo $\mathfrak{m}'$ to $\bar{\tau} \in \mathrm{Aut}(\mathbb{F}'/\mathbb{F})$.

For each $1 \le i \le d$, define $\alpha'_i := t(\bar{\alpha}_i)$ and $\beta'_i := t(\bar{\beta}_i)$. Here for any $u \in \mathcal{O}'$ we write $\bar{u}$ for the image of u in $\mathbb{F}'$. Clearly $\alpha'_i \equiv \alpha_i$ modulo $\mathfrak{m}'$, so that $m(x,\alpha) = m(x,\alpha')$ for each $x \in \mathbb{F}$. Moreover, by construction the α'_i are permuted by any Galois automorphism in $\mathrm{Aut}(\mathcal{O}'/\mathcal{O})$, so that any symmetric function in the α' lands in $\mathcal{O}$ and is hence congruent modulo $\mathfrak{m}$ to the corresponding symmetric function of the α. In particular the coefficients of $P' := (X-\alpha'_1)\cdots(x-\alpha'_d)$ are congruent to the coefficients of $P = (X-\alpha_1)\cdots(X-\alpha_d)$ modulo $\mathfrak{m}$. By Proposition 6.2, we have $\mathsf{p}_n(\alpha) \equiv \mathsf{p}_n(\alpha')$ modulo $n\mathfrak{m}$. Analogously, $m(x,\beta) = m(x,\beta')$ and $\mathsf{p}_n(\beta) \equiv \mathsf{p}_n(\beta')$ modulo $n\mathfrak{m}$. The upshot is that $\mathsf{p}_n(\alpha') \equiv \mathsf{p}_n(\beta') \mod n\mathfrak{m}$ and we can replace α_i by α'_i and β_i by β'_i in this investigation.

We now have, for all $n \ge 0$,

$$\mathsf{p}_n(\alpha) = \sum_{x \in \mathbb{F}'} m(x,\alpha)t(x)^n \quad \text{and} \quad \mathsf{p}_n(\beta) = \sum_{x \in \mathbb{F}'} m(x,\beta)t(x)^n; \tag{6.2.2}$$

we aim to prove that $m(x,\alpha) = m(x,\beta)$ for all $x \in \mathbb{F}'$ under the assumption that $\mathsf{p}_n(\alpha) \equiv \mathsf{p}_n(\beta)$ modulo $n\mathfrak{m}$.

Step 2: Show that $m(x,\alpha) \equiv m(x,\beta) \mod p^s$ for all $s \ge 1$. We proceed by induction on s. For the base case $s = 1$, consider the congruence $\mathsf{p}_n(\alpha) \equiv \mathsf{p}_n(\beta) \mod \mathfrak{m}$. Using (6.2.2), expand this as

$$\sum_{x \in \mathbb{F}'} m(x,\alpha)t(x)^n \equiv \sum_{x \in \mathbb{F}'} m(x,\beta)t(x)^n \mod \mathfrak{m}. \tag{6.2.3}$$

Linear independence of characters or trace version of Brauer-Nesbitt (see Appendix) now implies that for all x we have $m(x,\alpha) = m(x,\beta)$ as elements of $\mathbb{F}'$: in other words, $m(x,\alpha) \equiv m(x,\beta)$ modulo $\mathfrak{m}'$, and hence modulo p.

For the inductive step, suppose that $m(x,\alpha) \equiv m(x,\beta)$ modulo p^s for some $s \ge 1$. Fix ℓ greater than any $\log_p m(x,\alpha)$ or any $\log_p m(x,\beta)$. For every $x \in \mathbb{F}'$ express the integer $m(x,\alpha)$ in base p as

$$m(x,\alpha) = [m_\ell(x,\alpha)\ \cdots\ m_1(x,\alpha)\, m_0(x,\alpha)]_p,$$

where $m_0(x,\alpha), \ldots, m_\ell(x,\alpha)$ are the base-p digits of $m(x,\alpha)$, so that $0 \le m_j(x,\alpha) \le p-1$ and $m(x,\alpha) = \sum_j m_j(x,\alpha)p^j$. Analogously expand $m(x,\beta) = [m_\ell(x,\beta)\ \cdots\ m_1(x,\beta)\, m_0(x,\beta)]_p$.

By the inductive hypothesis, $m_j(x,\alpha) = m_j(x,\beta)$ for $0 \le j < s$, so that in particular

$$\sum_{x \in \mathbb{F}'} [m_{s-1}(x,\alpha)\ \cdots\ m_0(x,\alpha)]_p\, t(x)^n = \sum_{x \in \mathbb{F}'} [m_{s-1}(x,\beta)\ \cdots\ m_0(x,\beta)]_p\, t(x)^n. \tag{6.2.4}$$

Consider now those $n \ge 0$ that are divisible by p^s, expressing such n as $n = p^s n_s$. For such an n we have the congruence $\mathsf{p}_n(\alpha) \equiv \mathsf{p}_n(\beta) \mod p^s\mathfrak{m}$. Subtracting (6.2.4) from this congruence, we obtain

$$\sum_{x \in \mathbb{F}'} [m_\ell(x,\alpha)\cdots m_s(x,\alpha)\ \underbrace{0\cdots0}_{s}]_p\, t(x^{p^s})^{n_s} \equiv \sum_{x \in \mathbb{F}'} [m_\ell(x,\beta)\cdots m_s(x,\beta)\ \underbrace{0\cdots0}_{s}]_p\, t(x^{p^s})^{n_s} \mod p^s\mathfrak{m}.$$

Since we're in p-torsion-free algebra, we can divide by p^s to obtain, for all $n_s \ge 0$,

$$\sum_{x \in \mathbb{F}'} [m_\ell(x,\alpha)\ \cdots\ m_s(x,\alpha)]_p\, t(x^{p^s})^{n_s} \equiv \sum_{x \in \mathbb{F}'} [m_\ell(x,\beta)\ \cdots\ m_s(x,\beta)]_p\, t(x^{p^s})^{n_s} \mod \mathfrak{m}. \tag{6.2.5}$$

Since the p^{th} power map is an automorphism of $\mathbb{F}'$, the sets $\{x : x \in \mathbb{F}'\}$ and $\{x^{p^s} : x \in \mathbb{F}'\}$ are the same. Thus (6.2.5) is completely analogous to (6.2.3), so that we again use linear independence of characters / trace version of Brauer-Nesbitt, this time to deduce that $m_s(x,\alpha) = m_s(x,\beta)$. In other words, we've extended the congruence and $m(x,\alpha) \equiv m(x,\beta) \mod p^{s+1}$. By induction, $m(x,\alpha) = m(x,\beta)$ as elements of $\mathbb{Z}_p$, and hence as nonnegative integers. □

Remark 6.6. The same argument works if A is a domain, $\mathfrak{m}$ is a maximal divided-power ideal, $\mathbb{F}$ is perfect, and a Galois-equivariant section $t : \mathbb{F}' \to \mathcal{O}'$ exists. In particular, this argument works for any domain A with maximal divided power ideal $\mathfrak{m}$ if P, Q split into linear factors over A. △

6.3. **Complement: A generalization to virtual modules.** Here we prove Corollary 1.1. Recall that for a finite free $\mathbb{Z}_p$-module M we write $\overline{M}$ for $M \otimes \mathbb{F}_p$.

Corollary 6.7 (Restatement of Corollary 1.1)**.** *Let M_1, M_2, N_1, N_2 be free $\mathbb{Z}_p$-modules of finite rank, each with an action of an operator T. Suppose we have fixed T-equivariant embeddings $\iota_1 : \overline{N_1} \hookrightarrow \overline{M_1}$ and $\iota_2 : \overline{N_2} \hookrightarrow \overline{M_2}$ and consider the quotients*

$$W_1 := \overline{M_1}/\iota_1(\overline{N_1}), \qquad W_2 := \overline{M_2}/\iota_2(\overline{N_2}).$$

Then $W_1^{\mathrm{ss}} \simeq W_2^{\mathrm{ss}}$ as $\mathbb{F}_p[T]$-modules if and only if for every $n \geq 0$ we have

$$v_p\big(\operatorname{tr}(T^n|M_1) - \operatorname{tr}(T^n|N_1) - \operatorname{tr}(T^n|M_2) + \operatorname{tr}(T^n|N_2)\big) \geq 1 + v_p(n). \tag{6.3.1}$$

Proof. Using Theorem 6.1, the condition in (6.3.1) is equivalent to the $\mathbb{F}_p[T]$-module isomorphism

$$\big(\overline{M_1 \oplus N_2}\big)^{\mathrm{ss}} \simeq \big(\overline{M_2 \oplus N_1}\big)^{\mathrm{ss}}. \tag{6.3.2}$$

Taking a quotient on the left-hand side by $\iota_1(\overline{N_1})^{\mathrm{ss}} \oplus \overline{N_2}^{\mathrm{ss}}$ and on the right-hand side by $\iota_2(\overline{N_2})^{\mathrm{ss}} \oplus \overline{N_1}^{\mathrm{ss}}$ shows that (6.3.2) is equivalent to the isomorphism $W_1^{\mathrm{ss}} \simeq W_2^{\mathrm{ss}}$. □

Remark 6.8.
- In fact the congruence for $0 \leq n \leq \operatorname{rank} M_1 + \operatorname{rank} N_2$ suffices in (6.3.1).
- Corollary 6.7 also holds with $\mathbb{Z}_p, \mathbb{F}_p, 1 + v_p(n)$ replaced by $\mathcal{O}$, $\mathbb{F}$, $\frac{1}{e} + v_p(n)$, respectively, where $\mathcal{O}$ is a p-adic DVR with residue field $\mathbb{F}$ and ramification degree $e \leq p-1$ over $\mathbb{Z}_p$. △

Appendix A. Brauer-Nesbitt and linear independence of characters

We briefly review the Brauer-Nesbitt theorem and connections to linear independence of characters in the setting of this paper.

Theorem A.1 (Brauer-Nesbitt [CR, 30.16] or [Wie, Theorem 2.4.6 ff.] for convenient presentation)**.** *Let k be a field; R a k-algebra; V a semisimple R-module, finite dimensional as a k-vector space.*

(a) **Characteristic polynomial version:** *The characteristic polynomial map*

$$r \mapsto \operatorname{CharPoly}(r|V) \in k[X]$$

for every r in R (equivalently, in a k-basis of R) determines V uniquely.

(b) **Trace version:** *If $\operatorname{char} k = 0$ or if $\operatorname{char} k > \dim_k V$ then the trace map $r \mapsto \operatorname{tr}(a|V) \in k$ for every r in R (equivalently, in a k-basis of R) determines V uniquely.*

(c) **Trace version complement:** *If $\operatorname{char} k = p$, then the trace map $r \mapsto \operatorname{tr}(a|V) \in k$ for every r in R (equivalently, in a k-basis of R) determines the multiplicity modulo p of every irreducible component of V.*

Since elementary symmetric functions determine the power-sum symmetric functions over $\mathbb{Z}$, the characteristic polynomial version of Brauer-Nesbitt always implies the trace version. Conversely, if $\operatorname{char} k = 0$ or $\operatorname{char} k > \dim_k V$, then $(\dim_k V)!$ is invertible in k, so that the power-sum functions determine the relevant elementary symmetric functions over k (Corollary 3.3), and hence the trace version of Brauer-Nesbitt is equivalent to the characteristic-polynomial version. In the critical positive characteristic case $\operatorname{char} k < \dim_k V$, the trace version both assumes and concludes less than the characteristic polynomial version; neither implies the other. But if $R = k[T]$, then R is abelian, so that every irreducible R-module is one-dimensional over k. In this case, both the trace version and its complement follow from the well-known statement about linear independence of characters.

Theorem A.2 (Linear independence of characters (Artin). See, for example, [Lan, Theorem VI.4.1])**.** *Let B be a monoid and $\chi_1, \ldots, \chi_d : B \to k$ multiplicative characters from B to a field k. Then $\chi_1, \ldots, \chi_r$ are k-linearly independent.*

Proposition A.3. *Theorem A.2 implies parts (b) and (c) of Theorem A.1 for $R = k[T]$.*

Proof. Given two finite-dimensional k-vector spaces V, W each with the action of a single operator T, let $\alpha_1, \ldots, \alpha_d$ be the list of distinct eigenvalues appearing in either $T|V$ or $T|W$ and set $B := \mathbb{Z}^+$ and $\chi_i(n) := \alpha_i^n$. The statement that $\operatorname{tr}(T^n|V) = \operatorname{tr}(T^n|W)$ is equivalent to

$$\sum_{i=1}^{d} f_i(V)\chi_i(n) = \sum_{i=1}^{d} f_i(W)\chi_i(n),$$

where $f_i(V)$ is the multiplicity of α_i as an eigenvalue of the action of T on V, and the same for W. Linear independence of characters, then, tells us that for all i, $f_i(V) = f_i(W)$ in k. This simultaneously recovers for $R = k[T]$ both the trace version of Brauer-Nesbitt and its complement. $\square$

The converse — trace version of Brauer-Nesbitt and its complement implies linear independence of characters — is also true over a prime field ($k = \mathbb{Q}$ or $k = \mathbb{F}_p$ for some prime p).

References

[BO] Pierre Berthelot and Arthur Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[BP] John Bergdall and Robert Pollack. Slopes of modular forms and the ghost conjecture, II. *Trans. Amer. Math. Soc.*, 372(1):357–388, 2019.

[CR] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[Lan] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lur] Jacob Lurie. The Artin-Hasse exponential. Available at `https://www.math.ias.edu/~lurie/205notes/Lecture7-Exponential.pdf`, 2018.

[Mac] I. G. Macdonald. *Symmetric functions and Hall polynomials*. The Clarendon Press, Oxford University Press, New York, second edition, 2015.

[Rom] Matthieu Romagny. Some useful p-adic formulas. Available at `https://perso.univ-rennes1.fr/matthieu.romagny/notes/p_adic_formulas.pdf`.

[Wie] Gabor Wiese. Galois representations, 2012. Course notes. Available at `https://math.uni.lu/~wiese/notes/GalRep.pdf`.

Email address: samuele.anni@univ-amu.fr

Aix-Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille case 907, 163 avenue de Luminy, F13288 Marseille cedex 9, France

Email address: aghitza@alum.mit.edu *Website:* https://aghitza.org

School of Mathematics and Statistics, University of Melbourne, Parkville 3010, Victoria, Australia

Email address: medvedov@post.harvard.edu *Website:* http://math.bu.edu/people/medved/

Dept. of Mathematics & Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA