ELEMENTARY SYMMETRIC FUNCTIONS AND DEEP POWER-SUM CONGRUENCES

Samuele Anni[1]
Institut de Mathématiques de Marseille, Aix-Marseille Université, France
samuele.anni@univ-amu.fr

Alexandru Ghitza
School of Mathematics and Statistics, University of Melbourne, Australia
aghitza@alum.mit.edu

Anna Medvedovsky[2]
Max-Planck-Institut für Mathematik, Bonn, Germany
medvedov@post.harvard.edu

Received: 6/29/23, Revised: 9/2/23, Accepted: 4/24/24, Published: 5/20/24

Abstract

We prove that congruences modulo p between polynomials in $\mathbb{Z}_p[X]$ are equivalent to deeper p-power congruences between power-sum functions of their roots. This result generalizes to torsion-free $\mathbb{Z}_{(p)}$-algebras modulo divided-power ideals. Our approach is combinatorial: we introduce a p-equivalence relation on partitions, and use it to prove that certain linear combinations of power-sum functions are p-integral. We also include a second proof, short and algebraic, suggested by an anonymous referee. As a corollary we refine the Brauer-Nesbitt theorem for a single linear operator, motivated by the study of Hecke modules of modular forms modulo p.

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 $\mathrm{tr}(T^n|M)$ as an element of $\mathbb{Z}_p$ for enough n is plenty, for the following reason. The Brauer-Nesbitt theorem – or in this one-parameter case, simply linear independence of characters (see Appendix) – tell us that these traces

DOI: 10.5281/zenodo.11221647
[1]Partially funded by the Melodia ANR-20-CE40-0013 project.
[2]Partially supported by NSF postdoctoral research fellowship DMS-1703834.

determine $(M \otimes \mathbb{Q}_p)^{\mathrm{ss}}$. Therefore 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 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 $n \geqslant 0$ we have $\mathrm{tr}(T^n|M) = p\alpha^n \equiv 0 \bmod p$, and we cannot recover α modulo p from these trace data.

Thus knowing $\mathrm{tr}(T^n|M)$ in $\mathbb{Z}_p$ is more than we need and knowing $\mathrm{tr}(T^n|M)$ modulo p is less than we need. We 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. *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 $\overline{M}^{\mathrm{ss}} \simeq \overline{N}^{\mathrm{ss}}$ as modules over $\mathbb{F}_p[T]$ if and only if for every n with $1 \leqslant n \leqslant d$ 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 $\overline{M}^{\mathrm{ss}}$ and $\overline{N}^{\mathrm{ss}}$ refer to their semisimplifications. We highlight a few observations.

- 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 $v_p : \mathbb{Q}_p \to \mathbb{Z}$ 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 the image of $\mathrm{tr}(T^p|M) = p\alpha^p$ in $\mathbb{Z}/p^2\mathbb{Z}$ is tantamount to knowing the image of α^p in $\mathbb{Z}/p\mathbb{Z}$, which in turn determines the image of α in $\mathbb{Z}/p\mathbb{Z}$ 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 congruence modulo p. But given two elements of $\mathbb{Z}_p$ that are congruent modulo p, their $(p^k)^{\mathrm{th}}$ powers are congruent modulo p^{k+1} (see Lemma 25); the deeper congruence claim follows. Thus the heart of Theorem A is the "if" direction.
- Theorem A generalizes to valuation rings of p-adic fields that are not too ramified (see Theorem 37).

The proof of Theorem A, combinatorial in nature, follows from the slightly more general Theorem B, described in the next subsection.

Remark 1. An anonymous referee of this document suggested a much simpler proof of Theorem A than the one we present (see Section 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) – used in the proof of Theorem B, as well as the observation in Proposition 3 (which we have not seen in the literature), have something to offer, so we present them here. It is also possible to prove Theorem A purely algebraically, drawing inspiration from the proof of the characteristic-p refinement of the trace version of Brauer-Nesbitt theorem (see Theorem 40(c)) plus some algebra. The dedicated reader may find this third proof in our first Arxiv draft.

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 commutative $\mathbb{Z}_{(p)}$-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 Section 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 Section 3.2 for more and for the non-domain case. The following combinatorial theorem is a generalization of Theorem A.

Theorem B. *Let P, Q be monic polynomials in $A[X]$. Then $\overline{P} = \overline{Q}$ in $(A/\mathfrak{a})[X]$ if and only if $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \bmod n\mathfrak{a}$ for $1 \leqslant n \leqslant \max\{\deg P, \deg Q\}$.*

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 break up the sum using a new equivalence relation called *p-equivalence* on the space of partitions. The exact definition can be found in Section 5.1 – 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 of p-equivalence is the following proposition.

Proposition C. *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*

$$\mathsf{g}_\lambda := \sum_{\mu \in C_\lambda} \frac{(-1)^\mu}{z_\mu} \mathsf{p}_\mu \quad \textit{has coefficients in } \mathbb{Z}_{(p)}.$$

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 (see Section 3.1). The symmetric function p_μ is the product of power-sum functions associated to the parts of μ (see Section 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 Section 5.2 for details).

The elegant proof of Proposition C that we present in Section 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.

Corollary 2. *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 $n \geqslant 0$ we have

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

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 2 is the form of the result that we use in [1] to study the Hecke module structure on certain quotients of spaces of modular forms modulo p. 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 $k \geqslant 2$, 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 rank 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 $k \geqslant 4$, multiplication by the Eisenstein series E_{p-1} normalized to be in $1+p\mathbb{Z}_p[\![q]\!]$ induces an embedding $M_{k-p+1}(Np, \mathbb{F}_p) \hookrightarrow M_k(Np, \mathbb{F}_p)$; let

$$W_k(Np) := M_k(Np, \mathbb{F}_p)/M_{k-p+1}(Np, \mathbb{F}_p)$$

denote the quotient. In [1] we use Corollary 2 to prove that, for $p \geqslant 5$,

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

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). The notation

$W[1]$ stands for the Hecke module given by the vector space W on which T_m acts as mT_m for all m prime to Np. We also refine (1) to account for the action of the Atkin-Lehner involution at p – the main motivation for Theorem A.

1.5. Organization of this Paper

Sections 2 to 5 are devoted to the proof of Theorem B. In Section 2, we state Theorem 9, 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 include 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 9; in particular, Section 5 is the heart of our main work here. In Section 6, we return to the module-theoretic Theorem A and deduce it from Theorem 9. In the same section we also prove Corollary 2.

All rings and algebras are assumed to be commutative with unity.

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,

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

Write $\mathsf{p}_n(P) := \sum_{i=1}^{d} \alpha_i^n$ for the n^{th} power-sum function of the roots of P. For a general B, Newton's identities [6, I.2.11′] express p_n as an integer polynomial in $\mathsf{e}_1, \ldots, \mathsf{e}_d$, thus defining $\mathsf{p}_n(P)$, or see Section 3.2 below.

2.2. Divided-Power Ideals in Torsion-Free $\mathbb{Z}_{(p)}$-Algebras

Fix a torsion-free $\mathbb{Z}_{(p)}$-algebra[3] 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 $k \geqslant 1$ if for any a in $\mathfrak{a}$ we have $a^k/k!$ in $\mathfrak{a}$ as well. Since A is $\mathbb{Z}$-torsion free and a $\mathbb{Z}_{(p)}$-algebra, this last condition may be reformulated: indeed, we have

$$\frac{a^k}{k!} \text{ is in } \mathfrak{a} \quad \text{if and only if} \quad a^k \text{ is in } k!\mathfrak{a} \quad \text{if and only if} \quad a^k \text{ is in } p^{v_p(k!)}\mathfrak{a}.$$

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

An ideal $\mathfrak{a}$ that satisfies the divided power property for all $k \geqslant 1$ 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 $\mathfrak{a}$ [2, Section 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 3. *For an ideal $\mathfrak{b}$ in a 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. That (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 $k \geqslant 1$. Note that

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

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

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

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

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

as desired.

Now for general $n \geqslant 1$, 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 have 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 [7]). □

Corollary 4. *An ideal $\mathfrak{a}$ of A is a divided-power ideal if and only if:*

$$\textit{whenever } a \in \mathfrak{a} \textit{ we have } a^p \in p\mathfrak{a}.$$

In fact, it suffices to check the condition of Corollary 4 on generators.

Proposition 5. *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 $a \in S$.*

Proof. It suffices to show that for a_1, a_2 in S, and 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, the middle terms since $p \mid \binom{p}{k}$. □

Corollary 6. *If $\mathfrak{a} \subset A$ is a divided-power ideal, then so is $\mathfrak{ab}$ for any ideal $\mathfrak{b} \subseteq A$.*

Proof. For $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ we have $(ab)^p = a^p b^p \in (p\mathfrak{a})b^p \subseteq p(\mathfrak{ab})$. Now use Proposition 5. □

2.3. Divided-Power Ideals in p-Adic DVRs

Recall that $v_p : \mathbb{Q}_p \to \mathbb{Z}$ denotes 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. The latter 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 7. *An ideal $\mathfrak{a}$ of a p-adic DVR is a divided-power ideal if and only if*

$$v_p(\mathfrak{a}) \geqslant \tfrac{1}{p-1}.$$

Proof. Let $a \in \mathfrak{a}$ be a generator, so that $v_p(a) = v_p(\mathfrak{a})$. By Proposition 5, the ideal $\mathfrak{a}$ is a divided-power ideal if and only if $a^p \in p\mathfrak{a}$. In our p-adic DVR setting, this happens if and only if

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

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

Corollary 8. *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 $e \leqslant p - 1$. In particular, (p) is a divided-power ideal of $\mathbb{Z}_p$.*

Proof. This follows immediately from Lemma 7 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 9. *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* $n \geqslant 1$;

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

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

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

Remark 10. We do not require $\deg P = \deg Q$ here. Note that the statement $\deg P = \deg Q$ is the same as the congruence $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \bmod n\mathfrak{a}$ for $n = 0$. Therefore, if we like, we may replace $n \geqslant 1$ with $n \geqslant 0$ 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 9:

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

Example 11. Let $p = 2$, $A = \mathbb{Z}_p$, and consider the polynomials $P = X^2 + X + 3$ 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 is clear that $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod 2$ for every $n \geqslant 1$. See Table 1, where the last two columns illustrate Theorem 9:

$$v_2\big(\mathsf{p}_n(Q) - \mathsf{p}_n(P)\big) \geqslant 1 + v_2(n) \qquad \text{for } n \geqslant 1.$$

We now give a skeleton proof of Theorem 9. Technical details are postponed to Sections 4 and 5.

Proof of Theorem 9. 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 in Section 4.

Proposition 12. *Fix $N \geqslant 1$. If $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ for all $1 \leqslant n \leqslant N$, then $\mathsf{p}_N(P) \equiv \mathsf{p}_N(Q) \bmod N\mathfrak{a}$.*

We then show (c) $\implies$ (a) and (d) $\implies$ (b) by proving the following in Section 5.

Proposition 13. *Fix $N \geqslant 1$. If $\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \bmod n\mathfrak{a}$ for all $1 \leqslant n \leqslant N$, then $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ for all $1 \leqslant n \leqslant N$.*

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). □

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

Table 1: Congruences between e_n, deep congruences between p_n in Example 11.

The divided-power property of the ideal $\mathfrak{a}$ is crucial to both directions of Theorem 9. We illustrate this point by giving two counterexamples in the absence of this property. In both Example 14 and Example 15 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 8), having ramification degree p. In both cases, P and Q have the same degree p, so statements (a) and (b) of Theorem 9 are equivalent to the equality $\overline{P} = \overline{Q}$ in $\mathbb{F}_p[X]$.

Example 14. 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 9 hold but (c) and (d) do not.

Example 15. 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

$$\mathsf{p}_n(P) \equiv \mathsf{p}_n(Q) \equiv 0 \mod n\mathfrak{m} \quad \text{for } 1 \leqslant n \leqslant p.$$

Indeed, for any $n \geqslant 1$,

$$\begin{aligned}\mathfrak{p}_n(P) &= \big(\alpha + (p-1)\big)^n + (p-1)(-1)^n \\ &= \alpha^n + \sum_{i=1}^{n-1} \binom{n}{i} \alpha^i (p-1)^{n-i} + (p-1)^n + (p-1)(-1)^n \qquad (2) \\ &= (\text{terms divisible by } \alpha) + (p-1)^n + (p-1)(-1)^n.\end{aligned}$$

Since

$$(p-1)^n + (p-1)(-1)^n \equiv (-1)^n - (-1)^n \equiv 0 \bmod p = \alpha^p,$$

and $p = \alpha^p$, we have $\mathfrak{p}_n(P) \equiv 0 \bmod \mathfrak{m}$.

If further $n = p$, then the summation term in (2) 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

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

Here 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 25 below). And if $p = 2$ then

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

In either case, $\mathfrak{p}_p(P)$ is a sum of a term in $\mathfrak{m}^{p+1}$ and a term in $\mathfrak{m}^{2p}$, so $\mathfrak{p}_p(P) \in p\mathfrak{m}$, as required. Thus statement (d) of Theorem 9 holds but (a) and (b) do not. One can show analogously that (c) also does not hold, as $v_p\big(\mathfrak{p}_{2p}(P)\big) = 1$.

The relationships between the statements in Theorem 9 are not yet entirely clear. Here are some questions that arise naturally, but that we do not address further here as they are orthogonal to the main purpose of this paper:

- Is there a direct proof that (d) implies (c)? The divided-power property must play a role, as Example 15 above satisfies (d) but not (c).
- Although (d) does not imply (a) or (b) without the divided-power assumption (again, see Example 15 above), is it possible that (c) does?

The next three sections are devoted to the proof of Theorem 9.

3. Combinatorial Preliminaries

3.1. Partitions

A *partition* λ of an integer $n \geqslant 0$, denoted $\lambda \vdash n$, is a (finite or infinite) ordered tuple $(\lambda_1, \lambda_2, \ldots)$ with $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant 0$ and $\sum_{i \geqslant 1} \lambda_i = n$. 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 $\{i \geqslant 1 : \lambda_i > 0\}$. There is a unique partition of 0, namely $\varnothing \vdash 0$, the *empty* partition. The *weight* $|\lambda|$ of a partition $\lambda = (\lambda_1, \lambda_2, \ldots)$ is the number being partitioned: $|\lambda| := \sum_{i \geqslant 1} \lambda_i$. Write $r_a(\lambda)$ for 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 $\lambda = (\lambda_1, \ldots, \lambda_k)$, then $(-1)^\lambda = (-1)^{\sum_i (\lambda_i - 1)}$. Additionally, set

$$z_\lambda := \prod_{a \geqslant 1} a^{r_a(\lambda)} r_a(\lambda)!,$$

the order of the centralizer in S_n of any permutation of cycle structure λ. Then $n!/z_\lambda$ is the number of permutations of n with cycle structure λ. Accordingly, $z_\varnothing = 1$.

For $n \geqslant 0$, let $\mathcal{P}_n$ be the set of partitions of n, and let $\mathcal{P} := \bigcup_{n \geqslant 0} \mathcal{P}_n$ 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 $k \geqslant 0$, we may consider the partition $\lambda^k \vdash kn$.

Definition 16. Let p be a prime and $\lambda := (\lambda_1, \lambda_2, \ldots)$ a partition of $n \geqslant 0$. 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 v 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: $\Lambda_d = \bigoplus_{n \geqslant 0} \Lambda_d^n$, where $\Lambda_d^n \subseteq \Lambda_d$ are the homogeneous symmetric polynomials in $x_1, \ldots, x_d$ of degree n. For any $d \geqslant d'$ we have a graded map $\Lambda_d \twoheadrightarrow \Lambda_{d'}$ mapping x_i to x_i for $i \leqslant d'$ 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 $\Lambda := \bigoplus_{n \geqslant 0} \Lambda^n$. 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.

Definition 17 (Elementary symmetric functions)**.** For $n \geqslant 0$, let $\mathsf{e}_{n,d} \in \Lambda_d^n$ be the n^{th} *elementary symmetric polynomial*:

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

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 [6, I.2.4] – that

$$\Lambda = \mathbb{Z}[\mathsf{e}_1, \mathsf{e}_2, \ldots]. \tag{3}$$

Definition 18 (Power-sum symmetric functions)**.** Similarly, for $n \geqslant 0$, let $\mathsf{p}_{n,d} \in \Lambda^n_d$ be the n^{th} *power-sum polynomial*:

$$\mathsf{p}_{n,d} := \sum_{i=1}^{d} x_i^n \in \Lambda^n_d.$$

For $n \geqslant 1$ 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. One can check that $\Lambda_{\mathbb{Q}} = \mathbb{Q}[\mathsf{p}_1, \mathsf{p}_2, \ldots]$; see, for example, [6, I.2.12].

We use the following standard notation. Given a family of symmetric functions $\{f_n\}_{n\geqslant 1}$ (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 $\Lambda^n_{\mathbb{Q}}$.

Building on the above, we introduce notation for a symmetric function evaluated at a monic polynomial $Q = X^d + a_1 X^{d-1} + \cdots + a_d \in A[X]$. For $n \geqslant 0$, denote by

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

More generally, for any symmetric function f, let $f(Q) \in A$ be defined as follows: first use (3) 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 x's, 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 $\{\mathsf{p}_n(Q)\}_{n\geqslant 0}$ satisfies an A-linear recurrence of order $\deg Q$, closely related to Newton's identities (see, for example, [6, I.2.11′]).

3.3. Combinatorial Lemmas

Here we collect standard facts relating generating functions of various symmetric functions: see, for example, [6, I.2]. For a set of positive integers $S \subseteq \mathbb{N}$, let

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

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 19. *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. We have

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

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

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

The remaining statements of this section are completely standard.

Proposition 20. *We have $\mathsf{E}(t) = \exp \mathsf{P}(t)$.*

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

$$\begin{aligned}
\log \mathsf{E}(t) := \log \prod_{i=1}^{\infty} (1 + x_i t) &= \sum_{i=1}^{\infty} \log(1 + x_i t) = \sum_{i=1}^{\infty} \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(x_i t)^n}{n} \\
&= \sum_{n=1}^{\infty} (-1)^{n-1} \frac{t^n}{n} \sum_{i=1}^{\infty} x_i^n = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{\mathsf{p}_n}{n} t^n = \mathsf{P}(t).
\end{aligned}$$

□

Proposition 20 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 21 and Corollary 22.

Corollary 21 (Expressing e_n in terms of p_λ)**.** *For all $n \geqslant 0$, we have*

$$\mathsf{e}_n = \sum_{\lambda \vdash n} (-1)^\lambda \frac{\mathsf{p}_\lambda}{z_\lambda}. \tag{4}$$

Proof. Combining Proposition 20 with Proposition 19 for $S = \mathbb{N}$ yields

$$\sum_{\lambda} (-1)^\lambda \frac{\mathsf{p}_\lambda}{z_\lambda} t^{|\lambda|} = \sum_{n=0}^{\infty} \mathsf{e}_n t^n.$$

The statement follows from considering the coefficients of t^n on each side. □

As examples of Corollary 21, $\mathsf{e}_2 = \frac{\mathsf{p}_1^2 - \mathsf{p}_2}{2}$ and $\mathsf{e}_3 = \frac{\mathsf{p}_1^3 - 3\mathsf{p}_1\mathsf{p}_2 + 2\mathsf{p}_3}{6}$.

Corollary 22 (Expressing p_n in terms of e_λ)**.** *For $n \geqslant 1$, we have*

$$\mathsf{p}_n = (-1)^n \, n \sum_{\lambda \vdash n} \frac{(-1)^m}{m} \binom{m}{r_1(\lambda), r_2(\lambda), \ldots} \mathsf{e}_\lambda, \tag{5}$$

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

Proof. From Proposition 20 we have

$$\begin{aligned} \sum_{n=0}^{\infty} (-1)^{n-1} \frac{\mathsf{p}_n}{n} t^n = \mathsf{P}(t) = \log \mathsf{E}(t) &= \log \left(1 + \sum_{k=1}^{\infty} \mathsf{e}_k t^k \right) \\ &= \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \left(\sum_{k=1}^{\infty} \mathsf{e}_k t^k \right)^m \\ &= \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \sum_{1 \leqslant k_1, \ldots, k_m} \mathsf{e}_{k_1} \cdots \mathsf{e}_{k_m} t^{k_1 + \cdots + k_m}, \end{aligned}$$

where the last sum is over m-tuples $(k_1, \ldots, k_m)$ 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 $\binom{m}{r_1(\lambda), r_2(\lambda), \ldots}$ such m-tuples. Equating coefficients of t^n on each side, we obtain, as desired,

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

3.4. A Simple Proof of Theorem A

An anonymous referee of this paper suggested a simpler proof of Theorem A, which builds on the above discussion of the generating functions P and E.

Alternate proof of Theorem A. Let M, N be free $\mathbb{Z}_p$-modules of rank d, each endowed with an action of an operator T. Write $\mathsf{p}_n(M)$ 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

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

We note that we still have $\mathsf{P}(M,t) = \log \mathsf{E}(M,t)$ as in Proposition 20, which enables the following sequence of equivalent statements.

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

Along the way 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 Section 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 22 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 [7]. The generalization to any k is immediate through the formula

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

expressing multinomial coefficients in terms of binomial coefficients.

Theorem 23 (Kummer)**.** *The multinomial coefficient* $\binom{m}{r_1,\ldots,r_k}$ *has* p*-valuation equal to the sum of the carry digits when the addition* $r_1 + \cdots + r_k$ *is performed in base* p*.*

Corollary 24. *For any* i*, we have* $v_p(r_i) \geqslant v_p(m) - v_p\left(\binom{m}{r_1,\ldots r_k}\right)$.

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,

$$v_p\left(\binom{m}{r_1,\ldots r_k}\right) \geqslant v_p(m) - v_p(r_i). \qquad \square$$

The second statement we need (Corollary 26 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 25. *Suppose* $x \equiv y \bmod \mathfrak{a}$ *for some* $x, y \in A$*. Then*

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

(b) for all $n \geqslant 0$ *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 4 tells us that $a^p \in p\mathfrak{a}$. To prove the statement for $m > 1$ we proceed by induction using Corollary 6. $\square$

Corollary 26. *Let* $P, Q \in A[X]$ *be polynomials, and* $\{f_n\}_{n\geqslant 1}$ *a family of symmetric functions. If* $f_n(P) \equiv f_n(Q) \bmod \mathfrak{a}$ *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 (Section 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 25. $\square$

3.6. Artin-Hasse Exponential Series

We briefly recall the Artin-Hasse exponential series

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

here viewed merely as a formal power series, a priori in $\mathbb{Q}[\![z]\!]$. In Section 5.3 we will make use of the fact that $F(z)$ is actually p-integral (Corollary 29); here we briefly review this well-known result. We follow the convenient expository notes [5] of Jacob Lurie.

Proposition 27. *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. It satisfies the property

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Before giving the proof of Proposition 27, we need a lemma:

Lemma 28. *For prime p we have* $\sum_{d|n,\, p \nmid d} \mu(d) = \begin{cases} 1 & \text{if } n \text{ is a power of } p \\ 0 & \text{otherwise.} \end{cases}$

Proof. In general, 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 fact that f is multiplicative 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 prime to p. In the former case the claim is immediate; in the latter it follows from (6). □

Proof of Proposition 27. We have

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

where the last equality follows from Lemma 28. The claim follows. □

Corollary 29. *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 27 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. □

4. Proof of Proposition 12: e_n Congruent Implies p_n Deeply Congruent

Here we prove Proposition 12. The proof uses the combinatorial expression from Corollary 22 for p_n in terms of e_λ.

Proof of Proposition 12. Let $P, Q \in A[X]$ be monic polynomials, fix $N \geqslant 1$, and suppose that $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ for all n with $1 \leqslant n \leqslant N$. We seek to show that $\mathsf{p}_N(P) - \mathsf{p}_N(Q)$ is in $N\mathfrak{a}$.

From Corollary 22 we have

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

Corollary 26 for $f = \mathsf{e}$ tells us that our assumptions on the e_n imply that the difference $\mathsf{e}_\lambda(P) - \mathsf{e}_\lambda(Q)$ lies 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,

$$v_p(N) - v_p(m) + v_p\left(\binom{m}{r_1(\lambda), r_2(\lambda), \ldots}\right) + v_p(\lambda) \geqslant v_p(N).$$

Equivalently, canceling $v_p(N)$ and using the definition of $v_p(\lambda)$, we need to show that for every i,

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

But this is exactly Corollary 24. □

Incidentally, it is not a priori obvious that $\frac{n}{m}\binom{m}{r_1, r_2, \ldots}$ is integral for any sequence $r_1, r_2, \ldots$ of nonnegative integers almost all zero, with $m = \sum r_i$ and $n = \sum i r_i$. But this integrality does follow from Corollary 24.

5. Proof of Proposition 13: p_n Deeply Congruent Implies e_n Congruent

The aim of this section is to give a combinatorial proof of the "if" direction of Theorem 9: 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

The following definitions introduce an equivalence relation on the set $\mathcal{P}_n$ of partitions of an integer $n \geqslant 0$.

Definition 30. 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 $u \geqslant 1$, 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 $\lambda\nu$.

Definition 31. Let *p-equivalence*, written $\sim_p$, be the equivalence relation generated by the p-splitting relation. For $\lambda \vdash n$ let $C_\lambda := \{\mu \vdash n : \mu \sim_p \lambda\}$ denote the p-equivalence class of λ.

Definition 32. A partition λ is *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 33. Let $u \geqslant 1$ be prime to p and let $r \geqslant 0$. Then the partition $(u)^r$ is p-deprived and

$$C_{(u)^r} = \big\{\lambda \vdash ur \colon \lambda \text{ has parts in } \{up^j : j \geqslant 0\}\big\}.$$

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

$$\mathcal{P}_n = \{\lambda \vdash n\} = \bigsqcup_{\lambda \vdash^{(p)} n} C_\lambda. \tag{7}$$

5.2. The Contribution to e_n from a Single p-Equivalence Class

Fix $n \geqslant 0$ and $\lambda \vdash n$. Let

$$\mathsf{g}_\lambda := \sum_{\mu \sim_p \lambda} (-1)^\mu \frac{\mathsf{p}_\mu}{z_\mu}, \tag{8}$$

so that in particular $\mathsf{g}_\varnothing = 1$. In other words, g_λ is the piece of the expression for e_n from (4) that comes from all the partitions that are p-equivalent to λ. Because of (7), for any $n \geqslant 0$,

$$\mathsf{e}_n = \sum_{\lambda \vdash^{(p)} n} \mathsf{g}_\lambda. \tag{9}$$

To show that $\mathsf{e}_n(P) \equiv \mathsf{e}_n(Q) \bmod \mathfrak{a}$ in Proposition 13, 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 34. *Suppose $\lambda \vdash^{(p)} n$, $\mu \vdash^{(p)} m$ are partitions of $n, m \geqslant 0$ with no common parts. Then $\mathsf{g}_{\lambda\mu} = \mathsf{g}_\lambda \mathsf{g}_\mu$. Thus for $\lambda \vdash^{(p)} n$,*

$$\mathsf{g}_\lambda = \prod_{u \geqslant 1,\ p \nmid u} \mathsf{g}_{(u)^{r_u(\lambda)}}.$$

Proof. Any two partitions λ and μ, whether 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

$$\mathsf{g}_{(u)^r}(P) \equiv_{\mathfrak{a}} \mathsf{g}_{(u)^r}(Q) \tag{10}$$

for every $ur \leqslant n$ where $r \geqslant 0$ and $u \geqslant 1$ is prime to p. We prove this in Section 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.

Lemma 35. *If p is odd, then* $\mathsf{g}_\lambda = (-1)^\lambda \sum_{\mu \sim_p \lambda} \frac{\mathsf{p}_\mu}{z_\mu}$.

Proof. If p is odd, then for any $u \geqslant 1$ and $j \geqslant 0$, 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 (8) it is clear that g_λ is in $\Lambda_{\mathbb{Q}}$. However, one can show that g_λ is p-integral as a symmetric function.

Proposition 36. *For any partition $\lambda \vdash n \geqslant 0$, 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 34, it suffices to show that for any u prime to p and any $r \geqslant 0$, 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

$$G_u(t) := \sum_{r=0}^{\infty} \mathsf{g}_{(u)^r} t^{ur} \tag{11}$$

for the sequence $\{g_{(u)^r}\}_{r \geqslant 0}$ 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 29).

For p odd, let $\varepsilon_u = (-1)^{u-1}$ be the sign of (up^j) for $j \geqslant 0$ (Lemma 35). Then

$$G_u(t) = \exp\left(\sum_{j=0}^{\infty} \frac{\varepsilon_u \mathsf{p}_{up^j}}{up^j} t^{up^j}\right) = \exp\left(\frac{\varepsilon_u}{u} \sum_{j=0}^{\infty} t^{up^j} \frac{(x_1^{up^j} + x_2^{up^j} + \cdots)}{p^j}\right) \tag{12}$$
$$= F(x_1^u t^u)^{\varepsilon_u/u} F(x_2^u t^u)^{\varepsilon_u/u} \cdots,$$

where the first equality is Proposition 19 for the set $S = \{up^j : j \geqslant 0\}$ (see Example 33). 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 $p = 2$,

$$G_u(t) = \exp\left(\frac{2t^u \mathsf{p}_u}{u} - \sum_{j=0}^{\infty} \frac{t^{up^j}}{up^j} \mathsf{p}_{up^j}\right)$$
$$= \left(\sum_{k=0}^{\infty} \frac{2^k}{u^k k!} \mathsf{p}_u^k \, t^{uk}\right) F(x_1^u t^u)^{-1/u} F(x_2^u t^u)^{-1/u} \cdots. \tag{13}$$

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

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

so that the first factor in (13) is in $\Lambda_{\mathbb{Z}_{(p)}}[\![t]\!]$, the rest being as in (12). □

5.4. Proof of Proposition 13

Finally, we prove that deep congruences between power sum functions imply congruences between elementary symmetric functions, by building upon the p-integrality result of Section 5.3.

Proof of Proposition 13. Recall that we assume that $\mathsf{p}_n(P) - \mathsf{p}_n(Q) \in n\mathfrak{a}$ for all n with $1 \leqslant n \leqslant N$; 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 Section 5.2 to make some reductions: by (9), it suffices to show that

$$\mathsf{g}_\lambda(P) - \mathsf{g}_\lambda(Q) \in \mathfrak{a} \quad \text{for } \lambda \vdash^{(p)} n \text{ if } 1 \leqslant n \leqslant N.$$

By (10) 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 $ur \leqslant N$. As in (11), write

$$G_u(P)(t) := \sum_{r=0}^{\infty} \mathsf{g}_{(u)^r}(P)\, t^{ur} \tag{14}$$

and the same for Q. By Proposition 36 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 $up^j \leqslant N$. 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 (12) we have

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

Since the exponential of a sum is the product of corresponding exponentials, we may rewrite the latter (the congruences being modulo t^{N+1}):

$$\begin{aligned} G_u(P)(t) - G_u(Q)(t) &\equiv \exp\Big(\sum_{j=0}^{J} \varepsilon_u \frac{\mathsf{p}_{up^j}(Q)}{up^j}\, t^{up^j}\Big) \exp\Big(\sum_{j=0}^{J} \frac{\varepsilon_u a_j t^{up^j}}{u}\Big) - G_u(Q)(t) \\ &\equiv \exp\Big(\sum_{j=0}^{\infty} \varepsilon_u \frac{\mathsf{p}_{up^j}(Q)}{up^j}\, t^{up^j}\Big) \exp\Big(\sum_{j=0}^{J} \frac{\varepsilon_u a_j t^{up^j}}{u}\Big) - G_u(Q)(t) \\ &= G_u(Q)(t)\Big(\exp\Big(\sum_{j=0}^{J} \frac{\varepsilon_u a_j t^{up^j}}{u}\Big) - 1\Big) \\ &= G_u(Q)(t)\Big(\prod_{j=0}^{J} \exp\Big(\frac{\varepsilon_u a_j}{u}\, t^{up^j}\Big) - 1\Big) \\ &= G_u(Q)(t)\Big(\prod_{j=0}^{J} \Big(1 + \sum_{k=1}^{\infty} \frac{\varepsilon_u^k a_j^k\, t^{kup^j}}{u^k k!}\Big) - 1\Big). \end{aligned} \tag{15}$$

By assumption, $\mathfrak{a}$ is a divided-power ideal (see Section 2.2), so that $a_j^k/k! \in \mathfrak{a}$ for every $k \geqslant 1$. Moreover, $u^{-k} \in \mathbb{Z}_{(p)}$ since u is prime to p. Therefore, for each j, the expression $\displaystyle\sum_{k=1}^{\infty} \frac{\varepsilon_u^k a_j^k\, t^{kup^j}}{u^k k!}$ 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 $A[\![t]\!]$ (Proposition 36), we know that the last expression of (15), 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 (13) in place of (12), so that the analogue of (15) is

$$G_u(P)(t) - G_u(Q)(t) \equiv G_u(Q)(t)\left(\exp\left(\frac{2t^u a_0}{u}\right) \exp\left(\sum_{j=0}^{J} \frac{-a_j t^{up^j}}{u}\right) - 1\right),$$

again modulo t^{N+1}. But the additional term $\exp\left(\frac{2t^u a_0}{u}\right)$ is in $1 + \mathfrak{a}[\![t]\!]$ for the same reason as $\exp\left(\sum_{j=0}^{J} \frac{-a_j t^{up^j}}{u}\right)$.

Therefore Proposition 13 is proved for all primes p. □

6. Representation-Theory Corollaries

Suppose now that A, in addition to being a torsion-free $\mathbb{Z}_{(p)}$-algebra, is a domain and the divided-power ideal $\mathfrak{a}$ is maximal. Then 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 9 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 9; Theorem A is a special case.

Theorem 37. *Let $\mathcal{O}$ be a p-adic DVR with maximal ideal $\mathfrak{m}$ of ramification degree $e \leqslant p-1$ 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 $(M \otimes \mathbb{F})^{\text{ss}} \simeq (N \otimes \mathbb{F})^{\text{ss}}$ as $\mathbb{F}[T]$-modules if and only if for all n with $1 \leqslant n \leqslant d$ we have*

$$\operatorname{tr}(T^n|M) \equiv \operatorname{tr}(T^n|N) \pmod{n\mathfrak{m}}. \tag{16}$$

Proof. 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 10, Theorem 9 under the assumption $\deg P = \deg Q$ tells us that $\overline{P} = \overline{Q}$ in $\mathbb{F}[X]$ if and only if $\mathfrak{p}_n(P) \equiv \mathfrak{p}_n(Q) \mod n\mathfrak{m}$ for all $1 \leqslant n \leqslant d$. The latter condition is equivalent to (16), since $\operatorname{tr}(T^n|M) = \alpha_1^n + \cdots + \alpha_d^n = \mathfrak{p}_n(P)$, and similarly $\operatorname{tr}(T^n|N) = \mathfrak{p}_n(Q)$. The former condition $\overline{P} = \overline{Q}$ is equivalent to $\overline{P}$ and $\overline{Q}$ having the same multiset of roots with multiplicity in some extension of $\mathbb{F}$. But the roots of $\overline{P}$ (respectively, $\overline{Q}$) 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, (16) is equivalent to the statement that, up to reordering, we have equalities

$$\bar{\alpha}_1 = \bar{\beta}_1,\ \bar{\alpha}_2 = \bar{\beta}_2,\ \ldots,\ \bar{\alpha}_d = \bar{\beta}_d. \tag{17}$$

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 (17) is exactly equivalent to the up-to-semisimplification isomorphism $(M \otimes \mathbb{F})^{\mathrm{ss}} \equiv (N \otimes \mathbb{F})^{\mathrm{ss}}$. □

We finally return to the modular form motivation described in the introduction and prove Corollary 2. Recall that for a $\mathbb{Z}_p$-module M we write $\overline{M}$ for $M \otimes \mathbb{F}_p$.

Corollary 38 (Restatement of Corollary 2)**.** *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 $n \geqslant 0$ we have

$$v_p\big(\operatorname{tr}(T^n|M_1) - \operatorname{tr}(T^n|N_1) - \operatorname{tr}(T^n|M_2) + \operatorname{tr}(T^n|N_2)\big) \geqslant 1 + v_p(n). \tag{18}$$

Proof. Using Theorem 37, the condition in (18) is equivalent to the $\mathbb{F}_p[T]$-module isomorphism

$$\big(\overline{M_1 \oplus N_2}\big)^{\mathrm{ss}} \simeq \big(\overline{M_2 \oplus N_1}\big)^{\mathrm{ss}}. \tag{19}$$

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 (19) is equivalent to the isomorphism $W_1^{\mathrm{ss}} \simeq W_2^{\mathrm{ss}}$. □

Remark 39. The congruence for $0 \leqslant n \leqslant \operatorname{rank} M_1 + \operatorname{rank} N_2$ suffices in (18). We further note that Corollary 38 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 $e \leqslant p - 1$ over $\mathbb{Z}_p$.

Acknowledgments. First and foremost we thank Ira Gessel, both for his beautiful proof of Proposition 36 and for allowing us to use it here. We are also grateful to Preston Wake, who patiently and generously listened to an error-riddled early presentation on our motivating application and both pushed and helped us to articulate the precise conditions on the ring A in Theorem 9. We thank John Bergdall for helpful comments. Finally we are grateful to the Max Planck Institute for Mathematics in Bonn, whose generous hospitality allowed us to begin collaborating in 2018 and nurtured the third-named author during the Summer 2021 pandemic reprieve.

References

[1] S. Anni, A. Ghitza, and A. Medvedovsky, $\overline{\rho}$-refined dimensions of Atkin-Lehner eigenspaces, in preparation.

[2] P. Berthelot and A. Ogus, *Notes on crystalline cohomology*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006, reprint of the 1962 original.

[4] S. Lang, *Algebra*, 3rd ed., Springer-Verlag, New York, 2002.

[5] J. Lurie, The Artin-Hasse exponential, 2018.
See https://www.math.ias.edu/~lurie/205notes/Lecture7-Exponential.pdf

[6] I. G. Macdonald, *Symmetric functions and Hall polynomials*, 2nd ed., Oxford University Press, New York, 2015.

[7] M. Romagny, Some useful p-adic formulas.
See https://perso.univ-rennes1.fr/matthieu.romagny/notes/p_adic_formulas.pdf

[8] G. Wiese, Galois representations, 2012.
See https://math.uni.lu/~wiese/notes/GalRep.pdf

Appendix. 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 40 (Brauer-Nesbitt [3, 30.16] or [8, 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. Then the following statements hold.*

(a) (Characteristic polynomial version). The characteristic polynomial map

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

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

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

(c) (Trace version complement). If $\mathrm{char}\, k = p$ then the trace map $r \mapsto \mathrm{tr}(r|V)$ 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 $\mathrm{char}\, k = 0$ or $\mathrm{char}\, k > \dim_k V$, then $(\dim_k V)!$ is invertible in k, so that the power-sum functions determine the relevant elementary symmetric functions over k (Corollary 21), and hence the trace version of Brauer-Nesbitt is equivalent to the characteristic-polynomial version. In the critical positive characteristic case $\mathrm{char}\, k < \dim_k V$, 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 41 (Linear independence of characters (Artin). See, for example, [4, 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 42. *Theorem 41 implies parts (b) and (c) of Theorem 40 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 $\mathrm{tr}(T^n|V) = \mathrm{tr}(T^n|W)$ 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 we have $f_i(V) = f_i(W)$ in k. This simultaneously recovers for $R = k[T]$ both the trace version of Brauer-Nesbitt and its complement. □

The converse – that the trace version of Brauer-Nesbitt together with 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).