DEEP CONGRUENCES + THE BRAUER-NESBITT THEOREM

Samuele Anni
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
Max-Planck-Institut für Mathematik, Bonn, Germany
medvedov@post.harvard.edu

Abstract
We prove that mod-$p$ congruences between polynomials in $\mathbb{Z}_p[\mathbb{Z}_p]$ 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 obtain a refinement of the Brauer-Nesbitt theorem for a single linear operator, motivated by the study of Hecke modules of mod-$p$ modular forms.

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 $\text{tr}(T^n|M)$ as an element of $\mathbb{Z}_p$ for enough $n$ 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...
Deep congruences

\((M \otimes \mathbb{Q}_p)^{ss}\), 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 more than we need: we merely want to understand \(M\) modulo \(p\).

On the other hand, knowing all the \(\text{tr}(T^n|M)\) 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 \(\alpha\) in \(\mathbb{Z}_p\) then for every \(n \geq 0\) we have \(\text{tr}(T^n|M) = p\alpha^n \equiv 0 \mod p\), and we cannot recover \(\alpha\) mod \(p\) from this trace data.

Since knowing \(\text{tr}(T^n|M)\) in \(\mathbb{Z}_p\) is too much and knowing \(\text{tr}(T^n|M)\) modulo \(p\) is not enough, one can ask for some kind of in-between criterion depending on \(\text{tr}(T^n|M)\) 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 \(\text{tr}(T^n|M)\) 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 30). 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 \(\overline{M}^{ss} \simeq \overline{N}^{ss}\) as modules over \(\mathbb{F}_p[T]\) if and only if for every \(n\) with \(1 \leq n \leq d\) we have

\[
\text{tr}(T^n|M) \equiv \text{tr}(T^n|N) \mod pn.
\]

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 \(\overline{M}^{ss}\) and \(\overline{N}^{ss}\) 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 \(\text{tr}(T^p|M) = p\alpha^p \mod p^2\) is tantamount to knowing \(\alpha^p\) modulo \(p\), which in turn determines \(\alpha\) modulo \(p\) uniquely. Yet this information is not enough to pin down \(\alpha\) 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, \(\overline{M}^{ss} \simeq \overline{N}^{ss}\) implies that eigenvalues of \(M\) and \(N\) pair by mod-\(p\) congruence. But the \((p^k)^{\text{th}}\) powers of two mod-\(p\)-congruent elements of \(\mathbb{Z}_p\) are congruent modulo \(p^{k+1}\) (see Lemma 21); 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 30.

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

NB. 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 2 (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 33(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 $\mathbb{Z}(p)$-algebra; for the purposes of this introduction only, we also assume that $A$ is a domain. Let $a \subset A$ be a divided-power ideal — see Section 2.2 for details and discussion, but in short, we must have $a^p \in pa$ for any $a \in a$. For a monic polynomial $P \in A[X]$, write $\overline{P}$ for the image of $P$ in $(A/a)[X]$ and $p_n(P)$ 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** (see Theorem 8). Let $P, Q$ be monic polynomials in $A[X]$. Then

$$\overline{P} = \overline{Q} \text{ in } (A/a)[X] \iff p_n(P) \equiv p_n(Q) \text{ modulo } na$$

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 $a$ 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 Section 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 of $p$-equivalence is the following proposition.

**Proposition C** (see Proposition 29).

Fix a partition $\lambda$ of an integer $n$. Write $C_\lambda$ for the set of partitions of $n$ that are $p$-equivalent to $\lambda$. Then the symmetric function

$$g_\lambda := \sum_{\mu \in C_\lambda} (-1)^\mu \frac{z_\mu p_\mu}{z_\mu}$$

has coefficients in $\mathbb{Z}(p)$. 

Deep congruences

Here \((-1)^\nu\) is the sign in \(S_n\) of any permutation \(\sigma\) with cycle structure \(\mu\), and \(n!/z_\mu\) is the size of the \(S_n\)-conjugacy class of such a \(\sigma\) (Section 3.1); the symmetric function \(p_\mu\) is the product of power-sum functions associated to the parts of \(\mu\) (Section 3.2). For context, the elementary symmetric function \(e_n\) is the sum of the \(g_\lambda\) as \(\lambda\) 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 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 \(\iota_1 : N_1 \hookrightarrow M_1\) and \(\iota_2 : N_2 \hookrightarrow M_2\) and consider the quotients

\[ W_1 := M_1/\iota_1(N_1), \quad W_2 := M_2/\iota_2(N_2). \]

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

\[ v_p\left(\text{tr}(T^n|M_1) - \text{tr}(T^n|N_1) - \text{tr}(T^n|M_2) + \text{tr}(T^n|N_2)\right) \geq 1 + v_p(n). \]

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 is the form of the result that we use in [1] to study the Hecke module 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 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 \(k \geq 4\), 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 1 to prove that, for \(p \geq 5\),

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

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
Deep congruences

$W[1]$ 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.

Leitfaden. Sections 2 to 5 are devoted to the proof of Theorem B. In Section 2, we state Theorem 8, 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 8; 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 8. In the same section we also prove Corollary 1.

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 $e_n(P)$ 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 $e_n(P)$ is the $n$th elementary symmetric function in the $\alpha_i$: namely,

$$e_n(P) = \sum_{1 \leq i_1 < i_2 < \cdots < i_n \leq d} \alpha_{i_1} \cdots \alpha_{i_n}.$$  

Write $p_n(P) := \sum_{i=1}^d \alpha_i^n$ 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 $e_1, \ldots, e_d$, thus defining $p_n(P)$, 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 $A$; in particular, $A$ embeds into $A[\frac{1}{p}] = A \otimes_{\mathbb{Z}(p)} \mathbb{Q}$. We say that an ideal $a$ of $A$ satisfies the divided-power property at some $k \geq 1$ if $a \in a$ implies that $a^k/k!$ is also in $a$. Since $A$ is $\mathbb{Z}$-torsion free and a $\mathbb{Z}(p)$-algebra, this last condition may be reformulated: indeed, we have

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

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

---

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.
Deep congruences

An ideal \(a\) 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 \(a\) satisfying the above condition exactly means that the maps \(\gamma_k: a \to A\) given by \(\gamma_k(a) = \frac{a^k}{k!}\) define a divided-power structure on \(a\) \([2, \S 3]\).

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.** For an ideal \(b\) in a commutative ring \(B\), the following are equivalent

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

(b) For all \(a \in b\) we have \(a^p \in pb\).

**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

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

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

\[a^{p^{k+1}} = (a^{p^k})^p = (p^{v_p(p^k!)}b)^p = p^{pv_p(p^{k+1})}bp.\]

Since \(b \in b\), by the \((b)\) assumption we have \(bp \in pb\). Therefore

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

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 \(a \in b\) again. Since we have shown that for every \(i\) we have \(a^{p^i} \in p^{v_p(p^i!)}b\), we have \(a^{n_i p^i} \in p^{n_i v_p(p^i!)}b\), so that \(a^n \in p^{\sum_{i=0}^k n_i v_p(p^i!)}b\). The desired statement follows by observing that

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

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 3.**
The ideal \(a \subseteq A\) is a divided-power ideal if and only if \(a^p \in pa\) for every \(a \in a\).

In fact, it suffices to check the condition of **Corollary 3** on generators.

**Proposition 4.** Let \(S \subseteq A\) be a subset. Then the ideal \(a\) generated by \(S\) is a divided-power ideal if and only if \(a^p \in pa\) for every \(a \in S\).
Deep congruences

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 $pa$, then so is $(b_1a_1 + b_2a_2)^p$. We expand

$$(b_1a_1 + b_2a_2)^p = b_1^pa_1^p + \sum_{k=1}^{p-1} \binom{p}{k} b_1^ka_1^kb_2^{p-k}a_2^{p-k} + b_2^pa_2^p.$$ 

The first and last terms are in $pa$ by assumption; the middle terms because $p \mid \binom{p}{k}$. □

Corollary 5. If $a \subset A$ is a divided-power ideal, then so is $ab$ for any ideal $b \subseteq A$.

Proof. For $a \in a$, $b \in b$ we have $(ab)^p = a^pb^p \in (pa)b^p \subseteq p(ab)$. Then Proposition 4. □

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 $p$; 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 6.
An ideal $a$ of a $p$-adic DVR is a divided-power ideal if and only if $v_p(a) \geq \frac{1}{p-1}$.

Proof. Let $a \in a$ be a generator, so that $v_p(a) = v_p(a)$. By Proposition 4, the ideal $a$ is a divided-power ideal if and only if $a^p \in pa$, which happens in our $p$-adic DVR setting if and only if

$$pv_p(a) = v_p(a^p) \geq v_p(pa) = 1 + v_p(a);$$

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

Corollary 7. Let $m$ be the maximal ideal of a $p$-adic DVR $\mathcal{O}$. Let $e$ be the ramification degree of $m$ over $p$. Then $m$ 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 6 as $v_p(m) = \frac{1}{e}$ in this setting. □
2.4. Statement of the main theorem

We are ready to state the fullest version of Theorem B.

**Theorem 8.** Let $A$ be a torsion-free $\mathbb{Z}(p)$-algebra and $a$ a divided-power ideal, and let $P, Q$ be monic polynomials in $A[X]$. Then the following are equivalent:

(a) $e_n(P) \equiv e_n(Q) \pmod{a}$ for every $n \geq 1$;
(b) $e_n(P) \equiv e_n(Q) \pmod{a}$ for every $n$ with $1 \leq n \leq \max\{\deg P, \deg Q\}$;
(c) $p_n(P) \equiv p_n(Q) \pmod{na}$ for every $n \geq 1$;
(d) $p_n(P) \equiv p_n(Q) \pmod{na}$ for every $n$ with $1 \leq n \leq \max\{\deg P, \deg Q\}$.

**Remark 9.** We do not require $\deg P = \deg Q$ here. In fact, since the statement $\deg P = \deg Q$ is the same as the congruence $p_n(P) \equiv p_n(Q) \pmod{na}$ 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 8:

(e) $P = Q$ in $(A/a)[X]$. \qed

**Example 10.** Let $p = 2$ and $A = \mathbb{Z}_p$; given the polynomials $P = X^2 + X + 3$ and $Q = X^4 + 3X^3 + 5X^2 + 2X + 6$, we have

| $n$ | $e_n(P)$ | $e_n(Q)$ | $p_n(P)$ | $p_n(Q)$ | $v_2(p_n(Q) - p_n(P))$ | $1 + v_2(n)$ |
|-----|----------|----------|----------|----------|------------------------|-------------|
| 0   | 1        | 1        | 2        | 4        | 2                      | $\infty$    |
| 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           |

From matching up coefficients (or from the fact that $Q = (X^2 + 2X)P - (4X - 6)$), it is clear that $e_n(P) \equiv e_n(Q) \pmod{2}$ for every $n \geq 1$. In the table above, the last two columns illustrate Theorem 8:

$$v_2(p_n(Q) - p_n(P)) \geq 1 + v_2(n) \quad \text{for } n \geq 1.$$ \qed
We now give a skeleton proof of Theorem 8. Technical details are postponed to Sections 4 and 5.

**Proof of Theorem 8.** We clearly have (c) $\implies$ (d) and (a) $\implies$ (b); moreover since $e_n(P) = 0$ 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 11.** Fix $N \geq 1$. If $e_n(P) \equiv e_n(Q) \mod a$ for all $1 \leq n \leq N$, then $p_n(P) \equiv p_n(Q) \mod Na$.

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

**Proposition 12.** Fix $N \geq 1$. If $p_n(P) \equiv p_n(Q) \mod na$ for all $1 \leq n \leq N$, then $e_n(P) \equiv e_n(Q) \mod a$ 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 $a$ is crucial to both directions of Theorem 8. We illustrate this point by giving two counterexamples in the absence of this property. In both Example 13 and Example 14 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 $m$ of $\mathcal{O}$ is not a divided-power ideal (Corollary 7), having ramification degree $p$. In both cases, $P$ and $Q$ have the same degree $p$, so statements (a) and (b) of Theorem 8 are equivalent to the equality $P = Q$ in $F_p[X]$.

**Example 13.** 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 $m$. But $p_\alpha(P) = \alpha^p = p$ has $p$-valuation 1, and is not congruent to $p_\alpha(Q) = 0$ modulo $pm$, which has valuation $1 + \frac{1}{p}$. Thus statements (a) and (b) of Theorem 8 hold but (c) and (d) do not.

**Example 14.** Consider $P = (X - (\alpha + p - 1))(X + 1)^{p-1}$ and $Q = X^p$. Then $P$ and $Q$ are not congruent modulo $m$: indeed, the roots of $P$ are units in $\mathcal{O}$ whereas $Q$ has only zero as a root with multiplicity. But we show that $p_n(P) \equiv p_n(Q) \equiv 0 \mod nm$ for $1 \leq n \leq p$.

Indeed, for any $n \geq 1$,

$$p_n(P) = (\alpha + (p - 1))^{n} + (p - 1)(-1)^n$$

$$= \alpha^n + \sum_{i=1}^{n-1} \binom{n}{i} \alpha^i (p - 1)^{n-i} + (p - 1)^n + (p - 1)(-1)^n$$

$$= (\text{terms divisible by } \alpha) + (p - 1)^n + (p - 1)(-1)^n.$$
Deep congruences

Since \((p - 1)^n + (p - 1)(-1)^n \equiv (-1)^n - (-1)^n = 0\) modulo \(p = \alpha^p\), we have \(p_n(P) \equiv 0\) modulo \(m\).

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
\[
\alpha^p + (p - 1)p + (p - 1)(-1)^p = p + (p - 1)^2 - (p - 1) = (p - 1)^2 - (-1) \equiv 0 \mod p^2,
\]
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 21 below). And if \(p = 2\) then
\[
p + (p - 1)^p + (p - 1)(-1)^p = 2 + (-1)^2 + (1)(-1)^2 = 4.
\]

In either case, \(p_n(P)\) is a sum of a term in \(m^{p+1}\) and a term in \(m^{2p}\), so \(p_n(P) \in p\), as required. Thus statement \((d)\) of Theorem 8 holds but \((a)\) and \((b)\) do not. One can show analogously that \((c)\) also does not hold, as \(v_p(p_{2p}(P)) = 1\). \(\triangle\)

Questions. One can further ponder the relationship between the statements in Theorem 8:

- Is there a direct proof of \((d) \implies (c)\)? The divided-power property or a similar assumption must play a role, as Example 14 above satisfies \((d)\) but not \((c)\).
- Although \((d)\) does not imply \((a)\) or \((b)\) without the divided-power assumption (again, see Example 14 above), is it possible that \((c)\) does? \(\triangle\)

The next three sections are devoted to the proof of Theorem 8.

3. Combinatorial preliminaries

3.1. Partitions

A partition \(\lambda\) 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 \(\lambda_i\) are nonzero. The number of nonzero parts of \(\lambda\) is exactly the cardinality of \(\{i \geq 1 : \lambda_i > 0\}\). There is a unique partition of \(0\), namely \(\emptyset \vdash 0\), 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 \(\lambda\).
- For \(\lambda \vdash n\), let \((-1)^\lambda\) be the sign of a permutation in \(S_n\) with cycle structure \(\lambda\). 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 \( \lambda \), so that \( n!/z_\lambda \) is the number of permutations of \( n \) with cycle structure \( \lambda \). Accordingly, \( z_\emptyset = 1 \).

For \( n \geq 0 \), let \( P_n \) be the set of partitions of \( n \), and let \( \mathcal{P} := \bigcup_{n \geq 0} P_n \) be the set of all partitions, graded by weight. We can multiply two partitions as follows: for \( \lambda \) partition \( \{n \} \) for the integer \( \lambda \in \mathbb{N} \) of permutations of cycle structure \( \lambda \). 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 \( \lambda \) 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 \( \lambda \) as a \( (p^v)^{th} \) power: \( \lambda = \mu^{p^v} \), where \( \mu = (\lambda_1/p^v, \lambda_2/p^v, \ldots) \). Of course \( v_p(\emptyset) = \infty \). \( \square \)

### 3.2. Ring of symmetric functions

Let \( \Lambda_d \) be the ring of symmetric polynomials in \( d \) variables \( x_1, x_2, \ldots, x_d \) with integer coefficients: that is, \( \Lambda_d \) 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 \( \Lambda_d \) 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 \( \Lambda_d \rightarrow \Lambda_{d'} \) 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 \( \Lambda \) 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 \( e_{n,d} \in \Lambda^d_n \) be the \( n^{th} \) elementary symmetric polynomial:

\[
e_{n,d} := \sum_{1 \leq i_1 < i_2 < \cdots < i_n \leq d} x_{i_1} \cdots x_{i_n},
\]

and let \( e_n := \varprojlim_d e_{n,d} \in \Lambda^n \) be the \( n^{th} \) elementary symmetric function. In particular \( e_0 = e_{n,d} = 1 \). One can check — for example, see [6, I.2.4] — that

\[
\Lambda = \mathbb{Z}[e_1, e_2, \ldots].
\]  \( \tag{3} \)

• **Power-sum symmetric functions:** Similarly, for \( n \geq 0 \), let \( p_{n,d} \in \Lambda^d_n \) be
the \( n \)th power-sum polynomial:

\[
p_{n,d} := \sum_{i=1}^{d} x_i^n \in \Lambda_d^n.
\]

For \( n \geq 1 \) we also let \( p_n := \lim_{d \to \infty} p_{n,d} \in \Lambda^n \) be the \( n \)th power-sum function. Note that \( p_0, d = d \), so that these do not interpolate and \( p_0 \) is not defined.

One can check that \( \Lambda_Q = \mathbb{Q}[p_1, p_2, \ldots] \); see, for example, [6, I.2.12].

- **Symmetric functions depending on partition:** We use the following standard notation: given a family of symmetric functions \( \{f_n\}_{n \geq 1} \) — 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 \( f_\lambda \) as a map \( (n) \mapsto f_n \) and extend it to a map of multiplicative monoids \( \mathcal{P} \to \Lambda \). Note that \( f_\emptyset = 1 \). In particular, although \( p_0 \) is undefined, we do have \( p_\emptyset = e_\emptyset = e_0 = 1 \). We can also use the notation \( f_\lambda \) for any tuple \( \lambda \), not necessarily a partition. One can check that \( \{e_\lambda\}_{\lambda \vdash n} \) is a \( \mathbb{Z} \)-basis for \( \Lambda^n \) and \( \{p_\lambda\}_{\lambda \vdash n} \) is a \( \mathbb{Q} \)-basis for \( \Lambda^n_Q \).

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

\[
e_n(Q) := \begin{cases} 
1 & \text{if } n = 0 \\
(-1)^n a_n & \text{if } 1 \leq n \leq d \\
0 & \text{if } n > d.
\end{cases}
\]

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) to write \( f \) as a polynomial in the \( e_n \) and let \( f(Q) \) be the result of plugging \( e_n(Q) \) 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 \( p_0(Q) := \deg Q \). With this definition, the sequence \( \{p_n(Q)\}_{n \geq 0} \) 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

\[
P_S(t) := \sum_{s \in S} (-1)^{s-1} \frac{P_s}{s} t^s
\]
be the weighted and signed power-sum generating function. Also set \( P(t) := P_N(t) \).
On one hand, we can interpret the exponential of \( P_S(t) \) 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 15.** Let \( S \subseteq \mathbb{N} \) be a set of positive integers. Then

\[
\exp P_S(t) = \sum_{n=0}^{\infty} \sum_{\lambda \vdash n \text{ parts in } S} (-1)^{\lambda} \frac{P_\lambda}{z_\lambda} t^n.
\]

**Proof.**

\[
\exp P_S(t) = \exp \left( \sum_{s \in S} (-1)^{s-1} \frac{P_s}{s} t^s \right) = \prod_{s \in S} \exp \left( (-1)^{s-1} \frac{P_s}{s} t^s \right) = \prod_{s \in S} \sum_{r_s=0}^{\infty} \frac{1}{r_s!} (-1)^{r_s(s-1)} \frac{P_s^{r_s}}{s^{r_s}} t^{sr_s} = \sum_{(r_s) \in \mathbb{N}^S} (-1)^{\sum_s r_s(s-1)} \frac{\prod_{s} P_s^{r_s}}{\prod_{s} r_s! s^{r_s}} t^{\sum_s sr_s} = \sum_{\lambda \text{ has parts in } S} (-1)^{\lambda} \frac{P_\lambda}{z_\lambda} t^{\lambda}.
\]

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 \( \lambda \) 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 \( \exp P_S(t) \) as the generating function for the elementary symmetric functions. Let

\[
E(t) := \sum_{k \geq 0} e_k t^k = \prod_{i=1}^{\infty} (1 + x_i t).
\]

The remaining statements of this section are completely standard.

**Proposition 16.** \( E(t) = \exp P(t) \).

**Proof.** We show that \( \log E(t) = P(t) \):

\[
\log E(t) := \log \prod_{i=1}^{\infty} (1 + x_i t) = \sum_{i=1}^{\infty} \log (1 + x_i t) = \sum_{i=1}^{\infty} \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(x_i t)^n}{n} = \sum_{n=1}^{\infty} (-1)^{n-1} t^n \sum_{i=1}^{\infty} x_i^n = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{P_n}{n} t^n = P(t).
\]
Proposition 16 allows us to express $e_n$ as a $\mathbb{Q}$-linear combination of the $p_{\lambda}$ for $\lambda \vdash n$, and, conversely, $p_n$ as a $\mathbb{Z}$-linear combination of $e_{\lambda}$ over $\lambda \vdash n$: see Corollary 17 and Corollary 18.

**Corollary 17** (Expressing $e_n$ in terms of $p_{\lambda}$). For all $n \geq 0$, we have

$$e_n = \sum_{\lambda \vdash n} (-1)^{\lambda} \frac{p_{\lambda}}{z_{\lambda}}.$$  \hfill (4)

For example, $e_2 = \frac{p_1^2 - p_2}{2}$ and $e_3 = \frac{p_1^3 - 3p_1p_2 + 2p_3}{6}$.

**Proof.** Combining Proposition 16 with Proposition 15 for $S = \mathbb{N}$ yields

$$\sum_{\lambda} (-1)^{\lambda} \frac{p_{\lambda}}{z_{\lambda}} = \sum_{n=0}^{\infty} e_n t^n.$$

The statement follows from considering the coefficients of $t^n$ on each side. \hfill \Box

**Corollary 18** (Expressing $p_n$ in terms of $e_{\lambda}$). For $n \geq 1$, we have

$$p_n = (-1)^n n \sum_{\lambda \vdash n} \frac{(-1)^m}{m} \left( \frac{m}{r_1(\lambda), r_2(\lambda), \ldots} \right) e_{\lambda},$$  \hfill (5)

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

**Proof.** From Proposition 16 we have

$$\sum_{n=0}^{\infty} (-1)^{n-1} \frac{p_n}{n} t^n = P(t) = \log E(t) = \log \left( 1 + \sum_{k=1}^{\infty} e_k t^k \right)$$

$$= \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \left( \sum_{k=1}^{\infty} e_k t^k \right)^m = \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \sum_{1 \leq k_1, \ldots, k_m} e_{k_1} \cdots e_{k_m} t^{k_1+\ldots+k_m},$$

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 $\lambda$ of $\sum k_i$ into $m$ parts, with $r_a(\lambda)$ of the $k_i$s equal to $a$ and $m = \sum_{a} r_a(\lambda)$. Moreover, each such partition $\lambda$ 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,

$$p_n = (-1)^{n-1} n \sum_{m \geq 1} \sum_{\lambda \vdash n \text{ with } m \text{ parts}} \frac{(-1)^{m-1}}{m} \left( \frac{m}{r_1(\lambda), r_2(\lambda), \ldots} \right) e_{\lambda}. \hfill \Box$$
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 $E$.

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

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

we note that we still have $P(M, t) = \log E(M, t)$ as in Proposition 16, so that we may proceed as follows:

$$M^{ss} \simeq N^{ss} \iff \text{for all } 1 \leq n \leq d \text{ we have } e_n(M) \equiv e_n(N) \mod p$$

$$\iff E(M, t) \equiv E(N, t) \mod p\mathbb{Z}_p[t]$$

$$\iff E(M, t) = E(N, t) S(t) \text{ for some } S(t) \in 1 + tp\mathbb{Z}_p[t]$$

$$\iff \log E(M, t) = \log E(N, t) + \log S(t)$$

$$\iff P(M, t) = P(N, t) + R(t) \text{ for some } R(t) \in tp\mathbb{Z}_p[t]$$

$$\iff \text{for all } n \geq 1 \text{ we have } p_n(M) \equiv p_n(N) \mod np$$

$$\iff \text{for all } n \geq 1 \text{ we have } \text{tr}(T^n|M) \equiv \text{tr}(T^n|N) \mod np.$$

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 $a$ (see Section 2.2 for definitions), and the assumption rank $M = \text{rank } N$ relaxed.

3.5. $p$-valuation lemmas

Here we collect a few lemmas about $p$-valuations. First, in light of the expression in Corollary 18 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

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

expressing multinomial coefficients in terms of binomial coefficients.

Theorem 19 (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 $p$. 

Deep congruences

15
Deep congruences

Corollary 20. 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 22 below) is a partition version of the standard observation that the depth of the $p$-adic congruence of two integers increases upon taking $p^\text{th}$ powers.

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

Lemma 21. Suppose $x \equiv y \mod a$ for some $x, y \in A$. Then

(a) for all $m \geq 0$ we have $x^{p^m} \equiv y^{p^m} \mod p^ma$; more generally
(b) for all $n \geq 0$ we have $x^n \equiv y^n \mod na$.

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

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

We show that each of the terms on the right-hand side is in $pa$. This is clear for each term in the summation because for $0 < i < p$ we have both $p \mid \binom{p}{i}$ and $a^i \in a$.

Corollary 3 tells us that $a^p \in pa$. To prove the statement for $m > 1$ we proceed by induction using Corollary 5. □

Corollary 22. Let $P, Q \in A[X]$ be polynomials, and $\{f_n\}_{n \geq 1}$ a family of symmetric functions. If $f_n(P) \equiv f_n(Q) \mod a$ for all $n$, then for every partition $\lambda$

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

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

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

where the middle congruence modulo $p^va$ holds by Lemma 21. □
3.6. Artin-Hasse exponential series

We briefly recall the Artin-Hasse exponential series

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

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 25); here we briefly review this well-known result. We follow the convenient expository notes [5] of Jacob Lurie.

**Proposition 23.** We have

\[ F(z) = \prod_{p \nmid d} \left( 1 - z^d \right)^{-\mu(d)}. \]

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

\[ \sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases} \quad (6) \]

Before giving the proof of Proposition 23, we need a lemma:

**Lemma 24.** For prime \( p \) we have

\[ \sum_{d \mid n, p \nmid d} \mu(d) = \begin{cases} 1 & \text{if } n \text{ is a power of } p \\ 0 & \text{otherwise.} \end{cases} \]

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

\[ \phi(n) := \sum_{d \mid n, p \nmid d} f(n) \]

is also multiplicative. Indeed, say a divisor \( d \) of \( n \) is \( p \)-deprived if \( p \nmid d \). 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 \( \mu \) 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). \( \square \)
Proof of Proposition 23. We have
\[
\log \prod_{p|d} \left( 1 - z^d \right)^{-\frac{\mu(d)}{d}} = \sum_{p|d} \frac{\mu(d)}{d} \log \frac{1}{1 - z^d} = \sum_{p|d} \frac{\mu(d)}{d} \sum_{k \geq 1} \frac{z^{dk}}{k} = \sum_{n \geq 1} \frac{z^n}{n} \frac{\mu(d)}{d} = \sum_{n=p^j, j \geq 0} \frac{z^n}{n},
\]
where the last equality follows from Lemma 24. The claim follows.

Corollary 25. The Artin-Hasse exponential series \( F(z) \) is in \( \mathbb{Z}(z) \).

Proof. The coefficients of \( (1 - z^d)^{\pm 1/d} \) in the expression in Proposition 23 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 11: \( e_n \) congruent implies \( p_n \) deeply congruent

Here we prove Proposition 11. The proof uses the combinatorial expression from Corollary 18 for \( p_n \) in terms of \( e_\lambda \).

Proof of Proposition 11. Let \( P, Q \in A[\mathbb{F}] \) be monic polynomials, fix \( N \geq 1 \), and suppose that \( e_n(P) \equiv e_n(Q) \) modulo \( a \) for all \( n \) with \( 1 \leq n \leq N \). We seek to show that \( p_N(P) \equiv p_N(Q) \) modulo \( a \).

From Corollary 18 we have
\[
p_N(P) - p_N(Q) = (-1)^N N \sum_{m \geq 1} \sum_{\lambda \vdash N with \( m \) parts} \frac{(-1)^m}{m} \left( \begin{array}{c} m \\ r_1(\lambda), r_2(\lambda), \ldots \end{array} \right) (e_\lambda(P) - e_\lambda(Q)).
\]

Corollary 22 for \( f = e \) tells us that our assumptions on the \( e_n \) imply that the difference \( e_\lambda(P) - e_\lambda(Q) \) is in \( p^{v_p(\lambda)}a \) for each relevant \( \lambda \). Therefore it suffices to show that for every \( \lambda \vdash N \) with \( m \) parts,
\[
v_p(N) - v_p(m) + v_p \left( \begin{array}{c} m \\ r_1(\lambda), r_2(\lambda), \ldots \end{array} \right) + v_p(\lambda) \geq v_p(N),
\]
or, equivalently, canceling \( v_p(N) \) and using the definition of \( v_p(\lambda) \), that for every \( i \),
\[
-v_p(m) + v_p \left( \begin{array}{c} m \\ r_1(\lambda), r_2(\lambda), \ldots \end{array} \right) + v_p(r_i(\lambda)) \geq 0.
\]
But this is exactly Corollary 20.

Incidentally, although we know from the fact that the \( e_\lambda \) are a \( \mathbb{Z} \)-basis for \( \Lambda \) in (5) that \( \frac{m}{n} \left( r_1, r_2, \ldots \right) \) is always integral — here of course \( r_1, r_2, \ldots \) is a sequence of nonnegative integers almost all zero, \( m = \sum r_i \) and \( n = \sum ir_i \) — it is not a priori obvious. But this integrality does follow from Corollary 20.
5. Proof of Proposition 12: \( p_n \) deeply congruent implies \( e_n \) congruent

Here we give the first, combinatorial, proof of the “if” direction of Theorem 8: 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 \( n \geq 0 \).

**Definition.**

- If \( \lambda \) and \( \mu \) are in \( \mathcal{P}_n \), we say that \( \mu \) is a \( p \)-splitting of \( \lambda \) if \( \lambda \) contains an instance of the part \( pu \) for some \( u \geq 1 \), and \( \mu \) is obtained from \( \lambda \) by replacing \( pu \) with \( p \) copies of part \( u \). In other words, for every \( u \in \mathbb{N} \), the partition \( (\lambda)_{p^u} \) is a \( p \)-splitting of \( (\lambda u) \), and if \( \mu \) is a \( p \)-splitting of \( \lambda \), then \( \mu \nu \) is a \( p \)-splitting of \( \lambda \nu \).

- Let \( \sim_p \)-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 \( \lambda \).

- Call a partition \( \lambda \) of \( n \) \( p \)-deprived if none of its parts are divisible by \( p \). The empty partition \( \emptyset \) is a \( p \)-deprived partition of 0 for every \( p \). Write \( \lambda \vdash_{-p} n \) for a \( p \)-deprived partition \( \lambda \) of \( n \). \( \triangle \)

**Example 26.** Let \( u \geq 1 \) be prime to \( p \) and let \( r \geq 0 \). Then the partition \( (\lambda u)^r \) is \( p \)-deprived and

\[
C_{(\lambda u)^r} = \{ \lambda \vdash ur : \lambda \text{ has parts in } \{ up^j : j \geq 0 \} \}.
\]

\( \triangle \)

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

\[
\mathcal{P}_n = \{ \lambda \vdash n \} = \bigsqcup_{\lambda \vdash_{-p} n} C_\lambda.
\] (7)

5.2. The contribution to \( e_n \) from a single \( p \)-equivalence class

Fix \( n \geq 0 \) and \( \lambda \vdash n \). Let

\[
g_\lambda := \sum_{\mu \sim_p \lambda} (-1)^{\mu} \frac{p_\mu}{z_\mu},
\] (8)

so that in particular \( g_{\emptyset} = 1 \). In other words, \( g_\lambda \) is the piece of the expression for \( e_n \) from (4) that comes from all the partitions that are \( p \)-equivalent to \( \lambda \). Because of (7), for any \( n \geq 0 \),

\[
e_n = \sum_{\lambda \vdash_{-p} n} g_\lambda.
\] (9)

To show that \( e_n(P) \equiv e_n(Q) \pmod{a} \) in Proposition 12, it will therefore suffice to establish that \( g_\lambda(P) \equiv g_\lambda(Q) \pmod{a} \) for every \( \lambda \vdash_{-p} n \). But in fact we can break these up further:
Lemma 27. Suppose \( \lambda \vdash (p) n, \mu \vdash (p) m \) are partitions of \( n, m \geq 0 \) with no common parts. Then
\[
\mathcal{g}_{\lambda \mu} = \mathcal{g}_\lambda \mathcal{g}_\mu.
\]
Thus for \( \lambda \vdash (p) n \),
\[
\mathcal{g}_\lambda = \prod_{u \geq 1, p \not| u} \mathcal{g}_{(u)^{r_{\lambda}(u)}}.
\]

Proof. Any two partitions \( \lambda \) and \( \mu \), whether disjoint or not, satisfy \( p_{\lambda \mu} = p_\lambda p_\mu \) and \( (-1)^{\lambda \mu} = (-1)^\lambda (-1)^\mu \). If \( \lambda \) and \( \mu \) have no parts in common, then \( z_{\lambda \mu} = z_\lambda z_\mu \). And finally if both \( \lambda \) and \( \mu \) 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 \( \mathcal{g}_\lambda(P) \equiv_a \mathcal{g}_\lambda(Q) \) for every \( \lambda \vdash (p) n \), it suffices to show that
\[
\mathcal{g}_{(u)^r}(P) \equiv_a \mathcal{g}_{(u)^r}(Q)
\]
for every \( ur \leq n \) where \( r \geq 0 \) and \( u \geq 1 \) is prime to \( p \). We prove this in Section 5.4 after establishing a \( p \)-integrality result for the symmetric function \( \mathcal{g}_\lambda \).

5.3. \( p \)-integrality of \( \mathcal{g}_\lambda \)

First note that the signs \( (-1)^\mu \) in the definition of \( \mathcal{g}_\lambda \) are the same for every \( \mu \sim_p \lambda \) for odd \( p \). In other words,

Lemma 28. If \( p \) is odd, then \( \mathcal{g}_\lambda = (-1)^\lambda \sum_{\mu \sim_p \lambda} \frac{p_\mu}{z_\mu} \).

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:
\[
(-1)^{(up^j)} = (-1)^{up^j-1} = (-1)^{u-1} = (-1)^{p^j(u-1)} = (-1)^{(up)^j}.
\]
Then extend multiplicatively.

From the definition in (8) it is clear that \( \mathcal{g}_\lambda \) is in \( \Lambda_Q \). However, one can show that \( \mathcal{g}_\lambda \) is \( p \)-integral as a symmetric function.

Proposition 29. For any partition \( \lambda \vdash n \geq 0 \), we have \( \mathcal{g}_\lambda \) in \( \Lambda_{Z(p)} \).

The following elegant argument is due to Gessel.

Proof. Since every equivalence class \( C_\lambda \) has a unique representative with prime-to-\( p \) parts, it suffices to consider \( \mathcal{g}_\lambda \) for \( \lambda \vdash (p) n \). By Lemma 27, it suffices to show that
for any \( u \) prime to \( p \) and any \( r \geq 0 \), we have \( g(u)^r \in \Lambda_{\mathbb{Z}(p)} \). Equivalently, it suffices to show that for any \( u \) prime to \( p \), the generating function

\[
G_u(t) := \sum_{r=0}^{\infty} g(u)^r t^r
\]

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 25).

For \( p \) odd, let \( \varepsilon_u = (-1)^{u-1} \) be the sign of \( (up^j) \) for \( j \geq 0 \) (Lemma 28). Then

\[
G_u(t) = \exp \left( \sum_{j=0}^{\infty} \frac{\varepsilon_u \cdot p_{up^j}^{u \cdot p^j}}{up^j} \right) = \exp \left( \frac{\varepsilon_u}{u} \sum_{j=0}^{\infty} t^{up^j} \left( \frac{x_1^{up^j} + x_2^{up^j} + \cdots}{p^j} \right) \right)
\]

\[
= F(x_1^{ut})^{\varepsilon_u/u} F(x_2^{2ut})^{\varepsilon_u/2u} \cdots,
\]

where the first equality is Proposition 15 for the set \( S = \{up^j : j \geq 0\} \) (see Example 26). Since \( F(x_1^{ut}) \) has coefficients in \( \mathbb{Z}(p) \) and constant coefficient 1, and since binomial coefficients \( \binom{\varepsilon_u/u}{m} \) are in \( \mathbb{Z}_1^{1,1} \subset \mathbb{Z}(p) \), each \( F(x_1^{ut})^{\varepsilon_u/u} \) is in \( \mathbb{Z}(p)[x_1, t] \), so that \( G_u(t) \) is in \( \mathbb{Z}(p)[t, x_1, x_2, \ldots] \). We already know it to be in \( \Lambda_Q[t] \), 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 \( p = 2 \),

\[
G_u(t) = \exp \left( \frac{2t^u p_u}{u} - \sum_{j=0}^{\infty} \frac{t^{up^j} p_{up^j}}{up^j} \right)
\]

\[
= \left( \sum_{k=0}^{\infty} \frac{2^k}{k! k!} p_u^k t^{uk} \right) F(x_1^{u t})^{-1/u} F(x_2^{2 ut})^{-1/2u} \cdots.
\]

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

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

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 12

Recall that we assume that \( p_n(P) - p_n(Q) \in n \mathfrak{a} \) for all \( n \) with \( 1 \leq n \leq N \); we aim to show that \( e_n(P) - e_n(Q) \in \mathfrak{a} \) 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
\[ g_\lambda(P) - g_\lambda(Q) \in a \quad \text{for } \lambda \vdash (p) \text{ if } 1 \leq n \leq N; \]
by (10) it suffices to prove that \( g(u)^r(P) - g(u)^r(Q) \in a \) for all \( u \) prime to \( p \) and all \( r \) with \( ur \leq N \). As in (11), write
\[
G_u(P)(t) := \sum_{r=0}^{\infty} g(u)^r(P) t^ur
\]
and the same for \( Q \). By Proposition 29 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
\[
G_u(P)(t) - G_u(Q)(t) \in a[t] + (t^{N+1})
\]
under the assumption that \( p_{ap^j}(P) - p_{ap^j}(Q) = p^j a_j \) for some \( a_j \in a \) for every \( j \) with \( ap^j \leq N \). 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
\[
G_u(P)(t) - G_u(Q)(t) = \exp \left( \sum_{j=0}^{\infty} \varepsilon_u \frac{p_{apj}(P)}{up^j} t^up^j \right) - G_u(Q)(t)
\]
\[ = \exp \left( \sum_{j=0}^{J} \varepsilon_u \frac{p_{apj}(Q) + p^j a_j}{up^j} t^up^j \right) - G_u(Q)(t) \mod t^{N+1}. \]
Since the exponential of a sum is the product of corresponding exponentials, we may rewrite the latter (the congruences being modulo \( t^{N+1} \)):
\[
G_u(P)(t) - G_u(Q)(t) \equiv \exp \left( \sum_{j=0}^{J} \varepsilon_u \frac{p_{apj}(Q)}{up^j} t^up^j \right) \exp \left( \sum_{j=0}^{J} \varepsilon_u a_j t^up^j \right) - G_u(Q)(t)
\]
\[ \equiv \exp \left( \sum_{j=0}^{\infty} \varepsilon_u \frac{p_{apj}(Q)}{up^j} t^up^j \right) \exp \left( \sum_{j=0}^{J} \varepsilon_u a_j t^up^j \right) - G_u(Q)(t)
\]
\[ = G_u(Q)(t) \left( \exp \left( \sum_{j=0}^{J} \frac{\varepsilon_u a_j t^up^j}{u} \right) - 1 \right)
\]
\[ = G_u(Q)(t) \left( \prod_{j=0}^{J} \exp \left( \frac{\varepsilon_u a_j}{u} t^up^j \right) - 1 \right)
\]
\[ = G_u(Q)(t) \left( \prod_{j=0}^{J} \left( 1 + \sum_{k=1}^{\infty} \frac{\varepsilon_u a_j k t^up^j}{u^k k!} \right) - 1 \right). \]

By assumption, \( a \) is a divided-power ideal (Section 2.2), so that \( a_k^p/k! \in a \) for every \( k \geq 1 \). Moreover \( u^{-k} \in \mathbb{Z}((p)) \) since \( u \) is prime to \( p \). Therefore, for each \( j \), the
expression \[ \sum_{k=1}^{\infty} \frac{\varepsilon_k a_k t^{k+1}}{u^k k!} \] is in \( a[t] \); and hence the same is true for all of
\[ \prod_{j=0}^{J} \left( 1 + \sum_{k=1}^{\infty} \frac{\varepsilon_k a_k t^{k+1}}{u^k k!} \right) - 1. \]
Finally, since \( G_u(Q)(t) \) in \( A[t] \) (Proposition 29), we know that the last expression of (15), and thus \( G_u(P)(t) - G_u(Q)(t) \), is in \( a[t] \) modulo \( t^{N+1} \), as required.

For \( p = 2 \), use (13) in place of (12), so that the analogue of (15) is
\[ G_u(P)(t) - G_u(Q)(t) \equiv G_u(Q)(t) \left( \exp \left( \frac{2t^u a_0}{u} \right) \exp \left( \sum_{j=0}^{J} -a_j t^{u^j} \right) - 1 \right), \]
again modulo \( t^{N+1} \). But the additional term \( \exp \left( \frac{2t^u a_0}{u} \right) \) is in \( 1 + a[t] \) for the same reason as \( \exp \left( \sum_{j=0}^{J} -a_j t^{u^j} \right) \).

Therefore Proposition 12 is proved for all primes \( p \).

6. Representation theory corollaries

In the case where \( A \), in addition to being a torsion-free \( \mathbb{Z}_p \)-algebra, is a domain and the divided-power ideal \( a \) 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 8 then becomes a statement about congruences between traces of \( T^n \) implying isomorphisms between semisimplified \( (A/a)[T] \)-modules.

We focus on the case where \( A = \mathcal{O} \) is a \( p \)-adic DVR and \( a = m \) is its maximal ideal to state the following representation-theoretic version of Theorem 8; Theorem A is a special case.

**Theorem 30.** Let \( \mathcal{O} \) be a \( p \)-adic DVR with maximal ideal \( m \) 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 \( (M \otimes \mathcal{F})^{ss} \cong (N \otimes \mathcal{F})^{ss} \) as \( \mathcal{F}[T] \)-modules if and only if for all \( n \) with \( 1 \leq n \leq d \) we have
\[ \text{tr}(T^n|M) \equiv \text{tr}(T^n|N) \pmod{nm} \].

**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 9, Theorem 8 under the assumption \( \deg P = \deg Q \) tells us that \( T = Q \) in \( \mathcal{F}[X] \) if and only if \( p_n(P) \equiv p_n(Q) \pmod{nm} \) for all \( 1 \leq n \leq d \). The
Deep congruences

latter condition is equivalent to (16), since \( \text{tr}(T^n|M) = \alpha_1^n + \cdots + \alpha_d^n = p_n(P) \), and similarly \( \text{tr}(T^n|N) = p_n(Q) \). The former condition \( \mathcal{P} = \mathcal{Q} \) is equivalent to \( \mathcal{P} \) and \( \mathcal{Q} \) having the same multiset of roots with multiplicity in some extension of \( \mathbb{F} \). But the roots of \( \mathcal{P} \) (respectively, \( \mathcal{Q} \)) are the reductions \( \alpha_1, \ldots, \alpha_d \) (respectively, \( \beta_1, \ldots, \beta_d \)) modulo the maximal ideal \( m' \) of \( O' \) 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

\[
\bar{\alpha}_1 = \bar{\beta}_1, \quad \bar{\alpha}_2 = \bar{\beta}_2, \ldots, \quad \bar{\alpha}_d = \bar{\beta}_d.
\]

(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 \( M \otimes \mathbb{F} \equiv (N \otimes \mathbb{F}) \).

We now return to the modular form motivation described in the introduction and prove Corollary 1. Recall that for a \( \mathbb{Z}_p \)-module \( M \) we write \( M \) for \( M \otimes \mathbb{F}_p \).

**Corollary 31 (Restatement of Corollary 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 \( \iota_1 : N_1 \hookrightarrow M_1 \) and \( \iota_2 : N_2 \hookrightarrow M_2 \) and consider the quotients

\[
W_1 := M_1 / \iota_1(N_1), \quad W_2 := M_2 / \iota_2(N_2).
\]

Then \( W_1 \equiv W_2 \) as \( \mathbb{F}_p[T] \)-modules if and only if for every \( n \geq 0 \) we have

\[
v_p\left( \text{tr}(T^n|M_1) - \text{tr}(T^n|N_1) - \text{tr}(T^n|M_2) + \text{tr}(T^n|N_2) \right) \geq 1 + v_p(n). \tag{18}
\]

**Proof.** Using Theorem 30, the condition in (18) is equivalent to the \( \mathbb{F}_p[T] \)-module isomorphism

\[
(M_1 \oplus N_2) \equiv (M_2 \oplus N_1) \equiv (N_1 \oplus N_2) \equiv (M_1 \oplus N_1) \equiv (M_2 \oplus N_2). \tag{19}
\]

Taking a quotient on the left-hand side by \( \iota_1(N_1) \equiv \iota_2(N_2) \) and on the right-hand side by \( \iota_2(N_2) \equiv \iota_1(N_1) \) shows that (19) is equivalent to the isomorphism \( W_1 \equiv W_2 \). \( \square \)

**Remark 32.**

- The congruence for \( 0 \leq n \leq \text{rank } M_1 + \text{rank } N_2 \) suffices in (18).

- Corollary 31 also holds with \( \mathbb{Z}_p, \mathbb{F}_p, 1 + v_p(n) \) replaced by \( O, \mathcal{F}, \frac{1}{e} + v_p(n) \), respectively, where \( O \) is a \( p \)-adic DVR with residue field \( \mathbb{F} \) and ramification degree \( e \leq p - 1 \) over \( \mathbb{Z}_p \). \( \triangle \)

**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 33 (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.

(a) Characteristic polynomial version: The characteristic polynomial map
\[ r \mapsto \text{CharPoly}(r|V) \in k[X] \]
for every \( r \in R \) (equivalently, in a k-basis of R) determines V uniquely.

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

(c) Trace version complement: If \( \text{char } k = p \) then the trace map \( r \mapsto \text{tr}(r|V) \) 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 \( \text{char } k = 0 \) or \( \text{char } k > \dim_k V \), then \( (\dim_k V)! \) is invertible in \( k \), so that the power-sum functions determine the relevant elementary symmetric functions over \( k \) (Corollary 17), and hence the trace version of Brauer-Nesbitt is equivalent to the characteristic-polynomial version. In the critical positive characteristic case \( \text{char } k < \dim_k V \), 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 34 (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 35. Theorem 34 implies parts (b) and (c) of Theorem 33 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 \( \text{tr}(T^n|V) = \text{tr}(T^n|W) \) 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 \( \alpha_i \) 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 $p$).

Acknowledgments

First and foremost we thank Ira Gessel, both for his beautiful proof of Proposition 29 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 Theorem 8. 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, $\mathfrak{p}$-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, volume 211 of Grad. Texts in Math., Springer-Verlag, New York, third edition, 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, The Clarendon Press, Oxford University Press, New York, second edition, 2015.

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

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