Problem Set Week 7 Solutions

Math Olympiad Club Zurich

Spring 2025

Problem A-2 (IMC 1999)

Does there exist a bijective map $\pi\colon \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ such that

$$\sum_{n=1}^{\infty} \frac{\pi(n)}{n^2} < \infty?$$

Solutions:

Solution 1.

No. For a very quick and clever solution, if we let π be a permutation of $\mathbb{N}_{>0}$ and let $N \in \mathbb{N}$, we shall argue that

$$\sum_{n=N+1}^{3N} \frac{\pi(n)}{n^2} > \frac{1}{9}.$$

In fact, of the $2N$ numbers $\pi\left[\left[N+1; 3N\right]\right] = \{\pi(N+1), \ldots, \pi(3N)\}$, only N can be smaller than or equal to N, so at least N of them must be strictly bigger than N. Hence,

$$\sum_{n=N+1}^{3N} \frac{\pi(n)}{n^2} \geq \frac{1}{(3N)^2} \sum_{n=N+1}^{3N} \pi(n) \geq \frac{1}{9N^2} \cdot N \cdot N = \frac{1}{9}.$$

The result follows directly because we have the infinite decomposition $\mathbb{N}_{>0} = \bigsqcup_{N \in 3\mathbb{N}} \left[\left[N+1; 3N\right]\right]$.

Alternative solutions. There are two more solutions, both of which use the following fact:

Let π be a permutation of $\mathbb{N}^*$. Fix $N \in \mathbb{N}^*$: the set of numbers $\pi\left[\left[1; N\right]\right] = \{\pi(1), \ldots, \pi(N)\}$ is of size N, i.e., the numbers are distinct positive integers. Thus, it is easy to prove[1] by

[1] For the case $N = 1$, take $\iota_1 = \mathrm{id}_{[\![1;1]\!]}$. The condition holds vacuously as $[\![1; N-1]\!] = \varnothing$.

Now assume the result holds for $N \geq 1$. We prove it for $N+1$. By the inductive hypothesis, there exists a permutation $\iota_N\colon [\![1; N]\!] \hookrightarrow [\![1; N]\!]$ such that $\pi\left(\iota_N(i+1)\right) > \pi\left(\iota_N(i)\right)$ for all $i \in [\![1; N-1]\!]$. If $\pi(N+1) > \pi\left(\iota_N(N)\right)$, define $\iota_{N+1} = \iota_N \cup \{(N+1, N+1)\}$. This extends ι_N to $[\![1; N+1]\!]$ while preserving the order, so the result holds. Else, by injectivity, equality is impossible, so $\pi(N+1) < \pi\left(\iota_N(N)\right)$, and hence we can take k to be the smallest index in $[\![1; N]\!]$ such that $\pi(N+1) < \pi\left(\iota_N(k)\right)$. Define:

$$\iota_{N+1} = \iota_N|_{[\![1;k-1]\!]} \cup \{(k, N+1)\} \cup \{(t+1, \iota_N(t)) \,|\, t \in [\![k; N]\!]\}.$$

This changes the value at k to $N+1$ and shifts the rest to take the preceding value. Clearly, ι_N is a bijection, and $\iota_{N+1}|_{[\![1;k-1]\!]}$ preserves the order. By choice of k, $\pi\left(\iota_{N+1}(k)\right) = \pi(N+1) < \pi\left(\iota_N(k)\right) = \pi\left(\iota_{N+1}(k+1)\right)$. Now if $k > 1$, then by minimality (and again by injectivity), we have $\pi\left(\iota_{N+1}(k)\right) = \pi(N+1) > \pi\left(\iota_N(k-1)\right) = \pi\left(\iota_{N+1}(k-1)\right)$. In all cases, $\iota_{N+1}|_{[\![1;k+1]\!]}$ preserves the order. For $N \geq i > k$, we have $\pi\left(\iota_{N+1}(i+1)\right) = \pi\left(\iota_N(i)\right) > \pi\left(\iota_N(i-1)\right) = \pi\left(\iota_{N+1}(i)\right)$ by the inductive hypothesis. In total, ι_{N+1} satisfies the required ordering. This concludes the induction step and hence the induction.

induction over $\mathbb{N}^*$ that there exists a permutation $\iota_N \colon [\![1;N]\!] \hookrightarrow [\![1;N]\!]$ such that:

$$\forall i \in [\![1;N-1]\!], \quad \pi\left(\iota_N(i+1)\right) > \pi\left(\iota_N(i)\right).$$

Solution 2.

Fix $N \geq 1$. From our proposition above, it follows that there is a permutation ι_N of $[\![1;N]\!]$ such that for all $t \in [\![1;N-1]\!]$, $\pi\left(\iota_N(t+1)\right) > \pi\left(\iota_N(t)\right)$. In particular, since $\pi\left(\iota_N(1)\right) \geq 1$, we get trivially by induction that for all $t \in [\![1;N]\!]$, $\pi\left(\iota_N(t)\right) \geq t$, so that:

$$\sum_{i=1}^{N} \pi(i) = \sum_{i=1}^{N} \pi\left(\iota_N(i)\right) \geq \sum_{i=1}^{N} i = \frac{N(N+1)}{2},$$

and this holds for all $N \in \mathbb{N}^*$. Now we perform the very useful-to-know Abel transformation on the finite sequences $\pi|_{[\![1;N]\!]}$ and $\left(\frac{1}{n^2}\right)_{1 \leq n \leq N}$ to obtain:

$$\sum_{n=1}^{N} \frac{\pi(n)}{n^2} = \frac{1}{N^2}\left(\sum_{n=1}^{N} \pi(n)\right) + \sum_{n=1}^{N-1}\left(\sum_{j=1}^{n} \pi(j)\right)\left(\frac{1}{n^2} - \frac{1}{(n+1)^2}\right)$$

$$\geq \sum_{n=1}^{N-1}\left(\frac{n(n+1)}{2}\right)\left(\frac{1}{n^2} - \frac{1}{(n+1)^2}\right) = \sum_{n=1}^{N-1} \frac{2n+1}{2n(n+1)} \geq \sum_{n=1}^{N-1} \frac{1}{n+1} = \sum_{n=2}^{N} \frac{1}{n}.$$

Thus,

$$\liminf_{N \to +\infty} \sum_{n=1}^{N} \frac{\pi(n)}{n^2} \geq \liminf_{N \to +\infty} \sum_{n=2}^{N} \frac{1}{n} = +\infty.$$

Solution 3.

Fix $N \geq 1$. Again, from our proposition, there is a permutation ι_N of $[\![1;N]\!]$ such that for all $t \in [\![1;N-1]\!]$, $\pi\left(\iota_N(t+1)\right) > \pi\left(\iota_N(t)\right)$. We are in the following situation:

$$\frac{1}{N^2} \leq \cdots \leq \frac{1}{1^2}$$

$$\pi\left(\iota_N(1)\right) \leq \cdots \leq \pi\left(\iota_N(N)\right)$$

By the very useful-to-know rearrangement inequality, we obtain:

$$\sum_{n=1}^{N} \frac{\pi(n)}{n^2} \geq \sum_{n=1}^{N} \frac{\pi\left(\iota_N(n)\right)}{n^2}.$$

Since $\pi\left(\iota_N(1)\right) \geq 1$, we get trivially by induction that $\pi\left(\iota_N(t)\right) \geq t$, so that:

$$\sum_{n=1}^{N} \frac{\pi\left(\iota_N(n)\right)}{n^2} \geq \sum_{n=1}^{N} \frac{n}{n^2} = \sum_{n=1}^{N} \frac{1}{n}.$$

Thus,

$$\sum_{n=1}^{N} \frac{\pi(n)}{n^2} \geq \sum_{n=1}^{N} \frac{1}{n}.$$

In particular, as N was arbitrary, we get:

$$\liminf_{N \to +\infty} \sum_{n=1}^{N} \frac{\pi(n)}{n^2} \geq \liminf_{N \to +\infty} \sum_{n=2}^{N} \frac{1}{n} = +\infty.$$

Problem 2 (IMC 1994)

Let $f \in C^1\left(]a,b[\,,\mathbb{R}\right)$ with $\lim_{x\to a^+} f(x) = +\infty$, $\lim_{x\to b^-} f(x) = -\infty$, and $f'(x) + f^2(x) \geq -1$ for all $x \in]a,b[$. Prove that $b - a \geq \pi$ and give an example where $b - a = \pi$.

Solution:

From the inequality, we obtain:

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\arctan(f(x)) + x\right) = \frac{f'(x)}{1+f^2(x)} + 1 \geq 0$$

for all $x \in]a,b[$. Therefore, the function $\arctan(f(x)) + x$ is non-decreasing on $]a,b[$. Taking limits as x approaches the endpoints, we get:

$$\lim_{\substack{x\to a\\ >}} \left(\arctan(f(x)) + x\right) = \frac{\pi}{2} + a, \quad \lim_{\substack{x\to b\\ <}} \left(\arctan(f(x)) + x\right) = -\frac{\pi}{2} + b.$$

Hence,

$$\frac{\pi}{2} + a \leq -\frac{\pi}{2} + b,$$

which implies $b - a \geq \pi$.

Equality is achieved when:

$$f(x) = \cot(x) = \frac{\cos(x)}{\sin(x)}, \quad a = 0, \quad b = \pi,$$

since for any $x \in]0,\pi[$, we have:

$$f'(x) + f^2(x) = -\frac{1}{\sin^2(x)} + \frac{\cos^2(x)}{\sin^2(x)} = -\frac{\sin^2(x)}{\sin^2(x)} = -1,$$

and the boundary conditions are satisfied:

$$\lim_{\substack{x\to 0^+\\ >}} \cot(x) = +\infty, \quad \lim_{\substack{x\to \pi\\ <}} \cot(x) = -\infty.$$

Problem B-3 (IMC 2005)

In the linear space of all real $n \times n$ matrices, find the maximum possible $\mathbb{R}$-dimension of an $\mathbb{R}$-linear subspace V such that

$$\forall X, Y \in V, \quad \operatorname{tr}(XY) = 0.$$

(The trace of a matrix is the sum of its diagonal entries.)

Solution:

For $\{\mathbf{0}_{n\times n}\}$, we have

$$\operatorname{tr}(\mathbf{0}_{n\times n} \cdot \mathbf{0}_{n\times n}) = \operatorname{tr}(\mathbf{0}_{n\times n}) = 0,$$

so it is clear that an $\mathbb{R}$-subspace satisfying the condition exists. Denote by V such a subspace with the maximum possible $\mathbb{R}$-dimension (necessarily less than n^2).

Now, if A is a symmetric matrix, then:

$$\operatorname{tr}\left(A^2\right) = \operatorname{tr}\left(A^T A\right) = \sum_{i=0}^{n-1} \left(A^T A\right)_{ii} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \left(A^T\right)_{ij} A_{ji} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} (A_{ji})^2 = \|A\|_F^2,$$

which is the sum of the squared entries of A (the Frobenius norm squared), and is strictly positive as long as $A \neq \mathbf{0}_{n\times n}$. Therefore, V cannot contain any symmetric matrix except $\mathbf{0}_{n\times n}$.

Denote by S the $\mathbb{R}$-linear space of all real $n \times n$ symmetric matrices; its $\mathbb{R}$-dimension is clearly $\frac{n(n+1)}{2}$. Since $V \cap S = \{\mathbf{0}_{n\times n}\}$, we have

$$\dim_{\mathbb{R}}(V) + \dim_{\mathbb{R}}(S) \leq n^2,$$

which gives

$$\dim_{\mathbb{R}}(V) \leq n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2}.$$

Thus, the maximum $\mathbb{R}$-dimension is bounded above by $\frac{n(n-1)}{2}$. This bound is tight: the space of strictly upper triangular matrices clearly has $\mathbb{R}$-dimension $\frac{n(n-1)}{2}$ and satisfies the given condition.

Therefore, the maximum $\mathbb{R}$-dimension of subspaces V satisfying the given condition is $\frac{n(n-1)}{2}$.

Problem 4 (Bernoulli Competition 2024)

Let $n, m \in \mathbb{N}_{>0}$ be positive integers, with $m \geq 3$, and let $A \in \mathbb{Z}^{n\times n}$. Suppose A has finite order ($\exists k \in \mathbb{N}_{>0},\, A^k = I_n$) and satisfies

$$A \equiv I_n \pmod{m}[2].$$

Prove that $A = I_n$, and find counterexamples when $m = 2$.

Solutions:

Solution 1. of $A = I_n$

Since $A \equiv I_n \pmod{m}$, there exists $B \in \mathbb{Z}^{n\times n}$ such that $A = I_n + mB$. Then we have the following equality of characteristic polynomials:

$$P_{\text{char},A}(X) = \det_{\mathbb{Q}(X)}(XI_n - A) = \det_{\mathbb{Q}(X)}((X-1)I_n - mB) = P_{\text{char},mB}(X-1).$$

Therefore, $\alpha \in \mathbb{C}$ is an eigenvalue of A if and only if $\alpha - 1$ is an eigenvalue of mB; that is (since $m \neq 0$), if and only if $\frac{\alpha-1}{m}$ is an eigenvalue of B.

Since $\exists k \in \mathbb{N}_{>0}$ with $A^k = I_n$, any eigenvalue $\alpha \in \mathbb{C}$ of A satisfies $\alpha^k = 1$; thus, they are k-th roots of unity and lie on the unit circle $\mathbb{S}^1$, i.e., $|\alpha|_{\mathbb{C}} = 1$. Any eigenvalue $\beta \in \mathbb{C}$ of B then satisfies (here $m \geq 3$ is crucial):

$$|\beta|_{\mathbb{C}} = \left|\frac{\alpha-1}{m}\right|_{\mathbb{C}} \leq \frac{|\alpha|_{\mathbb{C}} + 1}{m} = \frac{2}{m} < 1.$$

Now we prove that 0 is the only eigenvalue of B: $\sigma(B) = \{0\}$.

From this point, there are multiple ways to proceed; we present two approaches here.

Using Vieta's formula.

Since $\mathbb{Z}$ is a unique factorisation domain (UFD), so is $\mathbb{Z}[X]$, and we can factor the characteristic polynomial of B (which is of degree $n \geq 1$), $P_{\text{char},B}(X) := \det_{\mathbb{Q}(X)}(XI_n - B) \in \mathbb{Z}[X]$, as a product of $l \in \mathbb{N}^*$ unique irreducible polynomials (up to invertible elements, which here are ± 1). Since $P_{\text{char},B}(X)$ is monic, the irreducible polynomials must have leading coefficients in $\mathbb{Z}^\times = \{\pm 1\}$. Therefore, they must have degree at least one (without this information they could have been irreducible elements of $\mathbb{Z} \subset \mathbb{Z}[X]$—namely, the primes up to sign). Hence, we may assume them to be monic (by multiplying, *ubi opus est*, by -1). That is,

$$\exists \{P_i(X) \mid \forall i \in l,\, P_i(X) \text{ is irreducible and monic}\} \subset \mathbb{Z}_{\text{irr}}[X] \setminus \mathbb{Z}$$

such that

$$P_{\text{char},B}(X) = \prod_{i\in l} P_i(X).$$

Now, let β be an eigenvalue of B, i.e., $\beta \in \text{Root}_{P_{\text{char},B}(X)}(\mathbb{C})$. Hence, there exists $j \in l$ such that $\beta \in \text{Root}_{P_j(X)}(\mathbb{C})$. For a certain $s_j \in \mathbb{N}_{>0}$ and distinct complex numbers $\{{}_j\beta_i \mid i \in s_j\} \subset \mathbb{C}$, we have

$$\text{Root}_{P_j(X)}(\mathbb{C}) = \{{}_j\beta_i \mid i \in s_j\}.$$

[2]For an integer $u \in \mathbb{Z}$, $\equiv \pmod{u}$ is the relation on the set of integer matrices $\bigcup_{r,l\in\mathbb{N}^*} \mathbb{Z}^{r\times l}$, where $C \equiv D \pmod{u} \Leftrightarrow \exists r, l \in \mathbb{N}^*, C, D \in \mathbb{Z}^{r\times l}, \forall (i,j) \in r \times l,\, u \mid (C-D)(i,j)$. It is an equivalence relation.

As we have seen above,

$$\mathrm{Root}_{P_{\mathrm{char},B}(X)}(\mathbb{C}) \subset \mathbb{D},$$

so $\{ {}_j\beta_i \mid i \in s_j\} \subset \mathbb{D}$. However, since these are the roots of $P_j(X)$, we must have, by Vieta's formula, that their product equals (up to a sign) the constant term of $P_j(X)$:

$$\prod_{i \in s_j} {}_j\beta_i \in \{\pm P_j(0)\}.$$

Then

$$|P_j(0)|_{\mathbb{C}} = \left| \prod_{i \in s_j} {}_j\beta_i \right|_{\mathbb{C}} = \prod_{i \in s_j} |{}_j\beta_i|_{\mathbb{C}} < 1.$$

Since $P_j(X) \in \mathbb{Z}[X]$, we must have $P_j(0) \in \mathbb{Z}$, and because $|P_j(0)|_{\mathbb{C}} < 1$ we must have $P_j(0) = 0$. Therefore, 0 is a root of P_j, and thus X divides $P_j(X)$ in $\mathbb{Z}[X]$. Since $P_j(X)$ has degree at least 1 and is irreducible in $\mathbb{Z}[X]$, this cannot happen unless $P_j(X)$ has degree 1. So $P_j(X) = kX$ for a certain $k \in \mathbb{Z} \setminus \{0\}$. Since $P_j(X)$ is monic, $k = 1$, and we conclude $P_j(X) = X$. Hence $\beta = 0$, since it is a root of $P_j(X)$ by choice of j. As $\beta \in \sigma(B)$ was arbitrary we conclude $\sigma(B) = \{0\}$ (because $\sigma(B) \neq \varnothing$).

Using the following equivalence.

Lemma. *One has* $\sigma(B) = \{0\} \Leftrightarrow \exists t \in \mathbb{N}, \forall k \in [\![1, n]\!], tr\left(B^{t+k}\right) = 0.$

This equivalence, along with several others, is proven in a generic form in Appendix [A.3].

It thus suffices to show that $\exists M \in \mathbb{N}, \forall N \in \mathbb{N}_{\geq M}, \mathrm{tr}\left(B^N\right) = 0$.

As shown earlier, all eigenvalues of B lie inside the unit disc: $\mathrm{Root}_{P_{\mathrm{char},B}(X)}(\mathbb{C}) \subset \mathbb{D}$. Let $\boldsymbol{\beta} \in \mathbb{D}^n$ be any vector (the order in this vector doesn't matter) of exactly all the eigenvalues of B, counted with their respective algebraic multiplicities, so that $\sigma(B) = \mathrm{Root}_{P_{\mathrm{char},B}(X)}(\mathbb{C}) = \{\beta_i \mid i \in n\}$. By the Spectral Mapping Theorem [A.1], one has that $\forall k \in \mathbb{N}$:

$$\mathrm{tr}\left(B^k\right) = \sum_{i \in n} \beta_i^k.$$

Let $\gamma \in \sigma(B)$ be an eigenvalue of B. Since $|\gamma|_{\mathbb{C}} < 1$, we have $\gamma^N \xrightarrow[\mathbb{N} \ni N \to +\infty]{|\cdot|_{\mathbb{C}}} 0$. Therefore:

$$\mathrm{tr}\left(B^N\right) \xrightarrow[\mathbb{N} \ni N \to +\infty]{|\cdot|_{\mathbb{C}}} 0,$$

as it is a finite sum comprising a total of n summands tending to zero. However, as $B \in \mathbb{Z}^{n \times n}$, we have $\forall k \in \mathbb{N}$, $B^k \in \mathbb{Z}^{n \times n}$, so for all $k \in \mathbb{N}$, $\mathrm{tr}\left(B^k\right) \in \mathbb{Z}$. Hence (standard), there exists $M \in \mathbb{N}$ such that for all $N \in \mathbb{N}_{\geq M}$, $\mathrm{tr}\left(B^N\right) = 0$, as desired.

This concludes the two different approaches to show that $\sigma(B) = \{0\}$. We can now quickly finish the problem. All the eigenvalues of B are 0; this is clearly equivalent to $P_{\mathrm{char},B}(X) = X^n$. According to the Cayley-Hamilton theorem, $B^n = \mathbf{0}_{n \times n}$, so B is nilpotent and thus mB is nilpotent. Now, use the following

Lemma. *Let* $\mathbb{F}$ *be a field of characteristic* $\mathrm{char}(\mathbb{F}) = 0$, $l \in \mathbb{N}_{>0}$, *and* $N \in \mathbb{F}^{l \times l}$ *be a nilpotent matrix. If* $I_l + N$ *has finite order, then* $N = \mathbf{0}_{l \times l}$.

The proof can be found in a slightly generalised framework in Appendix [A.6].

Apply this result to the field $\mathbb{Q}$ with $n \geq 1$; since $mB \in \mathbb{Q}^{n\times n}$ is nilpotent and $A = I_n + mB$ has finite order, we conclude that $mB = \mathbf{0}_{n\times n}$. Hence, $A = I_n$, and this concludes the proof.

Solution 2. of $A = I_n$

Assume for contradiction that $A \neq I_n$. Since $m \geq 3$, m must be divisible by some prime power greater than 2, that is, there exists $p \in \mathbb{P}$ a prime number and $c \geq 1$ such that $p^c \mid m$ and $p^c > 2$ (if $p = 2$, then $c \geq 2$ necessarily). In particular, from $A \equiv I_n \pmod{m}$, we must have $A \equiv I_n \pmod{p^c}$.

Since $A \neq I_n$, there is $(i,j) \in n \times n$ such that $(A - I_n)(i,j) \neq 0$, and so

$$c \leq v_p\left((A - I_n)(i,j)\right) \neq +\infty,$$

where $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ denotes the p-adic valuation. We can thus let

$$c' := \min\left\{v_p\left((A - I_n)(i,j)\right) \mid (i,j) \in n \times n\right\} \geq c.$$

Then $c' \in \mathbb{N}_{\geq c}$ is (by construction) the largest integer such that $A \equiv I_n \pmod{p^{c'}}$. Consequently, we define

$$B := \frac{1}{p^{c'}}(A - I_n) \in \mathbb{Q}^{n\times n},$$

for which (by definition of c'), $B \in \mathbb{Z}^{n\times n}$ and $B \not\equiv \mathbf{0}_{n\times n} \pmod{p}$.
Since A has finite order, there exists $k \in \mathbb{N}^*$ with $A^k = I_n$; furthermore, $k \geq 2$ because $A \neq I_n$.
We want to expand:

$$I_n = A^k = \left(I_n + p^{c'}B\right)^k.$$

This can be done (happily) by the binomial theorem since I_n and $p^{c'}B$ commute, and we obtain:

$$I_n = \sum_{i=0}^{k} \binom{k}{i} p^{ic'} B^i.$$

This implies:

$$\sum_{i=1}^{k} \binom{k}{i} p^{ic'} B^i = \mathbf{0}_{n\times n},$$

or equivalently (since $k \geq 2$), we obtain the equation:

$$\sum_{i=2}^{k} \binom{k}{i} p^{ic'} B^i = -kp^{c'}B.$$

We shall show that this leads to a contradiction. Let $c'' := v_p(k) \geq 0$. We prove:

$$-kp^{c'}B \not\equiv \mathbf{0}_{n\times n} \pmod{p^{c'+c''+1}}, \tag{1}$$

whilst

$$\sum_{i=2}^{k} \binom{k}{i} p^{ic'} B^i \equiv \mathbf{0}_{n\times n} \pmod{p^{c'+c''+1}}, \tag{2}$$

which is impossible by the derived equation above.
For (1): because $v_p\left(kp^{c'}\right) = c' + c''$ and $B \not\equiv \mathbf{0}_{n\times n} \pmod{p}$, we have $-kp^{c'}B \not\equiv \mathbf{0}_{n\times n}$

$(\text{mod } p^{c'+c''+1})$ (but obviously $kp^{c'}B \equiv \mathbf{0}_{n\times n} \ (\text{mod } p^{c'+c''})$).
For (2): let $2 \leq i \leq k$, note that $i!\binom{k}{i} = \frac{k!}{(k-i)!}$ is divisible by k, hence by $p^{c''}$, whilst the largest power of p dividing $i!$ is classically bounded above by the famous Legendre's formula:

$$v_p(i!) = {}^{3}\sum_{j=1}^{+\infty}\left\lfloor\frac{i}{p^j}\right\rfloor < \sum_{j=1}^{+\infty}\frac{i}{p^j} = \frac{i}{p-1}.$$

We claim that $v_p(i!) \leq \left\lfloor\frac{i-1}{p-1}\right\rfloor$. Assume for the sake of contradiction that $\left\lfloor\frac{i-1}{p-1}\right\rfloor < v_p(i!)$. Since both are integers, $\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1 \leq v_p(i!)$. As $v_p(i!) < \frac{i}{p-1}$ and $i \geq 2 \Rightarrow \left\lfloor\frac{i-1}{p-1}\right\rfloor + 1 \geq 1$, we obtain:

$$\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1 < \frac{i}{p-1} \Rightarrow (p-1)\left(\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1\right) < i.$$

Again, since $i, (p-1)\left(\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1\right)$ are integers, we have:

$$(p-1)\left(\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1\right) + 1 \leq i.$$

However, by definition of the floor function:

$$\frac{i-1}{p-1} < \left\lfloor\frac{i-1}{p-1}\right\rfloor + 1 \Rightarrow i < (p-1)\left(\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1\right) + 1.$$

Combining:

$$i < (p-1)\left(\left\lfloor\frac{i-1}{p-1}\right\rfloor + 1\right) + 1 \leq i,$$

that is, $i < i$, a contradiction. Thus, $v_p(i!) \leq \left\lfloor\frac{i-1}{p-1}\right\rfloor$. So:

$$v_p\left(\binom{k}{i}p^{ic'}\right) = v_p\left(\frac{i!\binom{k}{i}}{i!}p^{ic'}\right) = v_p\left(p^{ic'}\right) + v_p\left(i!\binom{k}{i}\right) - v_p(i!) \geq ic' + c'' - \left\lfloor\frac{i-1}{p-1}\right\rfloor.$$

If $p = 2$, then $c' \geq c \geq 2$ and $\frac{i-1}{p-1} = i-1$, so:

$$ic' + c'' - \left\lfloor\frac{i-1}{p-1}\right\rfloor = i(c'-1) + c'' + 1$$

$$\geq 2(c'-1) + c'' + 1 = c' + c'' + (c'-2) + 1 \geq c' + c'' + 1.$$

If $p \geq 3$, then $\frac{i-1}{p-1} \leq \frac{i-1}{2}$, so that $\left\lfloor\frac{i-1}{p-1}\right\rfloor \leq \left\lfloor\frac{i-1}{2}\right\rfloor$, and thus:

$$ic' + c'' - \left\lfloor\frac{i-1}{p-1}\right\rfloor \geq ic' + c'' - \left\lfloor\frac{i-1}{2}\right\rfloor$$

[3] A quick proof of this formula for $p \in \mathbb{P}$ and $i \geq 1$ proceeds as follows: define $M := \max\{v_p(t) \mid 1 \leq t \leq i\}$, then: $v_p(i!) = \sum_{t=1}^{i} v_p(t) = \sum_{t=1}^{i}\left(\sum_{\substack{j=1\\ p^j \mid_{\mathbb{Z}} t}}^{M} 1\right) = \sum_{\substack{(t,j)\in[\![1,i]\!]\times[\![1,M]\!]\\ p^j \mid_{\mathbb{Z}} t}} 1 = \sum_{j=1}^{M}\left(\sum_{\substack{t=1\\ p^j \mid_{\mathbb{Z}} t}}^{i} 1\right) = \sum_{j=1}^{M}\left|\left\{t \in [\![1,i]\!] \,\middle|\, p^j \mid_{\mathbb{Z}} t\right\}\right| = \sum_{j=1}^{M}\left|\left\{p^j s \leq i \,\middle|\, s \in \mathbb{N}_{>0}\right\}\right| = \sum_{j=1}^{M}\left|\left\{s \in \mathbb{N}_{>0} \,\middle|\, p^j s \leq i\right\}\right| = \sum_{j=1}^{M}\left\lfloor\frac{i}{p^j}\right\rfloor = \sum_{j=1}^{+\infty}\left\lfloor\frac{i}{p^j}\right\rfloor$. Here, we use the total multiplicativity of v_p for the first equality; the interchange of sums is justified by their finiteness. The final equality follows from the definition of M, since if $j \in \mathbb{N}$ is such that $j > M$, then $j > v_p(i)$, hence $\frac{i}{p^j} < 1$, and thus $\left\lfloor\frac{i}{p^j}\right\rfloor = 0$. The remaining equalities follow from elementary counting.

$$= c' + c'' + (i-1)\,c' - \left\lfloor \frac{i-1}{2} \right\rfloor \geq c' + c'' + (i-1) - \left\lfloor \frac{i-1}{2} \right\rfloor$$
$$= c' + c'' + \left\lceil \frac{i-1}{2} \right\rceil \geq c' + c'' + 1,$$

where we used the fact that for an integer $r \in \mathbb{Z}$, we have $r - \lfloor \frac{r}{2} \rfloor = \lceil \frac{r}{2} \rceil$ (for this equality, break r into two cases based on its parity: $2t$ or $2t+1$) and that $i - 1 > 0$.
In all cases for p:

$$v_p\left(\binom{k}{i} p^{ic'}\right) \geq c' + c'' + 1,$$

and so $p^{c'+c''+1}$ divides $\binom{k}{i} p^{ic'}$. As $2 \leq i \leq k$ was arbitrary, we get that:

$$\sum_{i=2}^{k} \binom{k}{i} p^{ic'} B^i \equiv \mathbf{0}_{n\times n} \pmod{p^{c'+c''+1}}.$$

This shows our desired contradiction. Thus, our initial assumption must be false and $A = I_n$. This concludes the proof.

A counterexample for general $n \geq 1$ is easy to find, for example, $-I_n$. If we want to find one that is not a diagonal matrix, we split the cases between even and odd dimensions. When $n = 2k > 0$, we place k copies of a 2×2 counterexample block (which satisfies the condition) along the diagonal; when $n = 2k+1 > 0$, we place k copies of the same 2×2 block and a final ± 1 on the diagonal:

$$\begin{pmatrix} 1 & 2 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 \\ 0 & 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \begin{matrix} 1 \\ 0 \end{matrix} & \begin{matrix} 2 \\ -1 \end{matrix} \end{pmatrix} \in \mathbb{Z}^{2k\times 2k},$$

$$\begin{pmatrix} 1 & 2 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \begin{matrix} 1 \\ 0 \end{matrix} & \begin{matrix} 2 \\ -1 \end{matrix} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \pm 1 \end{pmatrix} \in \mathbb{Z}^{(2k+1)\times(2k+1)}.$$

A

A.1

We recall the following important theorem:

Theorem 1 (Spectral Mapping Theorem)**.** *Let $\mathbb{F}$ be a field, $r \in \mathbb{N}_{>0}$, and $A \in \mathbb{F}^{r\times r}$. Let $\mathbb{F}^{alg} \supset \mathbb{F}$ be the algebraic closure of $\mathbb{F}$. Let $Q \in \mathbb{F}^{alg}[X]$. Let $\sigma(A) = \mathrm{Root}_{P_{char,A}(X)}\left(\mathbb{F}^{alg}\right)$ be the set of all eigenvalues of A, and for each $\lambda \in \sigma(A)$, let $m_\lambda := m_{P_{char,A}(X)}(\lambda)$ be the algebraic multiplicity of λ in $P_{char,A}(X)$. The Spectral Mapping Theorem (easy to prove once one knows that every matrix in $\left(\mathbb{F}^{alg}\right)^{r\times r}$ is similar to an upper triangular matrix over $\mathbb{F}^{alg}$) states precisely that $P_{char,Q(A)}(X) = \prod_{\lambda\in\sigma(A)}(X - Q(\lambda))^{m_\lambda}$. Recall that $0_{\mathbb{F}}^0 := 1_{\mathbb{F}}$. In particular:*

$$\sigma(Q(A)) = \{Q(\lambda) \mid \lambda \in \sigma(A)\} \subset \mathbb{F}^{alg},$$
$$\forall \kappa \in \mathbb{F}^{alg},\ m_{P_{char,Q(A)}(X)}(\kappa) = \sum_{\substack{\mu\in\sigma(A)\\ Q(\mu)=\kappa}} m_\mu.$$

If we let $\lambda \in \left(\mathbb{F}^{alg}\right)^r$ be any vector (the order in this vector doesn't matter) of exactly all the eigenvalues of A counted with their respective algebraic multiplicities, then $Q(\lambda) \in \left(\mathbb{F}^{alg}\right)^r$ (each coordinate is evaluated through Q) is a vector of exactly all the eigenvalues of $Q(A)$ with their respective algebraic multiplicities. Hence (by standard formula linking its trace and determinant to its eigenvalues):

$$\mathrm{tr}(Q(A)) = \sum_{i\in r} Q(\lambda_i),$$

$$\det_{\mathbb{F}^{alg}}(Q(A)) = \prod_{i\in r} Q(\lambda_i).$$

A.2

The following lemma is helpful.

Lemma. *Let R be a commutative unital ring which is a domain, together with the canonical morphism $\mathrm{can}_R\colon \mathbb{Z} \to R$, and write for any integer k: $k_R := \mathrm{can}_R(k)$. Then for all $m \in \mathbb{N}_{\geq 1}$ such that $\mathrm{char}(R) = 0$ or $m < \mathrm{char}(R)$, the set*

$$S_m := \left\{ \boldsymbol{\lambda}\colon m \to R \;\middle|\; \exists t \in \mathbb{N}, \forall k \in [\![1, m]\!], \sum_{i\in m} \lambda_i^{t+k} = 0_R \right\}$$

is equal to the singleton set $\{0_m\}$, where $0_m\colon m \to R$ is defined by $i \mapsto 0_R$ and where $x^0 = 1_R$ even if $x = 0_R$.

Proof. This is proven by induction on $m \in \mathbb{N}_{\geq 1}$, assuming $\mathrm{char}(R) = 0$ or $m < \mathrm{char}(R)$.

Base case $m = 1$: The condition $\mathrm{char}(R) = 0$ or $1 < \mathrm{char}(R)$ holds because if $\mathrm{char}(R) \neq 0$, it must be a prime number (since R is a domain), meaning $\mathrm{char}(R) \geq 2 > 1$. We then have:

$$S_1 = \left\{ \boldsymbol{\lambda}\colon 1 \to R \;\middle|\; \exists t \in \mathbb{N}, \forall k \in [\![1, 1]\!], \sum_{i\in 1} \lambda_i^{t+k} = 0_R \right\} \overset{\text{clear}}{=} \left\{ \boldsymbol{\lambda}\colon 1 \to R \;\middle|\; \exists t \in \mathbb{N}, \lambda_0^{t+1} = 0_R \right\}.$$

Clearly, since R is a domain, $\lambda_0^{t+1} = 0_R \Rightarrow \lambda_0 = 0_R$ (trivial induction). Hence, $S_1 = \{0_1\}$, which establishes the base case.

Induction step: Assume the statement holds for some $m \in \mathbb{N}_{\geq 1}$, so that $S_m = \{0_m\}$. We want to show it holds for $m+1 \in \mathbb{N}_{>1}$ (assuming $\mathrm{char}\,(R) = 0$ or $m+1 < \mathrm{char}\,(R)$).

Clearly, $\{0_{m+1}\} \subset S_{m+1}$. To show the converse, let any $\boldsymbol{\lambda} \in S_{m+1}$, we first show that $\exists k \in m+1$ such that $\lambda_k = 0_R$. This can be proven in (at least) three ways: The first one (the simplest) uses a direct computation, the second (quite related to the first) uses Newton's identities (with a full proof of them), finally the last one uses the Vandermonde matrix (whose determinant is proven in Appendix [A.5]):

Direct computation.

Fix $n \in \mathbb{N}_{>0}$. For $k \in \mathbb{N}$, let the k-th power sum polynomials in n variables be

$$p_k\left(\mathbf{X}\right) := \sum_{i \in n} X_i^k \in \mathbb{Z}\left[\mathbf{X}\right],$$

and the k-th elementary symmetric polynomials in n variables be

$$e_k\left(\mathbf{X}\right) := \sum_{\substack{A \in \mathscr{P}(n) \\ |A| = k}} \prod_{a \in A} X_a \in \mathbb{Z}\left[\mathbf{X}\right] \text{[4]}.$$

In our case, where the number of variables is $m+1 \geq 1$, we define, for all $k \geq 0$, the k-th power sum and the k-th elementary symmetric polynomial in the vector $\boldsymbol{\lambda}$, respectively:

$$p_k := p_k\left(\boldsymbol{\lambda}\right) = \sum_{i \in m+1} \lambda_i^k, \quad e_k := e_k\left(\boldsymbol{\lambda}\right) = \sum_{\substack{A \in \mathscr{P}(m+1) \\ |A| = k}} \prod_{a \in A} \lambda_a.$$

By the condition $\boldsymbol{\lambda} \in S_{m+1}$, it is clear that there exists a minimal $t_{\boldsymbol{\lambda}} \in \mathbb{N}$ such that $p_{t_{\boldsymbol{\lambda}}+k} = 0_R$ for all $k \in [\![1, m+1]\!]$. Consider the polynomial whose roots are the coordinates of $\boldsymbol{\lambda}$:

$$P\left(X\right) = \prod_{i \in m+1} \left(X - \lambda_i\right) = \sum_{j=0}^{m+1} \left(-1\right)_R^j e_j X^{m+1-j} \in R\left[X\right].$$

One has for all $i \in m+1$, $0_R = P\left(\lambda_i\right)$, so that:

$$0_R = \lambda_i^{t_{\boldsymbol{\lambda}}} \cdot P\left(\lambda_i\right) = \sum_{j=0}^{m+1} \left(-1\right)_R^j e_j \lambda_i^{t_{\boldsymbol{\lambda}}+m+1-j}.$$

Summing this identity over all $i \in m+1$ gives:

$$0_R = \sum_{i \in m+1} 0_R = \sum_{i \in m+1} \sum_{j=0}^{m+1} \left(-1\right)_R^j e_j \lambda_i^{t_{\boldsymbol{\lambda}}+m+1-j} = \sum_{j=0}^{m+1} \left(-1\right)_R^j e_j p_{t_{\boldsymbol{\lambda}}+m+1-j}$$

$$= \sum_{j=0}^{m} 0_R + \left(-1\right)_R^{m+1} e_{m+1} p_{t_{\boldsymbol{\lambda}}} \Rightarrow 0_R = e_{m+1} p_{t_{\boldsymbol{\lambda}}} = p_{t_{\boldsymbol{\lambda}}} \cdot \prod_{i \in m+1} \lambda_i,$$

[4] That is:

$$e_0\left(\mathbf{X}\right) = 1,\ e_1\left(\mathbf{X}\right) = \sum_{i \in n} X_i,\ e_2\left(\mathbf{X}\right) = \sum_{0 \leq i < j < n} X_i X_j,\ \ldots,\ e_n\left(\mathbf{X}\right) = \prod_{i \in n} X_i,$$

and $e_k\left(\mathbf{X}\right) = 0$ for $k > n$.

where we used that $p_{t_{\boldsymbol{\lambda}}+k} = 0_R$ for all $k \in [\![1, m+1]\!]$. By minimality of $t_{\boldsymbol{\lambda}}$, $p_{t_{\boldsymbol{\lambda}}} \neq 0_R$. Indeed, if $t_{\boldsymbol{\lambda}} = 0$, then $p_{t_{\boldsymbol{\lambda}}} = (m+1)_R$, which is not zero by hypothesis on the characteristic. Else $t_{\boldsymbol{\lambda}} \geq 1$, then assuming $p_{t_{\boldsymbol{\lambda}}} = 0_R$ yields a contradiction to the minimality of $t_{\boldsymbol{\lambda}}$ because then one could take $t_{\boldsymbol{\lambda}} - 1 \in \mathbb{N}$ and the condition would still hold for this integer.

This implies (as R is a domain) that there exists $k \in m+1$ such that $\lambda_k = 0_R$.

Using Newton's identities.

In the same settings as above, for $n \in \mathbb{N}_{>0}$ and $k \in \mathbb{N}$, the previous direct computation proof above hints that some of the k-th power sum polynomials in n variables and some of the k-th elementary symmetric polynomials in n variables are related. Indeed, they are related by the so-called Newton's identities (valid for $1 \leq k \leq n$) over $R[X_0, \ldots, X_{n-1}] = R[\mathbf{X}]$:

$$k_R e_k(\mathbf{X}) = \sum_{i=1}^{k} (-1)_R^{i-1} e_{k-i}(\mathbf{X}) p_i(\mathbf{X}).$$

For a short combinatorial proof of these identities, see [A.4].

By the condition $\boldsymbol{\lambda} \in S_{m+1}$, there exists $t_{\boldsymbol{\lambda}} \in \mathbb{N}$ such that $p_{t_{\boldsymbol{\lambda}}+k} = 0_R$ for all $k \in [\![1, m+1]\!]$. In our case, where the number of variables is $m+1 \geq 1$, we define, for all $k \geq 0$, the k-th power sum and the k-th elementary symmetric polynomial as before but this time in the vector $\boldsymbol{\lambda}^{t_{\boldsymbol{\lambda}}}$ (each coordinate of this vector is raised to the power $t_{\boldsymbol{\lambda}}$), respectively:

$$\tilde{p}_k := p_k\left(\boldsymbol{\lambda}^{t_{\boldsymbol{\lambda}}}\right) = \sum_{i \in m+1} \left(\lambda_i^{t_{\boldsymbol{\lambda}}}\right)^k, \quad \tilde{e}_k := e_k\left(\boldsymbol{\lambda}^{t_{\boldsymbol{\lambda}}}\right) = \sum_{\substack{A \in \mathscr{P}(m+1) \\ |A|=k}} \prod_{a \in A} \lambda_a^{t_{\boldsymbol{\lambda}}}.$$

Notice that $\tilde{p}_k = p_{t_{\boldsymbol{\lambda}}+k}(\boldsymbol{\lambda})$ and thus, for each $i \in [\![1, m+1]\!]$, $\tilde{p}_i = 0_R$. Newton's identities (for $1 \leq k = m+1 \leq m+1$) when evaluated at $\boldsymbol{\lambda}^{t_{\boldsymbol{\lambda}}}$ give:

$$0_R = \sum_{i=1}^{m+1} (-1)_R^{i-1} \tilde{e}_{m+1-i} \tilde{p}_i = (m+1)_R \tilde{e}_{m+1} = (m+1)_R \prod_{i \in m+1} \lambda_i^{t_{\boldsymbol{\lambda}}}.$$

Since $m+1 \geq 2$ and $\mathrm{char}(R) = 0$ or $m+1 < \mathrm{char}(R)$, we obtain $(m+1)_R \neq 0_R$.

This implies (as R is a domain) that there exists $k \in m+1$ such that $\lambda_k = 0_R$.

Using the Vandermonde matrix.

It is clear that there exists a bijection $\alpha^{\boldsymbol{\lambda}} \colon r \xrightarrow{\text{bij}} \mathrm{ran}(\boldsymbol{\lambda}) \subset R$, where $r := |\mathrm{ran}(\boldsymbol{\lambda})|$.

(Note that $\boldsymbol{\lambda} \neq \varnothing$ and $\mathrm{dom}(\boldsymbol{\lambda}) = m+1$ so that $r \in [\![1, m+1]\!]$). By hypothesis on $\boldsymbol{\lambda}$, there exists $t_{\boldsymbol{\lambda}} \in \mathbb{N}$ such that for all $k \in [\![1, m+1]\!]$:

$$0_R \overset{\text{hyp}}{=} \sum_{i \in m+1} \lambda_i^{t_{\boldsymbol{\lambda}}+k} \overset{\text{clear}}{=} \sum_{j \in r} \left|\boldsymbol{\lambda}^{-1}\left(\left\{\alpha^{\boldsymbol{\lambda}}(j)\right\}\right)\right|_R \cdot \left(\alpha^{\boldsymbol{\lambda}}(j)\right)^{t_{\boldsymbol{\lambda}}} \cdot \left(\alpha^{\boldsymbol{\lambda}}(j)\right)^k,$$

where the multiplicity $\left|\boldsymbol{\lambda}^{-1}\left(\left\{\alpha^{\boldsymbol{\lambda}}(j)\right\}\right)\right| \neq 0$ by construction, so that:

$$\left|\boldsymbol{\lambda}^{-1}\left(\left\{\alpha^{\boldsymbol{\lambda}}(j)\right\}\right)\right|_R \neq 0_R$$

either because $\mathrm{char}\,(R) = 0$ or because the multiplicity is bounded by $m+1 < \mathrm{char}\,(R)$.

Since $r \leq m+1$, we get the following system of equations:

$$M_{\alpha^{\boldsymbol{\lambda}}} \cdot v_{\alpha^{\boldsymbol{\lambda}}} = \mathbf{0}_r,$$

where $M_{\alpha^{\boldsymbol{\lambda}}} \in R^{r\times r}$ is defined by $(i,j) \mapsto \left(\alpha^{\boldsymbol{\lambda}}(j)\right)^{i+1}$ for $i,j \in r$, i.e.,

$$M_{\alpha^{\boldsymbol{\lambda}}} = \begin{pmatrix} \left(\alpha^{\boldsymbol{\lambda}}(0)\right)^1 & \dots & \left(\alpha^{\boldsymbol{\lambda}}(r-1)\right)^1 \\ \vdots & \ddots & \vdots \\ \left(\alpha^{\boldsymbol{\lambda}}(0)\right)^r & \dots & \left(\alpha^{\boldsymbol{\lambda}}(r-1)\right)^r \end{pmatrix},$$

and $v_{\alpha^{\boldsymbol{\lambda}}} \in R^{r\times 1}$ is the well-defined column vector given by $j \mapsto \left|\boldsymbol{\lambda}^{-1}\left(\left\{\alpha^{\boldsymbol{\lambda}}(j)\right\}\right)\right|_R \cdot \left(\alpha^{\boldsymbol{\lambda}}(j)\right)^{t_{\boldsymbol{\lambda}}}$.

Assume now towards a contradiction that $0_R \notin \mathrm{ran}\,(\boldsymbol{\lambda})$. Then $v_{\alpha^{\boldsymbol{\lambda}}} \in \ker\left(M_{\alpha^{\boldsymbol{\lambda}}}\right) \setminus \{\mathbf{0}_r\}$ (since there exists $j \in r$ with $\alpha^{\boldsymbol{\lambda}}(j) \neq 0_R$, which implies $\left(\alpha^{\boldsymbol{\lambda}}(j)\right)^{t_{\boldsymbol{\lambda}}} \neq 0_R$ even if $t_{\boldsymbol{\lambda}} = 0$). Thus, $M_{\alpha^{\boldsymbol{\lambda}}}$ is a matrix for which its associated R-linear operator is not injective. As is true in any commutative ring, we must have:

$$0_R = \det_R\left(M_{\alpha^{\boldsymbol{\lambda}}}\right) = \left(\prod_{j\in r} \alpha^{\boldsymbol{\lambda}}(j)\right) \det_R\left(V_{\alpha^{\boldsymbol{\lambda}}}^T\right),$$

where $\det_R$ is defined via the Leibniz formula (permutation summation formula), ensuring that all standard properties, such as being a monoid morphism, or being multilinear over the ring R hold. We used the multilinear property in the last equality to extract from each column j the factor $\alpha^{\boldsymbol{\lambda}}(j)$, and where $V_{\alpha^{\boldsymbol{\lambda}}} \in R^{r\times r}$ is the Vandermonde matrix of $\alpha^{\boldsymbol{\lambda}}$, with entries $V_{\alpha^{\boldsymbol{\lambda}}}(i,j) = \left(\alpha^{\boldsymbol{\lambda}}(i)\right)^j$.

By the lemma in Appendix [A.5]:

$$\det_R\left(V_{\alpha^{\boldsymbol{\lambda}}}^T\right) = \det_R\left(V_{\alpha^{\boldsymbol{\lambda}}}\right) = \prod_{0\leq i<j<r} \left(\alpha^{\boldsymbol{\lambda}}(j) - \alpha^{\boldsymbol{\lambda}}(i)\right) \neq 0_R,$$

because $\alpha^{\boldsymbol{\lambda}}$ is injective, and R is a domain! (Even if $r = 1$, the empty product is $1_R \neq 0_R$).

So we must have $\prod_{j\in r} \alpha^{\boldsymbol{\lambda}}(j) = 0_R$, which implies because R is a domain that there exists $j \in r$ such that $\alpha^{\boldsymbol{\lambda}}(j) = 0_R$, meaning $0_R \in \mathrm{ran}\,(\boldsymbol{\lambda})$, a contradiction. Thus our assumption is false and we must have $0_R \in \mathrm{ran}\,(\boldsymbol{\lambda})$.

Hence, there exists $k \in m+1$ such that $\lambda_k = 0_R$.

So all of these three proofs showed that $\exists k \in m+1,\ \lambda_k = 0_R$. Now define then $\boldsymbol{\lambda}' \colon m \to R$ by:

$$i \mapsto \begin{cases} \lambda_i & \text{if } i < k \\ \lambda_{i+1} & \text{if } i \geq k \end{cases}$$

From $\lambda_k = 0_R$ and $\boldsymbol{\lambda} \in S_{m+1}$, it must be true that $\boldsymbol{\lambda}' \in S_m = \{0_m\}$ (use the same t and the fact that $m \leq m+1$). So that in total (clear), $\boldsymbol{\lambda} = 0_{m+1}$ and hence $S_{m+1} \subset \{0_{m+1}\}$.

This concludes the converse and finishes the induction step. □

A.3

Lemma. *For $r \in \mathbb{N}_{>0}$ and any field $\mathbb{F}$ such that $\mathrm{char}\,(\mathbb{F}) = 0$ or $\mathrm{char}\,(\mathbb{F}) > r$, let $M \in \mathbb{F}^{r\times r}$ be a matrix. The following are equivalent:*

1. $M^r = \mathbf{0}_{r\times r}$,
2. *M is nilpotent,*
3. $\sigma\,(M) = \{0_{\mathbb{F}}\}$ *where* $\sigma\,(M) := \mathrm{Root}_{P_{char,M}(X)}\left(\mathbb{F}^{alg}\right)$,
4. $\forall k \in \mathbb{N}_{>0}, \mathrm{tr}\left(M^k\right) = 0_{\mathbb{F}}$,
5. $\exists t \in \mathbb{N}, \forall k \in [\![1, r]\!], \mathrm{tr}\left(M^{t+k}\right) = 0_{\mathbb{F}}$.

One cannot reduce the set of powers for which the trace is $0_{\mathbb{F}}$ to an arbitrary set $S \subset \mathbb{N}_{>0}$ of size r. If $\mathrm{char}\,(\mathbb{F}) \neq 0$, then one cannot relax the requirement that $\mathrm{char}\,(\mathbb{F}) > r$.

Proof. For the equivalences, it suffices to prove that each statement $i.$ implies $i+1.$ (for $i \in \{1, 2, 3, 4\}$) and that 5. implies 1.

1. $\Rightarrow$ 2.: This is trivial as $r > 0$ so it satisfies the definition of being nilpotent (in the ring $\mathbb{F}^{r\times r}$).

2. $\Rightarrow$ 3.: Let $k \in \mathbb{N}_{>0}$ be the index of nilpotency of M (we could take any power $t \in \mathbb{N}_{>0}$ that satisfies $M^t = \mathbf{0}_{r\times r}$). Any $\lambda \in \sigma\,(M)$ must (standard) satisfy the equation $\lambda^k = 0_{\mathbb{F}}$. Since $\mathbb{F}$ is a domain and $k > 0$, this implies that $\lambda = 0_{\mathbb{F}}$ thus $\sigma\,(M) = \{0_{\mathbb{F}}\}$ (because $\sigma\,(M) \neq \varnothing$).

3. $\Rightarrow$ 4.: Let $\boldsymbol{\lambda} \in \left(\mathbb{F}^{\mathrm{alg}}\right)^r$ be any vector (the order in this vector doesn't matter) of exactly all the eigenvalues of M counted with their respective algebraic multiplicities. By the Spectral Mapping Theorem [A.1] one has that for all $k \in \mathbb{N}_{>0}$:

$$\mathrm{tr}\left(M^k\right) = \sum_{i\in r} \lambda_i^k.$$

Because $\sigma\,(M) = \{0_{\mathbb{F}}\}$, we must have $\mathrm{ran}\,(\boldsymbol{\lambda}) = \{0_{\mathbb{F}}\}$. Hence (as $k > 0$), $\mathrm{tr}\left(M^k\right) = \sum_{i\in r} 0_{\mathbb{F}} = 0_{\mathbb{F}}$.

4. $\Rightarrow$ 5.: This is trivial (use $t = 0$).

To finish, we need to show that 5. $\Rightarrow$ 1.. Now, notice that 3. $\Rightarrow$ 1.: indeed, the characteristic polynomial has degree r, so $P_{\mathrm{char},M}\,(X) = \prod_{\lambda\in\sigma(M)} (X-\lambda)^{m_{P_{\mathrm{char},M}(X)}(\lambda)} \overset{\sigma(M)=\{0_{\mathbb{F}}\}}{=} X^r$. We have by the Cayley-Hamilton theorem (valid over any field) that $M^r = \mathbf{0}_{r\times r}$. Hence 1. $\Leftrightarrow$ 3., and so it suffices, in fact, to show 6. $\Rightarrow$ 3.. This relies on the lemma [A.2]. Let $\boldsymbol{\lambda} \in \left(\mathbb{F}^{\mathrm{alg}}\right)^r$ be any vector (the order in this vector doesn't matter) of exactly all the eigenvalues of M counted with their respective algebraic multiplicities. By the Spectral Mapping Theorem [A.1], for all $k \in \mathbb{N}_{\geq 1}$, $\mathrm{tr}\left(M^k\right) = \sum_{i\in r} \lambda_i^k$. Hence if there exists $t \in \mathbb{N}$ such that $\forall k \in [\![1, r]\!], \mathrm{tr}\left(M^{t+k}\right) = 0_{\mathbb{F}}$, then by our lemma [A.2], we have $\forall i \in r, \lambda_i = 0_{\mathbb{F}}$. Hence $\sigma\,(M) = \{0_{\mathbb{F}}\}$ (since $\sigma\,(M) \neq \varnothing$).

To show that a general set of powers $S \subset \mathbb{N}_{>0}$ of size equal to the dimension of the matrix does not suffice:

Let $r = 3$ and consider the field $\mathbb{C}$. Let $\omega = e^{2\pi i/3}$ be a primitive third root of unity, and define the diagonal matrix:

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

The eigenvalues of M are $1, \omega$, and ω^2. Since none are zero, M is not nilpotent. However, if we look at the non-consecutive set of powers $S = \{1, 2, 4\}$ (note $|S| = 3 = r$), we find (because $X^3 - 1 = (X - 1)(X^2 + X + 1)$):

- $\operatorname{tr}(M^1) = 1 + \omega + \omega^2 = 0$
- $\operatorname{tr}(M^2) = 1^2 + \omega^2 + \omega^4 = 1 + \omega^2 + \omega = 0$
- $\operatorname{tr}(M^4) = 1^4 + \omega^4 + \omega^8 = 1 + \omega + \omega^2 = 0$

Thus, r distinct and strictly positive powers can all have zero trace without the matrix being nilpotent.

To show that the characteristic must be 0 or strictly greater than r:

Let p be a prime and consider the field $\mathbb{F}_p$. Now take $r = p$ and take the identity matrix I_r. Then I_r is not nilpotent since $I_r^k = I_r \neq \mathbf{0}_{r\times r}$. However, $\operatorname{tr}\left(I_r^k\right) = \operatorname{tr}(I_r) = \sum_{i\in r} 1_{\mathbb{F}_p} = 0_{\mathbb{F}_p}$ (because $r = p$ and we are in characteristic p). □

Remark. Although one cannot use any set of r distinct powers for which the trace is $0_{\mathbb{F}}$, one can still apply this theorem in certain other special cases. One example is that for any $l \in \mathbb{N}_{>0}$ and $t \in \mathbb{N}$, the r distinct powers $\{l \cdot (t + k) \mid k \in [\![1, r]\!]\}$ suffice: simply apply the theorem to M^l to deduce that M^l is nilpotent and hence M is nilpotent.

A.4

Theorem 2 (Newton's Identities)**.** *Let R be a commutative unital ring together with the canonical morphism $\operatorname{can}_R\colon \mathbb{Z} \to R$, and write for any integer k: $k_R := \operatorname{can}_R(k)$. For positive integers $1 \leq k \leq n$, the following identity holds over the ring $R[X_0, \ldots, X_{n-1}] = R[\mathbf{X}]$:*

$$k_R \left(\sum_{\substack{A\in\mathscr{P}(n)\\|A|=k}} \prod_{a\in A} X_a \right) - \sum_{i=1}^{k} (-1)_R^{i-1} \left(\sum_{\substack{A\in\mathscr{P}(n)\\|A|=k-i}} \prod_{a\in A} X_a \right) \left(\sum_{j\in n} X_j^i \right) = 0_{R[\mathbf{X}]}.$$

The following short combinatorial proof is due to Doron Zeilberger (1983).

Proof. The left hand side of the identity is equal to:

$$\left(\sum_{\substack{A\in\mathscr{P}(n)\\|A|=k}} \sum_{j\in A} (-1)_R^0 \left(\prod_{a\in A} X_a \right) X_j^0 \right) + \left(\sum_{i=1}^{k} \sum_{\substack{A\in\mathscr{P}(n)\\|A|=k-i}} \sum_{j\in n} (-1)_R^i \left(\prod_{a\in A} X_a \right) X_j^i \right). \qquad (*)$$

We establish the identity by defining a sign-reversing involution on a combinatorial structure.

Define the set of 3-tuples:

$$\mathcal{A}(n,k) := \left\{ \langle A, j, i\rangle \;\middle|\; \begin{array}{l} A \in \mathscr{P}(n),\ |A| \leq k,\ j \in n,\ i = k - |A|, \\ \text{and if } i = 0 \text{ then } j \in A \end{array} \right\}.$$

The *weight* $w\colon \mathcal{A}(n,k) \to R[\mathbf{X}]$ is defined by $\langle A,j,i\rangle \mapsto (-1)^i_R \left(\prod_{a\in A} X_a\right) X_j^i \in R[\mathbf{X}] \backslash \left\{0_{R[\mathbf{X}]}\right\}$. The sum of the weights of all elements in $\mathcal{A}(n,k)$, namely $\sum_{e\in\mathcal{A}(n,k)} w(e)$, is readily seen to be equal to (*). To show this sum is zero, define the function $T\colon \mathcal{A}(n,k) \to \mathcal{A}(n,k)$ as:

$$T(\langle A,j,i\rangle) = \begin{cases} \langle A\setminus\{j\}, j, i+1\rangle, & \text{if } j\in A, \\ \langle A\cup\{j\}, j, i-1\rangle, & \text{if } j\notin A. \end{cases}$$

With a mental exercise, we see that T is well defined and satisfies:

$$w\circ T = -w, \quad T\circ T = \mathrm{id}_{\mathcal{A}(n,k)}.$$

Thus, every element $\langle A,j,i\rangle$ uniquely pairs with its image under T (since it is an involution (which has no fixed point)) and their weights cancel. Hence, the total sum is zero. Formally[5] $\exists P \subset \mathcal{A}(n,k)$ such that $\mathcal{A}(n,k) = \bigsqcup_{p\in P} \{p, T(p)\}$ (and for each $p\in P$, the set $\{p,T(p)\}$ has size 2) so that:

$$\sum_{e\in\mathcal{A}(n,k)} w(e) = \sum_{p\in P} (w(p) + w(T(p))) = \sum_{p\in P} (w(p) - w(p)) = \sum_{p\in P} 0_{R[\mathbf{X}]} = 0_{R[\mathbf{X}]}$$

(even if T had a fixed point the equation $w\circ T = -w$ would imply that the weight of it is $0_{R[\mathbf{X}]}$ so it wouldn't matter). □

A.5

Lemma (Vandermonde Determinant)**.** *Let R be a commutative unital ring and $n\in\mathbb{N}_{>0}$. For any vector $\boldsymbol{x}\in R^n$, let $V_{\boldsymbol{x}}\in R^{n\times n}$ be the Vandermonde matrix defined by $(i,j)\mapsto x_i^j$ for $i,j\in n$ (where $x^0 = 1_R$ even if $x = 0_R$), i.e.,*

$$V_{\boldsymbol{x}} = \begin{pmatrix} 1_R & x_0 & \dots & x_0^{n-1} \\ 1_R & x_1 & \dots & x_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1_R & x_{n-1} & \dots & x_{n-1}^{n-1} \end{pmatrix}.$$

Then:

$$\det_R(V_{\boldsymbol{x}}) = \prod_{0\le i<j<n} (x_j - x_i).$$

Proof. We proceed by induction on $n\in\mathbb{N}_{>0}$, quantifying over all vectors $\boldsymbol{x}\in R^n$.

Base case $n=1$: Let any $\boldsymbol{x}\in R^1$. The matrix is $V_{\boldsymbol{x}} = \left(1_R\right)$. Its determinant is 1_R, which matches the empty product $\prod_{0\le i<j<1}(x_j - x_i) = 1_R$.

Induction step: Assume the statement holds for some $n\in\mathbb{N}_{>0}$. We wish to prove it for $n+1$. Let any $\boldsymbol{x}\in R^{n+1}$. We perform elementary column operations, which do not alter the determinant over a commutative ring. For each column index j from n down to 1, we subtract x_0 times column $j-1$ from column j. Formally, the new columns C'_j are given by $C'_j := C_j - x_0 C_{j-1}$ for $j\in[\![1,n]\!]$, and $C'_0 := C_0$.

[5] Any involution τ on a set S induces a relation on S: $\sim_\tau \subset S\times S$ defined by $x\sim y \Leftrightarrow y = \tau(x)$. This is an equivalence relation and the equivalence class of $x\in S$ is $[x]_{\sim_\tau} = \{x,\tau(x)\}$ (which can have size 1 if x is a fixed point of τ). Recall that the set of equivalence classes partitions S. This implies (for an arbitrary set by the axiom of choice) (for a finite set by induction) that $\exists P\subset S$ with $S = \bigsqcup_{p\in P}[p]_{\sim_\tau}$.

The entries of the new matrix $V'_{\boldsymbol{x}}$ are:

$$V'_{\boldsymbol{x}}(i,j) = \begin{cases} 1_R & \text{if } j = 0 \\ x_i^j - x_0 x_i^{j-1} = x_i^{j-1}(x_i - x_0) & \text{if } j > 0 \end{cases}$$

In the first row ($i = 0$), for $j > 0$, the entries are $x_0^{j-1}(x_0 - x_0) = 0_R$. Thus, the first row is exactly $\begin{pmatrix} 1_R & 0_R & \dots & 0_R \end{pmatrix}$.

Expanding the determinant along the first row (using the Laplace expansion, which is valid over any commutative ring), we get:

$$\det_R(V_{\boldsymbol{x}}) = \det_R(V'_{\boldsymbol{x}}) = (-1_R)^{0+0} \cdot \det_R\left((V'_{\boldsymbol{x}})_{(0|0)}\right) = \det_R\left((V'_{\boldsymbol{x}})_{(0|0)}\right),$$

where $(V'_{\boldsymbol{x}})_{(0|0)} \in R^{n \times n}$ is the submatrix obtained by deleting row 0 and column 0.

By the multilinearity of the determinant with respect to the rows, we can factor out the common scalar $(x_{r+1} - x_0)$ from each row $r \in n$ of $(V'_{\boldsymbol{x}})_{(0|0)}$, to obtain:

$$\det_R\left((V'_{\boldsymbol{x}})_{(0|0)}\right) = \left(\prod_{r \in n}(x_{r+1} - x_0)\right) \det_R(V_{\boldsymbol{x}'}) = \left(\prod_{0<j<n+1}(x_j - x_0)\right) \det_R(V_{\boldsymbol{x}'}),$$

where $\boldsymbol{x}' \colon n \to R$ is defined by $k \mapsto x_{k+1}$. Hence, by the induction hypothesis, $\det_R(V_{\boldsymbol{x}'}) = \prod_{0 \le i < j < n}(x_{j+1} - x_{i+1}) = \prod_{1 \le i < j < n+1}(x_j - x_i)$.

Therefore:

$$\det_R(V_{\boldsymbol{x}}) = \left(\prod_{0<j<n+1}(x_j - x_0)\right) \prod_{1 \le i < j < n+1}(x_j - x_i) = \prod_{0 \le i < j < n+1}(x_j - x_i).$$

This completes the induction step and the proof. □

A.6

Lemma. *Let $l \in \mathbb{N}_{>0}$ and R be a commutative unital ring together with the canonical morphism $\mathrm{can}_R \colon \mathbb{Z} \to R$ and write for any integer k: $k_R := \mathrm{can}_R(k)$. Let $N \in R^{l \times l}$ be a nilpotent matrix. If $I_l + N$ has finite order $r \in \mathbb{N}_{>0}$ (where I_l is the identity matrix in $R^{l \times l}$) such that $r_R \in R^\times$ is invertible, then $N = \mathbf{0}_{R^{l \times l}}$.*

Proof. Let $r := \mathrm{ord}_{R^{l \times l}}(I_l + N) \in \mathbb{N}_{>0}$ be the order of $I_l + N$. Then, by the binomial theorem (noting that I_l and N commute),

$$I_l = (I_l + N)^r = \sum_{j=0}^{r} \binom{r}{j}_R N^j = I_l + \sum_{j=1}^{r} \binom{r}{j}_R N^j,$$

It follows that

$$\mathbf{0}_{R^{l \times l}} = \sum_{j=1}^{r} \binom{r}{j}_R N^j.$$

and because R is commutative, we can factor N to obtain:

$$\mathbf{0}_{R^{l \times l}} = N \left(\sum_{j=1}^{r} \binom{r}{j}_R N^{j-1}\right) = N \left(r_R I_l + \sum_{j=2}^{r} \binom{r}{j}_R N^{j-1}\right).$$

Let $S := r_R I_l + \sum_{j=2}^{r} \binom{r}{j}_R N^{j-1} \in R^{l\times l}$ be the right-hand factor in this product, and define $E := \sum_{j=2}^{r} \binom{r}{j}_R N^{j-1} \in R^{l\times l}$ (the sum is possibly empty if $r = 1$, in which case it is the empty sum and $E = \mathbf{0}_{l\times l}$). So $S = r_R I_l + E$, and we claim that S is invertible.

Indeed, N is nilpotent, and so are all of its powers. Since R is commutative, any scalar multiple λN^k with $\lambda \in R$ and $k \in \mathbb{N}_{>0}$ is nilpotent. Moreover, for any (possibly non-commutative) unital ring A (here $R^{l\times l}$), the set of nilpotent elements $\operatorname{Nil}(A)$ is closed[6] under finite sums and products, provided that the terms commute pairwise. Because R is commutative, we get that for any $\lambda, \lambda' \in R$ and $k, k' \in \mathbb{N}_{>0}$, the elements λN^k and $\lambda' N^{k'}$ commute. Hence $E \in \operatorname{Nil}\left(R^{l\times l}\right)$.

Now $r_R \in R^\times$, so we must have $r_R I_l \in \left(R^{l\times l}\right)^\times$. As E is nilpotent and E commutes with $r_R I_l$ (since R is commutative), the element $S := r_R I_l + E$, being the sum of an invertible element of $R^{l\times l}$ and a nilpotent one, must be invertible[7].

Thus, multiplying on the right by S^{-1} on both sides of the equation $\mathbf{0}_{R^{l\times l}} = NS$ yields $N = \mathbf{0}_{R^{l\times l}}$. □

[6] For the finite product, the index of nilpotency is bounded above by the minimum of the respective indices of nilpotency (use the commutativity of the factors). For the finite sum, the index of nilpotency is bounded above by 1 plus the sum of the nilpotency indices minus the number of summands. To see this, use the multinomial theorem (which is valid since the summands commute) and use the pigeonhole principle.

[7] This is a general fact about any (possibly non-commutative) unital ring A: if $a \in A^\times$, $b \in \operatorname{Nil}(A)$, and $ab = ba$, then $a + b \in A^\times$. Indeed, let $v \in \mathbb{N}_{>0}$ be the index of nilpotency of b. Then, since a and b commute, so do a^{-1} and b, and we have $\left(ba^{-1}\right)^v = b^v a^{-v} = 0_A$. A simple computation (using the fact that $\pm 1_A$ commutes with every element, and that a, b, and a^{-1} commute with one another, as do their powers) shows that the element

$$a^{-1}\left(\sum_{k=0}^{v-1} (-1_A)^k \left(ba^{-1}\right)^k\right) \in A,$$

is both a left and right inverse of $a + b = a\left(1_A + a^{-1}b\right) = \left(1_A + ba^{-1}\right)a$, and so $a + b \in A^\times$