Problem Set Week 8 Solutions

ETHZ Math Olympiad Club

7 April 2025

1 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 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 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:

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

2 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:

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

3 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 $\frac{n(n-1)}{2}$.

4 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 ($\exists k \in \mathbb{N}^*,\ A^k = I_n$) and satisfies

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

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

Solutions:

Solution 1.

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:

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

Therefore, $\alpha \in \mathbb{C}$ is an eigenvalue of A if and only if $\alpha - 1$ is an eigenvalue of mB; that is, 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., $|\alpha| = 1$. Any eigenvalue $\beta \in \mathbb{C}$ of B then satisfies (here $m \geq 3$ is crucial):

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

Now we prove that 0 is the only eigenvalue of B

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

Intermediate step 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 $n \geq 1$), $P_{\mathrm{char},B}(X) := \det_{\mathbb{Q}(X)}(XI_n - B) \in \mathbb{Z}[X]$, as a product of $l \in \mathbb{N}^*$ unique irreducible polynomials (up to invertible element here these are ± 1). Since $P_{\mathrm{char},B}(X)$ is monic, the irreducible polynomials must have leading coefficients in $\mathbb{Z}^\times = \{\pm 1\}$. Therefore, they must have degree at least one and cannot be 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,

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

such that

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

Now, let β be an eigenvalue of B, i.e., $\beta \in \mathrm{Root}_{P_{\mathrm{char},B}(X)}(\mathbb{C})$. Hence, there exists $j \in l$ such that $\beta \in \mathrm{Root}_{P_j(X)}(\mathbb{C})$. 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

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

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

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 $P_j(X)$:

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

Then

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

Since $P_j(X) \in \mathbb{Z}[X]$, we must have $P_j(0) \in \mathbb{Z}$, and because $|P_j(0)| < 1$ 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 $\sigma(B) = \{0\}$ as desired.

Alternative proof of intermediate step using Newton's identities.

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

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

and the k-th elementary symmetric polynomials in m

$$e_k(\mathbf{X}) := \sum_{\substack{A \in \mathscr{P}(m) \\ |A| = k}} \prod_{a \in A} X_a \in \mathbb{Z}[\mathbf{X}]^{[3]}.$$

The Newton's identities relate these polynomials by the identity (valid for $m \geq k \geq 1$):

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

For a short combinatorial proof of these identities, see the Appendix [A.1]. 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 the vector of eigenvalues of B, counted with multiplicity, so that $\sigma(B) = \mathrm{Root}_{P_{\mathrm{char},B}(X)}(\mathbb{C}) = \{\beta_i \mid i \in n\}$. In our case, where the number of variables is $n \geq 1$, we define, for all $k \geq 0$, the k-th power sum and the k-th elementary symmetric polynomial in the eigenvalues of B, respectively:

$$p_k := p_k(\boldsymbol{\beta}) = \sum_{i \in n} \beta_i^k, \quad e_k := e_k(\boldsymbol{\beta}) = \sum_{\substack{A \in \mathscr{P}(n) \\ |A| = k}} \prod_{a \in A} \beta_a.$$

Note that $p_k = \mathrm{tr}\left(B^k\right)$, and $e_k = c_{n-k}(P_{\mathrm{char},B}(X))$. Since $B \in \mathbb{Z}^{n \times n}$, we have $p_k \in \mathbb{Z}$ and $e_k \in \mathbb{Z}$.

[3] That is:

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

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

Let $\gamma \in \sigma(B)$ be an eigenvalue of B. Since $|\gamma| < 1$, we have $\gamma^N \overset{N\to+\infty}{\longrightarrow} 0$. Therefore, each term in the finite sum (comprising n summands) p_N tends to zero as $N \to +\infty$; that is,

$$p_N \overset{N\to+\infty}{\longrightarrow} 0.$$

However, as mentioned earlier, for all $N \in \mathbb{N}$, $p_N \in \mathbb{Z}$, so there exists $M \geq 0$ such that for all $N \geq M$, $p_N = 0$. We now show that this condition implies, surprisingly, that $\boldsymbol{\beta} = \mathbf{0}_n$. For this, we denote by $\boldsymbol{\beta}^M := \left(\beta_i^M\right)_{i\in n}$ the eigenvalues of B^M, and we define, for all $k \geq 0$,

$$\tilde{p}_k := p_k\left(\boldsymbol{\beta}^M\right) = \sum_{i\in n}\left(\beta_i^M\right)^k = p_{Mk}, \quad \tilde{e}_k := e_k\left(\boldsymbol{\beta}^M\right) = \sum_{\substack{A\in\mathscr{P}(n)\\|A|=k}}\prod_{a\in A}\beta_a^M.$$

Notice that $\tilde{e}_k = c_{n-k}\left(P_{\mathrm{char},B^M}(X)\right)$. We prove by induction that for $k \geq 1$, we have $\tilde{e}_k = 0$.

- For $k = 1$, $\tilde{e}_1 = \tilde{p}_1 = p_M = 0$.
- Let $k \geq 1$ and assume that for all j with $1 \leq j \leq k-1$, we have $\tilde{e}_j = 0$. Then Newton's identities give
$$k\tilde{e}_k = (-1)^{k-1}\tilde{e}_0\tilde{p}_k = (-1)^{k-1}\tilde{p}_k = (-1)^{k-1}p_{Mk}.$$
As $Mk \geq M$, we have $p_{Mk} = 0$, so $k\tilde{e}_k = 0$, and since $k \neq 0$, it follows that $\tilde{e}_k = 0$.

This implies that the characteristic polynomial of B^M is X^n, meaning all eigenvalues of B^M are zero; that is, $\boldsymbol{\beta}^M = \mathbf{0}_n$, and hence $\boldsymbol{\beta} = \mathbf{0}_n$[4].

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

The proof can be found in Appendix [A.2].

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 $mB = \mathbf{0}_{n\times n}$, and so $B = \mathbf{0}_{n\times n}$ (as $m \in \mathbb{Q}^\times$). Hence, $A = I_n$, and this concludes the proof.

[4] In fact, we have just proved a curious result: if we have $\boldsymbol{\lambda} \in \mathbb{C}^n$ such that there exists some $M \in \mathbb{N}$ for which, for all $N \geq M$, we have $p_N(\boldsymbol{\lambda}) = 0$, then it follows that $\boldsymbol{\lambda} = \mathbf{0}_n$. Indeed, one may either take the companion matrix of the monic polynomial $\prod_{i\in n}(X - \lambda_i)$—that is, the matrix whose characteristic polynomial is this one—and proceed as we have just done, or, without speaking of matrices at all, define for all $k \geq 0$ the elements $\hat{e}_k := e_k\left(\lambda^M\right)$, and prove by induction, as above, that each of them (starting from 1) is zero. Then perform a descending induction: $0 = \hat{e}_n = \prod_{i\in n}\lambda_i^M$, hence there is an $i_0 \in n$ with $\lambda_{i_0} = 0$. Now remove λ_{i_0} from the set $\{\lambda_i \mid i \in n\}$, obtaining a smaller set of size n'. If it is empty ($n' = 0$) then $\boldsymbol{\lambda} = \mathbf{0}_n$, else we consider the vector $\boldsymbol{\lambda}' \in \mathbb{C}^{n'}$ consisting of the remaining elements. Again, it is clear that for all $N \geq M$, each $p_N(\boldsymbol{\lambda}') = 0$ (where the N-th power sum polynomials are in n' variables); their k-th elementary symmetric sums in $(\boldsymbol{\lambda}')^M$ must again vanish (starting from $k = 1$ and applying the same induction), so $e_{n'}\left((\boldsymbol{\lambda}')^M\right) = 0$ and there is $i_1 \in n$ such that $\lambda_{i_1} \in \{\lambda_i \mid i \in n\} \setminus \{\lambda_{i_0}\}$ is 0. Continue this process until the entire set is exhausted. The advantage of the latter procedure is that we can, in fact, apply it to any integral ring R of characteristic 0, since it then canonically contains $\mathbb{Z} \hookrightarrow R$, and thus the Newton identities hold on R.

Solution 2.

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

$$B := \frac{1}{p^{c'}}(A - I_n),$$

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 $-kp^{c'}B \not\equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''+1}}$ (but obviously $kp^{c'}B \equiv \mathbf{0}_{n \times n} \pmod{p^{c'+c''}}$).

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[5]:

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

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:

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

[5] A quick proof of this formula for $p \in \mathbb{P}$ and $i \geq 1$ proceeds as follows: define $M := \max\{v_p(t) \,|\, 1 \leq t \leq i\}$, 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.

Counterexamples 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 case between even and odd dimension. When $n = 2k > 0$ we place k copies of a 2×2 counterexamples 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

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

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

5 problem (unknown)

For this problem, we strongly encourage you to try to recreate the scenario in the real world with a sufficiently long rope and some nails/pins fixed to a surface. We have $n \geq 1$ nails fixed to a wall and a sufficiently long rope wrapped around these nails in a non-trivial configuration (i.e., the rope must be physically engaged with the nails in such a way that it does not fall off initially). For any fixed $n \geq 1$, find **all** wrapping configuration around the n nails such that:

1. The rope remains securely wrapped (i.e., it does not fall off when all nails are present).
2. When **any single nail** is removed (regardless of which one), the entire rope falls from the wall (in practice, some friction might prevent it from falling, but we consider it as "falling" if it is no longer securely wrapped).

By "wrapping," we mean that the rope can make multiple loops around the nails in non-trivial ways (e.g., making loops around single nails or multiple nails, or passing under/over certain nails). Here are examples where we have labeled the nails c_0, c_1, and c_2:

Figure 1: *Nontrivial rope wrappings for $n = 1$* ***satisfying*** *the property. The first configuration has a single loop around c_0 (clockwise or counterclockwise), while the second has at least two loops around c_0 (clockwise or counterclockwise).*

Figure 2: *Nontrivial rope wrappings for $n = 2$ that* ***do not satisfy*** *the property. The first configuration has no loop around c_0 but at least two loops (clockwise or counterclockwise) around c_1. The second configuration has at least two loops (clockwise or counterclockwise) around both c_0 and c_1.*

Figure 3: *Nontrivial rope wrappings (performed from left to right) for $n = 3$* ***not satisfying*** *the property. The first configuration has a single clockwise loop around c_0, no loop around c_1, and a single clockwise loop around c_2. The second configuration has at least two clockwise loops around c_0, no loop around c_1, and at least two counter-clockwise loops around c_2.*

Solution:

Let $n \geq 1$. To formalize the mathematical model of wrappings, we consider a set of n distinct symbols $\{c_i \mid i \in n\}$, interpreted as n nails. For simplicity, we imagine nails pinned from left to right, with c_0 on the far left and c_{n-1} on the far right. What **only** matters in the wrapping are the orientations, counts, and adjacency relationships of the loops. (Visualization is simpler in a physical simulation!)

Fix an orientation convention (clockwise as 1, counterclockwise as -1). We observe that there is a simple recursive procedure that, given a wrapping process, outputs a word over the alphabet $C_n := \{c_i^1 \mid i < n\} \cup \left\{c_i^{-1} \,\middle|\, i < n\right\}$ by recursively recording loop orientations and positions from left to right. One key observation is that a "loop" need not form a closed circle as shown in the examples in the problem statement. Passing **above** a nail from left to right counts as a clockwise loop; passing from right to left counts as counterclockwise. Thus, we want to encode each action (c_i, θ), where $i < n$ and $\theta \in \{1, -1\}$, and their adjacency by writing them from left to right in the same order as the execution of the wrapping.

More formally, if one has partially constructed a word $w \in C_n^{<\omega}$ (including the empty word ε) from a partial wrapping process, then we update the word as follows. If no action is taken, w remains unchanged. Otherwise, performing a loop at c_i with orientation θ updates the word to $w \frown \left\langle c_i^\theta \right\rangle$. This procedure defines a word for any wrapping process: Each time an action updates the word. If the wrappings in the examples of the problem statement are performed from left to right, then they produce (for some $r, s \geq 2$) the words:

$$\left\langle {c_0}^1 \right\rangle, \left\langle {c_0}^1 \right\rangle^r, \left\langle {c_1}^1 \right\rangle^r, \left\langle {c_0}^1, {c_1}^1 \right\rangle^r, \left\langle {c_0}^1, {c_2}^1 \right\rangle^r, \left\langle {c_0}^1 \right\rangle^r \frown \left\langle {c_2}^{-1} \right\rangle^s \text{ respectively.}$$

Conversely, every word corresponds to a wrapping by executing its symbols from left to right recursively. This gives us a surjection from the set of words to the set of wrappings. For example, if $i < j < n$, the word $\langle c_i^1 \rangle^3 \frown \left\langle c_j^{-1} \right\rangle^4$ represents:

- 3 clockwise loops at c_i,
- Moving **below** intermediate nails $c_{i+1}, \ldots, c_{j-1}$ (to avoid creating unintended loops),
- 4 counterclockwise loops at c_j.

This correspondence, although being a surjective functional relation on one side, is not injective, as one may notice. Fix any word $w \in C_n^{<\omega}$, perform its corresponding wrapping as above, then making a loop at c_i with orientation θ and then performing another loop at c_i with orientation $-\theta$ *leaves* the physical state of the wrapping unchanged while resulting from two different words:

$$w \frown \left\langle c_i^\theta \right\rangle \frown \left\langle c_i^{-\theta} \right\rangle \neq w.$$

This is one instance that obstructs our attempt to establish a *bijective correspondence*. In fact, we observe that all problems that block our attempt arise from combinations of words with the *fundamental obstruction* mentioned above.

This discrepancy (the obstruction to injectivity) can always be resolved by defining the equivalence classes of words[6]. Thus, we choose to identify words that differ by canceling

[6]This is a general fact: if $f : A \twoheadrightarrow B$ is a surjective function, then the relation $\sim \subset A \times A$ defined by $a \sim a'$ if and only if $f(a) = f(a')$ is an equivalence relation. It induces a bijective function $\tilde{f}$ such that $\tilde{f} \circ q = f$, where $q : A \to A/\sim$ is the quotient map.

adjacent pairs $\left\langle c_i^{\theta} \right\rangle \frown \left\langle c_i^{-\theta} \right\rangle$, and we consider the smallest equivalence relation that contains this identification. To distinguish them from generic words, we will call these equivalence classes *wrapping words*. Those familiar with the subject will recognise that *wrapping words* over the alphabet C_n can be uniquely identified with elements of the free group $F\left(\{c_i \mid i < n\}\right)$. For the complete construction, see the appendix [B]. Conversely, each equivalence class of a word w over C_n corresponds to a unique physical wrapping of the rope around the nails via the retrieval procedure described above.

With this correspondence, we see that for each $i < n$, removing the nail c_i from a wrapping corresponding to an element $w \in F\left(\{c_i \mid i < n\}\right)$ obviously gives us another wrapping around the remaining nails $\{c_j \mid j < n, j \neq i\}$, which again corresponds (by our correspondence) to an equivalence class of a word written in the very same alphabet without $\left\{c_i^1, c_i^{-1}\right\}$. That is, an element in $F\left(\{c_j \mid j < n\} \setminus \{c_i\}\right)$. It is then easy to see that the unique function $\tilde{\pi}_i$ defined such that the following diagram commute:

$$\begin{array}{ccc} \{\text{wrappings on } \{c_j \mid j < n\}\} & \xrightarrow{\text{removing the nail } c_i} & \{\text{wrappings on } \{c_j \mid i \neq j < n\}\} \\ \| & & \| \\ F\left(\{c_j \mid j < n\}\right) & \xrightarrow[\tilde{\pi}_i]{} & F\left(\{c_j \mid i \neq j < n\}\right) \end{array}$$

is the one induced from the function π_i over $C_n^{<\omega}$ that removes every occurrence of c_i^1 and c_i^{-1} in any word $w \in C_n^{<\omega}$ and leaves the rest intact. That is:

$$\pi_i : C_n^{<\omega} \to \left(C_n \setminus \left\{c_i^1, c_i^{-1}\right\}\right)^{<\omega}$$

defined by:

$$\pi_i\left(w\right) = \frown_{\substack{j \in \mathrm{dom}(w) \\ w_j \notin \left\{c_i^1, c_i^{-1}\right\}}} \left\langle w_j \right\rangle$$

where the concatenation is in the order of the natural order of the indices in:

$$\left\{ j \in \mathrm{dom}\left(w\right) \,\middle|\, w_j \notin \left\{c_i^1, c_i^{-1}\right\} \right\}.$$

We now search the word that satisfies the property as stated in the problem statement. Notice that the rope that falls or is initially wrapped in trivial ways corresponds to any word $w \sim \varepsilon$ (the empty sequence). So we search for a word $w \in C_n^{<\omega}$ such that $w \not\sim \epsilon$. Moreover, each c_i must occur at least once in any equivalent word to w; otherwise, if there is a certain c_i not occurring in an equivalent word to w, then removing the nail c_i would not affect the underlying wrapping, and so the wrapping does not have the property that removing any single nail causes the entire rope to fall. So we search for a word $w \in C_n^{<\omega}$ such that:

$$\forall v \in [w]_\sim \, \forall i < n \quad v \notin \left(C_n \setminus \left\{c_i^1, c_i^{-1}\right\}\right)^{<\omega}.$$

We require the additional property that removing any nail makes the rope fall, i.e., every projection of the word is equivalent to the empty sequence $\pi_i\left(w\right) \sim \varepsilon$. Thus, the searched set of *wrapping words* is:

$$\mathcal{S}_n := \left\{ [w]_\sim \in \bigcap_{i<n} \ker\left(\tilde{\pi}_i\right) \,\middle|\, \forall v \in [w]_\sim \, \forall i < n \quad v \notin \left(C_n \setminus \left\{c_i^1, c_i^{-1}\right\}\right)^{<\omega} \right\}.$$

For $n = 1$, we have that $\left(C_1 \setminus \left\{c_0^1, c_0^{-1}\right\}\right)^{<\omega} = \varnothing^{<\omega} = \{\varepsilon\}$, so that:

$$\mathcal{S}_1 = \{[w]_\sim \in \ker\left(\tilde{\pi}_0\right) \mid \forall v \in [w]_\sim \quad v \neq \varepsilon\} = \ker\left(\tilde{\pi}_0\right) \setminus \{[\varepsilon]_\sim\}.$$

Indeed, this is quite obvious (in regard to the example given in the problem statement for $n = 1$) that all wrappings have the property as long as they are not the trivial one.

Now suppose $n \geq 2$. It is easy (though quite long) to prove by induction on n that $\bigcap_{i<n} \ker(\tilde{\pi}_i)$ is the subgroup generated by all k-th commutators for $2 \leq k \leq n$ of elements in $\{[c_i^1]_\sim \mid i < n\}$:

$$\bigcap_{i<n} \ker(\tilde{\pi}_i) = \left\langle \left\{ \left[\left[c_{j_0}^1\right]_\sim, \ldots, \left[c_{j_{k-1}}^1\right]_\sim \right] \,\middle|\, \exists k \exists j \quad 2 \leq k \leq n \wedge j : k \to n \right\} \right\rangle,$$

where we define recursively for $k = 2$ and any $j : 2 \to n$:

$$\left[\left[c_{j_0}^1\right]_\sim, \left[c_{j_1}^1\right]_\sim \right] := \left[c_{j_0}^1\right]_\sim^{-1^\frown} \left[c_{j_1}^1\right]_\sim^{-1^\frown} \left[c_{j_0}^1\right]_\sim^\frown \left[c_{j_1}^1\right]_\sim,$$

and for $3 \leq k$ and any $i : k \to n$:

$$\left[\left[c_{j_0}^1\right]_\sim, \ldots, \left[c_{j_{k-1}}^1\right]_\sim \right] = \left[\left[\left[c_{j_0}^1\right]_\sim, \ldots, \left[c_{j_{k-2}}^1\right]_\sim \right], \left[c_{i_{k-1}}^1\right]_\sim \right].$$

Since we must have at least each occurrence of c_i in our word, we must restrict ourselves to the set of all n-th commutators with distinct elements (that is, the indexation must be injective). Hence, for $n \geq 2$:

$$\mathcal{S}_n = \left\langle \left\{ \left[\left[c_{j_0}^1\right]_\sim, \ldots, \left[c_{j_{k-1}}^1\right]_\sim \right] \,\middle|\, \exists j \quad j : n \hookrightarrow n \right\} \right\rangle \setminus \{[\varepsilon]_\sim\}.$$

For example:

- When $n = 2$, the *wrapping words* are generated by the two generators:

  $$\left[\left[c_0{}^1\right]_\sim, \left[c_1{}^1\right]_\sim \right] := \left[c_0{}^1\right]_\sim^{-1^\frown} \left[c_1{}^1\right]_\sim^{-1^\frown} \left[c_0{}^1\right]_\sim^\frown \left[c_1{}^1\right]_\sim = \left[\left\langle c_0{}^{-1}, c_1{}^{-1}, c_0{}^1, c_1{}^1 \right\rangle \right]_\sim,$$

  and

  $$\left[\left[c_1{}^1\right]_\sim, \left[c_0{}^1\right]_\sim \right] := \left[c_1{}^1\right]_\sim^{-1^\frown} \left[c_0{}^1\right]_\sim^{-1^\frown} \left[c_1{}^1\right]_\sim^\frown \left[c_0{}^1\right]_\sim = \left[\left\langle c_1{}^{-1}, c_0{}^{-1}, c_1{}^1, c_0{}^1 \right\rangle \right]_\sim.$$

  i.e., the physical wrapping corresponding to these generator are (for $j \in \{0, 1\}$):

  - 1 counterclockwise loop at c_j,
  - 1 counterclockwise loop at c_{1-j},
  - 1 clockwise loop at c_j,
  - 1 clockwise loop at c_{1-j}.

  So that:

  $$\mathcal{S}_2 = \left\langle \left\{ \left[\left\langle c_0{}^{-1}, c_1{}^{-1}, c_0{}^1, c_1{}^1 \right\rangle \right]_\sim, \left[\left\langle c_1{}^{-1}, c_0{}^{-1}, c_1{}^1, c_0{}^1 \right\rangle \right]_\sim \right\} \right\rangle \setminus \{[\varepsilon]_\sim\},$$

  i.e., the set of composition of the above physical wrappings that do not make a trivial physical wrapping **is** the set of all physical wrappings that have the required property.

- Similarly, for $n = 3$, $\mathcal{S}_3$ is the set of *wrapping words* generated by all combinations of the following generators that do not yield the trivial *wrapping word*:

$$\left[\left[c_0{}^1\right]_\sim, \left[c_1{}^1\right]_\sim, \left[c_2{}^1\right]_\sim\right] = \left[\left\langle c_0{}^{-1}, c_1{}^{-1}, c_0{}^1, c_1{}^1, c_2{}^{-1}, c_1{}^{-1}, c_0{}^{-1}, c_1{}^1, c_0{}^1, c_2{}^1\right\rangle\right]_\sim,$$

$$\left[\left[c_0{}^1\right]_\sim, \left[c_2{}^1\right]_\sim, \left[c_1{}^1\right]_\sim\right] = \left[\left\langle c_0{}^{-1}, c_2{}^{-1}, c_0{}^1, c_2{}^1, c_1{}^{-1}, c_2{}^{-1}, c_0{}^{-1}, c_2{}^1, c_0{}^1, c_1{}^1\right\rangle\right]_\sim,$$

$$\left[\left[c_1{}^1\right]_\sim, \left[c_2{}^1\right]_\sim, \left[c_0{}^1\right]_\sim\right] = \left[\left\langle c_1{}^{-1}, c_2{}^{-1}, c_1{}^1, c_2{}^1, c_0{}^{-1}, c_2{}^{-1}, c_1{}^{-1}, c_2{}^1, c_1{}^1, c_0{}^1\right\rangle\right]_\sim,$$

$$\left[\left[c_1{}^1\right]_\sim, \left[c_0{}^1\right]_\sim, \left[c_2{}^1\right]_\sim\right] = \left[\left\langle c_1{}^{-1}, c_0{}^{-1}, c_1{}^1, c_0{}^1, c_2{}^{-1}, c_0{}^{-1}, c_1{}^{-1}, c_0{}^1, c_1{}^1, c_2{}^1\right\rangle\right]_\sim,$$

$$\left[\left[c_2{}^1\right]_\sim, \left[c_0{}^1\right]_\sim, \left[c_1{}^1\right]_\sim\right] = \left[\left\langle c_2{}^{-1}, c_0{}^{-1}, c_2{}^1, c_0{}^1, c_1{}^{-1}, c_0{}^{-1}, c_2{}^{-1}, c_0{}^1, c_2{}^1, c_1{}^1\right\rangle\right]_\sim,$$

$$\left[\left[c_2{}^1\right]_\sim, \left[c_1{}^1\right]_\sim, \left[c_0{}^1\right]_\sim\right] = \left[\left\langle c_2{}^{-1}, c_1{}^{-1}, c_2{}^1, c_1{}^1, c_0{}^{-1}, c_1{}^{-1}, c_2{}^{-1}, c_1{}^1, c_2{}^1, c_0{}^1\right\rangle\right]_\sim.$$

This concludes.

A

A.1

Theorem 1 (Newton's Identities)**.** *For positive integers $m \geq k \geq 1$, the following identity holds over the ring $\mathbb{Z}[X_0, \ldots, X_{m-1}] = \mathbb{Z}[\mathbf{X}]$:*

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

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

Proof. Alternatively, the identity can be rewritten as:

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

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

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

Define the set of 3-tuples:

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

The *weight* of $\langle A, j, i \rangle$ is defined as:

$$w\left(\langle A, j, i \rangle\right) := (-1)^i \left(\prod_{a \in A} X_a \right) X_j^i \in \mathbb{Z}[\mathbf{X}].$$

The sum of the weights of all elements in $\mathcal{A}(n,k)$ is readily seen to be equal to (*). To show this sum is zero, define the function $T : \mathcal{A}(n,k) \to \mathcal{A}(n,k)$ as:

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

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

- $w\left(T\left(\langle A, j, i \rangle\right)\right) = -w\left(\langle A, j, i \rangle\right)$,
- $T \circ T = \mathrm{id}_{\mathcal{A}(n,k)}$.

Thus, every element $\langle A, j, i \rangle$ uniquely pairs with its image under T (since it is an involution), and their weights cancel. Hence, the total sum is zero. □

A.2

Lemma. *Let $l \in \mathbb{N}_{>0}$ and R be a commutative unital ring together with the canonical morphism $\mathrm{can}_R : \mathbb{Z} \to R$. Let $N \in R^{l\times l}$ be a nilpotent matrix. If $I_l + N$ has finite order $r \in \mathbb{Z}_{>0}$ (where I_l is the identity matrix in $R^{l\times l}$) such that $\mathrm{can}_R(r) \overset{not.}{=} r_R \in R^\times$ is invertible, then $N = \mathbf{0}_{R^{l\times l}}$.*

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

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

where the binomial coefficient is interpreted through the canonical morphism $\mathrm{can}_R : \mathbb{Z} \to R$. 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 $\mathrm{Nil}(A)$ is closed[7] 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 $E \in \mathrm{Nil}\left(R^{l\times l}\right)$.

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[8].

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

[7] For the finite product, this is clear (the index of nilpotency being the minimum of the respective indices of nilpotency, and using commutativity of the factors). For the finite sum, the index of nilpotency is the maximum of the indices of nilpotency. To see this, use induction on the binomial theorem or directly apply the multinomial theorem (which is valid since the summands commute).

[8] This is a general fact about any (possibly non-commutative) unital ring A: if $a \in A^\times$, $b \in \mathrm{Nil}(A)$, 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 $a + b \in A^\times$

B

We define formally in Set theory (**ZF**) the free group generated on $\{c_i \,|\, i < n\}$, $F(\{c_i \,|\, i < n\})$ as follows. First, we introduce an orientation by defining $c_i^1 := (c_i, 1)$ and $c_i^{-1} := (c_i, -1)$. Then, we take the set of all possible words over the alphabet $C_n := \left\{c_i^1 \,|\, i \in n\right\} \cup \left\{c_i^{-1} \,\middle|\, i \in n\right\}$, that is, the set of all sequences w with a domain being an integer $\mathrm{dom}\,(w) \in \mathbb{N}$ and range being in the alphabet C_n, $\mathrm{ran}\,(w) \subset C_n$:

$$C_n^{<\omega} = \bigcup_{i \in \mathbb{N}} C_n^i.$$

We let the binary operation of concatenation $\frown\colon C_n^{<\omega} \times C_n^{<\omega} \to C_n^{<\omega}$ of two words $w, v \in C_n^{<\omega}$ defined by $w \frown v : \mathrm{dom}(w) + \mathrm{dom}(v) \to C_n$ defined by:

$$w \frown v = \begin{cases} w_i & \text{if } i < \mathrm{dom}(w), \\ v_j & \text{if } i = \mathrm{dom}(w) + j. \end{cases}$$

The reader may check that concatenation is internal, associative, admits a neutral element (namely the empty sequence $\varepsilon = \varnothing$), and that it is non-commutative as long as $n \geq 1$. Then, we let the smallest equivalence relation $\sim \subset C_n^{<\omega} \times C_n^{<\omega}$ containing the set:

$$C(n) := \left\{\left(\left\langle c_i^1, c_i^{-1}\right\rangle, \varepsilon\right) \,\middle|\, i < n\right\} \cup \left\{\left(\left\langle c_i^{-1}, c_i^1\right\rangle, \varepsilon\right) \,\middle|\, i < n\right\},$$

such that the operation of concatenation passes to the quotient:

$$\sim := \bigcap \left\{ R \in \mathscr{P}\left(C_n^{<\omega} \times C_n^{<\omega}\right) \,\middle|\, \begin{array}{l} \text{“}R \text{ is an equivalence relation”} \wedge C(n) \subset R \\ \wedge \quad \forall v, w, v', w' \in C_n^{<\omega} \\ \quad (v, v') \in R \wedge (w, w') \in R \to (v \frown w, v' \frown w') \in R \end{array} \right\}.$$

This set of such equivalence relations is non-empty, as it contains the trivial equivalence relation where everything is equivalent to everything, so the intersection is not over the empty set and is thus well-defined. It is easy to see that an arbitrary intersection of equivalence relations is an equivalence relation. Then $\forall v, w \in C_n^{<\omega}$: We can define a 2-ary relation $\widehat{} \subset (C_n^{<\omega}/_\sim \times C_n^{<\omega}/_\sim) \times C_n^{<\omega}/_\sim$ by:

$$\widehat{} := \left\{\left(\left([v]_\sim, [w]_\sim\right), [v \frown w]_\sim\right) \in \left(C_n^{<\omega}/_\sim \times C_n^{<\omega}/_\sim\right) \times C_n^{<\omega}/_\sim \,\middle|\, \exists v, w \in C_n^{<\omega}\right\}.$$

The construction of $\sim$ gives us that in fact $\widehat{}$ is a functional relation with domain $C_n^{<\omega}/_\sim \times C_n^{<\omega}/_\sim$:

$$\widehat{} : C_n^{<\omega}/_\sim \times C_n^{<\omega}/_\sim \to C_n^{<\omega}/_\sim$$

defined by:

$$[v]_\sim \,\widehat{}\, [w]_\sim = [v \frown w]_\sim.$$

(That is, $\widehat{}$ commutes with $\frown$ through the quotient map.) Now, the reader can verify that this new binary function $\widehat{}$ makes $F(\{c_j \,|\, j < n\}) := C_n^{<\omega}/_\sim$ into a group (its construction forces $\widehat{}$ to inherits the properties of $\frown$: closure, associativity, and the existence of a neutral element (here $[\varepsilon]_\sim$)). The inverse element of the equivalence class of a word $w \in C_n^{<\omega}$ is the equivalence class of the word obtained by reversing the order of w and inverting each exponent (changing 1 to -1 and *vice versa*). More formally, if we denote by $p_2 : \{c_i \,|\, i < n\} \times \{1, -1\} \to \{1, -1\}$ the projection onto the second coordinate, then the inverse is:

$$[w]_\sim^{-1} = \left[\frown_{i \in \mathrm{dom}(w)} \left\langle w_{\mathrm{dom}(w)-1-i}^{-p_2(w_{\mathrm{dom}(w)-1-i})} \right\rangle\right]_\sim$$

For example, since $\langle c_0^1 \rangle \frown \left\langle c_0^{-1} \right\rangle \sim \varepsilon$, we must have:

$$\left[\left\langle c_0^1 \right\rangle\right]_\sim^{-1} = \left[\left\langle c_0^{-1} \right\rangle\right]_\sim .$$

One can check that $\widehat{\ }$ is again non-commutative as long as $n \geq 2$ (since $c_0 \neq c_1$). This group has a "free" property (which we will not develop here), so that we call $F\left(\{c_j \,|\, j < n\}\right)$ the free group generated by $\{c_j \,|\, j < n\}$.

For simplicity, we define for any $w \in C_n^{<\omega}$ and $l \geq 0$ the abbreviation:

$$w^l := \frown_{s<l}^{l} w$$

(the order of concatenation does not matter here). For example, we have $w^0 = \varepsilon$, since we perform a concatenation with an index running over the empty set, which is then the empty set. Here is another example:

$$\left\langle c_0^1 \right\rangle^3 \frown \left\langle c_0^{-1} \right\rangle^4 = \left\langle c_0^1, c_0^1, c_0^1, c_0^{-1}, c_0^{-1}, c_0^{-1}, c_0^{-1} \right\rangle \sim \left\langle c_0^{-1} \right\rangle .$$

Every equivalent word will behave the same under the "new" concatenation by the construction of $\sim$. In particular, for any words $w, v \in C_n^{<\omega}$, any $i < n$, and any $r, s > 0$ we have that:

$$\text{if } r \geq s: \quad \left(w \frown \left\langle c_0^1 \right\rangle^r \frown \left\langle c_0^{-1} \right\rangle^s \frown v\right) \sim w \frown \left\langle c_0^1 \right\rangle^{r-s} \frown v,$$

$$\text{and } \left(w \frown \left\langle c_0^{-1} \right\rangle^r \frown \left\langle c_0^1 \right\rangle^s \frown v\right) \sim w \frown \left\langle c_0^{-1} \right\rangle^{r-s} \frown v,$$

while:

$$\text{if } r < s: \quad \left(w \frown \left\langle c_0^1 \right\rangle^r \frown \left\langle c_0^{-1} \right\rangle^s \frown v\right) \sim w \frown \left\langle c_0^{-1} \right\rangle^{s-r} \frown v,$$

$$\text{and } \left(w \frown \left\langle c_0^{-1} \right\rangle^r \frown \left\langle c_0^1 \right\rangle^s \frown v\right) \sim w \frown \left\langle c_0^1 \right\rangle^{s-r} \frown v.$$

Remark. In fact, if we replace $\{c_i \,|\, i < n\}$ with an arbitrary set J, we obtain—*mutatis mutandis*—the construction of the free group $F(J)$ generated by J (valid even if $J = \varnothing$). When working on $F(J)$, especially when writing its words, we usually omit for simplicity the pedantic notation of $[\_]_\sim$ and $\langle \_ \rangle$. However, note that we have not discussed what makes these groups "free"; for more information about this group, you can check the following Wikipedia page.