The Crystallographic Restriction Theorem: A Formalized Proof in Lean 4

James Kuzmanovich* Andrey Pavlichenkov Eric Vergo†

Abstract

...

0.1 Introduction

Finite groups of matrices with integer entries arise naturally in many areas of mathematics and physics. In crystallography, the symmetry groups of crystal lattices are realized as finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$, the group of $n \times n$ matrices with integer entries whose inverses also have integer entries. A fundamental question is: *which finite orders can elements of* $\mathrm{GL}(n, \mathbb{Z})$ *have?*

The answer involves a beautiful interplay between linear algebra, number theory, and algebra. Minkowski proved the remarkable result that $\mathrm{GL}(n, \mathbb{Z})$ contains only finitely many isomorphism classes of finite subgroups, which implies that there are only finitely many possible orders for elements of finite order. The crystallographic restriction theorem provides a precise characterization of these orders.

0.1.1 Historical Context

The name "crystallographic restriction" originates from the physical study of crystals. A crystal lattice in $\mathbb{R}^n$ is a discrete subgroup of translations, and the rotational symmetries of such a lattice must preserve the lattice structure. This requirement severely constrains the possible rotation angles.

In two and three dimensions, the classical crystallographic restriction states that a rotation preserving a lattice must have order 1, 2, 3, 4, or 6. This explains why crystals can have 2-fold, 3-fold, 4-fold, or 6-fold rotational symmetry, but never 5-fold or 7-fold symmetry—a fact observed experimentally long before it was proved mathematically.

The general theorem we formalize extends this to all dimensions, answering completely which orders are achievable in $\mathrm{GL}(N, \mathbb{Z})$ for any N.

0.1.2 Statement of the Main Result

The characterization involves a function $\psi : \mathbb{N} \to \mathbb{N}$ that we call the *dimensional cost function*. Informally, $\psi(m)$ measures the minimum dimension needed to construct an integer matrix of order m.

Theorem 0.1. *Let N be a positive integer. An $N \times N$ matrix with integer entries can have finite order m if and only if $\psi(m) \leq N$.*

*Wake Forest University. Original paper published in *The American Mathematical Monthly*, 109(2):173–186, 2002.
†Formalization in Lean 4.

The function ψ is defined as follows. For a prime power p^k:

$$\psi_{\text{pp}}(p,k) = \begin{cases} 0 & \text{if } k = 0, \\ 0 & \text{if } p = 2 \text{ and } k = 1, \\ \varphi(p^k) & \text{otherwise,} \end{cases}$$

where φ denotes Euler's totient function. For a general positive integer $m = \prod_i p_i^{k_i}$, we define $\psi(m) = \sum_i \psi_{\text{pp}}(p_i, k_i)$.

The special treatment of 2^1 reflects the fact that order 2 is "free" in any positive dimension: the matrix $-I$ has order 2 in any dimension $N \geq 1$.

0.1.3 Significance and Applications

The crystallographic restriction has several notable consequences:

1. **Classical 2D/3D restriction:** Since $\psi(m) \leq 2$ only for $m \in \{1, 2, 3, 4, 6\}$, these are the only achievable orders in dimensions 2 and 3, explaining the observed rotational symmetries of crystals.

2. **Dimension parity:** Since $\psi(m)$ is always even for $m > 2$, the achievable orders in dimension $2k$ are the same as in dimension $2k + 1$. This surprising result means that odd dimensions offer no new orders beyond their even predecessors.

3. **First occurrence of orders:** The theorem determines exactly when each order first becomes achievable. For instance, order 5 requires dimension at least 4 (since $\psi(5) = \varphi(5) = 4$), while order 7 requires dimension at least 6.

0.1.4 Overview of the Proof

Our formalization follows the proof structure of Kuzmanovich and Pavlichenkov [**?**]. The proof proceeds in two directions:

If an $N \times N$ integer matrix A has order m, we show $\psi(m) \leq N$. The key insight is that the minimal polynomial of A (viewed over $\mathbb{Q}$) must be a product of distinct cyclotomic polynomials Φ_d for various divisors d of m. The constraint that the order is exactly m forces the lcm of these divisors to equal m, leading to the dimension bound.

If $\psi(m) \leq N$, we construct an explicit $N \times N$ integer matrix with order m. The construction uses companion matrices of cyclotomic polynomials combined via block diagonal matrices.

The formalization required developing substantial supporting infrastructure, including properties of cyclotomic polynomials, companion matrices, block diagonal constructions, and the ψ function itself.

0.2 Preliminaries

We establish notation and recall the key definitions needed for the proof.

0.2.1 Notation and Conventions

Throughout, we use the following notation:

- $\mathbb{N}$ denotes the natural numbers $\{0, 1, 2, \ldots\}$
- $\mathbb{Z}$ denotes the integers
- $\mathbb{Q}$ denotes the rational numbers
- $\mathrm{GL}(N, \mathbb{Z})$ denotes the group of $N \times N$ invertible integer matrices
- $\varphi(m)$ denotes Euler's totient function
- $\Phi_m(X)$ denotes the m-th cyclotomic polynomial
- $\mathrm{ord}(A)$ denotes the multiplicative order of a matrix A (the smallest positive k with $A^k = I$)

For a matrix A with $A^m = I$ for some $m > 0$, we say A has *finite order*, and $\mathrm{ord}(A)$ is the smallest such m.

We write $p^k \| m$ to mean that p^k is the exact power of p dividing m, that is, $p^k \mid m$ but $p^{k+1} \nmid m$.

0.2.2 The Psi Function

The dimensional cost function ψ is central to the crystallographic restriction. We first define it on prime powers.

Definition 0.2. For a prime p and exponent $k \geq 0$, define

$$\psi_{\mathrm{pp}}(p, k) = \begin{cases} 0 & \text{if } k = 0, \\ 0 & \text{if } p = 2 \text{ and } k = 1, \\ \varphi(p^k) & \text{otherwise.} \end{cases}$$

The function $\psi_{\mathrm{pp}}(p, k)$ equals $\varphi(p^k) = (p-1)p^{k-1}$ in most cases, with two exceptions: $\psi_{\mathrm{pp}}(p, 0) = 0$ for any prime p, and $\psi_{\mathrm{pp}}(2, 1) = 0$. The latter exception captures the fact that order 2 requires no "dimensional cost" since $-I$ has order 2 in any positive dimension.

Definition 0.3. For a positive integer m with prime factorization $m = \prod_i p_i^{k_i}$, define

$$\psi(m) = \textstyle\sum_i \psi_{\mathrm{pp}}(p_i, k_i).$$

Equivalently, $\psi(m) = \sum_{\substack{p^k \| m \\ (p,k) \neq (2,1)}} \varphi(p^k)$.

0.2.3 Properties of Psi

Several properties of ψ are essential for the proof.

Lemma 0.4. *For small values of m:*

...

Proof. Direct computation: $\psi(1) = 0$, $\psi(2) = 0$ (special case), $\psi(3) = \varphi(3) = 2$, $\psi(4) = \varphi(4) = 2$, $\psi(5) = \varphi(5) = 4$, $\psi(6) = \psi(2) + \psi(3) = 0 + 2 = 2$, $\psi(7) = \varphi(7) = 6$, $\psi(8) = \varphi(8) = 4$, $\psi(9) = \varphi(9) = 6$, $\psi(10) = \psi(2) + \psi(5) = 0 + 4 = 4$, $\psi(11) = \varphi(11) = 10$, $\psi(12) = \psi(4) + \psi(3) = 2 + 2 = 4$. □

Lemma 0.5. *If $\gcd(m, n) = 1$, then $\psi(mn) = \psi(m) + \psi(n)$.*

Proof. Since m and n are coprime, their prime factorizations are disjoint: if $m = \prod_i p_i^{a_i}$ and $n = \prod_j q_j^{b_j}$, then $mn = \prod_i p_i^{a_i} \cdot \prod_j q_j^{b_j}$ with all primes p_i, q_j distinct. By definition,

$$\psi(mn) = \textstyle\sum_i \psi_{\mathrm{pp}}(p_i, a_i) + \sum_j \psi_{\mathrm{pp}}(q_j, b_j) = \psi(m) + \psi(n).$$ □

Lemma 0.6. *For all $m \geq 1$, we have $\psi(m) \leq \varphi(m)$.*

Proof. It suffices to show $\psi_{\mathrm{pp}}(p, k) \leq \varphi(p^k)$ for each prime power in the factorization of m, then sum. For $k = 0$, both sides are 0. For $k \geq 1$ with $(p, k) \neq (2, 1)$, we have $\psi_{\mathrm{pp}}(p, k) = \varphi(p^k)$. For $(p, k) = (2, 1)$, $\psi_{\mathrm{pp}}(2, 1) = 0 < 1 = \varphi(2)$.

□

Remark 0.7. The only case where $\psi(m) < \varphi(m)$ is when $2 \| m$ (that is, m is divisible by 2 but not by 4). In this case, the factor of 2 contributes $\varphi(2) = 1$ to the totient but 0 to ψ.

0.3 Companion Matrices

Companion matrices are the fundamental tool for constructing matrices with prescribed characteristic polynomials. They play a central role in the backward direction of our proof.

0.3.1 Definition and Basic Properties

Definition 0.8. Given a monic polynomial $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ of degree $n \geq 1$, its *companion matrix* $C(p)$ is the $n \times n$ matrix

$$\mathrm{C(p)} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Theorem 0.9. *The characteristic polynomial of $C(p)$ equals p. That is,* $\det(XI - C(p)) = p(X)$.

Proof. This is a standard result; we expand $\det(XI - C(p))$ by cofactors along the first row and use induction on the degree.

□

Corollary 0.10. *If p is irreducible over $\mathbb{Q}$, then p is also the minimal polynomial of $C(p)$.*

Proof. The minimal polynomial divides the characteristic polynomial. If p is irreducible, the only monic divisors of p are 1 and p itself. Since $C(p) \neq I$ for $\deg(p) \geq 1$, the minimal polynomial cannot be 1, so it must be p.

□

By the Cayley-Hamilton theorem, every matrix satisfies its characteristic polynomial. For companion matrices, this means the defining polynomial evaluates to zero at the companion matrix: $p(C(p)) = 0$.

Lemma 0.11. *If $p(X)$ divides $q(X)$ in $\mathbb{Q}[X]$, then $q(C(p)) = 0$.*

Proof. Write $q = p \cdot r$ for some polynomial r. Then $q(C(p)) = p(C(p)) \cdot r(C(p)) = 0 \cdot r(C(p)) = 0$.

□

Theorem 0.12. *If $p(X)$ divides $X^m - 1$, then $C(p)^m = I$.*

Proof. By Lemma **??**, $(X^m - 1)(C(p)) = C(p)^m - I = 0$.

□

0.3.2 Cyclotomic Companion Matrices

When we apply the companion matrix construction to cyclotomic polynomials, we obtain integer matrices with precisely controlled finite orders.

Recall that the m-th cyclotomic polynomial $\Phi_m(X)$ is the minimal polynomial over $\mathbb{Q}$ of a primitive m-th root of unity. It has three crucial properties:

1. $\Phi_m(X)$ has integer coefficients.
2. $\Phi_m(X)$ has degree $\varphi(m)$.
3. $\Phi_m(X)$ divides $X^m - 1$ but does not divide $X^k - 1$ for any $0 < k < m$.

Theorem 0.13. *For $m \geq 2$, the companion matrix $C(\Phi_m)$ has order exactly m.*

Proof. Upper bound: Since $\Phi_m \mid X^m - 1$, Theorem **??** gives $C(\Phi_m)^m = I$.

Lower bound: Suppose $C(\Phi_m)^d = I$ for some $0 < d < m$. Then $C(\Phi_m)$ is a root of $X^d - 1$ (as a polynomial in matrices). The minimal polynomial of $C(\Phi_m)$ is Φ_m (by Corollary **??**, since Φ_m is irreducible over $\mathbb{Q}$). Therefore $\Phi_m \mid X^d - 1$ in $\mathbb{Q}[X]$.

But the roots of Φ_m are the primitive m-th roots of unity ζ with $\zeta^m = 1$ and $\zeta^k \neq 1$ for $0 < k < m$. Such a ζ cannot be a root of $X^d - 1$ when $d < m$. This contradicts $\Phi_m \mid X^d - 1$.

Therefore $\operatorname{ord}(C(\Phi_m)) = m$.

□

Corollary 0.14. *For $m \geq 2$, the companion matrix $C(\Phi_m)$ belongs to $\mathrm{GL}(\varphi(m), \mathbb{Z})$ and has order m. In particular, order m is achievable in dimension $\varphi(m)$.*

Proof. Since Φ_m has integer coefficients, $C(\Phi_m)$ has integer entries. The matrix has finite order m, so it is invertible with $C(\Phi_m)^{-1} = C(\Phi_m)^{m-1}$, which also has integer entries.

□

Example 0.15. The cyclotomic polynomial $\Phi_3(X) = X^2 + X + 1$ has companion matrix

$$\mathrm{C}(\Phi_3) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

One can verify directly: $C(\Phi_3)^2 = -11$
-10 and $C(\Phi_3)^3 = I$. This 2×2 integer matrix has order exactly 3.

Example 0.16. The cyclotomic polynomial $\Phi_6(X) = X^2 - X + 1$ has companion matrix

$$\mathrm{C}(\Phi_6) = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

This 2×2 matrix has order 6, demonstrating that order 6 is achievable in dimension 2.

0.4 Block Diagonal Matrices

To construct matrices of arbitrary orders from companion matrices of cyclotomic polynomials, we use block diagonal combinations.

0.4.1 Definition

Definition 0.17. For matrices $A \in \mathrm{Mat}_{n_1}(\mathbb{Z})$ and $B \in \mathrm{Mat}_{n_2}(\mathbb{Z})$, the *block diagonal* matrix is

$$\mathrm{diag(A,\ B)} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in \mathrm{Mat}_{n_1+n_2}(\mathbb{Z}).$$

This extends naturally to any finite number of blocks.

0.4.2 Order of Block Diagonal Matrices

Lemma 0.18. *For any matrices A and B and any positive integer k,*

$$\mathit{diag(A,\ B)}^k = \mathrm{diag}(A^k, B^k).$$

Proof. By induction on k. The base case $k = 1$ is immediate. For the inductive step:

$$\text{diag(A, B)}^{k+1} = \text{diag}(A, B)^k \cdot \text{diag}(A, B) = \text{diag}(A^k, B^k) \cdot \text{diag}(A, B) = \text{diag}(A^{k+1}, B^{k+1}). \quad \square$$

Theorem 0.19. *If A has finite order a and B has finite order b, then* $\text{diag}(A, B)$ *has order* $\text{lcm}(a, b)$.

Proof. By Lemma **??**, $\text{diag}(A, B)^k = I$ if and only if $A^k = I$ and $B^k = I$. This happens precisely when $a \mid k$ and $b \mid k$, that is, when k is a common multiple of a and b. The smallest such positive k is $\text{lcm}(a, b)$.

$\square$

Corollary 0.20. *If A has order a, B has order b, and* $\gcd(a, b) = 1$*, then* $\text{diag}(A, B)$ *has order ab.*

Proof. When $\gcd(a, b) = 1$, we have $\text{lcm}(a, b) = ab$.

$\square$

Corollary 0.21. *If order a is achievable in dimension n_1 and order b is achievable in dimension n_2, then order* $\text{lcm}(a, b)$ *is achievable in dimension $n_1 + n_2$.*

0.5 The Forward Direction

We now prove that if an integer matrix has order m, then its dimension must be at least $\psi(m)$.

0.5.1 Minimal Polynomials of Matrices with Finite Order

Let $A \in \text{GL}(N, \mathbb{Z})$ be a matrix with finite order m. Since $A^m = I$, the polynomial $X^m - 1$ annihilates A. The minimal polynomial μ_A of A (over $\mathbb{Q}$) therefore divides $X^m - 1$.

Lemma 0.22. *Over $\mathbb{Q}$, we have the factorization*

$$X^m - 1 = \prod_{d|m} \Phi_d(X),$$

where the product is over all positive divisors d of m.

This is a standard result: every m-th root of unity is a primitive d-th root of unity for exactly one divisor d of m.

Lemma 0.23. *The minimal polynomial μ_A has the form*

$$\mu_A = \prod_{d \in S} \Phi_d$$

for some non-empty subset S of divisors of m. Moreover, μ_A has integer coefficients.

Proof. Since $\mu_A \mid X^m - 1$ and the cyclotomic polynomials are the irreducible factors of $X^m - 1$ over $\mathbb{Q}$, the minimal polynomial must be a product of distinct cyclotomic polynomials. Since $A \neq 0$, we have $\mu_A \neq 1$, so S is non-empty. The product of cyclotomic polynomials has integer coefficients since each Φ_d does.

□

0.5.2 The Order Constraint

Lemma 0.24. *If* $\mu_A = \prod_{d \in S} \Phi_d$, *then* $\operatorname{ord}(A) = \operatorname{lcm}(S)$.

Proof. Let $\ell = \operatorname{lcm}(S)$. For each $d \in S$, we have $d \mid \ell$, so $\Phi_d \mid X^\ell - 1$. Therefore $\mu_A \mid X^\ell - 1$, which gives $A^\ell = I$. Thus $\operatorname{ord}(A) \mid \ell$.

Conversely, let $k = \operatorname{ord}(A)$. Then $A^k = I$, so $\mu_A \mid X^k - 1$. For each $d \in S$, the polynomial Φ_d divides μ_A, hence divides $X^k - 1$. The roots of Φ_d are primitive d-th roots of unity, which are k-th roots of unity only if $d \mid k$. Therefore $d \mid k$ for all $d \in S$, giving $\ell = \operatorname{lcm}(S) \mid k$.

Together, $\operatorname{ord}(A) = \ell = \operatorname{lcm}(S)$.

□

Corollary 0.25. *If* $\operatorname{ord}(A) = m$, *then* $\operatorname{lcm}(S) = m$ *for the set* S *such that* $\mu_A = \prod_{d \in S} \Phi_d$.

0.5.3 The Key Inequality

The heart of the forward direction is the following combinatorial lemma about subsets of divisors.

Lemma 0.26. *Let* $m \geq 1$ *and let* S *be a non-empty set of positive divisors of* m *with* $\operatorname{lcm}(S) = m$. *Then*

$$\sum_{d \in S} \varphi(d) \geq \psi(m).$$

Proof. We use strong induction on m.

Base cases: For $m = 1$, the only possibility is $S = \{1\}$, and $\varphi(1) = 1 \geq 0 = \psi(1)$. For $m = 2$, we need $S = \{2\}$ or $S = \{1, 2\}$ (since $\operatorname{lcm}(S) = 2$). Either way, $\sum_{d \in S} \varphi(d) \geq \varphi(2) = 1 > 0 = \psi(2)$.

Inductive step: Assume $m \geq 3$ and the result holds for all $m' < m$. Write $m = \prod_p p^{k_p}$ with $k_p \geq 1$ for finitely many primes p.

If m is a prime power, say $m = p^k$ with $k \geq 1$, then $\operatorname{lcm}(S) = p^k$ requires $p^k \in S$. So $\sum_{d \in S} \varphi(d) \geq \varphi(p^k) = \psi_{\mathrm{pp}}(p, k) = \psi(m)$ (except if $(p, k) = (2, 1)$, but then $m = 2$ is a base case).

If m is not a prime power, write $m = ab$ with $\gcd(a, b) = 1$, $a, b > 1$. For each $d \in S$, write $d = d_a d_b$ with $d_a \mid a$ and $d_b \mid b$. Define $S_a = \{d_a : d \in S\}$ and $S_b = \{d_b : d \in S\}$. Then $\operatorname{lcm}(S_a) = a$ and $\operatorname{lcm}(S_b) = b$ (since $\operatorname{lcm}(S) = m = ab$ and the prime factorizations are disjoint).

By the Chinese Remainder Theorem structure:

$$\sum_{d \in S} \varphi(d) = \sum_{d \in S} \varphi(d_a)\varphi(d_b) \geq \sum_{d_a \in S_a} \varphi(d_a) + \sum_{d_b \in S_b} \varphi(d_b) - \varphi(1).$$

(The inequality uses that the map $d \mapsto (d_a, d_b)$ is injective, and some elementary bounds.)

By the inductive hypothesis, $\sum_{d_a \in S_a} \varphi(d_a) \geq \psi(a)$ and $\sum_{d_b \in S_b} \varphi(d_b) \geq \psi(b)$. Since $\psi(m) = \psi(a) + \psi(b)$ by coprime additivity, we obtain $\sum_{d \in S} \varphi(d) \geq \psi(m)$.

□

0.5.4 Proof of the Forward Direction

Theorem 0.27. *If $A \in \mathrm{GL}(N, \mathbb{Z})$ has order m, then $\psi(m) \leq N$.*

Proof. Let $\mu_A = \prod_{d \in S} \Phi_d$ be the minimal polynomial of A. By Corollary **??**, $\mathrm{lcm}(S) = m$.
The degree of μ_A is $\sum_{d \in S} \deg(\Phi_d) = \sum_{d \in S} \varphi(d)$.
By Lemma **??**, $\sum_{d \in S} \varphi(d) \geq \psi(m)$.
The minimal polynomial divides the characteristic polynomial, so $\deg(\mu_A) \leq \deg(\chi_A) = N$.
Combining: $\psi(m) \leq \sum_{d \in S} \varphi(d) = \deg(\mu_A) \leq N$.

□

0.6 The Backward Direction

We now show that every order satisfying the necessary condition is actually achievable.

0.6.1 Prime Power Orders

By Corollary **??**, for any prime power p^k with $k \geq 1$, the companion matrix $C(\Phi_{p^k})$ achieves order p^k in dimension $\varphi(p^k)$.

Lemma 0.28. *For a prime p and $k \geq 1$ with $(p, k) \neq (2, 1)$, order p^k is achievable in dimension $\psi_{\mathrm{pp}}(p, k) = \varphi(p^k)$.*

Proof. Take $C(\Phi_{p^k})$, which has dimension $\varphi(p^k)$ and order p^k.

□

0.6.2 Order 2 is Free

The special case $(p, k) = (2, 1)$ requires separate treatment.

Lemma 0.29. *For any $N \geq 1$, the $N \times N$ matrix $-I$ has order 2.*

Proof. We have $(-I)^2 = I$ and $-I \neq I$ (since $N \geq 1$).

□

This is why $\psi(2) = 0$: achieving order 2 costs nothing beyond having at least one dimension.

Lemma 0.30. *If $A \in \mathrm{GL}(N, \mathbb{Z})$ has odd order k, then $-A$ has order $2k$.*

Proof. We have $(-A)^{2k} = (-1)^{2k} A^{2k} = A^{2k} = (A^k)^2 = I$.

For the lower bound, suppose $(-A)^j = I$ for some $j \geq 1$. Then $(-1)^j A^j = I$, so $A^j = (-1)^j I$. If j is odd, then $A^j = -I$, so $A^{2j} = I$, giving $k \mid 2j$. Since k is odd, $k \mid j$. But then $A^j = A^k = I \neq -I$, contradiction. So j is even, say $j = 2\ell$, and $A^{2\ell} = I$, giving $k \mid 2\ell$. Since k is odd, $k \mid \ell$, so $j = 2\ell \geq 2k$. Thus $\mathrm{ord}(-A) = 2k$.

□

Corollary 0.31. *If order k (odd) is achievable in dimension N, then order $2k$ is achievable in dimension N.*

0.6.3 General Construction

Theorem 0.32. *If $\psi(m) \leq N$, then some matrix in $\mathrm{GL}(N, \mathbb{Z})$ has order m.*

Proof. We construct a matrix of order m in dimension $\psi(m)$, then pad with identity blocks to reach dimension N if needed.

Write $m = 2^a \cdot m'$ where m' is odd and $a \geq 0$.

Case 1: $a = 0$ (m is odd). Write $m' = \prod_i p_i^{k_i}$ with distinct odd primes p_i and $k_i \geq 1$. For each i, let $A_i = C(\Phi_{p_i^{k_i}})$, which has order $p_i^{k_i}$ and dimension $\varphi(p_i^{k_i})$.

Form $A = \mathrm{diag}(A_1, A_2, \ldots)$. By Theorem **??** and induction, A has order $\mathrm{lcm}(p_1^{k_1}, p_2^{k_2}, \ldots) = m'$ (since the prime powers are pairwise coprime). The dimension is $\sum_i \varphi(p_i^{k_i}) = \psi(m')$.

Case 2: $a = 1$ ($m = 2m'$ with m' odd). Construct A of order m' in dimension $\psi(m')$ as above. Then $-A$ has order $2m'$ by Lemma **??**, still in dimension $\psi(m') = \psi(2m') = \psi(m)$.

Case 3: $a \geq 2$. Include a block $C(\Phi_{2^a})$ of order 2^a and dimension $\varphi(2^a) = 2^{a-1}$. Combine with blocks for the odd part m' as in Case 1. The total order is $\mathrm{lcm}(2^a, m') = 2^a m' = m$, and total dimension is $\varphi(2^a) + \psi(m') = \psi_{\mathrm{pp}}(2, a) + \psi(m') = \psi(m)$.

In all cases, we achieve order m in dimension exactly $\psi(m)$.

If $\psi(m) < N$, adjoin identity blocks $I_{N-\psi(m)}$: $\mathrm{diag}(A, I_{N-\psi(m)})$ still has order m (since $\mathrm{lcm}(m, 1) = m$) and has dimension N.

□

Example 0.33. We have $12 = 4 \cdot 3 = 2^2 \cdot 3$, so we are in Case 3 with $a = 2$ and $m' = 3$.

For the factor $2^2 = 4$: $C(\Phi_4) = C(X^2 + 1) = 0 - 1$
10, which has order 4 and dimension $\varphi(4) = 2$.

For the factor 3: $C(\Phi_3) = 0 - 1$
$1 - 1$, which has order 3 and dimension $\varphi(3) = 2$.

The block diagonal

$$\mathrm{diag}(\mathrm{C}(\Phi_4), C(\Phi_3)) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

has order $\mathrm{lcm}(4, 3) = 12$ and dimension $2 + 2 = 4 = \psi(12)$.

0.7 The Crystallographic Restriction Theorem

We now combine the forward and backward directions.

0.7.1 The Main Result

Theorem 0.34. *Let $N \geq 1$ and $m \geq 1$. An $N \times N$ integer matrix can have finite order m if and only if $\psi(m) \leq N$.*

Proof. ($\Rightarrow$) This is Theorem **??**.

($\Leftarrow$) This is Theorem **??**.

□

Definition 0.35. For $N \geq 1$, let Ord_N denote the set of all positive integers m such that some matrix in $\mathrm{GL}(N, \mathbb{Z})$ has order m.

Corollary 0.36. $\mathrm{Ord}_N = \{m \geq 1 : \psi(m) \leq N\}$.

0.7.2 The Classical Crystallographic Restriction

Corollary 0.37. *In dimensions 2 and 3, the achievable orders are exactly* $\{1, 2, 3, 4, 6\}$.

Proof. From Lemma **??**, $\psi(m) \leq 2$ if and only if $m \in \{1, 2, 3, 4, 6\}$:

- $\psi(1) = \psi(2) = 0 \leq 2$ ✓
- $\psi(3) = \psi(4) = \psi(6) = 2 \leq 2$ ✓
- $\psi(5) = 4 > 2$ ×
- $\psi(7) = 6 > 2$ ×

Since $\psi(m) \leq 3$ if and only if $\psi(m) \leq 2$ (as $\psi(m)$ is always even for $m > 2$), the achievable orders in dimensions 2 and 3 coincide.

□

This explains why crystals in our three-dimensional world exhibit only 2-, 3-, 4-, and 6-fold rotational symmetries: these correspond to the elements of orders 2, 3, 4, and 6 in $\mathrm{GL}(3, \mathbb{Z})$.

0.7.3 Dimension Parity

Corollary 0.38. *For $k \geq 1$, the sets Ord_{2k} and Ord_{2k+1} are equal.*

Proof. For $m > 2$, the value $\psi(m) = \sum_{(p,k)\neq(2,1)} \varphi(p^k)$ is a sum of terms $\varphi(p^k) = (p-1)p^{k-1}$. Each such term is even: if p is odd, then $p - 1$ is even; if $p = 2$ and $k \geq 2$, then $p^{k-1} = 2^{k-1}$ is even.

Thus $\psi(m)$ is even for all $m \geq 1$. The condition $\psi(m) \leq 2k$ is equivalent to $\psi(m) \leq 2k + 1$.

□

This means that passing from an even dimension to the next odd dimension never unlocks new achievable orders.

0.7.4 First Occurrence Table

The following table shows when each small order first becomes achievable:

...

We observe:

- Orders 1 and 2 are achievable in dimension 1 (the smallest possible).
- Orders 3, 4, 6 first appear in dimension 2.
- Orders 5, 8, 10, 12 first appear in dimension 4.
- Orders 7, 9 first appear in dimension 6.
- Order 11 requires dimension 10.

References

..