Katholieke
Universiteit
Leuven

CRYSTALLOGRAPHIC GROUPS AND SYMMETRIES OF CRYSTALS

May 27, 2021

Gijs Jespers (r0762265)
Jasper Dekoninck (r0752109)

Supervisor: Joel Villatoro

Abstract

In this paper, we will prove properties related to symmetry groups of crystals in $\mathbb{R}^n$ and crystallographic groups. We will show how these groups are related using the first Bieberbach Theorem. We will also prove and explain the second and third Bieberbach Theorems and by doing so we can unearth some extra properties about these groups. The second Bieberbach Theorem actually gives an answer to a part of the 18th problem of Hilbert. Finally, we will show that crystallographic groups and integer matrices are related and using this relation, we will prove that there are only finitely many possible orders for elements in a crystallographic group of a given dimension.

Contents

1 Introduction

Firstly we would like to thank our supervisor Joel Villatoro without whom this bachelor thesis would not be what it is today. He helped us a lot throughout our process and helped us understand the material in this paper.

The study of groups is often motivated by the beautiful properties they have. Often these properties are related to some kind of symmetry hidden in the underlying structure of the group. A structure that seems trivial or not interesting at first might later show to have very interesting properties related to symmetries. In this paper we will look into a specific type of group, namely crystallographic groups, and we will unearth properties that show that the structure and their related symmetries are much more present than what one would expect based on the definition we will give. We will prove that these crystallographic groups are the groups that preserve some crystal in $\mathbb{R}^n$. We will also prove the relation of these groups with integer matrices and from this relation we will derive that elements from a crystallographic group in a given dimension have finitely many possible orders.

In order to prove the equivalence between crystallographic groups and symmetry groups of crystals, we will use the three Bieberbach Theorems. These theorems were formulated and proved by Ludwig Bieberbach in 1910. He stated these theorems as a response to the 18th problem of the 23 problems posed by David Hilbert in 1900. The 18th problem consisted of three parts. One was about optimal sphere packing, another about tiling in three dimensional Euclidean. The last part was about crystallographic groups and whether or not there are only finitely many of them up to an isomorphism for any given dimension. Bieberbach answered this question affirmatively with his second Theorem which we will also prove in this paper.

Before continuing with the basic notions and definitions necessary to understand and prove the Bieberbach Theorems, we will first elaborate a bit on the life of Ludwig Bieberbach. Born in 1886 in Germany, he studied at the universities of Heidelberg and Göttingen. In 1933 he joined the SA and later he became a member of the NSDAP, the political party of Adolf Hitler. During the World War he was actively involved in the persecution of Jews and in doing so he committed multiple atrocities and was part of the biggest crime in human history. The authors of this paper condemn Bieberbach for what he did even though he might have been a good mathematician. More information about his life can be found in [JJ 10].

2 Basic notions and definitions

In order to be able to state the Bieberbach Theorems and look into symmetry groups of crystals, we first introduce some background on algebra and geometry. This section is also meant to introduce most of the notation that will be used throughout this paper. Most of this background can be found in introductory courses and texts on algebra, geometry and analysis, see for example [Vey21], [Goe20] and [Qua19].

Definition 2.1. *The set of Euclidean transformations $E(n)$ is the set of all transformations $f : \mathbb{R}^n \to \mathbb{R}^n$ that preserve the distance between any two points of $\mathbb{R}^n$.*

The following theorem about $E(n)$ is well-known. A proof can for example be found in [Goe20].

Theorem 2.2. *$E(n)$ is a group of linear transformations. More specifically, we have:*

$$E(n) = \{f : \mathbb{R}^n \to \mathbb{R}^n : x \mapsto Ax + b | b \in \mathbb{R}^n \wedge A \in \mathbb{R}^{n\times n} \wedge A^T = A^{-1}\}$$

We will use the notation $O(n)$ for the group of matrices $\{A \in \mathbb{R}^{n\times n} | A^T = A^{-1}\}$.The group of translations in $E(n)$ will be denoted by $T(n)$. An element $f : \mathbb{R}^n \to \mathbb{R}^n : x \mapsto Ax + b$ of $E(n)$ will be denoted by $(A, b) \in \mathbb{R}^{n\times n} \times \mathbb{R}^n$. We will call A the rotational part of f and b the translational part of f. Note that we can view $O(n)$ as a subset of $\mathbb{R}^{n^2}$, $E(n)$ as a subset of $\mathbb{R}^{n^2+n}$ and $T(n)$ as a subset of $\mathbb{R}^n$. With some abuse of notation we will often denote an element $(I_n, a) \in E(n)$ simply by it's translational part a and we will identify the translation (I_n, a) with its translation vector a.

Apart from these notations we will also need the notion of compactness, together with some easy-to-prove statements about compactness.

Definition 2.3. *A set $C \subset \mathbb{R}^n$ is compact if it is bounded and closed.*

Another completely equivalent definition of compactness, is that for every open cover of $C \subset \mathbb{R}^n$ there exists a finite subcover. Another equivalent definition makes use of the Theorem of Bolzano-Weierstrass and states that a set is compact if and only if every sequence in that set has a convergent subsequence. For a proof of the equivalence of these definitions, we refer to [Qua19].

Because we can view $O(n)$ as a subset of $\mathbb{R}^{n^2}$, we can say something about the compactness of $O(n)$. We will prove that $O(n)$ is compact. The proof of its compactness is based on the proof given by our supervisor in one of our meetings [Vil21b].

Lemma 2.4. *$O(n)$ is compact.*

Proof. We show that $O(n)$ is both bounded and closed. Choose $A \in O(n)$ arbitrarily. We know that the rows of A must form an orthonormal basis (because $AA^T = I_n$) and therefore we must have that

$$|A| = \sqrt{\sum_{i,j=1}^{n} A_{ij}^2} = \sqrt{n}$$

Thus $O(n)$ is bounded. Define the function

$$F : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n} : A \mapsto AA^T$$

We get $F^{-1}(\{I_n\}) = \{A \in \mathbb{R}^{n\times n} | AA^T = I_n\} = O(n)$. Because F is continuous and $\{I_n\}$ is closed, $O(n)$ must be closed as well. □

One last definition surrounding compactness, is cocompactness.

Definition 2.5. *A subgroup $\Gamma \subset E(n)$ is cocompact if there exists a compact set $C \subset \mathbb{R}^n$ such that for all $x \in \mathbb{R}^n$ there exists a $g \in \Gamma$ such that $g(x) \in C$.*

Another very important notion in the study of the Bieberbach Theorems is the notion of discreteness. The definition matches what one would expect based on an intuitive sense of what "discrete" means:

Definition 2.6. *A subgroup $S \subset \mathbb{R}^n$ is discrete if for every point $x \in S$ there exists an open subset $U_x \subset \mathbb{R}^n$ such that $S \cap U_x = \{x\}$.*

Note that we can also talk about the discreteness of $\Gamma \subset E(n)$ because of the above mentioned view of $E(n)$ as a subset of $\mathbb{R}^{n^2+n}$. The following lemma will be useful later on.

Lemma 2.7. *If $S \subset \mathbb{R}^n$ is compact and discrete then it is finite.*

Proof. Assume S to be compact and discrete. Then by definition of discreteness, there is an open cover $\{U_s | s \in S \wedge S \cap U_s = \{s\}\}$ of S. Because S is compact, this open cover has a finite subcover and thus we find that S is finite. □

The following lemma will be used several times throughout this paper, it is mentioned without proof in [Szc12]:

Lemma 2.8. *A subset $S \subset \mathbb{R}^n$ is discrete if and only if every convergent sequence in S eventually becomes constant.*

Proof. Suppose S is discrete. Choose an arbitrary convergent sequence $(x_n) \to x \in S$. Because S is discrete there exists an open set $U_x \subset \mathbb{R}^n$ such that $S \cap U_x = \{x\}$ and thus there exists a $\delta > 0$ such that for every $y \in S$ with $|x-y| < \delta$ we have $y = x$. Now let $n_0 \in \mathbb{N}$ be large enough such that for every $n > n_0$, $|x_n - x| < \delta$. Then $x_n = x$ for all $n > n_0$.

Now suppose that S is not discrete. Then there exists an element $x \in S$ such that there exists no open U with $U \cap S = \{x\}$. Let U_n be an open sphere of radius $\frac{1}{n}$ centered around x. Because $x \in U_n \cap S$ and because $U_n \cap S \neq \{x\}$, there must exist another element $x_n \in U \cap S$ that doesn't equal x. The sequence (x_n) now converges to x but doesn't eventually become constant as every element of the sequence is different from x. □

In the statement of the first Bieberbach Theorem, there will appear some notions that might not be familiar to the reader. We define them in the following definitions.

Definition 2.9. *A group $(G, *)$ with identity element 1 is torsion free if for every element $g \in G$ with $g^n = 1$ for an $n \in \mathbb{Z}_{>0}$ we have $g = 1$.*

Definition 2.10. *An abelian group $(G, *)$ is finitely generated if there exists a subset $\{g_1, ..., g_N\} \subset G$ such that every element of $g \in G$ can be written as $g_1^{k_1} * g_2^{k_2} * ... * g_N^{k_N}$. The group is of rank n if the smallest set that generates G in such a way contains n elements.*

Definition 2.11. *A subgroup $H \subset G$ is maximal abelian if H is an abelian subgroup and there exists no abelian subgroup of G that strictly contains H.*

Definition 2.12. *$H \subset G$ is a normal subgroup of finite index of $(G, *)$ if it is normal (thus $g * H = H * g$ for every $g \in G$) and the quotient group G/H is finite.*

We define one last notion which is one of the most important ones in the paper:

Definition 2.13. *A subgroup $\Gamma \subset E(n)$ is a crystallographic group of dimension n if it is a cocompact and discrete subgroup of $E(n)$.*

In the entire paper, Γ will always be a crystallographic group of dimension n unless explicitly stated otherwise.

3 Crystals and their symmetries

In this section we introduce crystals and we look deeper into their symmetries. We will find that the set of all Euclidean transformations $f : \mathbb{R}^n \to \mathbb{R}^n$ that preserve some crystal $\mathcal{C}$ (the exact definition of a crystal will come in a moment) is a crystallographic group. In order to show the other implication, namely that every crystallographic group preserves some crystal, we will first need the first Bieberbach Theorem which will be introduced after this section. Thus, in some sense, the crystallographic groups are the only groups of Euclidean transformations that preserve some crystal. This section is based on the fact that there exists multiple definitions of crystallographic groups: in our project description [Vil21a] it was defined as a group that preserves some crystal while it was defined as we did in Definition 2.13 in other sources like [Szc12].

We first introduce the definition of a lattice and some basic notions about lattices. We do this because a crystal can only be defined in terms of lattices.

Definition 3.1. *A lattice Λ in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ with the property that there exist linearly independent vectors $\{v_1, ..., v_n\}$ such that:*

$$\Lambda = \{\lambda_1 v_1 + ... + \lambda_n v_n | \lambda_i \in \mathbb{Z}\}$$

A lattice point is an element of Λ. We call $\{v_1, ..., v_n\}$ the basis elements of Λ.

Before continuing we want to make sure that this definition of a lattice is the same as what one would expect intuitively. One aspect of a lattice should be that it is a discrete subset of $\mathbb{R}^n$, we prove this in the following theorem.

Theorem 3.2. *A lattice Λ is discrete.*

Proof. We can construct a continuous transformation between Λ and $\mathbb{Z}^n$ by mapping the basis vectors of Λ to the basis vectors of $\mathbb{Z}^n$. This continuous transformation is linear. Note that $\mathbb{Z}^n$ is discrete. We now use Lemma 2.8. Suppose we have a convergent sequence (x_n) of Λ that converges to $x \in \Lambda$. By applying our

transformation, we find a sequence (y_n) in $\mathbb{Z}^n$ that converges to $y \in \mathbb{Z}^n$. Lemma 2.8 now implies that (y_n) is eventually constant and by applying the inverse of the transformation we find that (x_n) is also eventually constant. □

We can now define a crystal.

Definition 3.3. *A crystal $\mathcal{C}$ is a non-empty, discrete subset of $\mathbb{R}^n$ such that there exists a lattice Λ of $\mathbb{R}^n$ such that $\mathcal{C} + \Lambda = \mathcal{C}$.*

Obviously a lattice is a crystal. In order to get a better feeling for what a crystal is, we first give an example.

Example 3.4. Let Λ be the lattice in $\mathbb{R}^2$ with basis vectors $(1, 0)$ and $(0, 1)$. We consider the following subset of $\mathbb{R}^2$:

$$\mathcal{C} = \left\{(0,0) \cup \left(\frac{1}{4}, \frac{1}{4}\right)\right\} + \Lambda$$

The crystal can be seen in figure 1. The black points are all points in the set $\{(0, 0)\} + \Lambda$ while the blue points are all the points in the set $\{(\frac{1}{4}, \frac{1}{4})\} + \Lambda$. This is indeed a crystal because the sum of any point in $\mathcal{C}$ and any vector in Λ is again in $\mathcal{C}$. Note that this crystal isn't a lattice because any lattice that contains $(\frac{1}{4}, \frac{1}{4})$ must also contain $(\frac{1}{2}, \frac{1}{2})$, which is not the case here.

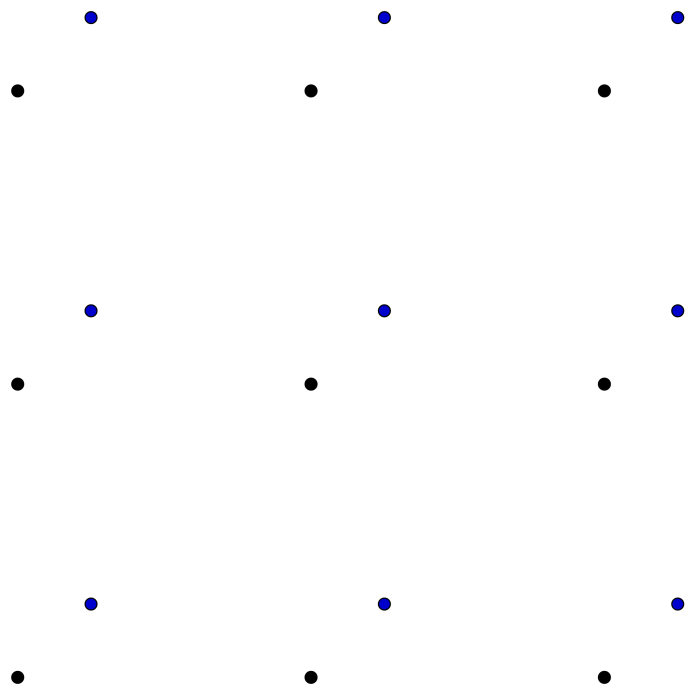

Figure 1: Crystal in $\mathbb{R}^2$

Because of this example, one might wonder whether every crystal is a union of translated lattices. This is the content of the following theorem.

Theorem 3.5. *For any crystal $\mathcal{C}$, there exists a lattice Λ and a finite number of points $\{c_1, ..., c_k\}$ such that $\mathcal{C} = \bigcup_{i=1}^{k} (c_i + \Lambda)$.*

Proof. Suppose there is no finite number of points $\{c_1, ..., c_k\}$ and lattice Λ such that $\mathcal{C} = \bigcup_{i=1}^{k}(c_i + \Lambda)$. We will prove that this contradicts the discreteness of $\mathcal{C}$. First let Λ be any lattice such that $\mathcal{C} + \Lambda = \mathcal{C}$. We construct a convergent sequence in $\mathcal{C}$ that does not become constant. Take an arbitrary $a_1 \in \mathcal{C}$. Let $a_k \in \mathcal{C}$ be a point not in $\bigcup_{i=1}^{k-1}(a_i + \Lambda)$. Note that this is possible because $\mathcal{C}$ cannot be written as a finite union of translated lattices. Let $\{v_1, ..., v_n\}$ be the set of basis vectors of Λ. By adding linear integer combinations of $\{v_1, ..., v_n\}$ to a_i we can assume for each a_i that $|a_i| \leqslant \sum_{j=1}^{n} |v_j|$. We have found a bounded sequence and by the Theorem of Bolzano-Weierstrass there must be a convergent subsequence (b_k). Note that this sequence cannot eventually become constant because otherwise there would exist an $n \in \mathbb{N}$ such that $b_n \in \bigcup_{i=1}^{n-1}(b_i + \Lambda)$ which is impossible. We have constructed a convergent sequence in $\mathcal{C}$ that does not become constant, which gives us the desired contradiction by Lemma 2.8. □

We now define what we mean by a crystal symmetry.

Definition 3.6. *A Euclidean transformation $f : \mathbb{R}^n \to \mathbb{R}^n$ is a crystal symmetry if it preserves some crystal $\mathcal{C}$, thus $f(\mathcal{C}) = \mathcal{C}$.*

In what follows we will always use "symmetry" instead of "crystal symmetry" to shorten the term.

If we for example find that $f(x) = -x$ is a symmetry, we know that $\mathcal{C}$ doesn't change by reflecting it over the origin. Other symmetries will thus tell us something different about how $\mathcal{C}$ does not change. We will denote the set of all symmetries of $\mathcal{C}$ by $\mathrm{Aut}(\mathcal{C})$.

One might wonder why we require f to be a Euclidean transformation and not just any transformation or just a linear transformation. First of all, note that if we were to allow every transformation, a transformation that randomly permutes the points of the crystal, would also be a symmetry. This however does not correspond to a symmetry in the intuitive sense of the word. Similarly, if we were to allow linear, non-Euclidean, transformations, one would get "symmetries" that feel very counterintuitive. For example, take the lattice in $\mathbb{R}^2$ with basis elements $(1, 0)$ and $(0, 2)$ and let the crystal $\mathcal{C}$ be equal to that lattice. The linear transformation that maps the basis elements to one another, is not a symmetry because one could argue that the x-axis and y-axis are different for the crystal. Indeed, the transformation maps the x-axis to the y-axis (and the other way around), which means they should be the same for our crystal, but the points of the crystal on one axis are twice as dense as on the other axis.

In order to show that $\mathrm{Aut}(\mathcal{C})$ is a crystallographic group, we first need to show that it is a group:

Lemma 3.7. *$Aut(\mathcal{C})$ is a group.*

Proof. The identity element is definitely an element of $\mathrm{Aut}(\mathcal{C})$. Let $f, g \in \mathrm{Aut}(\mathcal{C})$ be arbitrary elements. Because $f(\mathcal{C}) = \mathcal{C}$, we must have $f^{-1}(\mathcal{C}) = \mathcal{C}$ and thus $f^{-1} \in \mathrm{Aut}(\mathcal{C})$. Because $g(\mathcal{C}) = \mathcal{C}$, it must also be true that $f(g(\mathcal{C})) = \mathcal{C}$ and therefore $f \circ g \in \mathrm{Aut}(\mathcal{C})$. □

Theorem 3.8. *$Aut(\mathcal{C})$ is a crystallographic group.*

Proof. We first show that $\mathrm{Aut}(\mathcal{C})$ is cocompact. Suppose it isn't. Choose an arbitrary $c \in \mathcal{C}$ and let Λ be a lattice such that $\mathcal{C} = \Lambda + \mathcal{C}$. Denote with $\{v_1, ..., v_n\}$ the basis vectors of Λ. Note that any translation over integer linear combinations of these basis vectors is an element of $\mathrm{Aut}(\mathcal{C})$. Let C be the following compact set:

$$C = \left\{ y \in \mathbb{R}^n \middle| |y - c| \leqslant \sum_{i=1}^{n} |v_i| \right\}$$

Because $\mathcal{C}$ is not cocompact, there is an $x \in \mathbb{R}^n$ such that $g(x) \notin C$ for every $g \in \mathrm{Aut}(\mathcal{C})$. Because $\{v_1, ..., v_n\}$ are linearly independent, we can write $x = \lambda_1 v_1 + ... + \lambda_n v_n$ and $c = \mu_1 v_1 + ... + \mu_n v_n$ with $\lambda_i, \mu_i \in \mathbb{R}$. Let $k_i \in \mathbb{Z}$ be a number such that $|\lambda_i + k_i - \mu_i| \leqslant 1$. We now take a look at the translation $(I_n, k_1 v_1 + ... + k_n v_n) \in \mathrm{Aut}(\mathcal{C})$. We note that:

$$(I_n, k_1 v_1 + ... + k_n v_n)(x) = \sum_{i=1}^{n} (\lambda_i + k_i) v_i$$

Moreover:

$$\left| \sum_{i=1}^{n} (\lambda_i + k_i) v_i - c \right| \leqslant \sum_{i=1}^{n} |\lambda_i + k_i - \mu_i| |v_i| \leqslant \sum_{i=1}^{n} |v_i|$$

Because of this $(I_n, k_1v_1+...+k_nv_n)(x)$ must be an element of C, but this is impossible because the translation is an element of $\mathrm{Aut}(\mathcal{C})$. We therefore arrive at a contradiction.

Now we will show that $\mathrm{Aut}(\mathcal{C})$ is discrete. Choose an arbitrary sequence $((A_k, b_k))_k$ in $\mathrm{Aut}(\mathcal{C})$ that converges to $(A, b) \in \mathrm{Aut}(\mathcal{C})$. By Lemma 2.8 it is sufficient to show that $((A_k, b_k))_k$ eventually becomes constant. Let Λ be a lattice such that $\mathcal{C} + \Lambda = \mathcal{C}$ and denote the basis elements of Λ by $\{v_1, ..., v_n\}$. Let $v_0 = 0$. Choose an arbitrary point $c \in \mathcal{C}$. We know that $\mathcal{C}$ is discrete and that $(A, b)(c+v_i)$ are all elements of $\mathcal{C}$. Therefore there is an open subset U_i around each of these points such that $\mathcal{C} \cap U_i = \{(A, b)(c+v_i)\}$. Because $((A_k, b_k))_k \to (A, b)$, $(A_k, b_k)(c + v_i)$ must come arbitrarily close to $(A, b)(c + v_i)$ for k large enough. However, because such an open set U_i exists, we thus find a $k_i \in \mathbb{N}$ such that for every $k > k_i$, we must have that $(A_k, b_k)(c + v_i) \in U_i$. Therefore we find that $(A_k, b_k)(c + v_i) = (A, b)(c + v_i)$. If we take $K = \max\{k_0, ..., k_n\}$, then we know that $(A_k, b_k)(c + v_i) = (A, b)(c + v_i)$ for every $k > K$ and for every $i \in \{0, ..., n\}$. Now subtracting the equality $A_kc + b_k = Ac + b$ from all other equalities we have, we get: $A_kv_i = Av_i$ for every $i \in \{1, ..., n\}$ and for $k > K$. Because $\{v_1, ..., v_n\}$ is a basis of $\mathbb{R}^n$ we thus find that $A_k = A$ for $k > K$. Because $A_kc + b_k = Ac + b$, we also find that $b_k = b$ for $k > K$. Therefore the sequence $((A_k, b_k))_k$ eventually becomes constant.

□

Example 3.9. As an example, we will look at the lattice in $\mathbb{R}^n$ given by $\Lambda = \mathbb{Z}^n$. The crystal we will look at is just the lattice itself. Let $f = (A, b)$ be a symmetry of Λ. Because f is Euclidean, A must map a unit vector to another unit vector of Λ. Therefore A is given by a matrix that contains exactly one 1 or -1 in every row and column: A thus permutes the unit vectors of Λ. Simply counting the amount of possible matrices gives exactly $n!2^n$ Euclidean matrices that preserve Λ. We already noted earlier that b must be an element of Λ (by applying f on 0). It is clear that any translation over an element of Λ would preserve the lattice. Note that the group of all Euclidean transformations that suffice the previous conditions on A and b is indeed a crystallographic group. We explicitly give the 8 matrices in the crystallographic group for $n = 2$ and mention the symmetry of Λ they entail:

$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$	$\begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}$	$\begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}$
identity	reflection x-axis	reflection y-axis	reflection origin
$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}$
reflection $(x = y)$-axis	rotation $\frac{-\pi}{2}$	rotation $\frac{\pi}{2}$	reflection $(x = -y)$-axis

4 First Bieberbach Theorem

In order to show that every crystallographic group is a symmetry group for some lattice Λ we will need the first Bieberbach Theorem. The Bieberbach Theorems tell us something about the structure of a crystallographic group, they will thus not only imply that every crystallographic group is a symmetry group, but they will also help us understand how these symmetry groups are structured.

Theorem 4.1 (**first Bieberbach Theorem**). *Let $\Gamma \subset E(n)$ be a crystallographic group. Then the set of translations $\Gamma \cap T(n)$ is a torsion free and finitely generated abelian group of rank n, and is a maximal abelian and normal subgroup of Γ of finite index.*

The first Bieberbach Theorem says that the translations of Γ can be seen as a lattice in $\mathbb{R}^n$ as we will explain later in greater detail. It also says that there are only finitely many different matrices in the group $\{A | \exists b \in \mathbb{R}^n : (A, b) \in \Gamma\}$. Thus Γ introduces a structure in $\mathbb{R}^n$ with lots of symmetries, as will become more apparent in the proof of the theorem.

Some aspects of the first Bieberbach Theorem are easily proven. Indeed, that $T = \Gamma \cap T(n)$ is torsion free immediately follows from the definition of torsion free. The fact that it is abelian follows from the fact that translations commute with each other.

We can also show that it is maximal abelian. Say there exists an abelian group $H \subset \Gamma$ that strictly contains $\Gamma \cap T(n)$. Then there must be an element $(A, b_1) \in H$ with $A \neq I_n$. For a translation (I_n, b_2), we have that

$(A, b_1) \circ (I_n, b_2) = (A, Ab_2 + b_1)$ and $(I_n, b_2) \circ (A, b_1) = (A, b_2 + b_1)$. Thus b_2 must be an eigenvector of A with eigenvalue 1 because H is abelian. Now the first Bieberbach Theorem says that $\Gamma \cap T(n)$ is of rank n (we will prove this later) and thus there exists n linearly independent vectors in $\Gamma \cap T(n)$. Applying the previous argument to the n linearly independent vectors, would imply that they all are eigenvectors belonging to eigenvalue 1. But this would imply that A is the identity, which is a contradiction.

The proof of the other aspects of the first Bieberbach Theorem, namely that $\Gamma \cap T(n)$ is finitely generated of rank n and that it is a normal subgroup of finite index, is more complex. We first need to prove some lemmas before we can show this.

4.1 Proof of the first Bieberbach Theorem

In this section we will prove the final aspects of the first Bieberbach Theorem. The lemmas and their proofs given in this section are based on the lemmas and proofs of [Bus85] and [Pan19]. However, several details were left out in these sources which have been added here. Most notably, the sources don't mention how the lemmas imply the final aspects of the first Bieberbach Theorem which we do at the end of this section.

Lemma 4.2. *Let $\Gamma \subset E(n)$ be a crystallographic group of dimension n. Then its translation subgroup has n linearly independent elements.*

In order to prove the lemma, we will need some other lemmas and some new notations. Take $A \in O(n)$ arbitrary. Define

$$m(A) := \max \left\{ \frac{|Ax - x|}{|x|} \;\middle|\; x \in \mathbb{R}^n \setminus \{0\} \right\}$$

We need to prove that the maximum is attained for some x and thus that $m(A)$ is well defined. Take

$$m_p(A) := \sup \left\{ \frac{|Ax - x|}{|x|} \;\middle|\; x \in \mathbb{R}^n \setminus \{0\} \right\}$$

Now note that for $x \in \mathbb{R}^n \setminus \{0\}$, $\lambda \in \mathbb{R} \setminus \{0\}$ and $y = \lambda x$:

$$\frac{|Ay - y|}{|y|} = \frac{|A\lambda x - \lambda x|}{|\lambda x|} = \frac{|\lambda| \cdot |Ax - x|}{|\lambda| \cdot |x|} = \frac{|Ax - x|}{|x|}$$

and thus all unique values of $\frac{|Ax-x|}{|x|}$ are achieved for x on the unit sphere. Because the unit sphere is compact, the supremum is achieved for some x on the unit sphere. This proves that $m(A)$ is well defined. Note that $m(A)$ is some measure of how different A is from I_n: if $m(A)$ is very small, then $|Ax|$ is always close to x (relatively to the size of $|x|$).

We also define the following subgroup of $\mathbb{R}^n$:

$$E_A := \{x \in \mathbb{R}^n \mid |Ax - x| = m(A)|x|\}$$

Lemma 4.3. *E_A is a non-trivial, A-invariant subspace.*

Proof. We first prove the A-invariance of E_A. If $x \in E_A$, then we have:

$$|A(Ax) - (Ax)| = |Ax - x| = m(A)|x| = m(A)|Ax|$$

where we used the fact that $|Ay| = |y|$ for all $y \in \mathbb{R}^n$ because $A \in O(n)$. Thus $Ax \in E_A$. If $Ax \in E_A$ an analogous calculation with A^{-1} gives $x \in E_A$.

We now prove that E_A is a subspace of $\mathbb{R}^n$. Let $x, y \in E_A$. We have

$$\begin{aligned} 2m(A)^2(|x|^2 + |y|^2) &= 2\left(\left(\frac{|Ax - x|}{|x|}\right)^2 |x|^2 + \left(\frac{|Ay - y|}{|y|}\right)^2 |y|^2\right) \\ &= 2\left(|Ax - x|^2 + |Ay - y|^2\right) \end{aligned}$$

By the parallelogram law, which says that $|v|^2 + |w|^2 = |v+w|^2 + |v-w|^2$ for $v, w \in \mathbb{R}^n$, and the fact that $|Az - z| \leqslant m(A)|z|$ for every $z \in \mathbb{R}^n$ we now have:

$$\begin{aligned} 2m(A)^2(|x|^2 + |y|^2) &= |(Ax - x) + (Ay - y)|^2 + |(Ax - x) - (Ay - y)|^2 \\ &= |A(x+y) - (x+y)|^2 + |A(x-y) - (x-y)|^2 \\ &\leqslant (m(A)|x+y|)^2 + (m(A)|x-y|)^2 \\ &= 2m(A)^2(|x|^2 + |y|^2) \end{aligned}$$

Since the first and last equation are the same, the inequality in the middle is an equality and thus we find:

$$\begin{aligned} |A(x+y) - (x+y)| &= m(A)|x+y| \\ |A(x-y) - (x-y)| &= m(A)|x-y| \end{aligned}$$

From this it follows that $x + y, x - y \in E_A$. We have already proven that if $x \in E_A$ then $y = \lambda x \in E_A$ for every $\lambda \in \mathbb{R} \setminus \{0\}$. Thus E_A is a subspace of $\mathbb{R}^n$. □

We now define the commutator of two matrices $A, B \in O(n)$ as

$$[A, B] := ABA^{-1}B^{-1}$$

Lemma 4.4. *Let $A, B \in O(n)$. Then $m([A, B]) \leqslant 2m(A)m(B)$.*

Proof. First we prove a useful equality:

$$\begin{aligned} \Big((A - I_n)(B - I_n) - (B - I_n)(A - I_n)\Big)A^{-1}B^{-1} &= (AB - BA)A^{-1}B^{-1} \\ &= ABA^{-1}B^{-1} - I_n \\ &= [A, B] - I_n \end{aligned}$$

Because both $A, B \in O(n)$, we have that $A^{-1}B^{-1} \in O(n)$ and thus $|A^{-1}B^{-1}x| = |x|$. Also note that for all $x \in \mathbb{R}^n$

$$\begin{aligned} |(A - I_n)(B - I_n)x| &\leqslant |Ax - x|m(B) \\ &\leqslant m(A)m(B)|x| \end{aligned}$$

It follows that for all $x \in \mathbb{R}^n$:

$$\begin{aligned} |[A, B]x - x| &= \Big|\Big((A - I_n)(B - I_n) - (B - I_n)(A - I_n)\Big)x\Big| \\ &\leqslant m(A)m(B)|x| + m(B)m(A)|x| \\ &= 2m(A)m(B)|x| \end{aligned}$$

The desired result is obtained after division by $|x|$ and taking the maximum over both sides. □

Let $\angle(u, b)$ be the angle between the vectors $u, b \in \mathbb{R}^n$. We now need two more lemmas before we are able to show Lemma 4.2. Lemma 4.5 says that for every unit vector there is a transformation in Γ that is almost a translation. Lemma 4.6 says that transformations that are almost translations, must be translations.

Lemma 4.5. *Let $u \in \mathbb{R}^n$ be an arbitrary unit vector. Then for all $\epsilon, \delta > 0$ there exists a $\beta = (B, b) \in \Gamma$, such that the following holds:*

1. $b \neq 0$
2. $\angle(u, b) \leqslant \delta$
3. $m(B) \leqslant \epsilon$

Proof. Since Γ is cocompact, there exists a $d \in \mathbb{R}$ so that for all $x \in \mathbb{R}^n$ there exists an $(A, a) \in \Gamma$ so that $|Ax + a| \leqslant d$. Take for each $k \in \mathbb{N}$ an element $\alpha_k = (A_k, a_k) \in \Gamma$ such that $|A_k(ku) + a_k| \leqslant d$. Now take $\beta_k = (B_k, b_k) = \alpha_k^{-1} = (A_k^{-1}, -A_k^{-1}a_k)$. Then

$$|ku - b_k| = |A_k(ku - b_k)| = |A_k(ku + A_k^{-1}a_k)| = |A_k(ku) + a_k|$$

and thus $|ku - b_k| \leqslant d$. Because $b_k \to \infty$ and its stays close to ku, we find that $\angle(u, b_k) \to 0$. Since $O(n)$ is compact, there exists a subsequence of (β_k) such that the rotational part of this subsequence (B_k) converges to a matrix B. We will now assume that (β_k) is that subsequence.

Choose $\epsilon, \delta > 0$ arbitrarily. Because $\angle(u, b_k) \to 0$, there exists an $n_0 \in \mathbb{N}$ such that for every $n > n_0$ we have $\angle(u, b_n) \leqslant \frac{\delta}{2}$. Because $B_k \to B$, we find that $B_n B_m^{-1}$ becomes arbitrarily close to I_n for $n, m \to \infty$. Because $m(I_n) = 0$ and because m is continuous, we can choose an $n_1 \in \mathbb{N}$ such that for every $n, m > n_1$, we have $m(B_n B_m^{-1}) \leqslant \epsilon$. Now choose $i \in \mathbb{N}$ such that $i > \max(n_0, n_1)$. Because $|b_i|$ is finite and $b_k \to \infty$, there must be a $j > i$ large enough such that $|b_i| \leqslant \frac{\delta}{4}|b_j|$.

We have:

$$m(B_j B_i^{-1}) \leqslant \epsilon, \quad \angle(u, b_j) \leqslant \frac{\delta}{2}, \quad |b_i| \leqslant \frac{\delta}{4}|b_j|$$

Now consider the element

$$\beta = (B, b) = \beta_j \beta_i^{-1} = (B_j B_i^{-1}, -B_j B_i^{-1} b_i + b_j)$$

Then $m(B) = m(B_j B_i^{-1}) \leqslant \epsilon$. Because $| - B_j B_i^{-1} b_i| = |b_i| \leqslant \frac{\delta}{4}|b_j|$ we find that the angle between u and b suffices the following inequalities:

$$\begin{aligned} \angle(u, b) &= \angle(u, -B_j B_i^{-1} b_i + b_j) \\ &\leqslant \angle(u, b_j) + \angle(b_j, -B_j B_i^{-1} b_i + b_j) \\ &\leqslant \frac{\delta}{2} + \frac{\delta}{2} = \delta \end{aligned}$$

Thus we find that β suffices the conditions in the lemma. □

Before continuing to the next lemma, we first define $m^\perp(A)$ for a matrix $A \in O(n)$:

$$m^\perp(A) := \max \left\{ \frac{|Ax - x|}{|x|} \Big| x \in E_A^\perp \setminus \{0\} \right\}$$

Here $E_A^\perp$ is the space orthogonal to E_A. Note that $m^\perp(A) < m(A)$. Indeed, if equality would hold, we would have an $x \in E_A^\perp$ such that $\frac{|Ax-x|}{|x|} = m(A)$. But this would mean that $x \in E_A$ and thus $x = 0$, which is impossible.

We also know that $E_A \oplus E_A^\perp = \mathbb{R}^n$. Thus we can write every $x \in \mathbb{R}^n$ as $x^\perp + x^E$ with $x^\perp \in E_A^\perp$ and $x^E \in E_A$.

Lemma 4.6. *If $\alpha = (A, a) \in \Gamma$ satisfies $m(A) \leqslant \frac{1}{2}$, then α is a translation.*

Proof. Take $\alpha \in \Gamma$ with $m(A) \leqslant 1/2$. We need to prove that $A = I_n$ or equivalently that $m(A) = 0$. Suppose $m(A) \neq 0$ and consider the following non-empty set:

$$T_1 = \{\alpha = (A, a) \in \Gamma | 0 < m(A) \leqslant 1/2\}$$

Take $\alpha = (A, a) \in T_1$ so that $|a|$ is minimal (we can choose such an α because Γ is discrete). We have proven that $m^\perp(A) < m(A)$ for $A \neq I_n$. Thus $\frac{1}{8}(m(A) - m^\perp(A)) > 0$. Define the set

$$T_2 = \left\{ \beta = (B, b) \Big| b \neq 0 \wedge m(B) \leqslant \frac{1}{8}(m(A) - m^\perp(A)) \wedge |b^\perp| < |b^E| \right\}$$

Lemma 4.5 applied to a random unit vector $u \in E_A$ provides an element $\beta \in T_2$ and thus T_2 is non-empty. We can consider the element $\beta = (B, b) \in T_2$ with the smallest translational part $b \neq 0$. Consider

$\gamma = [\alpha, \beta] = (C, c)$. We want to show that $\gamma \in T_2$ with $|c| < |b|$ which is a contradiction. Let $b = b^\perp + b^E$ and $c = c^\perp + c^E$ with $b^\perp, c^\perp \in E_A^\perp$ and $b^E, c^E \in E_A$.

We have

$$\begin{aligned}\gamma(x) = [\alpha, \beta](x) &= A\left(B\left(A^{-1}\left(B^{-1}x - B^{-1}b\right) - A^{-1}a\right) + b\right) + a \\ &= [A, B]x - [A, B]b - ABA^{-1}a + Ab + a \\ &= [A, B]x + (A - I_n)b + (I_n - [A, B])b + A(I_n - B)A^{-1}a \\ &= [A, B]x + (A - I_n)b^E + (A - I_n)b^\perp + r\end{aligned}$$

where we have defined

$$r := (I_n - [A, B])b + A(I_n - B)A^{-1}a$$

Thus $C = [A, B]$ and $c = (A - I_n)b^E + (A - I_n)b^\perp + r$.

If β is a pure translation, we know that:

$$\begin{aligned}r &= (I_n - [A, I])b + A(I_n - I_n)A^{-1}a \\ &= (I_n - AI_nA^{-1}I_n^{-1})b = 0\end{aligned}$$

Now suppose β is not a pure translation. Note that $m(B) \leqslant \frac{1}{8}(m(A) - m^\perp(A)) \leqslant m(A) \leqslant 1/2$ and thus $\beta \in T_1$ from which it follows that $|a| \leqslant |b|$. On top of that we have $m(C) = m([A, B]) \leqslant 2m(A)m(B) \leqslant m(B)$ using Lemma 4.4. Thus:

$$\begin{aligned}|r| &= |(I_n - [A, B])b + A(I_n - B)A^{-1}a| \\ &\leqslant |(I_n - C)b| + |(I_n - B)a| \\ &\leqslant m(C)|b| + m(B)|a| \\ &\leqslant (m(C) + m(B))|b| \\ &\leqslant 2m(B)|b| \\ &< 4m(B)|b^E| \\ &\leqslant \frac{1}{2}(m(A) - m^\perp(A))|b^E|\end{aligned}$$

The above inequality thus holds always, also if β is a pure translation because $r = 0$ in that case.

Write $r = r^E + r^\perp$ with $r^E \in E_A$ and $r^\perp \in E_A^\perp$. Substituting this into $c = (A - I_n)b^E + (A - I_n)b^\perp + r$ gives

$$c^E - (A - I_n)b^E - r^E = -c^\perp + (A - I_n)b^\perp + r^\perp$$

Now both sides are in perpendicular subspaces and equal to each other, therefore they must be 0. This gives

$$\begin{aligned}|c^\perp| &= |(A - I_n)b^\perp + r^\perp| \\ &\leqslant |(A - I_n)b^\perp| + |r^\perp| \\ &\leqslant m^\perp(A)|b^\perp| + |r| \\ &< m^\perp(A)|b^E| + \frac{1}{2}(m(A) - m^\perp(A))|b^E| \\ &= \frac{1}{2}(m(A) + m^\perp(A))|b^E|\end{aligned}$$

and

$$\begin{aligned}
|c^E| &= |(A - I_n)b^E + r^E| \\
&\geqslant |(A - I_n)b^E| - |r^E| \\
&= m(A)|b^E| - |r^E| \\
&\geqslant m(A)|b^E| - |r| \\
&\geqslant m(A)|b^E| - \frac{1}{2}(m(A) - m^\perp(A))|b^E| \\
&= \frac{1}{2}(m(A) + m^\perp(A))|b^E|
\end{aligned}$$

All together this gives that $|c^\perp| < |c^E|$, $m(C) \leqslant m(B)$ and $c \neq 0$. Therefore $\gamma = (C, c) \in T_2$. But

$$\begin{aligned}
|c| &\leqslant |(A - I_n)b| + |r| \\
&\leqslant m(A)|b| + 2m(B)|b| \\
&\leqslant m(A)|b| + 2\frac{1}{8}(m(A) - m^\perp(A))|b| \\
&\leqslant \frac{1}{2}|b| + \frac{1}{4}|b| \\
&< |b|.
\end{aligned}$$

Which gives the desired contradiction. □

Now we are finally ready to prove Lemma 4.2.

Proof. Using Lemma 4.5 with n linearly independent unit vectors and $\epsilon = \frac{1}{2}$ we find n transformations $(B_1, b_1), ...(B_n, b_n)$ for which the translational parts are independent and $m(B_i) \leqslant \frac{1}{2}$. Then using Lemma 4.6 we find that all these transformations must be translations, which concludes the proof of Lemma 4.2. □

We are now ready to prove the final aspects of the first Bieberbach Theorem. The parallelepiped-argument given in this proof is based on a similar argument given to us by our supervisor [Vil21b].

Proof. We first prove that $H = (\Gamma \cap T(n))$ is normal. Choose $g = (A, a) \in \Gamma, (I_n, b) \in H$ arbitrarily. We want to prove that $g \circ (I_n, b) \circ g^{-1} \in H$. We do this by calculating $g \circ (I_n, b) \circ g^{-1}$:

$$\begin{aligned}
g \circ (I_n, b) \circ g^{-1} &= (A, a)(I_n, b)(A^{-1}, -A^{-1}a) \\
&= (A, a)(A^{-1}, b - A^{-1}a) \\
&= (I_n, Ab)
\end{aligned}$$

Obviously $(I_n, Ab) \in H$ and thus we find that H is normal.

We will now prove that $\Gamma/(\Gamma \cap T(n))$ is finite (and thus that $\Gamma \cap T(n)$ is of finite index). Define the function $f : E(n) \to O(n) : (A, b) \mapsto A$. Note that f is continuous. We use Lemma 2.8 to show that $f(\Gamma)$ is discrete. Let $(A_n) \to A$ be a convergent sequence in $f(\Gamma)$ and suppose it is not eventually constant. Then there must be a subsequence (B_k) such that $B_k \neq A$ for all $k \in \mathbb{N}$. Because f is a projection, there must exist a sequence $((B_k, b_k))_{k\in\mathbb{N}}$ in Γ. Because of Lemma 4.6, we have n linearly independent vectors $v_1, ..., v_n \in \mathbb{R}^n$ such that $(I_n, v_i) \in \Gamma$. We can write $b_k = \lambda_{1,k}v_1 + ... + \lambda_{n,k}v_n$. By applying (I_n, v_i) or its inverse $(I_n, -v_i)$ several times on (B_k, b_k), we can assume that $0 \leqslant \lambda_{i,k} \leqslant 1$. Thus we find that $|b_k| \leqslant |v_1| + ... + |v_n|$ which implies that the sequence (b_k) is bounded. Therefore, there exists a convergent subsequence such that $(B_k, b_k) \to (A, b)$. Now because Γ is discrete, we know that this subsequence must eventually become constant. Thus there exists a $k \in \mathbb{N}$ such that $B_k = A$. This is a contradiction with $B_k \neq A$. We thus find that $f(\Gamma)$ is discrete.

We will now show that it is compact. Let (A_n) be an arbitrary sequence in $f(\Gamma)$. Because $O(n)$ is compact, we know there must be a converging subsequence (B_n) with limit B. Then $(B_n B_{n+1}^{-1})$ converges to I_n and it is a sequence in $f(\Gamma)$. Because $I_n \in f(\Gamma)$ and because $f(\Gamma)$ is discrete, there is an open set U around I_n such that $U \cap f(\Gamma) = \{I_n\}$. Therefore, there must exist an $n_0 \in \mathbb{N}$ such that for every $k > n_0$, $B_k B_{k+1}^{-1} = I_n$. Therefore

the row (B_n) eventually becomes constant and thus $B_k = B$ for k large enough. Consequently, $B \in f(\Gamma)$ and thus we find that $f(\Gamma)$ is compact because we have shown that every sequence in $f(\Gamma)$ has a converging subsequence with limit in $f(\Gamma)$. Now we can apply Lemma 2.7 to say that $f(\Gamma)$ is finite. Consequently, we have proven that $\Gamma/(\Gamma \cap T(n))$ is finite.

We now show that $\Gamma \cap T(n)$ is finitely generated and of rank n. Because of Lemma 4.6, we have n linearly independent vectors $v_1, ..., v_n \in \mathbb{R}^n$ such that $(I_n, v_i) \in \Gamma$. Now define the parallelepiped P as:

$$P = \{\alpha_1 v_1 + ... + \alpha_n v_n | \alpha_i \in [0, 1]\}$$

Now we can find a basis $w_1, ..., w_n \in P$ of $\mathbb{R}^n$ such that the volume of the associated parallelepiped is minimal. This basis exists since $\Gamma \cap T(n) \cap P$ is finite (P is compact and Γ is discrete). Define P_w to be the associated parallelepiped. Now let $(I_n, w) \in \Gamma$ be arbitrary. Because $w_1, ..., w_n$ is a basis, we know there exists $a_i \in \mathbb{R}$ such that $w = a_1 w_1 + ... + a_n w_n$. If we now show that $a_i \in \mathbb{Z}$, we have proven that every translation in Γ can be written as in Definition 2.10 because the group action of Γ, the composition, on two translations is the sum of those two translations. By subtracting and adding w_i from w, we can assume $0 \leqslant a_i < 1$. Suppose $a_k \neq 0$. Then $w \neq 0$ and thus we find that $w \in P_w$ and w not on the edge of P_w since $a_i < 1$. This means that the parallelepiped formed by $w_1, ..., w_{k-1}, w, w_{k+1}, ..., w_n$ strictly lies within P_w. This is a contradiction with our assumption that P_w has minimal volume. □

5 Crystallographic groups are symmetry groups

As previously announced in Section 3 we are now able to prove that crystallographic groups preserve some crystal. The proof of the following theorem is partially based on the proof given by our supervisor [Vil21b].

Theorem 5.1. *Let Γ be any crystallographic group of dimension n. Then there exists a crystal $\mathcal{C}$ such that Γ preserves that crystal and thus $\Gamma \subset Aut(\mathcal{C})$.*

Proof. We first show that there exist crystals such that every transformation in Γ preserves that crystal. Let $w \in \mathbb{R}^n$ and let $\mathcal{C}_w = \Gamma w = \{f(w) | f \in \Gamma\}$ be the orbit of w. Because Γ is a group, we definitely have that $f(\mathcal{C}_w) = \mathcal{C}_w$ for any $f \in \mathcal{C}_w$. We now only need to show that $\mathcal{C}$ is a crystal. Note that $\mathcal{C}_w$ is non-empty because Γ is non-empty.

Suppose $\mathcal{C}_w$ is not discrete. Then there would exist a convergent sequence $(x_n) \to x$ in $\mathcal{C}$ that is not eventually constant. Now x_n can be written as $f_n(w)$ for an $f_n = (A_n, b_n) \in \Gamma$. Because $O(n)$ is compact, we can assume that (A_n) is convergent. By the first Bieberbach Theorem, we can assume that (b_n) is bounded (the argument why is completely analogous to the one given in the final part of the proof of the first Bieberbach Theorem which eventually showed that (b_k) was bounded). Because of Bolzano-Weierstrass, we can also assume that (b_n) is convergent. But this means that (f_n) is convergent and therefore eventually constant because Γ is discrete. Therefore (x_n) must eventually become constant which is a contradiction.

Because of the first Bieberbach Theorem there are n linearly independent vectors in the translations of Γ, we can choose them such that the translations of Γ are linear integer combinations of these translations. For each of these translations v_i, we must have $\mathcal{C}_w + v_i = \mathcal{C}_w$. Let Λ be the lattice with basis elements $\{v_1, ..., v_n\}$. Then $\mathcal{C}_w + \Lambda = \mathcal{C}_w$ and thus we find that $\mathcal{C}_w$ is a crystal. □

In fact, we can even construct a crystal such that $\Gamma = \text{Aut}(\mathcal{C})$ and not just $\Gamma \subset \text{Aut}(\mathcal{C})$. Unfortunately, the proof of this theorem is bit too long to put here and we didn't find a good source that explains how to construct such a crystal. If the reader is interested in the proof of this theorem, they can certainly contact us.

6 Second Bieberbach Theorem

There is more structure to be found in crystallographic groups, and the other Bieberbach Theorems give us some more insight in those groups. The second Bieberbach Theorem says that there are only finitely many

crystallographic groups for any dimension (up to an isomorphism). It is this theorem that gives an answer to the 18th problem of Hilbert.

Theorem 6.1 (**second Bieberbach Theorem**). *For any $n \in \mathbb{Z}_{>0}$ there are finitely many isomorphism classes of crystallographic groups of dimension n.*

We introduce the notion of a normal crystallographic group.

Definition 6.2. *A crystallographic group is called normal if $\Gamma \cap T(n)$ satisfies the following conditions:*

(i) the distance between any two distinct vectors in $\Gamma \cap T(n)$ is bigger than or equal to 1.

(ii) It contains n linearly independent unit vectors.

Note that the condition that the distances between two distinct vectors in $\Gamma \cap T(n)$ is bigger or equal to 1 is equivalent to the condition that every element of $\Gamma \cap T(n)$ has size bigger or equal to 1. We will also need to extend the definition of lattice a little:

Definition 6.3. *A sublattice Λ of dimension k in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ with the property that there exist linearly independent vectors $\{v_1, ..., v_k\}$ such that:*

$$\Lambda = \{\lambda_1 v_1 + ... + \lambda_k v_k | \lambda_i \in \mathbb{Z}\}$$

A lattice point is an element of Λ. The basis elements of Λ are $\{v_1, ..., v_k\}$. If we are not interested in the dimension of Λ, we will simply call Λ a sublattice.

The proof and the lemmas we will give are based on [Bus85]. The idea behind it is to prove that every crystallographic group is isomorphic to some normal crystallographic group. The proof is concluded by proving that up to isomorphism there are only finitely many different normal crystallographic groups.

6.1 Proof of the second Bieberbach Theorem

We first prove some lemmas that we will need in order to prove that every crystallographic group is isomorphic to some normal subgroup.

Lemma 6.4. *Let Λ be a sublattice in $\mathbb{R}^n$ such that every two distinct vectors of Λ have distance bigger than or equal to 1. Let $N(p)$ be the number of lattice points in Λ whose distance from the origin is smaller than or equal to $p \in \mathbb{R}^+$. Then*

$$N(p) \leqslant (2p+1)^n$$

Proof. Consider the spheres of radius $\frac{1}{2}$ around the $N(p)$ lattice points whose distance from the origin is smaller than or equal to p. The spheres are all disjoint since the pairwise distance between points is greater than 1. Since the distance from the origin is smaller than or equal to p for each of those points, the spheres are all contained in a sphere with radius $p+\frac{1}{2}$. Thus the sum of the volumes of the spheres around each point must be smaller than the volume of the sphere with radius $p+\frac{1}{2}$. The volume of an n-dimensional sphere with radius r is given by Ar^n where A is some constant dependent on n. Thus

$$N(p)A\left(\frac{1}{2}\right)^n \leqslant A\left(p+\frac{1}{2}\right)^n$$

From this it follows that

$$N(p) \leqslant (2p+1)^n$$

□

Lemma 6.5. *Let Λ be a sublattice of dimension k in $\mathbb{R}^n$ such that every two distinct vectors of Λ have distance bigger than or equal to 1. Let $w_1, ..., w_k \in \Lambda$ be k linearly independent vectors and $E = span\{w_1, ..., w_k\}$. Let $w \in L$ be an arbitrary lattice point and $w = w^E + w^\perp$ with $w^E \in E$ and $w^\perp \in E^\perp$. If $w^\perp \neq 0$ (and thus $w \notin E$), then*

$$|w^\perp| \geqslant (3 + |w_1| + ... + |w_k|)^{-n}$$

Proof. Let N be the biggest integer smaller or equal to $(3 + |w_1| + ... + |w_k|)^n$. Then we know that

$$1/N \geqslant (3 + |w_1| + ... + |w_k|)^{-n}$$

Now suppose we have a $w \in \Lambda$ with $0 < |w^\perp| \leqslant (3 + |w_1| + ... + |w_k|)^{-n}$. Then it follows that $0 < |w^\perp| \leqslant 1/N$. Consider the set of vectors $A = \{0, w, 2w, ..., Nw\}$. We have for each vector λw in this set that $0 \leqslant \lambda |w^\perp| \leqslant 1$. For any vector $v \in E$ it is possible to add an integer linear combination $a_1 w_1 + ... + a_k w_k$ with $a_i \in \mathbb{Z}$ such that

$$|v + a_1 w_1 + ... + a_n w_k| \leqslant \frac{1}{2}(|w_1| + ... + |w_k|)$$

Therefore we can add to each vector λw a suitable integer linear combination $a_{1,\lambda} w_1 + ... + a_{k,\lambda} w_k$ so that

$$|(\lambda w)^E + a_{1,\lambda} w_1 + ... + a_{k,\lambda} w_k| \leqslant \frac{1}{2}(|w_1| + ... + |w_k|)$$

Let B be the set that contains all these new vectors. Thus

$$B = \{\lambda w + a_{1,\lambda} w_1 + ... + a_{k,\lambda} w_k | \lambda \in \{0, ..., N\}\}$$

Note that each vector in A has a different perpendicular component. Because adding a linear combination of vectors in E to any vector of A does not change the perpendicular component, we find that all elements in B are distinct. For any $v = v^\perp + v^E \in B$, we have

$$|v^\perp| \leqslant 1$$

and

$$|v^E| \leqslant \frac{1}{2}(|w_1| + ... + |w_k|)$$

Thus we have found $N + 1$ different lattice points with distance smaller or equal to $1 + \frac{1}{2}(|w_1| + ... + |w_k|)$ from the origin. Using Lemma 6.4 we have

$$\begin{aligned} N\left(1 + \frac{1}{2}(|w_1| + ... + |w_k|)\right) &\leqslant \left(2\left(1 + \frac{1}{2}(|w_1| + ... + |w_k|)\right) + 1\right)^n \\ &\leqslant (3 + |w_1| + ... + |w_k|)^n \\ &< N + 1 \end{aligned}$$

which is a contradiction. Thus

$$|w^\perp| \geqslant (3 + |w_1| + ... + |w_k|)^{-n}$$

. □

Lemma 6.6. *If $\alpha = (A, a) \in \Gamma$ and $(I_n, b) \in \Gamma \cap T(n)$, then $(I_n, Ab) \in \Gamma \cap T(n)$.*

Proof. Because Γ is a group, we must have $\alpha \circ (I_n, b) \circ \alpha^{-1} \in \Gamma$. A simple calculation gives that

$$\alpha \circ (I_n, b) \circ \alpha^{-1} = (I_n, Ab)$$

Thus $(I_n, Ab) \in \Gamma \cap T(n)$. □

We now need one last lemma before proving the second Bieberbach Theorem.

Lemma 6.7. *Each crystallographic group Γ is isomorphic to a normal crystallographic group.*

Proof. By scaling we may assume that the shortest non-zero vector in $\Gamma \cap T(n)$ is a unit vector. Assume by induction that $\Gamma \cap T(n)$ satisfies Definition 6.2 (i) and contains $k < n$ unit vectors $w_1, ..., w_k$ which span a k dimensional linear subspace E of $\mathbb{R}^n$. It remains to find a group Γ' isomorphic to Γ such that $\Gamma \cap T(n)$ contains $k + 1$ linearly independent unit vectors and also satisfies 6.2 (i).

We will make a distinction between two cases:

1. $\exists \alpha = (A, a) \in \Gamma : \exists w_i \in E : A(w_i) \notin E$
2. $\forall \alpha = (A, a) \in \Gamma : \forall w_i \in E : A(w_i) \in E$

In the first case we use Lemma 6.6 which states that $A(w_i) \in \Gamma \cap T(n)$ for $w_i \in \Gamma \cap T(n)$. Since $A(w_i) \notin E$ and $|Aw_i| = |w_i| = 1$, we have found the $(k+1)$th linear independent unit vector.

In the second case all rotational parts of transformations in Γ leave E invariant. Since they leave E invariant, they also leave $E^\perp$ invariant. Now consider the transformation Φ_μ ($\mu \in \mathbb{R}$) given by

$$\Phi_\mu(x^E + x^\perp) = x^E + \mu x^\perp$$

By creating a basis of $\mathbb{R}^n$ consisting of the vectors $\{w_1, ..., w_k\}$ together with a basis of $E^\perp$, we see that Φ_μ is an affine transformation with matrix

$$\begin{bmatrix} I_k & 0 \\ 0 & \mu I_{n-k} \end{bmatrix}$$

with respect to this basis.

We prove that this transformation commutes with the rotational parts of Γ. Let A be the rotational part of a transformation $\alpha \in \Gamma$. Because A leaves E and $E^\perp$ invariant, we find that the matrix given with respect to the same basis as the matrix of Φ_μ is:

$$\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$

with $A_1 \in \mathbb{R}^{k \times k}$ and $A_2 \in \mathbb{R}^{(n-k)\times(n-k)}$. Because the identity matrix commutes with every matrix, we find that Φ_μ commutes with A.

Define the group $\Gamma_\mu = \Phi_\mu \Gamma \Phi_\mu^{-1}$. This group is conjugate to the group Γ and therefore isomorphic to Γ. Thus Γ_μ is also a crystallographic group. Since the rotational parts of Γ commute with Φ_μ we know that the rotational parts of Γ_μ also preserve E.

We now prove that $\Gamma_\mu \cap T(n) = \Phi_\mu(\Gamma \cap T(n))$. Take $\alpha = (I_n, a) \in \Gamma_\mu \cap T(n)$, then $\Phi_\mu^{-1} \circ \alpha \circ \Phi_\mu \in \Gamma$ and

$$(\Phi_\mu^{-1} \circ \alpha \circ \Phi_\mu)(x) = \Phi_\mu^{-1}(\Phi_\mu(x) + a) = x + \Phi_\mu^{-1}(a)$$

From this it follows that $(I_n, \Phi_\mu^{-1}(a)) \in \Gamma \cap T(n)$ so that $\alpha \in \Phi_\mu(\Gamma \cap T(n))$. Now take $\alpha = (I_n, a) \in \Gamma \cap T(n)$, then

$$(\Phi_\mu \circ \alpha \circ \Phi_\mu^{-1})(x) = \Phi_\mu\left(\Phi_\mu^{-1}(x) + a\right) = x + \Phi_\mu(a)$$

Thus $(I_n, \Phi_\mu(a)) \in \Gamma_\mu \cap T(n)$ and because of that we find $\Gamma_\mu \cap T(n) = \Phi_\mu(\Gamma \cap T(n))$.

Because $k < n$ there exists at least one non-zero vector in $E^\perp \cap \Gamma \cap T(n)$. Because $\Gamma \cap T(n)$ is discrete, we can choose a smallest non-zero vector $v \in E^\perp \cap \Gamma \cap T(n)$. Let $\mu = 1/|v|$. Then $E^\perp \cap \Gamma_\mu \cap T(n)$ must contain at least one unit vector, namely $\Phi_\mu(v)$. Moreover, $\Gamma_\mu \cap T(n)$ does not contain any vector with size smaller than 1, otherwise v would not be the smallest non-zero vector in $E^\perp \cap \Gamma \cap T(n)$. Now $\Gamma_\mu \cap T(n)$ has the required properties, since it has k unit vectors in E and one extra linearly independent unit vector in $\Gamma_\mu \cap T(n) \setminus E$. This proves the lemma by induction. □

We complete the proof of the second Bieberbach Theorem by showing that

1. Each normal crystallographic group Γ is uniquely characterized by some integers $m_{ijk}, v(j,k)$ and N (which we will define later).
2. The absolute values of $m_{ijk}, v(j,k)$ and N have an upper bound which is only dependent on n.

We first prove the first point.

Proof. Let Γ be an arbitrary normal crystallographic group. By Definition 6.2 we can take n linearly independent transformations $\omega_i = (I_n, w_i) \in \Gamma \cap T(n)$ for $i \in \{1, ..., n\}$. Take $\Lambda = \Gamma \cap T(n)$, thus Λ is the following lattice

$$\Lambda = \{m_1 w_1 + ... + m_n w_n | m_1, ..., m_n \in \mathbb{Z}\}$$

For each left coset of the form $\alpha\Lambda$ we choose a representative ω with translational part w such that

$$|w| \leqslant \frac{1}{2}\left(|w_1| + ... + |w_n|\right) = \frac{n}{2}$$

Because of the finiteness of $\frac{\Gamma}{\Lambda}$, there are finitely many such representatives. Let us denote these representatives with $\omega_{n+1}, ..., \omega_N$. Now every element $\alpha \in \Gamma$ can be written as

$$\alpha = (m_1 w_1 + ... + m_n w_n) \circ \omega_\nu$$

where the integers $m_1, ..., m_n$ are unique for each element in a given coset and $n+1 \leqslant \nu \leqslant N$. Let

$$\omega_j \circ \omega_k = (m_{1jk} w_1 + ... + m_{njk} w_n) \circ \omega_{\nu(j,k)}$$

for some integers $m_{ijk}, \nu(j,k)$. Note that a (finite) table consisting of N rows and N columns containing the numbers $m_{1jk}, m_{ijk}, ..., m_{njk}, \nu(j,k)$ on the j-th row and the k-th column would completely determine Γ up to an isomorphism because this table would contain all information to determine $\alpha \circ \beta$ for $\alpha, \beta \in \Gamma$ given the representatives $\omega_1, ..., \omega_N$. Thus if we know all integers $m_{ijk}, \nu_(j,k)$ and N, then Γ is determined up to an isomorphism. □

We are left to prove that the absolute value of the integers $m_{ijk}, \nu(j,k)$ and N have an upper bound which is only dependent on n. This would mean that there only exist finitely many tables described above and thus we would find that there are only finitely many crystallographic groups of dimension n (up to an isomorphism).

Proof. First we try to find an upper bound for m_{ijk}. Consider the translation

$$(m_{1jk} w_1 + ... + m_{njk} w_n) = \omega_j \circ \omega_k \circ \omega_{\nu(j,k)}^{-1}$$

. We try to find a bound on the length of this transformation. We have chosen each representative ω_ν such that $|w_\nu| \leqslant \frac{n}{2} < n$ where w_ν is the translational part of ω_ν. We also have $|w_1|, ..., |w_n| = 1 \leqslant n$. Therefore our translation $\omega_j \circ \omega_k \circ \omega_{\nu(j,k)}^{-1}$ has length $\leqslant 3n$. Now consider for every $i \in \{1, ..., n\}$ the hyperplane E spanned by the vectors $\{w_1, ..., w_{i-1}, w_{i+1}, ..., w_n\}$. We get for $|w_i^\perp|$, the component of $|w_i|$ perpendicular to E, that

$$|m_{ijk} w_i^\perp| \leqslant |m_{1jk} w_1 + ... + m_{njk} w_n| \leqslant 3n$$

And by Lemma 6.5 we have $|w_i^\perp| \geqslant (3 + |w_1| + ... + |w_{i-1}| + |w_{i+1}| + ... + |w_n|)^{-n} = (n+2)^{-n}$. Therefore

$$|m_{ijk}| \leqslant 3n(n+2)^n$$

Now we want to find a bound for N, the number of representatives ($+n$ because $\omega_1, ..., \omega_n$ are the basis elements and they thus might not be representatives). We do this by proving there are only finitely many possibilities for each representative ω_i $(i > n)$.

Let us first find a bound for the number of rotational parts of the representatives. Let A be the rotational part of an arbitrary representative ω_i. The linear transformation A is uniquely determined by the images of the basis vectors $w_1, ..., w_n$. By Lemma 6.6 each of these images $A(w_i)$ is a unit vector of $\Gamma \cap T(n)$. Thus by Lemma 6.4 with $p = 1$, there are at most 3^n lattice points that suffice this condition. Therefore at most $(3^n)^n$ possible different rotational parts are possible for the elements of Γ.

Now we want to find a bound on the number of possible translational parts for a given representative with rotational part A. If two representatives ω_i and ω_j have the same rotational part then $\omega_i \circ \omega_j^{-1}$ is a translation with length $\leqslant \frac{n}{2} + \frac{n}{2} = n$. By Lemma 6.4 we have that the number of possible options for the translational part is $\leqslant (2n+1)^n$. All together this gives a maximum of $(3^n)^n (2n+1)^n$ possibilities for ω_i with $i > n$ and thus

$$N \leqslant n + (3^n)^n (2n+1)^n$$

Now $\nu(j,k) \leqslant N$ and thus we have found upper bounds for all values. This completes the proof. □

7 Third Bieberbach Theorem

The third Bieberbach Theorem states that isomorphic crystallographic groups are conjugate. Note that conjugate groups are always isomorphic, the converse thus holds for crystallographic groups. A very brief version of this proof can be found in [Szc12], but we have extended it in order to be more comprehensible.

Theorem 7.1 (**third Bieberbach Theorem**). *Two crystallographic groups of dimension n are isomorphic if and only if they are conjugate in $A(n)$.*

Proof. Suppose Γ_1 and Γ_2 are isomorphic and let $h : \Gamma_1 \to \Gamma_2$ be an isomorphism. Let g be the restriction of h on $\Gamma_1 \cap T(n)$. We prove that g is a linear map. Indeed, let $\{e_i\}$ be the n linearly independent vectors of $\Gamma_1 \cap T(n)$. For an arbitrary $v = \lambda_1 e_1 + ... + \lambda_n e_n \in \Gamma_1 \cap T(n)$ ($\lambda_i \in \mathbb{Z}$), we find

$$g(v) = g(\lambda_1 e_1 + ... + \lambda_n e_n) = \lambda_1 g(e_1) + ... + \lambda_n g(e_n)$$

because $\lambda_i e_i + \lambda_{i+1} e_{i+1}$ is a composition of two translations and g is an homomorphism. Thus we can write $g(v) = Av$ for a matrix $A \in \mathrm{GL}(n, \mathbb{R})$. Let $\Gamma_2' = A^{-1}\Gamma_2 A$. Define the function $f : \Gamma_1 \to \Gamma_2'$ as

$$f(B, b) = (A^{-1}, 0) \circ h(B, b) \circ (A, 0)$$

Now note:

$$\begin{aligned} f(I_n, e_i) &= (A^{-1}, 0) \circ h(I_n, e_i) \circ (A, 0) \\ &= (A^{-1}, 0) \circ (I_n, Ae_i) \circ (A, 0) \\ &= (I_n, e_i) \end{aligned}$$

If Γ_1 is conjugate to Γ_2', then it must also be conjugate to Γ_2 because Γ_2 and Γ_2' are conjugate. It thus suffices to show that Γ_1 and Γ_2' are conjugate.

Choose an arbitrary $(A_1, b_1) \in \Gamma_1$ and let $f(A_1, b_1) = (A_2, b_2) \in \Gamma_2'$. We know that

$$f((A_1, b_1) \circ (I, e_i) \circ (A_1, b_1)^{-1}) = f(A_1, b_1) \circ f(I, e_i) \circ f(A_1, b_1)^{-1}$$

By calculating both sides of this equation, we find that $A_2 e_i = A_1 e_i$. Because this is true for every basis vector e_i, we find $A_2 = A_1$. Therefore $f(A_1, b_1) = (A_1, b_2)$. Let $p_2 : E(n) \to \mathbb{R}^n : (B, b) \mapsto b$ be the projection of $E(n)$ on $\mathbb{R}^n$. Define the function $f' : \Gamma_1 \to A(n)$ as

$$f'(B, b) = (B, b - p_2(f(B, b))$$

We show that f' is a homomorphism. Let $(B, b), (C, c) \in \Gamma_1$. We find:

$$\begin{aligned} f'((B, b) \circ (C, c)) &= \Big(BC, Bc + b - p_2\big(f(BC, Bc + b)\big)\Big) \\ f'(B, b) \circ f'(C, c) &= \Big(BC, B\big(c - p_2(f(C, c))\big) + b - p_2\big(f(B, b)\big)\Big) \end{aligned}$$

It is therefore sufficient to show that

$$p_2\big(f(B, b)\big) + Bp_2\big(f(C, c)\big) = p_2\big(f(BC, Bc + b)\big)$$

But this immediately follows from the fact that f is a homomorphism and

$$p_2(f(B, b)) + Bp_2(f(C, c)) = p_2(f(B, b) \circ f(C, c))$$

We prove that the kernel of f' is $\Gamma_1 \cap T(n)$. Indeed, suppose (B, b) is in the kernel of f'. Then $f'(B, b) = (I_n, 0)$ and thus $B = I_n$. Therefore $(B, b) \in \Gamma_1 \cap T(n)$. Now suppose $(I_n, b) \in \Gamma_1 \cap T(n)$. Because $f(I_n, b) = (I_n, b)$, we find that $b = p_2(f(I_n, b))$ for every b and thus we find that $f'(B, b) = (I_n, 0)$ and therefore (I_n, b) is in the kernel.

Now we prove that $f'(\Gamma_1)$ has a fixed point (this part of the proof is based on a similar argument given in [Mil72]). Because $\Gamma_1/(\Gamma_1 \cap T(n))$ is finite, we know that the orbit for $f'(\Gamma_1)$ of an arbitrary point $x \in \mathbb{R}^n$

is finite (note that it is important here that the kernel of f' is $\Gamma_1 \cap T(n)$). Let $f'(\Gamma_1)(x) = \{x_1, ..., x_n\}$ and define $y = \frac{1}{n}(x_1 + ... + x_n)$. We prove that y is a fixed point. Indeed, choose an arbitrary $(B, b) \in \Gamma_1$. Then:

$$f'(B,b)(y) = \frac{1}{n}\sum_{i=1}^{n} f'(B,b)(x_i)$$

because $f'(B, b)$ is a linear transformation. We know $f'(B, b)(x_i) \in f'(\Gamma_1)(x)$ because Γ_1 is a group. Note that

$$f'(B,b)(x_i) \neq f'(B,b)(x_j)$$

if $i \neq j$. From this follows that the elements $f'(B, b)(x_i)$ permute $f'(\Gamma_1)(x)$ and therefore the average of those elements must once again equal y. Thus y is a fixed point. We find

$$f'(B,b)(y) = (B, b - p_2(f(B,b)))(y) = By + b - p_2(f(B,b)) = y$$

This gives the explicit formula $p_2(f(B, b)) = By + b - y$.

We now show that $(I_n, y)\Gamma_2'(I_n, -y) = \Gamma_1$. Suppose $(B, b) \in (I_n, y)\Gamma_2'(I_n, -y)$. Then there is an element $(C, c) \in \Gamma_2'$ such that

$$(B,b) = (I_n, y) \circ (C, c) \circ (I_n, -y) = (C, -Cy + c + y) = f^{-1}(C, c)$$

The last equality holds since:

$$f(C, -Cy + c + y) = (C, Cy + (-Cy + c + y) - y) = (C, c)$$

Therefore $(B, b) \in f^{-1}(\Gamma_2')$ and thus $(B, b) \in \Gamma_1$.

Now suppose $(B, b) \in \Gamma_1$. Then

$$f(B,b) = (B, By + b - y) = (I_n, -y) \circ (B, b) \circ (I_n, y)$$

Because $f(B, b) \in \Gamma_2'$, we thus find that $(B, b) \in (I_n, y)\Gamma_2'(I_n, -y)$.

We found that Γ_1 and Γ_2' are conjugate. □

8 Integer matrices and crystallographic groups

The three Bieberbach Theorems show there is a lot of structure in crystallographic groups. In the remaining sections of the paper we prove something else about crystallographic groups: we will give a very specific condition that tells us what the possible orders of elements in the crystallographic groups are. We will find that the number of possible orders of a symmetry in a given dimensions is rather small which is a quite surprising results. We can use this fact in very concrete situations. For example, one might think there exists a crystal in 2 dimensions which is invariant under a rotation over 30 degrees. However, this is impossible because this rotation has order 12 and 12 is not a possible order for a 2-dimensional crystal.

One might wonder what this has to do with integer matrices. Well, we will show that crystallographic groups and finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ are intertwined and that the possible orders of elements in finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ are the same as the ones in crystallographic groups of dimension n. Using this fact, we will focus on finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ and prove our theorem for those groups. In this section we will prove the connection between finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ and crystallographic groups. The proofs given in this section are based on what we discussed with our supervisor [Vil21b].

Theorem 8.1. *There exists a crystallographic group of dimension n with an element of order $m < \infty$ if and only if there exists a finite subgroup of $GL(n, \mathbb{Z})$ with an element of order m.*

Before proving the theorem, we will first prove the following lemmas:

Lemma 8.2. *Let Γ be a crystallographic group of dimension n. Then there exists an isomorphic crystallographic group Γ' of dimension n of which the rotational parts are integer valued matrices.*

Proof. Let $\Lambda = \Gamma \cap T(n)$. Note that $(I_n, 0) \in \Lambda$. The first Bieberbach Theorem gives us n linearly independent elements $\{v_1, ..., v_n\}$ of Λ such that every element of Λ can be written as an integer linear combination of these elements. Let A be the matrix with as columns the elements $\{v_1, ..., v_n\}$. Because $Ae_i = v_i$ with e_i the i-th element of the standard orthonormal basis of $\mathbb{R}^n$, we find: $A\mathbb{Z}^n = \Lambda$. Because of Lemma 6.6 we know that for any element $(B, b) \in \Gamma$, that $B\Lambda = \Lambda$ (note that B must be invertible and $(B^{-1}, -B^{-1}b) \in \Gamma$ thus equality holds). Therefore $BA\mathbb{Z}^n = A\mathbb{Z}^n$ or $A^{-1}BA(\mathbb{Z}^n) = \mathbb{Z}^n$. Thus we have that $A^{-1}BA$ is a matrix with integer entries. Let $\Gamma' = A^{-1}\Gamma A$. Then Γ' satisfies the conditions of the lemma. □

Lemma 8.3. *If $(B, b) \in E(n)$ has order m, then B has order m.*

Proof. Because $(B, b)^m = (B^m, c)$ with c some element of $\mathbb{R}^n$, we find that $B^m = I_n$ and thus that the order of B is a divisor of m. Suppose that $k < m$ is the order of B. We show that $(B, b)^k = (I_n, 0)$ which is impossible because m is the order of (B, b). In order to show that $(B, b)^k = (I_n, 0)$, we first rewrite $(B, b)^m$:

$$\begin{aligned}(B,b)^m &= \left(B^m, \sum_{i=0}^{m-1} B^i b\right) \\ &= \left(I_n, \sum_{j=0}^{\frac{m}{k}-1} \sum_{i=0}^{k-1} B^{jk+i} b\right) \\ &= \left(I_n, \sum_{j=0}^{\frac{m}{k}-1} \sum_{i=0}^{k-1} B^{i} b\right) \\ &= \left(I_n, \frac{m}{k} \sum_{i=0}^{k-1} B^{i} b\right)\end{aligned}$$

Now because $(B, b)^m = (I_n, 0)$, we find that $\sum_{i=0}^{k-1} B^i b = 0$, but this in turn implies that:

$$(B,b)^k = \left(B^k, \sum_{i=0}^{k-1} B^i b\right) = (I_n, 0)$$

which is a contradiction. □

We now prove Theorem 8.1.

Proof. Suppose there is a crystallographic group Γ of dimension n with an element of order m. By Lemma 8.2 we can assume that all matrices in Γ have integer entries. We now prove that $G = \Gamma/\Lambda$ is isomorphic to a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$. Define the function $f : G \to \mathrm{GL}(n, \mathbb{Z}) : [(A, a)] \mapsto A$. Note that f is well defined because any other representative of $[(A, a)]$ has the same rotational part. We prove that f is a homomorphism. If this is the case, then f is an isomorphism between G and a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$ and therefore there exists a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$ with an element of order m. We have:

$$f\Big([(A, a)] \circ [(B, b)]\Big)(x) = f([(AB, Ab + a)])(x) = ABx$$

and:

$$\Big(f\big([(A, a)]\big) \circ f\big([(B, b)]\big)\Big)(x) = f([(A, a)])(Bx) = ABx$$

This implies that f is an homomorphism.

Now suppose there is a finite subgroup G of $\mathrm{GL}(n, \mathbb{Z})$ with an element of order m. We first define an inner product for each $B \in G$. Let

$$\langle ., . \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} : v \times w \mapsto \langle v, w \rangle = v_1 w_1 + ... + v_n w_n$$

be the standard dot product in $\mathbb{R}^n$. The inner product associated with B is defined as:

$$\langle ., . \rangle_B : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} : v \times w \mapsto \langle v, w \rangle_B = \langle Bv, Bw \rangle$$

$\langle .,. \rangle_B$ is indeed a dot product because the three requirements for a dot product (linearity, symmetry and positive-definiteness) are true. Based on these dot products, we will define one more dot product:

$$\langle .,. \rangle_{\text{avg}} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} : v \times w \mapsto \langle v, w \rangle_{\text{avg}} = \frac{1}{|G|} \sum_{B \in G} \langle v, w \rangle_B$$

Once again it is easy to check the three requirements for a dot product. Let $B \in G$ be arbitrary. Note that $GB = G$ because B is invertible. Thus we find:

$$\begin{aligned} \langle Bv, Bw \rangle_{\text{avg}} &= \frac{1}{|G|} \sum_{C \in G} \langle Bv, Bw \rangle_C \\ &= \frac{1}{|G|} \sum_{C \in G} \langle v, w \rangle_{CB} \\ &= \frac{1}{|G|} \sum_{C \in G} \langle v, w \rangle_C = \langle v, w \rangle_{\text{avg}} \end{aligned}$$

Now let $\{e_i\}$ be an orthonormal basis with respect to $\langle .,. \rangle_{\text{avg}}$. Let A be the matrix with these elements as columns. We will prove that AGA^{-1} is a subset of $O(n)$. It is sufficient to prove that every element in AGA^{-1} is a distance preserving transformation (with respect to the standard dot product). Let $\{u_i\}$ be the standard orthonormal basis. Thus $Au_i = e_i$. We therefore know:

$$\delta_{ij} = \langle e_i, e_j \rangle_{\text{avg}} = \langle Au_i, Au_j \rangle_{\text{avg}}$$

and thus

$$\delta_{ij} = \langle u_i, u_j \rangle = \langle Au_i, Au_j \rangle_{\text{avg}}$$

Because a dot product is linear, this implies that for two arbitrary vectors $v, w \in \mathbb{R}^n$:

$$\begin{aligned} \langle v, w \rangle &= \langle Av, Aw \rangle_{\text{avg}} \\ \langle A^{-1}v, A^{-1}w \rangle &= \langle v, w \rangle_{\text{avg}} \end{aligned}$$

Using these relations we find for an arbitrary $B \in G$:

$$\begin{aligned} \langle (A^{-1}BA)v, (A^{-1}BA)w \rangle &= \langle A^{-1}(BAv), A^{-1}(BAw) \rangle \\ &= \langle BAv, BAw \rangle_{\text{avg}} \\ &= \langle Av, Aw \rangle_{\text{avg}} \\ &= \langle v, w \rangle \end{aligned}$$

Thus AGA^{-1} is distance preserving. We can now construct a very simple crystallographic group

$$AGA^{-1} \times A(\mathbb{Z}^n) = \{(B, c) | B \in AGA^{-1}, c \in A(\mathbb{Z}^n)\}$$

This group is indeed crystallographic because it is both discrete and cocompact (these facts can easily be checked). Moreover, this crystallographic group has an element of order m and thus we have proven the theorem. □

9 Orders of elements of integer matrices

As previously shown in Theorem 8.1, the possible orders of elements in crystallographic groups of dimension n are the same as the ones in finite subgroups of $\text{GL}(n, \mathbb{Z})$. It is thus of great interest to us to determine the possible orders of elements of finite subgroups of $\text{GL}(n, \mathbb{Z})$. In order to determine the possible orders for finite subgroups of $\text{GL}(n, \mathbb{Z})$, we determine the possible orders for finite subgroups of $\text{GL}(n, \mathbb{Q})$. The following theorem states that this is sufficient as it implies that the possible orders for finite subgroups of $\text{GL}(n, \mathbb{Q})$ and finite subgroups of $\text{GL}(n, \mathbb{Z})$ are the same. In this entire section we will loosely follow the arguments and theorems given in [KP02].

Theorem 9.1. *Any finite subgroup of $GL(n,\mathbb{Q})$ is conjugate to a finite subgroup of $GL(n,\mathbb{Z})$.*

Before proving this, we first prove a lemma that we are going to need.

Lemma 9.2. *Let $A \in \mathbb{Q}^{n\times n}$. Then $A \in \mathbb{Z}^{n\times n}$ if and only if $Ab \in \mathbb{Z}^n$ for all $b \in \mathbb{Z}^n$.*

Proof. If $A \in \mathbb{Z}^{n\times n}$, then it is clear that $Ab \in \mathbb{Z}^n$ for all $b \in \mathbb{Z}^n$. If $Ab \in \mathbb{Z}^n$ for all $b \in \mathbb{Z}^n$, then we can apply this statement for the standard basis in $\mathbb{R}^n$ and this obviously implies that $A \in \mathbb{Z}^{n\times n}$. □

Now we can prove the theorem. The proof is based on [KP02]. However, several aspects of the proof were rewritten in order to make it easier to understand.

Proof. Let G be an arbitrary finite subgroup of $\mathrm{GL}(n,\mathbb{Q})$, suppose $G = \{A_1, ..., A_N\}$. Note that $\mathrm{GL}(n,\mathbb{Q})$ is the subset of all invertible matrices in $\mathbb{Q}^{n\times n}$. Let

$$F = \left\{ \sum_{i=1}^{N} A_i(v_i) | v_i \in \mathbb{Z}^n \right\}$$

Note that F is a group if we supply it with addition as operation. We will show that it is isomorphic to $(\mathbb{Z}^n, +)$. Now let $\{e_1, ..e_n\}$ be the standard orthonormal basis of $\mathbb{R}^n$. We note that the set

$$B = \{Ae_i | i \in \{1, ..., n\}, A \in G\}$$

is a finite set and $B \subset F$. Moreover, every element in F can be written as a linear combination of the elements in B and therefore we find that F is finitely generated by B. Because B is finite and a subset of $\mathbb{Q}^n$, we can find an integer d such that dB only contains elements of $\mathbb{Z}^n$. Because F is finitely generated by B, we must have that dF is finitely generated by dB and therefore we find that $dF \subset \mathbb{Z}^n$. dF and F are trivially isomorphic.

Because F has n linearly independent elements ($e_i \in F$ because $I_n \in G$), dF must also have n linearly independent elements $\{v_1, ..., v_n\}$. Now note that $dF \subset \mathbb{Z}^n$ is discrete and therefore we know that the parallelepiped $P = \{\alpha_1 v_1 + ...\alpha_n v_n | \alpha_i \in [0, 1]\}$ can only contain finitely many elements of dF. We can replace v_i by one of the elements inside P (maybe on its edge) while making sure that $\{v_1, ..., v_n\}$ are linearly independent. By repeating this process only a finite amount of times, we can ensure that $P \cap dF = \{0, v_1, ..., v_n\}$. Now suppose there is an element $x \in dF$ that can not be written as a linear integer combination of $\{v_1, ..., v_n\}$, then by subtracting or adding v_i of x several times, we can assume that $x \in P$ and $x \notin \{0, v_1, ..., v_n\}$, but this is impossible. Therefore every element in dF can be written as a linear integer combination of $\{v_1, ..., v_n\}$ and because dF is a group, every linear integer combination of $\{v_1, ..., v_n\}$ is also an element of dF. By now applying the transformation that maps $\{v_1, ..., v_n\}$ to $\{e_1, ..., e_n\}$ we find that this is an isomorphism between dF and $\mathbb{Z}^n$.

Therefore $\mathbb{Z}^n$ and F are isomorphic and an isomorphism is given by the transformation matrix C that transforms $\{e_1, ..., e_n\}$ into $\{\frac{v_1}{d}, ..., \frac{v_n}{d}\}$. Because $A_i(F) \subset F$ and $C\mathbb{Z}^n = F$, we find that $C^{-1}A_iC(\mathbb{Z}_n) \subset \mathbb{Z}^n$. Because of this and Lemma 9.2 we thus find that $C^{-1}GC \in \mathrm{GL}(n,\mathbb{Z})$ and we have proven the theorem. □

To determine the orders of the elements of $\mathrm{GL}(n,\mathbb{Q})$ we need to introduce roots of unity, cyclotomic polynomials and the companion matrix of a polynomial. A brief overview of the upcoming section provides some early motivation for the importance and the use of these concepts. For this motivation it is sufficient to know that cyclotomic polynomials are polynomials with some nice properties and that the companion matrix of a polynomial is a matrix that is characterised by the polynomial. We want to find the possible orders of the elements in $\mathrm{GL}(n,\mathbb{Q})$. A good start would be to ask the opposite question: given an order m, is it possible to find an $n \in \mathbb{N}$ such that there exists an $A \in \mathrm{GL}(n,\mathbb{Z})$ of order m? The matrix A must suffice the equation $A^m - 1 = 0$ or equivalently it must be a root of the polynomial $x^m - 1$. We will prove that the factorisation of the polynomial $x^m - 1$ is a product of cyclotomic polynomials. If we find a matrix A that is a root of one of these cyclotomic polynomials, it will also be a root of $x^m - 1$. Now it turns out that the companion matrix C of the m^{th} cyclotomic polynomial is a root of that cyclotomic polynomial and furthermore this companion matrix has integer entries. We will use this fact to construct a matrix A as some kind of combination of the cyclotomic polynomials.

9.1 Cyclotomic polynomials

This section contains basic facts and theorems about the cyclotomic polynomials. We based ourselves on [Vey21] to write this section.

Definition 9.3. *An m^{th} root of unity, where m is a positive integer, is an element $x \in \mathbb{C}$ satisfying the equation*

$$x^m - 1 = 0$$

Let $\omega_m = e^{\frac{2\pi i}{m}}$. The m^{th} roots of unity in the complex plane are given by $\{\omega_m, \omega_m^2, ..., \omega_m^m\}$. A number ω_m^k is a primitive k^{th} root of unity if $\gcd(k, m) = 1$.

The set of roots $\{\omega_m, \omega_m^2, ..., \omega_m^m\}$ form a cyclic group under multiplication of complex numbers. They are used to define the cyclotomic polynomials.

Definition 9.4. *The m^{th} cyclotomic polynomial is given by*

$$\Phi_m(x) = \prod_{\substack{1 \leqslant k \leqslant m \\ \gcd(k,m)=1}} (x - \omega_m^k)$$

We will now prove that the polynomial $x^m - 1$ factorises into a product of cyclotomic polynomials. This is stated in the following theorem:

Theorem 9.5. *For $m \in \mathbb{Z}_{>0}$ we have*

$$x^m - 1 = \prod_{\substack{1 \leqslant d \leqslant m \\ d|m}} \Phi_d(x)$$

Proof. Because the roots of unity are given by $\{\omega_m, \omega_m^2, ..., \omega_m^m\}$ we can factor $x^m - 1$ giving the equality:

$$x^m - 1 = \prod_{k=1}^{m} \left(x - \omega_m^k\right)$$

Now if we take a fixed integer $1 \leqslant k \leqslant m$ we have a unique $1 \leqslant d \leqslant m$ such that $\gcd(k, m) = d$. Therefore we can write the right hand side of the previous equation a bit differently by rearranging the factors:

$$\prod_{k=1}^{m} \left(x - \omega_m^k\right) = \prod_{\substack{1 \leqslant d \leqslant m \\ d|m}} \left(\prod_{\substack{1 \leqslant k \leqslant m \\ \gcd(k,m)=d}} \left(x - \omega_m^k\right) \right)$$

We now substitute $k = ld$. This gives:

$$x^m - 1 = \prod_{\substack{1 \leqslant d \leqslant m \\ d|m}} \left(\prod_{\substack{1 \leqslant l \leqslant \frac{m}{d} \\ \gcd(l, \frac{m}{d})=1}} \left(x - \omega_m^{ld}\right) \right)$$

If d is a divisor of m we have

$$\omega_m^d = (e^{\frac{2\pi i}{m}})^d = e^{\frac{2\pi i}{m/d}} = \omega_{m/d}$$

Substituting this and using definition 9.4 gives:

$$\begin{aligned} x^m - 1 &= \prod_{\substack{1 \leqslant d \leqslant m \\ d \mid m}} \left(\prod_{\substack{1 \leqslant l \leqslant \frac{m}{d} \\ \gcd(l, \frac{m}{d}) = 1}} \left(x - \omega_{m/d}^l \right) \right) \\ &= \prod_{\substack{1 \leqslant d \leqslant m \\ d \mid m}} \Phi_{m/d}(x) \\ &= \prod_{\substack{1 \leqslant r \leqslant m \\ r \mid m}} \Phi_r(x) \end{aligned}$$

□

We use this result to prove that a cyclotomic polynomial has integer coefficients. This result is needed to make sure that the companion matrix will have integer entries.

Theorem 9.6. *The cyclotomic polynomial $\Phi_m(x)$ is a monic polynomial with integer coefficients.*

Proof. We use induction on m. The case $m = 1$ is trivial. Suppose that the coefficients of Φ_d with $d < m$ are all integers. By Theorem 9.5 we have $x^m - 1 = \Phi_m(x)g(x)$ where g is defined to be the following function:

$$g := \prod_{\substack{1 \leqslant d < m \\ d \mid m}} \Phi_d \quad \in \mathbb{Z}[x]$$

Using the induction hypothesis we know that g has integer coefficients. By the division algorithm in $\mathbb{C}[x]$ we can find unique $q, r \in \mathbb{C}[x]$ so that $x^m - 1 = q(x)g(x) + r(x)$ with $\deg(r) < \deg(g)$. But we already have $x^m - 1 = \Phi_m(x)g(x)$ so that $q(x) = \Phi_m(x)$ is the unique quotient with remainder $r(x) = 0$. Now the division algorithm in $\mathbb{Z}[x]$ also yields unique $q', r' \in \mathbb{Z}[x]$ so that $x^m - 1 = q'(x)g(x) + r'(x)$ with $\deg(r') < \deg(g)$. But because $q', r' \in \mathbb{Z}[x]$ we also have $q', r' \in \mathbb{C}[x]$ so that $q = q', r = r'$ by the uniqueness of our solution in $\mathbb{C}[x]$. This means that $q = \Phi_m = q' \in \mathbb{Z}[x]$. □

The degree of the m^{th} cyclotomic polynomial is given by Euler's totient function

$$\phi(m) = \#\{k \in \{1, 2, ..., m\} |\ \gcd(k, m) = 1\}$$

If we write $m = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$ where $p_1, ..., p_k$ are all distinct prime numbers, we get the following formula for $\phi(m)$

$$\phi(m) = (p_1 - 1)p_1^{e_1 - 1} \cdot ... \cdot (p_k - 1)p_k^{e_k - 1}$$

We state one last theorem about cyclotomic polynomials. The need for this theorem will become clear in the proof of Theorem 9.10.

Theorem 9.7. *Each $\Phi_m(x)$ is irreducible over $\mathbb{Q}$.*

Unfortunately the proof of this theorem is quite long and diverges a bit from the main point of this paper. Therefore we won't prove it here, but we refer the reader to the following paper [H.W13].

9.2 Companion matrix

In the following section we prove that for a fixed integer m it is possible to construct a matrix of order m with dimension $\phi(m)$. First we define the companion matrix. The arguments in this section are based on the following source [KP02].

Definition 9.8. *Given a monic polynomial $p(x) = x^k + a_{k-1}x^{k-1} + ... + a_1x + a_0$, the companion matrix C of $p(x)$ is defined as:*

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{k-1} \end{pmatrix}$$

Note that the degree of our polynomial is equal to the dimension of the companion matrix. The following theorem will prove to be useful. The statement is also mentioned in [KP02] without a proof.

Theorem 9.9. *If C is the companion matrix of a polynomial $p(x)$ then $p(C) = 0$.*

Proof. By the Cayley-Hamilton Theorem [Vey21], which states that a matrix is a root of its own characteristic polynomial, it is enough to prove that $p(x)$ is the characteristic polynomial of C. We use induction on $k = \deg(p)$. For $k = 1$, we substitute $C = -a_0$ into $x + a_0$ which yields 0 as needed. The induction hypothesis now states that for any polynomial q with $\deg(q) < k$, $p(x)$ is the characteristic polynomial of its companion matrix. Now

$$\det(xI_m - C) = \det \begin{pmatrix} x & 0 & \dots & 0 & a_0 \\ -1 & x & \dots & 0 & a_1 \\ 0 & -1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & x + a_{k-1} \end{pmatrix}$$

Expanding along the first row yields:

$$\det(xI_m - C) = x \det \begin{pmatrix} x & 0 & \dots & 0 & a_1 \\ -1 & x & \dots & 0 & a_2 \\ 0 & -1 & \dots & 0 & a_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & x + a_{k-1} \end{pmatrix} + (-1)^{k+1} a_0 \det \begin{pmatrix} -1 & x & \dots & 0 & 0 \\ 0 & -1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}$$

$$= x \det(xI_m - C_2) + (-1)^{k+1} a_0 \det \begin{pmatrix} -1 & x & \dots & 0 & 0 \\ 0 & -1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}$$

where C_2 is the companion matrix of the polynomial $x^{k-1} + a_{k-2}x^{k-2} + ... + a_2x + a_1$. Using the induction hypothesis on this companion matrix gives:

$$\begin{aligned} \det(xI_m - C) &= x\left(x^{k-1} + a_{k-1}x^{k-2} + ... + a_2x + a_1\right) + (-1)^{k+1} a_0 (-1)^{k-1} \\ &= x^k + a_{k-1}x^{k-1} + ... + a_1x + a_0 \end{aligned}$$

This proves our theorem by induction. □

We are now ready to prove the following important result, which combines all previous results of the subsections on the companion matrices and the cyclotomic polynomials. The proof is based on [KP02].

Theorem 9.10. *The companion matrix of the m^{th} cyclotomic polynomial is a matrix of order m and dimension $\phi(m)$.*

Proof. Consider the m^{th} cyclotomic polynomial $\Phi_m(x)$. The companion matrix A of this polynomial is a matrix whose entries are integers since by Theorem 9.6 the polynomial is a monic polynomial with integer coefficients. Note that the dimension of this matrix is equal to $\phi(m)$ since $\Phi_m(x)$ has degree $\phi(m)$. Using

Theorem 9.9 we find that $\Phi_m(A) = 0$. Because of Theorem 9.5 we know that $\Phi_m(x)$ is a factor of the polynomial $x^m - 1$ and thus $A^m = 1$. In order to prove that the order of A is equal to m we need to prove that there is no $s < m$ so that $A^s = 1$. Theorem 9.7 tells us that the factor $\Phi_m(x)$ is irreducible. Because the minimal polynomial of A divides any polynomial for which A is a root (see for example [Vey21]), $\Phi_m(x)$ must be the minimal polynomial of A for otherwise it would be reducible. Suppose there is a smaller integer $s < m$ such that $A^s = 1$. By Theorem 9.5 we can write

$$x^s - 1 = \prod_{\substack{1 \leqslant d \leqslant s \\ d|s}} \Phi_d(x)$$

Because $\Phi_m(x)$ is the minimal polynomial, it must be a divisor of $x^s - 1$ and thus $m|s$ which contradicts $s < m$. This proves A has order m. □

Corollary 9.11. *There exists a matrix A of order p^k and dimension $(p-1)\,p^{k-1}$ for every integer k and prime p.*

Proof. This is a direct result of the previous theorem with $m = p^k$. □

Example 9.12. The proof of the previous theorem is a constructive one. Thus we can given an example following the construction given there. Take $m = 6$. The 6^{th} cyclotomic polynomial is found using definition 9.4:

$$\begin{aligned}
\Phi_6(x) &= \prod_{\substack{1 \leqslant k \leqslant 6 \\ \gcd(k,6)=1}} (x - \omega_6^k) \\
&= \left(x - e^{\frac{2\pi i}{m}}\right)\left(x - \left(e^{\frac{2\pi i}{m}}\right)^5\right) \\
&= x^2 - x + 1
\end{aligned}$$

Using definition 9.2 we find the following companion matrix of $x^2 - x + 1$:

$$C = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

It is easy to check that C is a matrix of order 6. Also note that the dimension of C is equal to 2 which is equal to $\phi(6)$.

9.3 Order of elements

For every $m \in \mathbb{N}$, we have proven the existence of a matrix A of order m and dimension $\phi(m)$. A natural question to ask ourselves is whether there exists a lower dimensional matrix or order m. We also haven't answered the main question we were looking for: given a certain n, what are all the possible orders of the matrices in $\mathrm{GL}(n, \mathbb{Z})$? The following theorem answers both of these questions.

In order to simplify notation throughout the theorem, we define:

$$W : \mathbb{Z} \mapsto \mathbb{Z} : m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \mapsto \begin{cases} \sum_{i=2}^{k} (p_i - 1)\, p_i^{e_i - 1} & \text{for } p_1^{e_1} = 2 \\ \sum_{i=1}^{k} (p_i - 1)\, p_i^{e_i - 1} & \text{for } p_1^{e_1} \neq 2 \end{cases}$$

with $p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ the prime decomposition of m. The proof given here is based on [KP02].

Theorem 9.13. *For every positive integer m with prime decomposition $p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$, $GL(n, \mathbb{Q})$ has an element of order m if and only if $W(m) \leqslant n$.*

Proof. Suppose that we have an integer $m = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ with $W(m) \leqslant n$ then we construct a matrix A in $\mathrm{GL}(n, \mathbb{Q})$ of order m. First let us prove that if $\sum_{i=1}^{k} (p_i - 1)\, p_i^{e_i - 1} \leqslant n$, we can find a matrix B of order m

and dimension $\sum_{i=1}^{k}(p_i-1)\,p_i^{e_i-1}$. Consider the matrix

$$B = A_1 \oplus A_2 \oplus ... \oplus A_k \oplus I_s := \begin{pmatrix} A_1 & 0 & 0 & ... & 0 \\ 0 & A_2 & 0 & ... & 0 \\ 0 & 0 & A_3 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & ... & I_s \end{pmatrix}$$

Here A_i is the matrix constructed in the final part of section 9.2 of order $p_i^{e_i}$ with dimension $(p_i-1)\,p_i^{e_i-1}$ and I_s is the identity matrix of dimension $s = n - \sum_{i=1}^{k}(p_i-1)\,p_i^{e_i-1}$. Obviously the dimension of B is n. Now the order of B is the least common multiple of the orders of $A_1, ..., A_k, I_s$, which is exactly m, thus we have found a matrix B of order m and dimension n. Now consider the special case where $p_1^{e_1} = 2$. As before, we can find a matrix B with order $\frac{m}{2} = p_2^{e_2} \cdot ... \cdot p_k^{e_k}$ and dimension n. We consider the matrix $-B$, because $\frac{m}{2}$ is odd we have

$$(-B)^{\frac{m}{2}} = (-1)^{\frac{m}{2}} B^{\frac{m}{2}} = -I_n$$

and since $(-B)^m = I_n$ the order of $-B$ is equal to m. We have found a matrix of order m with dimension n. This proves the first implication.

Suppose we have a matrix $A \in \mathrm{GL}(n, \mathbb{Q})$ with order $m = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$. This means that $A^m = 1$ or equivalently that the polynomial $x^m - 1$ has A as a root. Consider the minimal polynomial $m_A(x)$ of A. Because $A^m - 1 = 0$, we know that $m_A(x)$ is a divisor of $x^m - 1$. From Theorem 9.5 we know that

$$x^m - 1 = \prod_{\substack{1 \leqslant d \leqslant m \\ d \mid m}} \Phi_d(x)$$

Therefore $m_A(x)$ is of the form $\Phi_{d_1}(x) \cdot ... \cdot \Phi_{d_s}(x)$, where for each $1 \leqslant i \leqslant s$ we have $d_i | m$. Because $d_i | m$, we find that $\mathrm{lcm}(d_1, ..., d_s) | m$. If $k = \mathrm{lcm}(d_1, ..., d_s) < m$, we have

$$x^k - 1 = \prod_{\substack{1 \leqslant d \leqslant k \\ d \mid k}} \Phi_d(x) = m_A(x) P(x)$$

where $P(x)$ is some polynomial. Now $m_A(A) = 0$ so that $A^k - 1 = 0$ which contradicts the fact that A has order m. Thus $\mathrm{lcm}(d_1, ..., d_s) = m$. Because the minimal polynomial of A is $m_A(x) = \Phi_{d_1}(x) \cdot ... \cdot \Phi_{d_s}(x)$ we can make a decomposition of A in matrices A_i such that the minimal polynomial of A_i is $\Phi_{d_i}(x)$. More specifically we find up to a conjugation of A that:

$$A = A_1 \oplus A_2 \oplus ... \oplus A_s$$

Let l_i be the dimension of the matrix A_i. Since the minimal polynomial $\Phi_{d_i}(x)$ divides the characteristic polynomial and since the characteristic polynomial has degree l_i, we have $\deg(\Phi_{d_i}(x)) = \phi(d_i) \leqslant l_i$. From this it follows that $\sum_{i=1}^{s} \phi(d_i) \leqslant \sum_{i=1}^{s} l_i = n$.

It now suffices to prove that $W(m) \leqslant \sum_{i=1}^{s} \phi(d_i)$. We will make use of the fact that $\{d_1, ..., d_s\}$ is a set of distinct divisors of m such that $\mathrm{lcm}(d_1, ..., d_s) = m$. First we construct a set of integers $\{c_1, c_2, ..., c_s\}$ such that $c_i | d_i$ for each i, $\gcd(c_i, c_j) = 1$ for $i \neq j$ and $c_1 c_2 ... c_s = m$. The easiest way to construct such a set is by using an iterative procedure. At first take all c_i to be 1. For each $j \in \{1, ..., k\}$ take a $i \in \{1, ..., s\}$ so that $p_j^{e_j} | d_i$ and multiply c_i by $p_j^{e_j}$. Note that this i exists since $\mathrm{lcm}(d_1, ..., d_s) = m$.

Because c_i divides d_i for all i, we have $\sum_{i=1}^{s} \phi(c_i) \leqslant \sum_{i=1}^{s} \phi(d_i)$. For each $i \in \{1, ..., s\}$ let

$$S_i = \left\{ j \in \{1, ..., k\} \,\middle|\, c_i \text{ is a divisor of } p_j^{e_j} \right\}$$

Notice that $\{S_1, ..., S_s\}$ partitions the set $\{p_1^{e_1}, p_2^{e_2}, ..., p_k^{e_k}\}$. We have $c_i = \prod_{j \in S_i} p_j^{e_j}$ for all $i \in \{1, ..., s\}$. Assume, renumbering if necessary, that $p_1^{e_1}$ divides c_1. We use the fact that for coprime numbers $a, b > 2$ we have $\phi(ab) \geqslant \phi(a) + \phi(b)$ to obtain for all $i > 1$:

$$\phi(c_i) \geqslant \sum_{j \in S_i} \phi(p_j^{e_j})$$

If $p_1^{e_1} \neq 2$, we have by the same reasoning:

$$\phi(c_1) \geqslant \sum_{j \in S_1} \phi(p_j^{e_j})$$

so that

$$\sum_{i=1}^{s} \phi(c_i) \geqslant \sum_{i=1}^{s} \sum_{j \in S_i} \phi(p_j^{e_j}) = \sum_{i=1}^{k} \phi(p_i^{e_i}) = W(m)$$

If $p_1^{e_1} = 2$ we have:

$$\phi(c_1) \geqslant \sum_{\substack{j \in S_1 \\ j \neq 1}} \phi(p_j^{e_j})$$

so that

$$\sum_{i=1}^{s} \phi(c_i) \geqslant \sum_{\substack{j \in S_1 \\ j \neq 1}} \phi(p_j^{e_j}) + \sum_{i=2}^{s} \sum_{j \in A_i} \phi(p_j^{e_j}) = \sum_{i=2}^{k} \phi(p_i^{e_i}) = W(m)$$

□

This is a remarkable result, for every $n \in \mathbb{N}$ we have found all possible orders of matrices in $\mathrm{GL}(n, \mathbb{Z})$. Remember that the reason we are interested in these orders is because of the connection with crystallographic groups given by Theorem 8.1. Thus we have found the possible orders of any element in any finite crystallographic group. An interesting corollary of this theorem states that no new orders are possible when we increase our dimension from an even to an odd dimension.

Corollary 9.14. *The elements in $GL(2n, \mathbb{Z})$ have the same possible orders as the elements in $GL(2n+1, \mathbb{Z})$.*

Proof. We first prove that $W(m)$ is even for any $m \in \mathbb{N}$. It is sufficient to prove that every term of $W(m)$ is even. Now any term of the sum $W(m)$ is of the form $(p_i - 1)p_i^{e_i - 1}$ where p_i is a prime and $p_i^{e_i} \neq 2$. If $p_i \neq 2$, the first factor, $p_i - 1$, is even. If $p_i = 2$, then $e_i \geqslant 2$ and thus the second factor, $p_i^{e_i - 1}$ is even. This implies that $W(m) \leqslant 2n + 1$ if and only if $W(m) \leqslant 2n$ and therefore the elements in $\mathrm{GL}(2n, \mathbb{Z})$ have the same possible orders as the elements in $\mathrm{GL}(2n + 1, \mathbb{Z})$. □

9.4 Example possible orders of elements of integer matrices

Let us consider an example to get a better idea of the previous theorem. Theorem 9.13 can be used to determine the possible orders of elements of integer matrices for any dimension n. The case $n = 2$ already yields some interesting and rather surprising results. After determining the possible orders we will give some crystallographic groups that has elements with the allowed orders.

We need to find all possible $m \in \mathbb{N}$ such that $W(m) \leqslant 2$. Using the equation for $W(m)$, we find that $W(m) \leqslant 2$ if $m \in \{1, 2, 3, 4, 6\}$. We show that these are the only options. First note that if $k|m$ then $W(m) \geqslant W(k)$. Now $W(p) > 2$ if p is a prime greater than 5. Thus every factor of the prime decomposition of m must be smaller than 5. This gives the following constraint on the possibilities for m:

$$m \in \{2^k 3^s |\ k, s \in \mathbb{N}\}$$

Now $W(2^k) \leqslant 2$ implies $k < 3$ and $W(3^s) \leqslant 2$ implies $s < 2$. Thus we have

$$m \in \{2^k 3^s |\ k \in \{0, 1, 2\} \text{ and } s \in \{0, 1\}\} = \{1, 2, 3, 4, 6, 12\}$$

Because $W(12) = 4$, we can conclude that $W(m) \leqslant 2$ if and only if $m \in \{1, 2, 3, 4, 6\}$. We have proven that every element in any subgroup of $\mathrm{GL}(2, \mathbb{Z})$ has order $1, 2, 3, 4$ or 6. Using Theorem 8.1 we conclude that all elements in any crystallographic group of dimension 2 have orders $1, 2, 3, 4$ or 6.

Let us give some examples of crystallographic groups with elements of this order.

Example 9.15. The first one is the symmetry group of the lattice with basis vectors $(0,1)$ and $(1,0)$ given in figure 2. The symmetry group of this lattice contains the identity, the rotation over 90°and 180°. Therefore this crystallographic group contains elements of order 1, 2 and 4. Note that any rotational part of a symmetry of the lattice must be a rotation over a multiple of 90°. Note that the group also contains elements of order ∞, for example the translation over $(1,0)$. This is not a contradiction with our theorems because Theorem 8.1 only talks about finite orders, not about an infinite order. We thus find that this group only contains elements of order 1, 2, 4 and ∞.

Example 9.16. Another group is the symmetry group of the lattice with basis vectors $(0,1)$ and $\left(\sin\left(\frac{\pi}{3}\right), \cos\left(\frac{\pi}{3}\right)\right)$ given in figure 3. The symmetry group of this lattice contains the identity, a rotation over 60°a rotation over 120°and a rotation over 180°. Therefore it contains elements of order 1, 2, 3 and 6. Analogously as before, we can now say that it contains only elements of order 1, 2, 3, 6 and ∞.

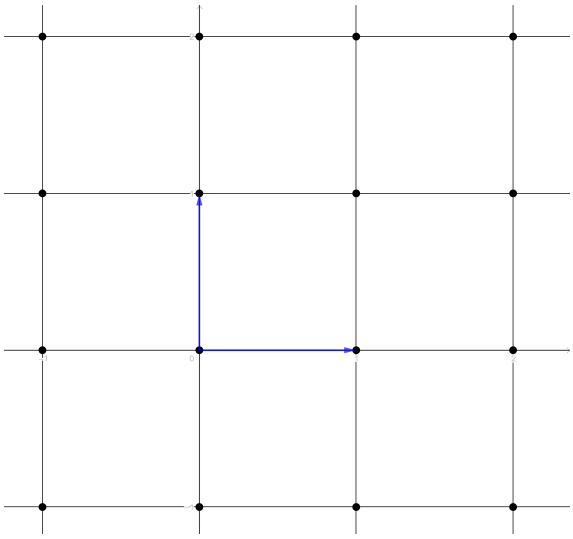

Figure 2: Lattice with basis vectors $(0,1)$ and $(1,0)$.

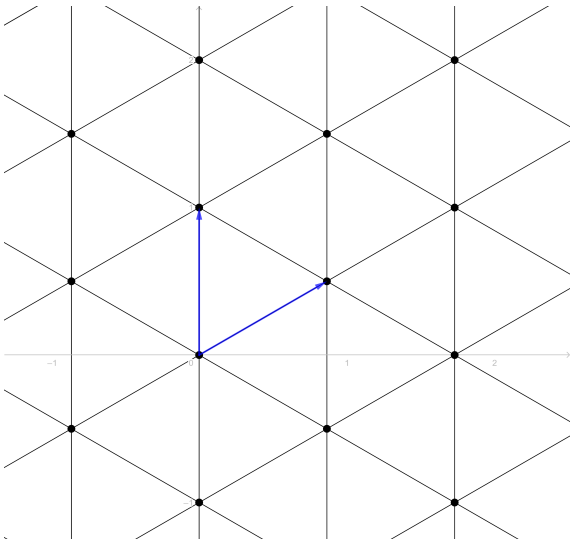

Figure 3: Lattice with basis vectors $(0,1)$ and $\left(\sin\left(\frac{\pi}{3}\right), \cos\left(\frac{\pi}{3}\right)\right)$

Now one might be surprised there doesn't exist elements of orders different from the ones previously mentioned in 2D. Surely there must exist a lattice which is invariant to a rotation over for example 45°? However, our theorems imply that no such lattice can exist. This feels very counter-intuitive and one might come up with a very simple "counter-example" namely the lattice that contains the 8 unit vectors as indicated in figure 4. However, we can show that a set that contains all these vectors cannot be a lattice. By subtracting the vector $(\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2})$ of the vector $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$, we find that the "lattice" must also contain $(\sqrt{2}, 0)$. This means that the "lattice" contains both $(1,0)$ and $(\sqrt{2},0)$, but this allows us to make linear integer combinations of these two vectors that that become arbitrarily close to $(0,0)$ which is impossible for a lattice.

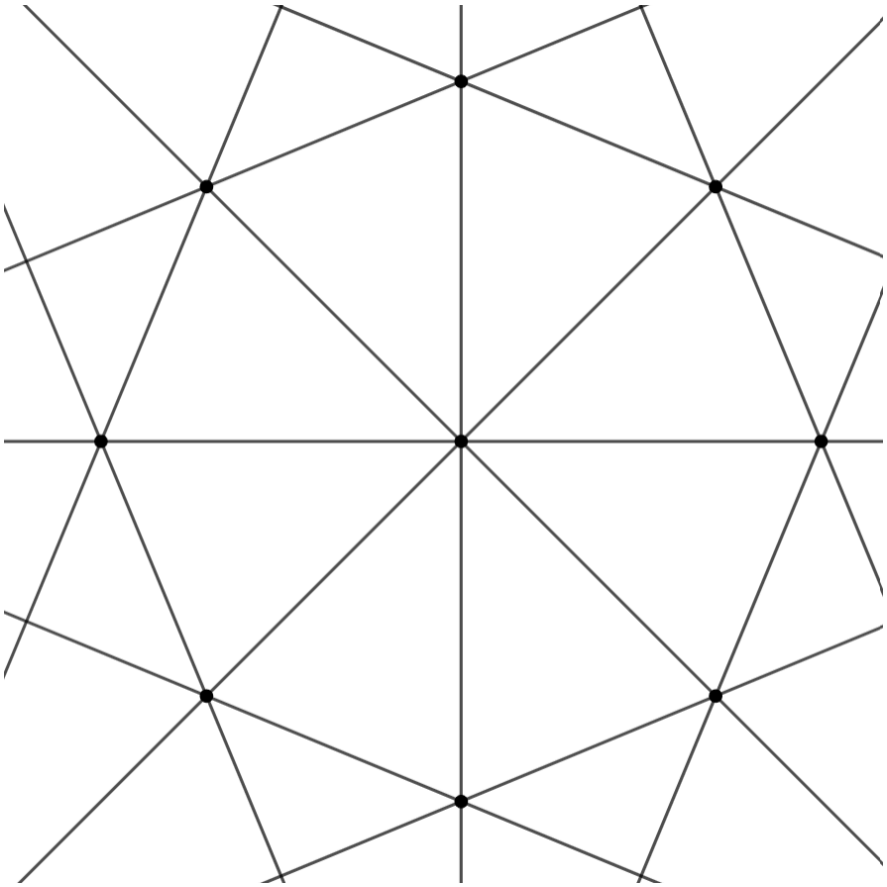

Figure 4: Possible lattice with element of order 8.

10 Conclusion

In this bachelor thesis we took a look at the structure of crystallographic groups. We managed to prove that they are related to symmetry groups of crystals using the first Bieberbach Theorem and we also proved the second and third Bieberbach Theorems. The second Bieberbach Theorem gives us a solution for a part of one of the famous 23 problems of Hilbert that he posed in 1900. Moreover, these Bieberbach Theorems showed us a closer look at how these crystallographic groups look like: they are discrete sets with only a finite non-translational part, for any given dimension there are only finitely many of them (up to an isomorphism) and isomorphic crystallographic groups are conjugate. However, the structure in crystallographic groups doesn't end there. Using their connection to finite groups of integer matrices, we managed to prove that there are only finitely many possible orders for elements in a crystallographic groups and we proved a very specific formula that allows us to easily calculate what these orders could be. This gives rise to the surprising fact that there for example doesn't exist a crystal that is invariant for a rotation over 45° in two dimensions. All this structure shows that crystallographic groups are much more interesting than what one would expect based on its definition.

11 References

[Bus85] Peter Buser. A geometric proof of bieberbach's theorems on crystallographic groups. *L'Enseignement Mathématique*, pages 137–145, 1985.

[Goe20] Wendy Goemans. *Meetkunde I.* KU Leuven, Scientica Cursusdienst, 02 2020.

[H.W13] Steven H.Weintraub. Several proofs of the irreducibility of the cyclotomic polynomials. *The American mathematical monthly*, 120:537–545, 2013.

[JJ 10] JJ O'Connor and EF Robertson. Ludwig georg elias moses bieberbach. `https://mathshistory.st-andrews.ac.uk/Biographies/Bieberbach/`, 2010. Accessed: 2021-04-03.

[KP02] James Kuzmanovich and Andrey Pavlichenkov. Finite groups of matrices whose entries are integers. *The American Mathematical Monthly*, 109(2):173–186, 2002.

[Mic11] Michiel Hazewinkel. Hilbert problems. Encyclopedia of Mathematics, `https://encyclopediaofmath.org/wiki/Hilbert_problems`, 2011. Accessed: 2021-04-03.

[Mil72] Willard Miller. The crystallographic groups. In *Pure and Applied Mathematics*, volume 50, pages 16–60. Elsevier, 1972.

[Pan19] Jiayin Pan. Nonnegative ricci curvature and virtually abelian structure. 2019.

[Qua19] Johan Quaegebeur. *Analyse I.* KU Leuven, Scientica Cursusdienst, 02 2019.

[Szc12] Andrzej Szczepański. *Geometry of crystallographic groups.* World scientific publishing, 01 2012.

[Vey21] Wim Veys. *Algebra I.* KU Leuven, Scientica Cursusdienst, 02 2021.

[Vil21a] Joel Villatoro. Crystallography and symmetry. Description Bachelor thesis, 2021.

[Vil21b] Joel Villatoro. Meetings: Bachelor thesis. Meetings, 2021.