

# Introduzione e motivazioni



# Capitolo 1

## Primo teorema di Bieberbach

Questo capitolo contiene gli strumenti fondamentali necessari per dare una dimostrazione geometrica del primo teorema di Bieberbach e la dimostrazione stessa.

### 1.1 Preliminari

In questa sezione si enunciano alcune definizioni e risultati fondamentali per approcciare la dimostrazione (che si trova nella sezione successiva). In particolare in questa sezione sono contenute informazioni che esulano dalla definizione di gruppo cristallografico e dall'enunciato del primo teorema di Bieberbach.

Nella prima parte riprendo la definizione di spazio euclideo  $n$ -dimensionale e del suo gruppo di isometrie, descrivo una loro rappresentazione come composizione dell'applicazione di una matrice ortogonale e di una traslazione; definisco poi il coniugio di due isometrie.

La lunghezza e la direzione del vettore traslazione di una data isometria mi danno immediatamente informazioni su come questa traslazione agisce sui punti di  $\mathbb{R}^n$ ; più complicato è invece capire, data una matrice ortogonale, come questa trasformi lo spazio.

Nella seconda sezione definisco quindi una funzione che stima per eccesso di quanto ogni matrice ortogonale si discosta dalla matrice identità; definisco poi attraverso essa una scomposizione dello spazio in due spazi ortogonali. Infine dimostro un teorema che mi dà una stima della "misura" del commutatore di due matrici a partire dalle loro "misure".

#### 1.1.1 Spazio euclideo $\mathbb{E}^n$ ed isometrie

Considero lo spazio vettoriale  $n$ -dimensionale  $\mathbb{R}^n$

con il prodotto scalare 
$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$$

E la norma associata 
$$\|\mathbf{x}\| = \sqrt{\mathbf{x} \cdot \mathbf{x}} \quad \forall \mathbf{x} \in \mathbb{R}^n$$

Definisco la distanza 
$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\| \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$$

e l'angolo fra due vettori

$$\angle(\mathbf{x}, \mathbf{y}) = \arccos\left(\frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|}\right) \in [0, \pi]$$

Imponendo questa metrica sullo spazio vettoriale  $\mathbb{R}^n$  ottengo lo spazio euclideo  $\mathbb{E}^n$ .

E' noto dall'algebra lineare che gli automorfismi di  $\mathbb{R}^n$  (ovvero le applicazioni lineari biettive da  $\mathbb{R}^n$  in sé stesso) formano il gruppo  $GL(n, \mathbb{R})$  con l'operazione di composizione di applicazioni lineari. Se compongo tali automorfismi con traslazioni di vettori in  $\mathbb{R}^n$  ottengo il gruppo affine  $Aff(n, \mathbb{R}) \cong \mathbb{R}^n \rtimes GL(n, \mathbb{R})$ .

**Definizione 1.1.1.** Un'isometria di  $\mathbb{E}^n$  è un funzione  $\alpha : \mathbb{R}^n \longrightarrow \mathbb{R}^n$  tale che  $\forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$  vale

$$d(\alpha(\mathbf{x}), \alpha(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$$

Il seguente teorema è enunciato senza dimostrazione in quanto si tratta di un risultato classico dell'algebra lineare.

**Teorema 1.1.1.** *Data un'isometria di  $\mathbb{E}^n$ , questa può essere scritta in modo unico come composizione di una rotazione e di una traslazione*

$$\alpha : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$\mathbf{x} \longmapsto \mathbf{Ax} + \mathbf{a}$$

dove  $\mathbf{A} = \text{rot}(\alpha) \in O(n)$  è detta componente di rotazione di  $\alpha$   
e  $\mathbf{a} = \text{trans}(\alpha) \in \mathbb{R}^n$  è detta componente di traslazione di  $\alpha$ .

**Lemma 1.1.2.** *L'insieme delle isometrie di  $\mathbb{E}^n$  è un gruppo rispetto all'operazione di composizione di applicazioni lineari. Lo chiamiamo  $\text{Isom}(n)$  e posso dire*

$$\text{Isom}(n) \cong \mathbb{R}^n \rtimes O(n) < \mathbb{R}^n \rtimes GL(n, \mathbb{R})$$

All'interno di ogni gruppo è definito il commutatore di due elementi, posso quindi anche definirlo per  $\text{Isom}(n)$ .

**Lemma 1.1.3.** *Comunque prese  $\alpha, \beta \in \text{Isom}(n)$ , posso scriverle come  $\alpha : \mathbf{x} \longmapsto \mathbf{Ax} + \mathbf{a}$  e  $\beta : \mathbf{x} \longmapsto \mathbf{Bx} + \mathbf{b}$ . Definisco il loro commutatore come  $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ . Valgono le due seguenti uguaglianze:*

$$\text{rot}([\alpha, \beta]) = [\mathbf{A}, \mathbf{B}] = \mathbf{ABA}^{-1}\mathbf{B}^{-1} \quad (1.1)$$

$$\text{trans}([\alpha, \beta]) = (\mathbf{A} - \text{id})\mathbf{b} + (\text{id} - [\mathbf{A}, \mathbf{B}])\mathbf{b} + \mathbf{A}(\text{id} - \mathbf{B})\mathbf{A}^{-1}\mathbf{a} \quad (1.2)$$

*Dimostrazione.*  $[\alpha, \beta](\mathbf{x}) = (\alpha\beta\alpha^{-1}\beta^{-1})(\mathbf{x})$ .

Dato che  $\alpha : \mathbf{x} \longmapsto \mathbf{Ax} + \mathbf{a}$ , allora sicuramente  $\alpha^{-1} : \mathbf{y} \longmapsto \mathbf{A}^{-1}(\mathbf{y} - \mathbf{a})$ .

Allo stesso modo, dato che  $\beta : \mathbf{x} \longmapsto \mathbf{Bx} + \mathbf{b}$ , so che  $\beta^{-1} : \mathbf{y} \longmapsto \mathbf{B}^{-1}(\mathbf{y} - \mathbf{b})$ .

$$\begin{aligned} [\alpha, \beta](\mathbf{x}) &= (\alpha\beta\alpha^{-1}\beta^{-1})(\mathbf{x}) = (\alpha\beta\alpha^{-1})(\mathbf{B}^{-1}(\mathbf{x} - \mathbf{b})) = \\ &= (\alpha\beta\alpha^{-1})(\mathbf{B}^{-1}\mathbf{x} - \mathbf{B}^{-1}\mathbf{b}) = \\ &= (\alpha\beta)(\mathbf{A}^{-1}(\mathbf{B}^{-1}\mathbf{x} - \mathbf{B}^{-1}\mathbf{b} - \mathbf{a})) = \\ &= (\alpha\beta)(\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x} - \mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{A}^{-1}\mathbf{a}) = \\ &= (\alpha)(\mathbf{B}(\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x} - \mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{A}^{-1}\mathbf{a}) + \mathbf{b}) = \\ &= (\alpha)(\mathbf{BA}^{-1}\mathbf{B}^{-1}\mathbf{x} - \mathbf{BA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{BA}^{-1}\mathbf{a} + \mathbf{b}) = \\ &= \mathbf{A}(\mathbf{BA}^{-1}\mathbf{B}^{-1}\mathbf{x} - \mathbf{BA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{BA}^{-1}\mathbf{a} + \mathbf{b}) + \mathbf{a} = \\ &= \mathbf{A}(\mathbf{BA}^{-1}\mathbf{B}^{-1}\mathbf{x} - \mathbf{BA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{BA}^{-1}\mathbf{a} + \mathbf{b}) + \mathbf{a} = \\ &= \mathbf{ABA}^{-1}\mathbf{B}^{-1}\mathbf{x} - \mathbf{ABA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{ABA}^{-1}\mathbf{a} + \mathbf{Ab} + \mathbf{a} \end{aligned}$$

Quindi ho che  $\text{rot}([\alpha, \beta]) = \mathbf{ABA}^{-1}\mathbf{B}^{-1}$  e

$$\begin{aligned} \text{trans}([\alpha, \beta]) &= -\mathbf{ABA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{ABA}^{-1}\mathbf{a} + \mathbf{Ab} + \mathbf{a} = \\ &= \mathbf{Ab} + \mathbf{a} - \mathbf{ABA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{ABA}^{-1}\mathbf{a} = \\ &= (\mathbf{A} - \text{id})\mathbf{b} + \mathbf{b} + \mathbf{a} - \mathbf{ABA}^{-1}\mathbf{B}^{-1}\mathbf{b} - \mathbf{ABA}^{-1}\mathbf{a} = \\ &= (\mathbf{A} - \text{id})\mathbf{b} + (\text{id} - [\mathbf{A}, \mathbf{B}])\mathbf{b} + \mathbf{a} - \mathbf{ABA}^{-1}\mathbf{a} = \\ &= (\mathbf{A} - \text{id})\mathbf{b} + (\text{id} - [\mathbf{A}, \mathbf{B}])\mathbf{b} + (\text{id} - \mathbf{ABA}^{-1})\mathbf{a} = \\ &= (\mathbf{A} - \text{id})\mathbf{b} + (\text{id} - [\mathbf{A}, \mathbf{B}])\mathbf{b} + \mathbf{A}(\text{id} - \mathbf{B})\mathbf{A}^{-1}\mathbf{a} \end{aligned}$$

□

### 1.1.2 "Misura di rotazione"

**Definizione 1.1.2.** *Comunque preso  $\mathbf{A} \in O(n)$  definisco*

$$m(\mathbf{A}) = \max \left\{ \frac{\|\mathbf{Ax} - \mathbf{x}\|}{\|\mathbf{x}\|} \mid \mathbf{x} \in \mathbb{R}^n - \mathbf{0} \right\}$$

Questa funzionemi dice quanto una data matrice ortogonale si comporta in modo diverso dalla matrice identità; descrive infatti quanto al massimo un vettore unitario viene "spostato" dall'azione di tale matrice.

**Lemma 1.1.4.** *La precedente è una buona definizione e inoltre vale*

$$m(\mathbf{A}) = \max \left\{ \|\mathbf{Ax} - \mathbf{x}\| \mid \mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1 \right\}$$

*Dimostrazione.*  $\forall \mathbf{x} \in \mathbb{R}^n - \mathbf{0} \exists \mathbf{y} \in \mathbb{R}^n - \mathbf{0}$  tale che

$$\mathbf{x} = \lambda \mathbf{y}, \lambda \in \mathbb{R} \wedge \|\mathbf{y}\| = 1.$$

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

$$m(\mathbf{A}) = \max \left\{ \|\mathbf{Ax} - \mathbf{x}\| \mid \mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1 \right\}$$

L'insieme  $\mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1$  è un compatto in  $\mathbb{R}^n$ , quindi per il teorema di Weierstrass esiste una  $\mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1$  che mi verifica il max.  $\square$

**Lemma 1.1.5.** *Comunque preso  $\mathbf{x} \in \mathbb{R}^n$  vale*

$$\|\mathbf{Ax} - \mathbf{x}\| \leq m(\mathbf{A})\|\mathbf{x}\|$$

*Dimostrazione.* Infatti vale  $\forall \mathbf{x} \in \mathbb{R}^n - \mathbf{0}$  e vale anche per  $\mathbf{x} = \mathbf{0}$   $\square$

Una volta definita la funzione  $m$  posso definire il sottoinsieme di  $\mathbb{R}^n$  che contiene tutti e soli i vettori che realizzano il massimo nella sua definizione.

**Definizione 1.1.3.**

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

**Lemma 1.1.6.**  $E_{\mathbf{A}}$  è un sottospazio di  $\mathbb{R}^n$  non banale ed  $A$ -invariante

*Dimostrazione.* •  $\mathbf{0} \in E_{\mathbf{A}}$

$$\bullet \forall \mathbf{x} \in E_{\mathbf{A}}, \forall \lambda \in \mathbb{R} \\ \mathbf{x} \in E_{\mathbf{A}} \implies \|\mathbf{Ax} - \mathbf{x}\| = m(\mathbf{A})\|\mathbf{x}\| \implies \|\mathbf{A}\lambda\mathbf{x} - \lambda\mathbf{x}\| = |\lambda|m(\mathbf{A})\|\mathbf{x}\| \implies \lambda\mathbf{x} \in E_{\mathbf{A}}$$

$$\bullet \forall \mathbf{x}, \mathbf{y} \in E_{\mathbf{A}} \text{ voglio verificare che } \mathbf{x} + \mathbf{y}, \mathbf{x} - \mathbf{y} \in E_{\mathbf{A}} \\ \mathbf{x} \in E_{\mathbf{A}} \implies \|\mathbf{Ax} - \mathbf{x}\| = m(\mathbf{A})\|\mathbf{x}\| \\ \mathbf{y} \in E_{\mathbf{A}} \implies \|\mathbf{Ay} - \mathbf{y}\| = m(\mathbf{A})\|\mathbf{y}\|$$

$$\begin{aligned} \|\mathbf{A}(\mathbf{x} + \mathbf{y}) - (\mathbf{x} + \mathbf{y})\|^2 + \|\mathbf{A}(\mathbf{x} - \mathbf{y}) - (\mathbf{x} - \mathbf{y})\|^2 &= \|\mathbf{Ax} - \mathbf{x} + \mathbf{Ay} - \mathbf{y}\|^2 + \|\mathbf{Ax} - \mathbf{x} - (\mathbf{Ay} - \mathbf{y})\|^2 = \\ &= 2\|\mathbf{Ax} - \mathbf{x}\|^2 + 2\|\mathbf{Ay} - \mathbf{y}\|^2 = 2(\|\mathbf{Ax} - \mathbf{x}\|^2 + \|\mathbf{Ay} - \mathbf{y}\|^2) = 2m(\mathbf{A})^2(\|\mathbf{x}\|^2 + \|\mathbf{y}\|^2) \end{aligned} \quad (1.3)$$

Da (3) segue

$$\begin{aligned} 2m(\mathbf{A})^2(\|\mathbf{x}\|^2 + \|\mathbf{y}\|^2) &= \|\mathbf{A}(\mathbf{x} + \mathbf{y}) - (\mathbf{x} + \mathbf{y})\|^2 + \|\mathbf{A}(\mathbf{x} - \mathbf{y}) - (\mathbf{x} - \mathbf{y})\|^2 \leq m(\mathbf{A})^2(\|\mathbf{x} + \mathbf{y}\|^2 + \|\mathbf{x} - \mathbf{y}\|^2) \\ &= m(\mathbf{A})^2(\|\mathbf{x} + \mathbf{y}\|^2 + \|\mathbf{x} - \mathbf{y}\|^2) = 2m(\mathbf{A})^2(\|\mathbf{x}\|^2 + \|\mathbf{y}\|^2) \end{aligned} \quad (1.4)$$

Quindi il segno di disuguaglianza in (4) è un'uguaglianza, in particolare

$$\|\mathbf{A}(\mathbf{x} + \mathbf{y}) - (\mathbf{x} + \mathbf{y})\|^2 + \|\mathbf{A}(\mathbf{x} - \mathbf{y}) - (\mathbf{x} - \mathbf{y})\|^2 = m(\mathbf{A})^2(\|\mathbf{x} + \mathbf{y}\|^2 + \|\mathbf{x} - \mathbf{y}\|^2)$$

Spostando i termini da parte a parte ottengo

$$\begin{aligned} \|\mathbf{A}(\mathbf{x} + \mathbf{y}) - (\mathbf{x} + \mathbf{y})\|^2 - m(\mathbf{A})^2\|\mathbf{x} + \mathbf{y}\|^2 &= m(\mathbf{A})^2\|\mathbf{x} - \mathbf{y}\|^2 - \|\mathbf{A}(\mathbf{x} - \mathbf{y}) - (\mathbf{x} - \mathbf{y})\|^2 \\ \left( \|\mathbf{A}(\mathbf{x} + \mathbf{y}) - (\mathbf{x} + \mathbf{y})\| + m(\mathbf{A})\|\mathbf{x} + \mathbf{y}\| \right) \left( \|\mathbf{A}(\mathbf{x} + \mathbf{y}) - (\mathbf{x} + \mathbf{y})\| - m(\mathbf{A})\|\mathbf{x} + \mathbf{y}\| \right) &= \\ - \left( \|\mathbf{A}(\mathbf{x} - \mathbf{y}) - (\mathbf{x} - \mathbf{y})\| + m(\mathbf{A})\|\mathbf{x} - \mathbf{y}\| \right) \left( \|\mathbf{A}(\mathbf{x} - \mathbf{y}) - (\mathbf{x} - \mathbf{y})\| - m(\mathbf{A})\|\mathbf{x} - \mathbf{y}\| \right) & \end{aligned} \quad (1.5)$$

Distinguiamo alcuni casi:

- Se  $\mathbf{A} = \mathbf{id} \implies m(\mathbf{A}) = 0 \implies E_{\mathbf{A}} = \mathbb{R}^n$  ed in quel caso ho chiuso la dimostrazione.
- Se  $\mathbf{x} = \mathbf{y}$  o  $\mathbf{x} = -\mathbf{y}$  ho già chiuso la dimostrazione per il punto precedente (rispettivamente con  $\lambda = +1$  e  $\lambda = -1$ ).

- Nei restanti casi posso osservare che nell'equazione (5) il primo fattore a sinistra dell'uguaglianza è strettamente positivo, mentre il secondo fattore è  $\leq 0$ . Allo stesso modo a destra dell'uguaglianza ho un meno che mi modifica il segno del prodotto; il primo fattore è strettamente positivo ed il secondo è  $\leq 0$ .

L'uguaglianza in (5) deve quindi per forza coincidere con  $0 = 0$  e questo mi implica

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

$$\implies \mathbf{x} + \mathbf{y}, \mathbf{x} - \mathbf{y} \in E_{\mathbf{A}}$$

Ho concluso la dimostrazione del fatto che  $E_{\mathbf{A}}$  è un sottospazio vettoriale di  $\mathbb{R}^n$

- Mostro che  $E_{\mathbf{A}}$  è non banale.

$$m(\mathbf{A}) = \max \left\{ \|\mathbf{A}\mathbf{x} - \mathbf{x}\| \mid \mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1 \right\}$$

L'insieme degli  $\mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1$  è un compatto; l'applicazione  $\mathbf{x} \mapsto \|\mathbf{A}\mathbf{x} - \mathbf{x}\|$  è continua in quanto composizione di funzioni continue, quindi sicuramente esiste un  $\mathbf{x} \in \mathbb{R}^n \wedge \|\mathbf{x}\| = 1$  che mi verifica il massimo. In particolare  $\mathbf{x} \neq \mathbf{0}$  (perché ha norma 1) e

$$\|\mathbf{A}\mathbf{x} - \mathbf{x}\| = m(\mathbf{A}) = m(\mathbf{A})\|\mathbf{x}\| \implies \mathbf{x} \in E_{\mathbf{A}}$$

- Mostro che  $E_{\mathbf{A}}$  è  $\mathbf{A}$ -invariante.

$\forall \mathbf{x} \in E_{\mathbf{A}}$  voglio mostrare che  $\mathbf{A}\mathbf{x} \in E_{\mathbf{A}}$

$$\mathbf{x} \in E_{\mathbf{A}} \implies \|\mathbf{A}\mathbf{x} - \mathbf{x}\| = m(\mathbf{A})\|\mathbf{x}\|$$

Dato che  $\mathbf{A} \in O(n)$  ho la seguente catena di uguaglianze:

$$\|\mathbf{A}(\mathbf{A}\mathbf{x}) - \mathbf{A}\mathbf{x}\| = \|\mathbf{A}(\mathbf{A}\mathbf{x} - \mathbf{x})\| = \|\mathbf{A}\mathbf{x} - \mathbf{x}\| = m(\mathbf{A})\|\mathbf{x}\| = m(\mathbf{A})\|\mathbf{A}\mathbf{x}\| \implies \mathbf{A}\mathbf{x} \in E_{\mathbf{A}}$$

□

**Lemma 1.1.7.**  $E_{\mathbf{A}}$  sottospazio vettoriale di  $\mathbb{R}^n$  non banale, quindi posso definire il suo complemento ortogonale  $E_{\mathbf{A}}^{\perp} \neq \mathbb{R}^n$  ed anche questo è  $\mathbf{A}$ -invariante.

**Definizione 1.1.4.**

$$m^{\perp}(\mathbf{A}) = \begin{cases} \max \left\{ \frac{\|\mathbf{A}\mathbf{x} - \mathbf{x}\|}{\|\mathbf{x}\|} \mid \mathbf{x} \in E_{\mathbf{A}}^{\perp} - \mathbf{0} \right\} & \text{se } E_{\mathbf{A}}^{\perp} \neq \mathbf{0} \\ 0 & \text{se } E_{\mathbf{A}}^{\perp} = \mathbf{0} \end{cases}$$

**Lemma 1.1.8.**  $m^{\perp}(\mathbf{A}) < m(\mathbf{A})$  se  $\mathbf{A} \neq \text{id}$

$m^{\perp}(\mathbf{A}) = m(\mathbf{A}) = 0$  se  $\mathbf{A} = \text{id}$

*Dimostrazione.* • Se  $\mathbf{A} = \text{id} \implies m(\mathbf{A}) = 0 \wedge E_{\mathbf{A}} = \mathbb{R}^n$ . Quindi  $E_{\mathbf{A}}^{\perp} = \mathbf{0} \implies m^{\perp}(\mathbf{A}) = 0$

- Se  $\mathbf{A} \neq \text{id}$

$$m(\mathbf{A}) = \max \left\{ \frac{\|\mathbf{A}\mathbf{x} - \mathbf{x}\|}{\|\mathbf{x}\|} \mid \mathbf{x} \in \mathbb{R}^n - \mathbf{0} \right\} \geq \max \left\{ \frac{\|\mathbf{A}\mathbf{x} - \mathbf{x}\|}{\|\mathbf{x}\|} \mid \mathbf{x} \in E_{\mathbf{A}}^{\perp} - \mathbf{0} \right\} = m^{\perp}(\mathbf{A})$$

Se valesse  $m(\mathbf{A}) = m^{\perp}(\mathbf{A}) \implies \exists \mathbf{x} \in E_{\mathbf{A}}^{\perp} - \mathbf{0} : \|\mathbf{A}\mathbf{x} - \mathbf{x}\| = m(\mathbf{A})\|\mathbf{x}\| \implies \mathbf{x} \in E_{\mathbf{A}}$  ma questo implica  $\mathbf{x} \in E_{\mathbf{A}} \cap E_{\mathbf{A}}^{\perp} = \mathbf{0} \implies \mathbf{x} = \mathbf{0}$ ; questo è però assurdo perché ho imposto che  $\mathbf{x} \neq \mathbf{0}$

□

**Lemma 1.1.9.**  $\forall \mathbf{x} \in \mathbb{R}^n$  posso scrivere  $\mathbf{x}$  in modo unico in decomposizione ortogonale.

$\mathbf{x} = \mathbf{x}^E + \mathbf{x}^{\perp}$  dove  $\mathbf{x}^E \in E_{\mathbf{A}}$  e  $\mathbf{x}^{\perp} \in E_{\mathbf{A}}^{\perp}$

Valgono inoltre le proprietà:

$$\|\mathbf{A}\mathbf{x}^E - \mathbf{x}^E\| = m(\mathbf{A})\|\mathbf{x}^E\|$$

$$\|\mathbf{A}\mathbf{x}^{\perp} - \mathbf{x}^{\perp}\| \leq m(\mathbf{A})\|\mathbf{x}^{\perp}\|$$

**Lemma 1.1.10.**  $\forall \mathbf{A}, \mathbf{B} \in O(n)$  vale la disuguaglianza  $m([\mathbf{A}, \mathbf{B}]) \leq 2m(\mathbf{A})m(\mathbf{B})$

*Dimostrazione.*

$$\begin{aligned} [\mathbf{A}, \mathbf{B}] - \text{id} &= \mathbf{A}\mathbf{B}\mathbf{A}^{-1}\mathbf{B}^{-1} - \text{id} = (\mathbf{A}\mathbf{B} - \mathbf{B}\mathbf{A})\mathbf{A}^{-1}\mathbf{B}^{-1} = [(\mathbf{A} - \text{id})(\mathbf{B} - \text{id}) - (\mathbf{B} - \text{id})(\mathbf{A} - \text{id})]\mathbf{A}^{-1}\mathbf{B}^{-1} = \\ &= (\mathbf{A} - \text{id})(\mathbf{B} - \text{id})\mathbf{A}^{-1}\mathbf{B}^{-1} - (\mathbf{B} - \text{id})(\mathbf{A} - \text{id})\mathbf{A}^{-1}\mathbf{B}^{-1} \end{aligned}$$

$$\begin{aligned} \|([\mathbf{A}, \mathbf{B}] - \text{id})\mathbf{x}\| &\leq \|(\mathbf{A} - \text{id})(\mathbf{B} - \text{id})\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| + \|(\mathbf{B} - \text{id})(\mathbf{A} - \text{id})\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| \leq \\ &\leq m(\mathbf{A})\|(\mathbf{B} - \text{id})\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| + m(\mathbf{B})\|(\mathbf{A} - \text{id})\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| \leq \\ &\leq m(\mathbf{A})m(\mathbf{B})\|\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| + m(\mathbf{B})m(\mathbf{A})\|\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| \end{aligned} \quad (1.6)$$

Dato che  $\mathbf{A}, \mathbf{B} \in O(n)$  posso scrivere  $\|\mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{x}\| = \|\mathbf{x}\|$ , quindi

$$\|([\mathbf{A}, \mathbf{B}] - \text{id})\mathbf{x}\| \leq 2m(\mathbf{A})m(\mathbf{B})\|\mathbf{x}\| \quad (1.7)$$

Quindi segue immediatamente la tesi.  $\square$

## 1.2 Primo teorema di Bieberbach

In questa sezione viene dimostrato il primo teorema di Bieberbach. Si dà prima di tutto una definizione precisa di gruppo cristallografico e viene esplicitato il contenuto del teorema nella forma in cui verrà dimostrato. Per dimostrare effettivamente il teorema, bisogna passare attraverso un paio di teoremi preliminari che verranno esposti nella seconda parte. Infine nella sottosezione finale verrà data la dimostrazione.

### 1.2.1 Enunciati

**Teorema 1.2.1.** *Dato un gruppo discreto di isometrie di  $\mathbb{R}^n$  a dominio fondamentale compatto, questo contiene  $n$  traslazioni linearmente indipendenti.*

In questo elaborato utilizzo la seguente definizione di gruppo cristallografico:

**Definizione 1.2.1.** *Sia  $\Gamma$  un sottogruppo di  $\text{Isom}(n)$ , dico che è un gruppo cristallografico  $n$ -dimensionale se valgono le seguenti condizioni:*

1.  $\forall t \in \mathbb{R} : t > 0$  esistono solo un numero finito di  $\alpha \in \Gamma$  tali che  $|\alpha| \leq t$
2.  $\exists d \in \mathbb{R} : \forall \mathbf{x} \in \mathbb{R}^n \exists \alpha \in \Gamma : \|\mathbf{a} - \mathbf{x}\| \leq d$

Se considero lo spazio topologico  $\mathbb{R}^n$  con la metrica data dalla distanza euclidea ed un gruppo di isometrie che agisce su di esso, la condizione 1. implica che agisce in modo propriamente discontinuo, mentre la condizione 2. significa che ha dominio fondamentale limitato. Dato uno spazio topologico  $X$  ed un gruppo  $G$  che agisce su di esso, un dominio fondamentale è un sottoinsieme di  $X$  che contiene uno ed un solo punto di ogni orbita dell'azione.

Posso quindi rifrasare il primo teorema di Bieberbach come

**Teorema 1.2.2.** *Ogni gruppo cristallografico  $n$ -dimensionale contiene  $n$  traslazioni linearmente indipendenti*

### 1.2.2 Mini Bieberbach e teorema di caratterizzazione delle traslazioni

**Teorema 1.2.3.** *Mini Bieberbach. Sia  $\Gamma$  un gruppo cristallografico di  $\mathbb{R}^n$*

$$1. \mathbf{a} \neq 0$$

$$\forall \mathbf{u} \in \mathbb{R}^n : \|\mathbf{u}\| = 1, \forall \epsilon, \delta > 0$$

$$\exists \beta \in \Gamma \text{ che soddisfa}$$

$$2. \angle(\mathbf{u}, \mathbf{a}) \leq \delta$$

$$3. m(\mathbf{A}) \leq \epsilon$$

*Dimostrazione.* Per la seconda proprietà dei gruppi cristallografici so che  $\exists d \in \mathbb{R} : \forall k \in \mathbb{N} \exists \beta_k \in \Gamma :$

$$\beta_k \mathbf{x} = \mathbf{B}_k \mathbf{x} + \mathbf{b}_k \wedge \|\mathbf{b}_k - \mathbf{k}\mathbf{u}\| \leq d$$

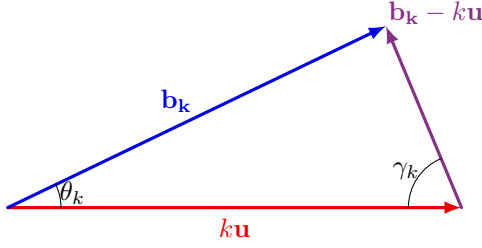
Se  $k \rightarrow \infty$  allora sicuramente  $\|\mathbf{b}_k\| \rightarrow \infty$ .

Infatti se, per assurdo, questo non fosse vero  $\exists M \in \mathbb{R} : \|\mathbf{b}_k\| \leq M \forall k \in \mathbb{N}$

$$d \geq \|\mathbf{b}_k - \mathbf{k}\mathbf{u}\| \geq \|\mathbf{b}_k\| - k$$

Nella disequazione precedente, se la successione è limitata allora l'ultimo termine diverge ma questo è assurdo perché è maggiorato da  $d$ .

Considero ora la successione degli angoli fra il vettore  $\mathbf{u}$  e  $\mathbf{b}_k$ , voglio mostrare che la loro ampiezza tende a 0.



$$\begin{aligned}\angle(\mathbf{u}, \mathbf{b}_k) &= \angle(\mathbf{ku}, \mathbf{b}_k) =: \theta_k \\ \frac{\|\mathbf{b}_k\|}{\sin(\gamma_k)} &= \frac{\|\mathbf{b}_k - \mathbf{ku}\|}{\sin(\theta_k)} \leq \frac{d}{\sin(\theta_k)} \\ \sin(\theta_k) &\leq \frac{\sin(\gamma_k)d}{\|\mathbf{b}_k\|} \rightarrow 0 \implies \theta_k \rightarrow 0\end{aligned}$$

Ho definito la successione  $\{\beta_k\}_{k \in \mathbb{N}}$  con  $\beta_k \mathbf{x} = \mathbf{B}_k \mathbf{x} + \mathbf{b}_k$   $\beta_k \in \Gamma \implies \mathbf{B}_k \in O(n)$   $O(n)$  è compatto e  $\{\mathbf{B}_k\}_{k \in \mathbb{N}}$  successione in  $O(n)$  ammette quindi almeno un punto di accumulazione per il teorema di Bolzano-Weierstrass.

Estraggo da  $\{\mathbf{B}_k\}_{k \in \mathbb{N}}$  una sottosuccessione  $\{\mathbf{A}_k\}_{k \in \mathbb{N}} = \{\mathbf{B}_{k_j}\}_{j \in \mathbb{N}}$  convergente.

La funzione  $m : O(n) \rightarrow \mathbb{R}$  è continua in quanto composizione di funzioni continue ( $\mathbf{A} \mapsto \max \|\mathbf{A}\mathbf{x} - \mathbf{x}\|$ ), quindi con  $i, j \in \mathbb{B} \rightarrow \infty$  sicuramente  $m(\mathbf{A}_j \mathbf{A}_i^{-1}) \rightarrow m(\mathbf{id}) = 0$

Associata a questa sottosuccessione ho ovviamente una sottosuccessione di  $\{\beta_k\}_{k \in \mathbb{N}}$  che chiamo  $\{\alpha_k\}_{k \in \mathbb{N}}$  con  $\alpha_k \mathbf{x} = \mathbf{A}_k \mathbf{x} + \mathbf{a}_k$

Dato che valgono tutte le proprietà di cui sopra, è immediato verificare che  $\exists i, j \in \mathbb{N}$  tali che  $i < j$  e che valgano contemporaneamente

$$\begin{cases} \angle(u, \mathbf{a}_j) \leq \frac{\delta}{2} \\ \|\mathbf{a}_i\| \leq \frac{\delta}{4} \|\mathbf{a}_j\| \\ m(\mathbf{A}_j \mathbf{A}_i^{-1}) \leq \epsilon \end{cases}$$

Considero l'isometria definita da  $\alpha \in \Gamma$  come

$$\alpha : x \mapsto \alpha_j \alpha_i^{-1} \mathbf{x} = \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{x} + \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i$$

Questa isometria verifica tutte le proprietà richieste dalla tesi

- È ovvio che  $m(\mathbf{A}) = m(\mathbf{A}_j \mathbf{A}_i^{-1}) \leq \epsilon$
- Verifico  $\mathbf{a} = \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i \neq 0$

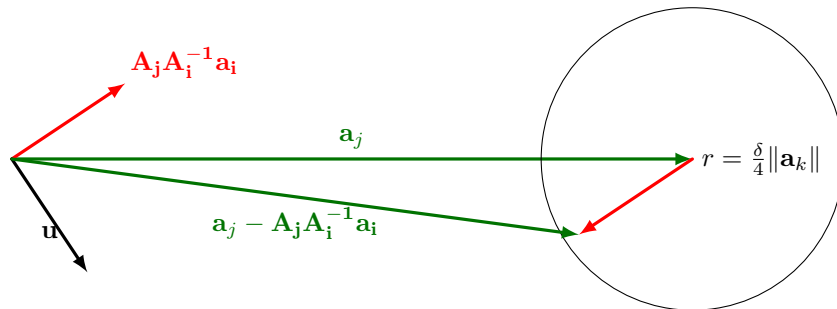
$$\|\mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i\| \geq \left| \|\mathbf{a}_j\| - \|\mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i\| \right| \geq \left| \|\mathbf{a}_j\| + \|\mathbf{a}_i\| \right| \geq \|\mathbf{a}_i\| \left| \frac{4}{\delta} - 1 \right|$$

$$\|\mathbf{a}_i\| \neq 0 \implies \mathbf{a} \neq 0$$

- Verifico  $\angle(\mathbf{u}, \mathbf{a}) = \angle(\mathbf{u}, \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i) \leq \delta$ .

$$\angle(\mathbf{u}, \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i) \leq \angle(\mathbf{u}, \mathbf{a}_j) + \angle(\mathbf{a}_j, \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i) \quad (1.8)$$

Dato che  $\|\mathbf{a}_i\| \leq \frac{\delta}{4} \|\mathbf{a}_k\|$ , la punta del vettore  $\mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i$  cade all'interno di una palla n-dimensionale che ha come centro la punta di  $\mathbf{a}_j$  e raggio  $r = \frac{\delta}{4} \|\mathbf{a}_k\|$





Considero una situaizone come quella nel disegno precedente;  
 $\forall P$  scelto all'interno della circonferenza  
 $\widehat{PAO} \leq \widehat{TAO}$

$$\frac{\overline{TO}}{\sin(\widehat{TAO})} = \frac{\overline{AO}}{\sin(\widehat{ATO})}$$

Quindi

$$\sin(\widehat{PAO}) \leq \sin(\widehat{TAO}) = \frac{\overline{TO}}{\overline{AO}} = \frac{\delta}{4}$$

So quindi che

$$\sin(\angle(\mathbf{a}_j, \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i)) \leq \frac{\delta}{4} \implies \angle(\mathbf{a}_j, \mathbf{a}_j - \mathbf{A}_j \mathbf{A}_i^{-1} \mathbf{a}_i) \leq \frac{\delta}{4} + o\left(\frac{\delta^2}{16}\right) \leq \frac{\delta}{2} \quad (1.9)$$

E (9) insieme con (8) e  $\angle(\mathbf{u}, \mathbf{a}_j) \leq \frac{\delta}{2}$  implica che

$$\angle(\mathbf{u}, \mathbf{a}) \leq \delta$$

□

**Teorema 1.2.4.** *Comunque scelta  $\alpha \in \Gamma: x \mapsto \mathbf{A}x + \mathbf{a}$  tale per cui  $m(\mathbf{A}) \leq \frac{1}{2}$ , questa isometria è una traslazione pura*

*Dimostrazione.* Se  $m(\mathbf{A}) = 0 \implies A = id \implies \alpha$  è una traslazione pura.

Fra le isometrie in  $\Gamma$  che soddisfano la condizione  $0 < m(\mathbf{A}) \leq \frac{1}{2}$  scelgo quella che ha  $\|\mathbf{a}\|$  minimo (posso farlo perché vale la condizione (1) sugli elementi di un gruppo cristallografico).

So che  $m(\mathbf{A}) > m^\perp(\mathbf{A})$  se  $\mathbf{A} \neq id$ .

$\forall \mathbf{u} \in E_{\mathbf{A}}$  vettore unitario,

$$\epsilon := \frac{1}{8} (m(\mathbf{A}) - m^\perp(\mathbf{A}))$$

ed applico il teorema Mini Bieberbach.

$$\exists \beta \in \Gamma : m(\mathbf{B}) \leq \epsilon; \mathbf{b} \neq 0; \angle(\mathbf{u}, \mathbf{b}) \leq \delta$$

In particolare scelgo  $\delta$  in modo da avere  $\|\mathbf{b}^\perp\| \leq \|\mathbf{b}^E\|$ , posso farlo come da figura.

Fra questi  $\beta$  scelgo quello per cui  $\|\mathbf{b}\|$  è minimo ( $\neq 0$ , posso farlo per la prima proprietà dei gruppi cristallografici).

Osservo che, se  $\beta$  non è una traslazione, allora

$\|\mathbf{b}\| \geq \|\mathbf{a}\|$ , questo perché  $m(\mathbf{B}) \leq \frac{1}{8}m(\mathbf{A}) \leq \frac{1}{4}$  e  $\alpha$  è stato scelto fra le isometrie in  $\Gamma$  con in modo da minimizzare il modulo della componente traslatoria).

Definisco una nuova isometria  $\tilde{\beta} := [\alpha, \beta] \in \Gamma$

So dal lemma 1.3 e dal lemma 1.10 che

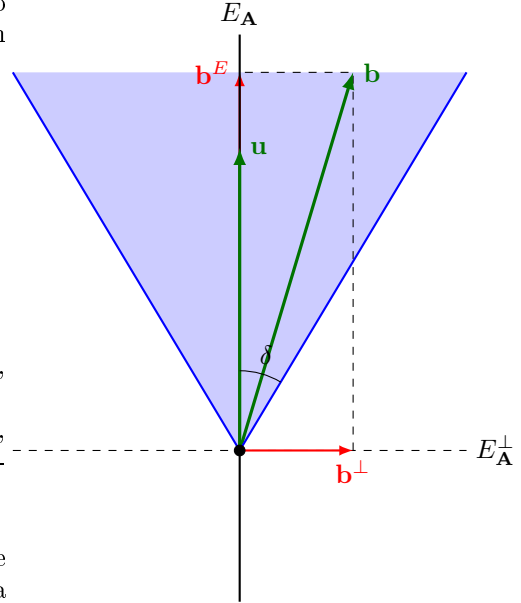
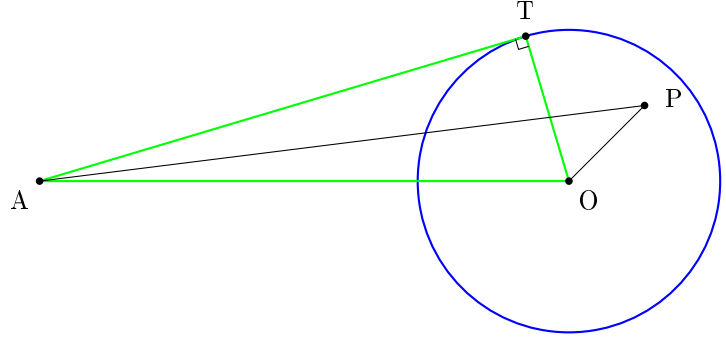
$$m(\tilde{\beta}) = m[\mathbf{A}, \mathbf{B}] \leq 2m(\mathbf{A})m(\mathbf{B}) \leq 2\frac{1}{2}m(\mathbf{B}) = m(\mathbf{B})$$

$$\text{trans}(\tilde{\beta}) = (\mathbf{A} - id)\mathbf{b} + (id - [\mathbf{A}, \mathbf{B}])\mathbf{b} + \mathbf{A}(id - \mathbf{B})\mathbf{A}^{-1}\mathbf{a} = (\mathbf{A} - id)\mathbf{b} + \mathbf{r}$$

Con  $\mathbf{r} = (id - \tilde{\mathbf{B}})\mathbf{b} + \mathbf{A}(id - \mathbf{B})\mathbf{A}^{-1}\mathbf{a}$  e  $\tilde{\mathbf{b}}^\perp = (\mathbf{A} - id)\mathbf{b}^\perp + \mathbf{r}$ .

- Se  $\beta$  è una traslazione  $\implies \mathbf{B} = id = \tilde{\mathbf{B}} \implies \mathbf{r} = 0$ .
- Se  $\beta$  non è una traslazione  $\implies \|\mathbf{b}\| \geq \|\mathbf{a}\|$  e quindi

$$\|\mathbf{r}\| \leq m(\tilde{\mathbf{B}})\|\mathbf{b}\| + m(\mathbf{B})\|\mathbf{a}\| \leq (m(\tilde{\mathbf{B}}) + m(\mathbf{B}))\|\mathbf{b}\| \leq 2m(\mathbf{B})(\mathbf{b}^E + \mathbf{b}^\perp) < 4m(\mathbf{B})\|\mathbf{b}^E\| \leq \frac{1}{2}(m(\mathbf{A}) - m^\perp(\mathbf{A}))\|\mathbf{b}^E\|$$



In entrambi i casi ho che  $\|\mathbf{r}\| < \frac{1}{2}(m(\mathbf{A}) - m^\perp(\mathbf{A}))\|\mathbf{b}^E\|$ .

Posso scrivere

$$\tilde{\mathbf{b}}^E - (\mathbf{A} - \mathbf{id})\mathbf{b}^E - \mathbf{r}^E = (\mathbf{A} - \mathbf{id})\mathbf{b}^\perp + \mathbf{r}^\perp - \tilde{\mathbf{b}}^\perp = 0$$

Usando la caratterizzazione  $\|\mathbf{b}^\perp\| \leq \|\mathbf{b}^E\|$  ottengo

$$\|\tilde{\mathbf{b}}^\perp\| \leq m^\perp(\mathbf{A})\|\mathbf{b}^\perp\| + \|\mathbf{r}^\perp\| < m^\perp(\mathbf{A})\|\mathbf{b}^E\| + \frac{1}{2}(m(\mathbf{A}) - m(\mathbf{A}^\perp))\|\mathbf{b}^E\|$$

Sommando a destra ottengo

$$\|\tilde{\mathbf{b}}^\perp\| < \frac{1}{2}(m(\mathbf{A}) + m(\mathbf{A}^\perp))$$

D'altro canto, utilizzando la disuguaglianza triangolare inversa, posso scrivere

$$\|\mathbf{b}^E\| = \|(\mathbf{A} - \mathbf{id})\mathbf{b}^E + \mathbf{r}^E\| \geq \left| m(\mathbf{A})\|\mathbf{b}^E\| - \|\mathbf{r}\| \right| > m(\mathbf{A})\|\mathbf{b}^E\| - \frac{1}{2}(m(\mathbf{A}) - m^\perp(\mathbf{A}))\|\mathbf{b}^E\| = \frac{1}{2}(m(\mathbf{A}) + m(\mathbf{A}^\perp))\|\mathbf{b}^E\|$$

In particolare quindi

$$\|\mathbf{b}^E\| > \|\mathbf{b}^\perp\|$$

So inoltre che

$$\|\tilde{\mathbf{b}}\| \leq m(\mathbf{A})\|\mathbf{b}\| + \|\mathbf{r}\| < m(\mathbf{A})\|\mathbf{b}\| + \frac{1}{2}(m(\mathbf{A}) - m^\perp(\mathbf{A}))\|\mathbf{b}^E\| \leq \|\mathbf{b}\| \left( \frac{1}{2} + \frac{1}{4} \right) < \|\mathbf{b}\|$$

Ho un assurdo perché  $\beta$  era stato scelto fra tutti quelli che soddisfavano le condizioni in modo da minimizzare la norma di  $b$ .

□

### 1.2.3 Dimostrazione del primo teorema di Bieberbach

Posso quindi concludere la dimostrazione del primo teorema di Bieberbach.

*Dimostrazione.* Considero la base standard di  $\mathbb{R}^N$ ; se applico ad ognuno dei vettori di tale base il teorema Mini Bieberbach con  $\epsilon = \frac{1}{2}$  e  $\delta = 1/N \forall N \in \mathbb{N}$ , ottengo  $n$  successioni di elementi in  $\Gamma$  che sono traslazioni pure (per il teorema 6.2). Se passo al limite per  $N \rightarrow \infty$  so che ognuna di queste successioni converge ad un elemento in  $\Gamma$

(NON è VEROOOOOOOO!!! come faccio qui? devo far vedere che converge ad una direzione, ma non saprei come farlo. Inoltre come faccio a dire che se tot vettori distano ognuno meno di  $\delta$  da un vettore della base standard, allora questi sono linearmente indipendenti? posso fare il limite per  $n \rightarrow$  infinito? non convergono necessariamente i moduli)

□

## Capitolo 2

## Secondo teorema di Bieberbach

**Definizione 2.0.1.** *Un reticolo  $L$  è un gruppo cristallografico che contiene solo traslazioni.*

*Gli elementi di  $L$  possono essere identificati con i vettori di  $\mathbb{R}^n$  corrispondenti alla propria componente di traslazione e vengono chiamati punti di reticolo.*

Dato un elemento  $\omega \in L$ , per abuso di notazione scriveremo  $\omega = trans(\omega) = \mathbf{w}$ . Enunciamo il seguente risultato senza dimostrarlo.

**Lemma 2.0.1.** *Ogni reticolo  $L$  di dimensione  $n$  è isomorfo a  $\mathbb{Z}^n$ .*

Di conseguenza  $L$  è abeliano e la distanza minima fra due punti di reticolo coincide con la lunghezza del minimo vettore non nullo in  $L$ .

**Lemma 2.0.2.** *Sia  $L$  un reticolo in  $\mathbb{E}^n$  i cui vettori abbiano distanza a coppie  $\geq 1$ .*

Sia  $\rho > 0$ , chiamo  $P(\rho)$  il numero di punti di reticolo in  $L$  con distanza dall'origine  $\leq \rho$ .

$$P(\rho) \leq (2\rho + 1)^n$$

*Dimostrazione.* Per ogni punto di reticolo a distanza inferiore o uguale di  $\rho$  dall'origine posso considerare una palla aperta  $n$ -dimensionale centrata in esso e di raggio  $\frac{1}{2}$ . Queste palle sono sicuramente disgiunte in quanto la distanza fra due punti del reticolo è superiore al doppio dei raggi; sono inoltre tutte contenute nella palla  $n$ -dimensionale centrata nell'origine di raggio  $\rho + \frac{1}{2}$ . Il volume della palla centrata nell'origine è sicuramente superiore alla somma dei volumi delle singole palle di raggio  $\frac{1}{2}$ , confrontando i volumi ottengo

$$\begin{aligned} P(\rho)\left(\frac{1}{2}\right) &\leq \left(\rho + \frac{1}{2}\right) \\ P(\rho) &\leq (2\rho + 1) \end{aligned}$$

☐

**Lemma 2.0.3.** *Sia  $L$  un reticolo in  $\mathbb{E}^n$  i cui vettori abbiano distanza a coppie  $> 1$ .*

Consideriamo un sottospazio lineare di  $\mathbb{R}^n$  generato da  $k$  vettori  $\mathbf{w}_i \in L$  con  $i = 1, \dots, k$ .

Se un punto di reticolo  $\mathbf{w} \in L$  non è contenuto in  $E$ , allora la sua componenete in  $E^\perp$  è tale che

$$\|\mathbf{w}^\perp\| \geq \left(3 + \sum_{i=1}^k \|\mathbf{w}_i\|\right)^{-n}$$

*Dimostrazione.* Sia

$$N = \left| \left( 3 + \sum_{i=1}^k \|\mathbf{w}_i\| \right)^n \right|$$

Suppongo per assurdo che  $0 < \|\mathbf{w}^\perp\| < \frac{1}{N}$ .

In questa situazione i vettori  $j\mathbf{w}$  con  $j = 0, \dots, N$  hanno distanze da  $E$  inferiori a 1.

Aggiungendo ad ognuno di questi una combinazione lineare di  $\{\mathbf{w}_i\}_{1 \leq i \leq k}$  posso modificarne la componente in  $E$  senza andare a toccare la componente perpendicolare.

In particolare scelgo la combinazione in modo che  $j\mathbf{w}^E \leq \frac{1}{2} \left( \sum_{i=1}^k \|\mathbf{w}_i\| \right) \quad \forall j = 0, ..., N$ . Posso farlo in quanto (??? devo rimanere nel reticolo, quindi dovrei fare combinazioni lineari intere, se fossero combinazioni lineari generiche sarebbe immediato; come lo faccio vedere?).

Questi  $N + 1$  punti di reticolo hanno quindi una distanza dall'origine inferiore a alla somma delle loro distanze da  $E$  ed  $E^\perp$ , in quanto l'origine appartiene ad entrambi i sottospazi.

$$d(j\mathbf{w}, \mathbf{0}) \leq 1 + \frac{1}{2} \left( \sum_{i=1}^k \|\mathbf{w}_i\| \right)$$

Questa è una contraddizione al lemma (8.2) in quanto ho

$$N + 1 \leq P \left( 1 + \frac{1}{2} \left( \sum_{i=1}^k \|\mathbf{w}_i\| \right) \right) \leq \left( 3 + \sum_{i=1}^k \|\mathbf{w}_i\| \right)^{-n} \leq \frac{1}{N}$$

E non esistono  $N \in \mathbb{N}^+$  che mi soddisfino questa disequazione.

□