

# Groupes cristallographiques

Zaïd Allybokus – Oscar Blumberg – sous la direction de Philippe Gille

## Résumé

Cet exposé introduit le sujet des groupes cristallographiques, que l'on peut voir comme les groupes de symétrie d'agencements réguliers dans un espace euclidien, tel un cristal. Leur étude, motivée par la cristallographie, permet par exemple de déterminer certaines propriétés physiques de cristaux. On y démontre quelques théorèmes de classification qui mettent en lumière la structure de ces groupes.

En particulier, à équivalence géométrique près, il n'en existe qu'un nombre fini à dimension fixée. L'outil principal utilisé est la *cohomologie de groupes* qu'on appliquera de manière *ad hoc*. On expliquera de plus schématiquement les étapes pour obtenir une description complète de cette classe de groupe.

## Table des matières

<b>1</b>	<b>Préliminaires</b>	<b>2</b>
1.1	Isométries . . . . .	2
1.2	Prérequis sur les réseaux euclidiens . . . . .	2
1.3	Groupes cristallographiques et classes de cristaux . . . . .	3
<b>2</b>	<b>Finitude des classes de cristaux</b>	<b>6</b>
<b>3</b>	<b>Cohomologie de groupes et théorème de Bieberbach</b>	<b>9</b>
3.1	Cohomologie de degré 1 . . . . .	9
3.2	Cohomologie de degré 2 . . . . .	10
3.3	Théorème de Bieberbach . . . . .	12
<b>4</b>	<b>Classification</b>	<b>15</b>
4.1	Dimension 2 . . . . .	18
4.2	Des chiffres sur la dimension 3 . . . . .	21

# 1 Préliminaires

Dans toute cette partie,  $(E, \langle \cdot | \cdot \rangle)$  désigne un espace euclidien. On commence par quelques rappels sur les isométries de  $E$  et ses réseaux.

## 1.1 Isométries

On appelle *isométrie* de  $E$  toute bijection de  $E$  conservant la distance. On désigne, pour tout  $v \in E$ , par  $\tau_v$  la translation de vecteur  $v$ . L'ensemble des translations de  $E$  forme évidemment un groupe d'isométries de  $E$ , ainsi que le groupe des transformations orthogonales  $O(E)$ . La proposition suivante caractérise toutes les isométries de  $E$ .

**Proposition 1.1** *Soit  $\sigma$  une isométrie. Alors il existe un unique  $v \in E$  et un unique  $\varphi \in O(E)$  tels que  $\sigma = \tau_v \varphi$ .*

**Preuve** Il suffit de poser  $v = \sigma(0)$  et  $\varphi = \tau_{-v} \sigma$ . En effet, l'application  $\varphi$  ainsi définie conserve alors la distance (car  $\sigma$  le fait), puis la norme (car  $\varphi(0) = 0$ ), puis, par polarisation, le produit scalaire. On en déduit que  $\varphi$  est linéaire :

$$\langle \varphi(\lambda u + \mu v) | \varphi w \rangle = \langle \lambda u + \mu v | w \rangle = \lambda \langle \varphi u | \varphi w \rangle + \mu \langle \varphi v | \varphi w \rangle,$$

ce qui montre que  $\varphi(\lambda u + \mu v) - (\lambda \varphi u + \mu \varphi v)$  est à la fois dans l'espace engendré par l'image de  $\varphi$  et son orthogonal, donc est nul.  $\square$

L'unicité est évidente, et montre que  $\sigma \mapsto \varphi$  est bien définie ; on note alors  $\varphi = \vec{\sigma}$ , et on l'appelle *linéarisé* de  $\sigma$ . La formule

$$\sigma \tau_v \sigma^{-1} = \tau_{\vec{\sigma}(v)}$$

montre que la linéarisation est un homomorphisme. Remarquons de plus que  $\sigma$  est une translation si et seulement si son linéarisé est l'identité. Ainsi, on dispose d'une suite exacte :

$$E \xrightarrow{\tau} \text{Isom}(E) \rightarrow O(E).$$

De la même façon, soit  $G$  un groupe d'isométries. Notons  $L(G) = \{v \in E | \tau_v \in G\}$  son groupe de vecteurs de translation et  $\vec{G}$  l'image de  $G$  par linéarisation, appelée le *groupe ponctuel* de  $G$ . On a alors une suite exacte :

$$L(G) \hookrightarrow G \rightarrow \vec{G}.$$

## 1.2 Prérequis sur les réseaux euclidiens

On entend par *réseau* tout sous-groupe additif d'un espace de dimension  $n$  engendré par  $n$  vecteurs linéairement indépendants. Lorsque l'espace en question est euclidien,

on parle de *réseau euclidien*. Tous les réseaux ici sont euclidiens et on omettra donc la mention “euclidien”.

**Proposition 1.2** *Soit  $L$  un réseau (de  $E$ ). Tout ensemble borné de  $E$  contient un nombre fini de points de  $L$ .*

**Preuve** Soit  $(e_1, \dots, e_n)$  une base de  $L$  (i.e. une base de  $E$  qui engendre  $L$ ). Pour tout  $x \in E$ , on pose  $Q(x) = \left( \sum_{i=1}^n x_i^2 \right)^{1/2}$ , où les  $x_i$  sont les coefficients de  $x$  sur  $(e_i)_i$ . C’est une norme sur  $E$ , donc équivalente à la norme euclidienne. Une partie  $V$  bornée de  $E$  est donc aussi bornée pour  $Q$ , d’où il existe  $r > 0$  tel que pour tout  $x \in L \cap V$ ,

$$Q(x)^2 = \sum_{i=1}^n m_i^2 \leq r.$$

Mais les  $m_i$  sont entiers, d’où le résultat. □

Cette propriété de finitude est cruciale : si  $L$  est un réseau, on considère le groupe  $O(L)$  des automorphismes orthogonaux de  $E$  qui préservent  $L$ . Si  $B$  est une boule de rayon fini centrée en 0 qui contient une base de  $L$ , on constate alors, puisque tout automorphisme orthogonal conserve la norme, qu’il y a un nombre fini de choix pour les images respectives des éléments de cette base (puisque ces images sont encore dans  $L \cap B$ , fini). On a donc la propriété suivante :

**Proposition 1.3** *Soit  $L$  un réseau. Alors  $O(L) = \{\varphi \in O(E) \mid \varphi(L) = L\}$  est fini.*

### 1.3 Groupes cristallographiques et classes de cristaux

Soit  $G$  un sous-groupe de  $\text{Isom}(E)$ .

**Définition** On dit que  $G$  est *cristallographique* lorsque le groupe  $L(G)$  des vecteurs de translation de  $G$  forme un réseau de  $E$ . On appelle alors  $L(G)$  le *réseau de translations* de  $G$ , et  $T = \tau(L(G))$  le *sous-groupe des translations* de  $G$ .

Cette définition correspond bien à l’image intuitive qu’on a du groupe de symétrie d’un cristal (ou d’un pavage en dimension 2) régulier qui contient  $n$  translations linéairement indépendantes. On va voir qu’on peut classifier de manière mécanique tous ces groupes.

On suppose dans la suite que  $G$  est cristallographique et on note  $L$  son réseau de translation. Le sous-groupe des translations de  $G$  est particulier : il est caractérisé par des propriétés de théorie générale des groupes. Ces caractérisations seront utiles pour la suite.

**Proposition 1.4** *Avec ces notations,  $T$  est le plus grand sous-groupe abélien distingué de  $G$ . Il est isomorphe à  $\mathbf{Z}^n$ , est d’indice fini dans  $G$ , et  $C_G(T)$  (le commutant de  $T$  dans  $G$ ) est réduit à  $T$ .*

**Preuve** L'isomorphisme de  $T$  à  $\mathbf{Z}^n$  est clair par choix d'une base de  $L$ .

Remarquons que pour tout  $\varphi \in G$ ,  $\vec{\varphi}$  préserve  $L$ . En effet pour  $v \in L$ ,  $\varphi\tau_v\varphi^{-1} = \tau_{\vec{\varphi}v} \in G$ , d'où  $\vec{\varphi}v \in L$ . Ainsi  $T$  est distingué dans  $G$ . De plus, comme  $T$  est le noyau de la linéarisation,  $G/T$  est isomorphe à  $\vec{G}$ , qui, d'après la remarque et le paragraphe précédents, est fini. Ainsi  $T$  est d'indice fini dans  $G$ .

Soit  $\varphi \in G$  commutant avec tous les éléments de  $T$ . Donc pour tout  $v \in L$ , la relation  $\varphi\tau_v\varphi^{-1} = \tau_v$  donne que  $\vec{\varphi}v = v$ . Ceci vaut pour tout  $v \in L$ , donc sur une base de  $L$ , donc sur une base de  $E$  :  $\vec{\varphi} = \text{Id}$ , donc  $\varphi$  est une translation de  $G$ , donc dans  $T$ . Ceci montre que  $T = C_G(T)$ .

Enfin, soit  $R$  un sous-groupe abélien de  $G$  distingué dans  $G$ . Soit  $r \in R$ , et  $\rho$  son linéarisé : il s'agit de montrer que  $\rho = \text{Id}$ . Pour tout  $t \in T$ , on a alors  $s := trt^{-1} \in R$ . Comme  $R$  est abélien, cela entraîne que  $sr = rs$ . Ainsi, pour tout  $v \in L$ ,  $r(\tau_v r \tau_{-v}) = (\tau_v r \tau_{-v})r$ , d'où, en utilisant la relation de conjugaison d'une translation par un automorphisme, on tire :

$$\rho^2 v - 2\rho v + v = 0.$$

Ceci vaut pour tout  $v \in L$ , donc pour tout  $x \in E$  car  $L$  engendre  $E$ . Ainsi  $(\rho - \text{Id})^2 = 0$ . Mais  $\rho \in \text{O}(E)$ , et comme  $\ker(\rho - \text{Id})$  et  $\text{im}(\rho - \text{Id})$  sont supplémentaires dans  $E$  (connu), nécessairement  $\rho = \text{Id}$ , ou encore  $r \in T$ . Par suite  $R \subset T$ , ce qui termine la preuve.  $\square$

La principale conséquence de ce résultat est qu'étant donnés deux groupes cristallographiques  $G$  et  $H$ , tout isomorphisme de groupes entre eux envoie le sous-groupe de translations de  $G$  sur le sous-groupe de translations de  $H$ , puisque l'isomorphisme préserve les propriétés ci-dessus. Cela permettra de relever la restriction d'un isomorphisme de  $G$  sur  $H$  à  $L(G)$  par un isomorphisme de réseaux de  $L(G)$  sur  $L(H)$ , ce qui rendra de précieux services.

On a vu dans la preuve précédente qu'un groupe cristallographique normalise son réseau de translations. Réciproquement, étant donné un sous-groupe  $G < \text{Gl}(E)$ , on dit que  $G$  satisfait la condition de cristal lorsqu'existe un réseau stable sous  $G$ . D'après ce qui précède,  $G$  est alors nécessairement fini dès lors qu'il est orthogonal. De plus, lorsque  $G$  satisfait la condition de cristal, pour un réseau  $L$ , pour tout  $\sigma \in \text{Gl}(E)$ ,  $\sigma G \sigma^{-1}$  satisfait la condition de cristal pour le réseau  $\sigma(L)$ . Cette remarque nous amène à introduire les définitions suivantes :

**Définition** On appelle *cristal* tout couple  $(\Gamma, L)$  où  $L$  est un réseau et  $\Gamma$  un groupe linéaire fini qui stabilise  $L$ .

On considère l'ensemble des groupes orthogonaux finis vérifiant la condition de cristal : deux tels groupes sont dans la même classe géométrique s'ils sont conjugués dans  $\text{Gl}(E)$ . On appelle *classe géométrique de cristaux* (ou simplement classe géométrique) toute classe de conjugaison de sous-groupes finis de  $\text{O}(E)$  vérifiant la condition de cristal, et on note  $\mathcal{C}_g$  l'ensemble de ces classes.

Une *classe arithmétique de cristaux* est une classe de conjugaison de cristaux, c'est-à-dire l'ensemble des couples  $(a\Gamma a^{-1}, a(L))$  où  $a$  parcourt  $\text{Gl}(E)$  et où  $(\Gamma, L)$  est un cristal. On note  $\mathcal{C}_a$  l'ensemble de ces classes.

**Remarque** Ces deux notions ne coïncident pas, comme on le voit en considérant, dans le réseau  $L_q$  quadratique de dimension 2,  $A = \langle \sigma_1 \rangle$  et  $B = \langle \sigma_2 \rangle$  où  $\sigma_1$  et  $\sigma_2$  sont respectivement les symétries d'axe  $(0, 1)$  et  $(1, 1)$  : ces deux groupes sont clairement conjugués, donc dans la même classe géométrique, mais les cristaux  $(A, L_q)$  et  $(B, L_q)$  ne le sont pas. On peut donc très bien avoir plusieurs classes arithmétiques différentes dans la même classe géométrique. Cela se voit encore mieux avec la proposition 1.5.

On va avoir besoin de plusieurs classes de groupes finis qu'on introduit d'un coup ici :

**Définition** On note  $\mathcal{C}_{\mathbf{Z}}$ ,  $\mathcal{C}_{\mathbf{Q}}$ ,  $\mathcal{C}_{\mathbf{R}}$  les classes de conjugaison de sous-groupes finis de, respectivement,  $\text{Gl}_n(\mathbf{Z})$ ,  $\text{Gl}_n(\mathbf{Q})$  et  $\text{Gl}_n(\mathbf{R})$ . On impose également aux classes de  $\mathcal{C}_{\mathbf{R}}$  de conserver un réseau.

**Proposition 1.5** *L'ensemble  $\mathcal{C}_a$  est aussi l'ensemble des classes de conjugaison de sous-groupes finis de  $\text{Gl}_n(\mathbf{Z})$ . Autrement dit  $\mathcal{C}_a \simeq \mathcal{C}_{\mathbf{Z}}$ .*

**Preuve** À tout cristal  $(\Gamma, L)$ , on associe un sous-groupe fini  $G$  de  $\text{Gl}_n(\mathbf{Z})$  formé par l'ensemble des matrices des éléments de  $\Gamma$  dans une base  $\mathcal{B}$  de  $L$  (qui sont bien à coefficients entiers puisque  $\Gamma$  stabilise  $L$ ). Si on choisit une autre base  $\mathcal{B}'$  de  $L$ , on obtient alors un autre sous-groupe fini de  $\text{Gl}_n(\mathbf{Z})$ , disons  $G'$ . Mais alors  $G$  et  $G'$  sont conjugués dans  $\text{Gl}_n(\mathbf{Z})$ . En effet, si  $h$  désigne l'automorphisme de passage entre les deux bases, la matrice  $H$  de  $h$  dans  $\mathcal{B}$  est à coefficients entiers puisque  $h(L) = L$ . De plus, on a alors  $G = HG'H^{-1}$ .

Avec les notations précédentes, on a donc montré que l'application

$$\chi : \mathcal{C}_a \rightarrow \mathcal{C}_{\mathbf{Z}}, [(\Gamma, L)] \mapsto [G]$$

est bien définie. On va montrer qu'elle est bijective.

La surjectivité est claire puisqu'à toute classe de conjugaison  $c$  de  $\text{Gl}_n(\mathbf{Z})$  correspond la classe de cristaux  $\{(hgh^{-1}, h(\mathbf{Z}^n)) \mid g \in c, h \in \text{Gl}(E)\}$ .

Remarquons que dans chaque classe de cristaux existe un représentant de la forme  $(\Gamma, \mathbf{Z}^n)$ , obtenu en conjuguant un cristal par l'automorphisme envoyant une base de son réseau sur une base de  $\mathbf{Z}^n$ .

Considérons à présent deux tels représentants  $(\Gamma_1, \mathbf{Z}^n)$  et  $(\Gamma_2, \mathbf{Z}^n)$ . L'application  $\chi$  envoie alors ces cristaux sur les classes de conjugaisons dans  $\text{Gl}_n(\mathbf{Z})$  des sous-groupes formés des matrices de  $\Gamma_1$  et  $\Gamma_2$  dans la base canonique. Si ces dernières classes coïncident, c'est qu'il y a une conjugaison entière entre ces deux sous-groupes. La matrice opérant cette conjugaison définit alors un automorphisme stabilisant  $\mathbf{Z}^n$ , ce qui, vu la définition de conjugaison de cristaux, nous dit exactement que les cristaux sont conjugués, donc qu'on a affaire à une seule classe de cristaux. Cela montre que  $\chi$  est bijective.  $\square$

Ainsi, il y a plus de classes arithmétiques que de classes géométriques. On va montrer dans la partie suivante qu'en plus,  $\mathcal{C}_g \simeq \mathcal{C}_{\mathbf{Q}}$  ce qui justifie *a posteriori* les noms "arithmétique" et "géométrique".

Il est alors intéressant de se demander combien il y a de classes de cristaux de  $E$ . En réalité, il y en a toujours un nombre fini.

## 2 Finitude des classes de cristaux

Le but de cette section est de montrer le résultat ci-après.

**Théorème 2.1 (Finitude des classes de cristaux)** *Les classes géométriques  $\mathcal{C}_g$  de cristaux sont en nombre fini et  $|\mathcal{C}_g| \leq |\mathcal{C}_a|$ .*

Montrer que  $\mathcal{C}_a$  est fini est beaucoup plus difficile, on peut en trouver une preuve dans [3], où l'on montre que  $\mathcal{C}_{\mathbf{Z}}$  est fini.

On s'appuiera sur ce résultat dans la partie 3 mais on ne l'admet pas ici. En effet il implique trivialement la finitude de  $\mathcal{C}_g$ .

On va voir dans la partie suivante qu'il n'y a en fait qu'un nombre fini de classes de conjugaisons affines de groupes cristallographiques associés à chaque classe de  $\mathcal{C}_a$ , donc un nombre fini de groupe cristallographiques à conjugaison affine près.

Pour prouver le théorème 2.1 nous allons caractériser  $\mathcal{C}_a$  et  $\mathcal{C}_g$  comme des classes de conjugaisons de différents groupes linéaires. Le schéma de la preuve est le suivant :

$$\mathcal{C}_a \xrightarrow{\sim} \mathcal{C}_{\mathbf{Z}} \twoheadrightarrow \mathcal{C}_{\mathbf{Q}} \xrightarrow{\sim} \mathcal{C}_{\mathbf{R}} \xleftarrow{\sim} \mathcal{C}_g$$

**Lemme 2.2** *Soit  $G$  un sous-groupe fini de  $\mathrm{Gl}(E)$ . Il existe sur  $E$  un produit scalaire invariant sous  $G$ , c'est-à-dire rendant  $G$  orthogonal pour la structure euclidienne induite.*

**Preuve** Voici une formule qui convient :

$$\langle x|y \rangle_G := \sum_{g \in G} \langle gx|gy \rangle.$$

□

**Lemme 2.3** *Étant donnés deux morphismes de  $G$  dans  $\mathrm{O}(E)$ , s'il existe un isomorphisme  $G$ -invariant, alors il existe une isométrie  $G$ -invariante.*

**Preuve** Soit  $g : E \rightarrow E$  un isomorphisme  $G$ -invariant. Soit  $f = (g^{-1})^*g^{-1}$ . On vérifie que  $f$  est un endomorphisme symétrique positif de  $E$ ,  $G$ -invariant. Soit  $r$  sa racine carrée. Elle est aussi  $G$ -invariante, et on a la relation :

$$\forall x \in E \quad \forall y \in E \quad \langle rx|ry \rangle = \langle g^{-1}x|g^{-1}y \rangle.$$

Cela montre que  $rg$  convient.

□

En munissant  $E$  d'une nouvelle structure euclidienne, on constate que les groupes orthogonaux respectifs sont conjugués par l'automorphisme de passage d'une base orthonormée pour une structure à une base orthonormée pour l'autre structure. Donc, tout sous-groupe fini de  $\text{Gl}(E)$  est conjugué à un sous-groupe fini de  $\text{O}(E)$ . Nous pouvons alors prouver le

**Théorème 2.4** *L'injection  $\text{O}(E) \hookrightarrow \text{Gl}(E)$  induit une bijection sur les classes de conjugaison de sous-groupes finis. En particulier,  $\mathcal{C}_{\mathbf{R}} \simeq \mathcal{C}_g$ .*

**Preuve** Il suffit donc de prouver que si  $G$  et  $G'$  sont deux sous-groupes finis orthogonaux conjugués dans  $\text{Gl}(E)$ , ils le sont déjà dans  $\text{O}(E)$ . Soit donc  $g \in \text{Gl}(E)$  tel que  $gGg^{-1} = G'$ . En considérant les morphismes  $G \rightarrow \text{O}(E)$  donnés par l'inclusion et la conjugaison par  $g$ , le lemme précédent permet de trouver un automorphisme orthogonal  $G$ -invariant, i.e. vérifiant :

$$\forall \gamma \in G \quad f\gamma = g\gamma g^{-1}f.$$

Mais cela se réécrit :

$$\forall \gamma \in G \quad f\gamma f^{-1} = g\gamma g^{-1}.$$

En particulier,  $G' = fGf^{-1}$ , ce qui termine la preuve.  $\square$

**Théorème 2.5** *Soit  $K \hookrightarrow L$  une extension de corps de caractéristique nulle. Si deux sous-groupes finis de  $\text{Gl}_n(K)$  sont conjugués dans  $\text{Gl}_n(L)$  alors ils le sont dans  $\text{Gl}_n(K)$ .*

**Preuve** Soient  $H$  et  $H'$  deux sous-groupes finis de  $\text{Gl}_n(K)$  conjugués dans  $\text{Gl}_n(L)$ . Regardons  $H$  et  $H'$  comme deux représentations d'un groupe  $G$  dans  $\text{Gl}_n(L)$ . Elles sont conjuguées dans  $\text{Gl}_n(L)$  et ont donc même caractère  $\chi$ . Cependant  $\chi$  ne dépend pas du corps dans lequel il est calculé.  $H$  et  $H'$  ont donc le même caractère dans  $\text{Gl}_n(K)$  et sont donc conjugués dans  $\text{Gl}_n(K)$ .  $\square$

**Proposition 2.6** *Tout sous-groupe fini  $G \subset \text{Gl}_n(\mathbf{Q})$  conserve un réseau. Autrement dit, on a bien une flèche  $\mathcal{C}_{\mathbf{Q}} \rightarrow \mathcal{C}_{\mathbf{R}}$ .*

**Preuve** Posons

$$L = \sum_{\gamma \in G} \gamma(\mathbf{Z}^n)$$

qui est évidemment stable par  $G$ . Prenons  $q \in \mathbf{N}$  tel que :  $q\gamma \in \text{Gl}_n(\mathbf{Z}) \forall \gamma \in G$ . On a alors  $q^{-1}\mathbf{Z}^n \supseteq L \supseteq \mathbf{Z}^n$  donc  $L$ , sous-module d'un module libre sur l'anneau principal  $\mathbf{Z}$ , et d'autre part de rang  $n$ , est bien un réseau.  $\square$

**Proposition 2.7** *Tout sous-groupe fini  $G$  de  $\text{Gl}_n(\mathbf{R})$  conservant un réseau est conjugué à un sous-groupe fini de  $\text{Gl}_n(\mathbf{Z})$ .*

**Preuve** Il suffit de prendre une base de  $L$  et de remarquer que les matrices de  $G$  dans cette base sont à coefficients entiers, et sont bien sûr inversibles dans  $\text{Gl}_n(\mathbf{Z})$ .  $\square$



**Remarque** En fait, on vient de montrer la surjectivité de la flèche  $\mathcal{C}_{\mathbf{Z}} \rightarrow \mathcal{C}_{\mathbf{R}}$ . Or,  $\mathcal{C}_{\mathbf{Q}} \rightarrow \mathcal{C}_{\mathbf{R}}$  est injective, donc bijective. On a alors  $\mathcal{C}_{\mathbf{Q}} \simeq \mathcal{C}_{\mathbf{R}}$  et  $\mathcal{C}_{\mathbf{Z}} \xrightarrow{\sim} \mathcal{C}_{\mathbf{Q}}$ .

Maintenant qu'on a établi le diagramme plus haut, il reste à montrer la finitude de  $\mathcal{C}_{\mathbf{Z}}$  et  $\mathcal{C}_{\mathbf{Q}}$ . Dans le cas de  $\mathcal{C}_{\mathbf{Z}}$  c'est un résultat fort qu'on ne peut démontrer ici. On peut cependant montrer que  $\mathcal{C}_{\mathbf{Q}}$  est fini avec des outils élémentaires comme suit.

On va commencer par montrer qu'il y a, à isomorphisme près, un nombre fini de sous-groupes de  $\mathrm{Gl}_n(\mathbf{Z})$ . La pierre angulaire de ce résultat est le théorème suivant.

On suppose ici  $p \geq 3$  premier. On va montrer que la projection  $\mathrm{Gl}_n(\mathbf{Z}) \rightarrow \mathrm{Gl}_n(\mathbf{F}_p)$  induit une bijection sur les sous-groupes finis. Plus précisément :

**Théorème 2.8 (Minkowski)** *La flèche  $\mathrm{Gl}_n(\mathbf{Z}) \rightarrow \mathrm{Gl}_n(\mathbf{F}_p)$  (pour  $p$  premier impair) a un noyau sans torsion, qui ne contient donc pas d'élément d'ordre fini.*

**Preuve** Soit  $X$  dans le noyau et écrivons  $X = I_n + pV$ . Supposons par l'absurde que  $X$  admette un ordre fini  $m$  et que  $V$  soit non nul. Notons  $m = \prod q^{v_q(m)}$  et soit  $q_0$  tel que  $v_{q_0}(m) > 0$ . On voit donc, si  $k = \frac{n}{v_{q_0}(m)-1}$ , que  $X^k$  est d'ordre  $q_0$ . On suppose donc sans restriction que  $m$  est premier. On suppose de plus sans restriction que les coefficients de  $V$  sont premiers entre eux (sinon remplacer  $V$  par  $dV$  dans le calcul ci-dessous n'influe en rien le résultat)

La relation  $X^m = I_n$  donne :

$$\sum_{j=1}^m \binom{m}{j} p^j V^j = 0.$$

D'où

$$mV + \binom{m}{2} pV^2 + \sum_{j=1}^{m-1} \binom{m}{j+1} p^j V^{j+1} = 0.$$

On en déduit que  $p$  divise chacun des coefficients de  $mV$ . Si  $p$  ne divise pas  $m$ , il divise tous les coefficients de  $V$  ce qui n'est pas, par hypothèse. Donc  $p$  divise  $m$ , puis  $p = m$ . Par suite  $m \geq 3$  et en divisant la relation ci-dessus par  $m$ , et en remarquant que  $m$  divise  $\binom{m}{2}$  (c'est un nombre premier impair), nécessairement  $m$  divise encore tous les coefficients de  $V$ . Cela est absurde, et cette contradiction termine la preuve.  $\square$

Le groupe (fini)  $\mathrm{Gl}_n(\mathbf{F}_3)$  ne contient qu'un nombre fini de sous-groupes, et parmi eux, tous les types d'isomorphie de sous-groupes finis de  $\mathrm{Gl}_n(\mathbf{Z})$ , qui sont donc en nombre fini.

Nous pouvons désormais prouver le résultat principal de cette section.

### Preuve du théorème 2.1

Considérons l'application qui, à une classe de conjugaison de sous-groupes finis de  $\mathrm{Gl}_n(\mathbf{Q})$ , associe sa classe d'isomorphisme dans  $\mathrm{Gl}_n(\mathbf{Z})$ . Cette application est bien définie

car dans chaque classe existe au moins un sous-groupe de  $\text{Gl}_n(\mathbf{Z})$  d'après la proposition 2.6, et comme groupes conjugués, tous les éléments d'une même classe sont isomorphes. Le nombre de classes d'isomorphismes en question est fini comme le montre le théorème 2.5.

De plus, elle est à fibre finie, car les classes de conjugaisons de  $\text{Gl}_n(\mathbf{Q})$  de type  $G < \text{Gl}_n(\mathbf{Z})$  sont les représentations non-isomorphes de  $G$  dans  $\text{Gl}_n(\mathbf{Q})$ . Il y en a moins que de représentations complexes non-isomorphes de  $G$  par le théorème 2.7, qui sont en nombre fini.  $\square$

### 3 Cohomologie de groupes et théorème de Bieberbach

Tout groupe cristallographique  $G$  s'insère dans une suite exacte du type :

$$L \hookrightarrow G \twoheadrightarrow \overrightarrow{G}$$

où  $L = T_G$  est son réseau de translations.

Pour classifier et comprendre ces groupes il s'agit donc de connaître les sous-groupes finis de  $O(E)$  conservant un réseau  $L$  et de pouvoir énumérer, étant donné un tel sous-groupe  $\Gamma$ , tous les groupes cristallographiques s'insérant au milieu de la suite exacte  $L \hookrightarrow ? \twoheadrightarrow \Gamma$ .

Ce travail, appelé *classification des extensions de  $L$  par  $\Gamma$*  se fait en utilisant la *cohomologie de groupes*. Dans le cadre qui nous intéresse on a seulement besoin d'une partie simple de cette théorie (uniquement jusqu'à l'ordre 2). De plus, les extensions de  $L$  par  $\Gamma$  dépendent, dans le cas général, d'une action de  $\Gamma$  sur  $L$ . Elle est ici fixée car tous nos groupes sont inclus dans  $\text{Aff}(E)$ . Réciproquement, fixer l'action nous assure que toutes nos extensions sont effectivement plongeables dans  $\text{Aff}(E)$ .

#### 3.1 Cohomologie de degré 1

Dans toute la suite on suppose que  $\Gamma$  est un groupe fini et  $M$  un  $\Gamma$ -module, à savoir, comme dit plus haut, que l'action de  $\Gamma$  sur  $M$  est fixée. Nous allons donner une description explicite de  $H^1(\Gamma, M)$  et montrer qu'il caractérise, entre autres, les automorphismes d'extensions de  $M$  par  $\Gamma$ .

**Définition** Soit  $s$  une application de  $\Gamma \rightarrow M$ . On dit que  $s$  est un *(1-)cocycle* si, pour  $\alpha, \beta \in \Gamma$ , on a :

$$s(\alpha\beta) = s(\alpha) + \alpha \cdot s(\beta)$$

On note  $Z(\Gamma, M)$  l'ensemble des cocycles. On dit de plus que  $s$  est un *cobord* s'il s'écrit  $s(\alpha) = k - \alpha \cdot k$  pour  $k \in M$  fixé. L'ensemble des cobords est noté  $B(\Gamma, M)$ .

Enfin, on pose  $H^1(\Gamma, M) = Z(\Gamma, M)/B(\Gamma, M)$

**Définition** Soit  $M \hookrightarrow E_1 \twoheadrightarrow \Gamma$  et  $M \hookrightarrow E_2 \twoheadrightarrow \Gamma$  deux extensions de  $M$  par  $\Gamma$ . On dit que  $\varphi : E_1 \rightarrow E_2$  est un *morphisme d'extensions* s'il rend le diagramme suivant

commutatif :

$$\begin{array}{ccc}
 & E_1 & \\
 \nearrow & \downarrow \varphi & \searrow \\
 M & & \Gamma \\
 \searrow & & \nearrow \\
 & E_1 &
 \end{array}$$

Une des utilités de  $H^1$  est qu'il classifie les différentes sections – à conjugaison par un élément de  $M$  près –  $\sigma : \Gamma \rightarrow G$  donnant lieu au (seul) produit semi-direct  $M \rtimes \Gamma$  respectant l'action. Cela est équivalent à classifier les automorphismes d'extension de  $M \rtimes \Gamma$ .

**Proposition 3.1** *Fixons  $M \hookrightarrow E = M \rtimes \Gamma \twoheadrightarrow \Gamma$  une extension scindée.  $H^1(\Gamma, M)$  est en bijection avec les automorphismes d'extension de  $E \rightarrow E$  lorsqu'ils sont considérés à conjugaison par un élément de  $M$  près.*

**Preuve** Soit  $\varphi$  un automorphisme de  $E$  qui respecte l'extension. On a  $\varphi(gM) = gM$  pour tout  $g \in E$ . Donc,  $s(g) = g^{-1}\varphi(g) \in M$ . L'extension étant scindée on peut considérer que  $\Gamma \subset E$ . Le fait que  $\varphi$  est l'identité sur  $M$  et un automorphisme implique que  $s$  est un 1-cocycle de  $\Gamma \rightarrow M$ .

Si maintenant  $s$  est un cobord, l'automorphisme associé s'écrit :  $\varphi(\gamma) = \gamma s(\gamma) = \gamma\gamma^{-1}k^{-1}\gamma k = k^{-1}\gamma k$ . Donc  $\varphi$  est une conjugaison par un élément  $k \in M$ .  $\square$

Autrement dit,  $H^1(\Gamma, M)$  mesure l'obstruction à ce que, dans une extension scindée de  $M$  par  $\Gamma$ , tout automorphisme d'extension soit intérieur. Dans le cas où l'extension n'est pas scindée,  $H^1$  agit quand-même transitivement sur de tels automorphismes.

### 3.2 Cohomologie de degré 2

Il existe une description de  $H^2$  analogue à celle de  $H^1$  en termes de 2-cocycles.

**Définition** Un 2-cocycle est une application de  $\Gamma \times \Gamma \rightarrow M$  vérifiant l'axiome suivant :

$$s(g_1g_2, g_3) = g_1 \cdot s(g_2, g_3) + s(g_1, g_2g_3) - s(g_1, g_2)$$

et on dit que c'est un cobord si, pour  $s' : \Gamma \rightarrow M$ , on peut écrire

$$s(\alpha, \beta) = s'(\alpha\beta) - \alpha s'(\beta) - s'(\alpha)$$

pour tous les  $\alpha, \beta \in \Gamma$ . De même qu'en degré 1,  $H^2$  est le quotient des 2-cocycles par les 2-cobords.

Le résultat suivant, fondamental, décrit l'information contenue dans  $H^2$ . On ne donne pas la preuve.

**Théorème 3.2**  $H^2(\Gamma, M)$  *classifie les extensions de  $M$  par  $\Gamma$  à isomorphisme d'extension près.*

**Preuve** Voir [2] □

**Corollaire 3.3** *Si  $H^2(\Gamma, M) = 0$ , toute extension de  $M$  par  $\Gamma$  est scindée.*

**Preuve** Il existe au moins une extension scindée, celle où l'on choisit comme action de  $\Gamma$  sur  $M$  précisément celle de la structure de  $M$  comme  $\Gamma$ -module. Si  $H^2 = 0$ , toutes les extensions sont isomorphes, donc scindées en remontant la section que l'on vient de décrire. □

On a dans ce cas, à isomorphisme près, un seul produit semi-direct. Encore une fois, c'est le cas car on a déjà fixé l'action de  $G$  sur  $M$ .

On aura également besoin du résultat fondamental suivant :

**Théorème 3.4** *Les groupes de cohomologie de  $\Gamma$  sont annulés par  $|\Gamma|$  :*

$$|\Gamma|H^n(\Gamma, M) = 0$$

*En particulier, si la multiplication par  $|\Gamma|$  est bijective dans  $M$ , alors  $H^n(\Gamma, M) = 0$  pour  $n \geq 1$ .*

**Preuve** On ne le prouve que pour  $n = 1$  par un argument de moyenne.

Soit  $s \in Z(\Gamma, M)$ , calculons :

$$\sum_{\gamma \in \Gamma} s(\gamma) = \sum_{\gamma \in \Gamma} s(\alpha\gamma) = |\Gamma|s(\alpha) + \alpha \sum_{\gamma \in \Gamma} s(\gamma)$$

pour  $\alpha \in \Gamma$ . Donc, avec  $k = \sum_{\gamma} s(\gamma)$ , on obtient :  $|\Gamma|s(\alpha) = k - \alpha k$ . Si la multiplication par  $|\Gamma|$  est bijective,  $s$  est bien un cobord. On a alors enfin,  $H^1(\Gamma, M) = 0$ . □

La raison pour laquelle  $H^2$  n'apparaît que très peu dans la suite est que, dans notre cas, on peut en fait le retrouver dans un objet plus simple. La suite exacte ci-après ne sert pas directement dans la preuve du théorème de Bieberbach mais est primordiale pour la classification de nos groupes.

**Proposition 3.5** *La suite*

$$\dots \rightarrow H^k(G, L) \rightarrow H^k(G, E) \rightarrow H^k(G, E/L) \rightarrow H^{k+1}(G, L) \rightarrow \dots$$

*est exacte. En particulier, si  $E$  est un espace vectoriel,  $H^1(G, E/L) \simeq H^2(G, L)$ .*

**Preuve** C'est le lemme du serpent (résultat connu d'algèbre homologique qu'on admettra ici) appliqué à la suite exacte de  $\Gamma$ -modules  $F(\Gamma, L) \hookrightarrow F(\Gamma, E) \twoheadrightarrow F(\Gamma, E/L)$ . □

### 3.3 Théorème de Bieberbach

La première utilisation que nous allons faire de la cohomologie de groupes est dans la preuve du résultat suivant :

**Théorème 3.6 (de Bieberbach)** *Tout isomorphisme abstrait de groupes cristallographiques se réalise par conjugaison affine.*

Pour cette preuve nous allons affaiblir temporairement la définition de groupe cristallographique pour introduire la notion de groupe cristallographique affine pour lesquels  $\text{Aff}(E)$  joue le rôle de  $\text{Isom}(E)$ . Le résultat suivant nous assure que nous pouvons travailler avec cette plus grande classe de groupes :

**Lemme 3.7** *Tout groupe cristallographique affine est conjugué dans  $\text{Aff}(E)$  à un groupe cristallographique.*

**Preuve** Soit  $G$  un groupe cristallographique affine. D'après (2.4) il existe un  $\alpha \in \text{Gl}(E)$  tel que  $\alpha \overrightarrow{G} \alpha^{-1} \subset \text{O}(E)$ . Soit  $\sigma = \tau\beta \in G$  avec  $\tau$  une translation et  $\beta \in \text{Gl}(E)$ . On a  $\alpha\tau\alpha^{-1}\alpha\beta\alpha^{-1} \in \text{Isom}(E)$ . D'où  $\alpha G \alpha^{-1} \subset \text{Isom}(E)$ .  $\square$

Passons au théorème de Bieberbach. Prenons  $G_1, G_2$  deux groupes cristallographiques et  $\Phi : G_1 \rightarrow G_2$  un isomorphisme. Pour démontrer le théorème 3.6, à savoir que  $\Phi$  est en fait une conjugaison affine, on commence par conjuguer  $G_1$  de manière à se ramener au cas où  $L_{G_1} = L_{G_2}$ ,  $\overrightarrow{G_1} = \overrightarrow{G_2}$  et  $\Phi$  est un isomorphisme d'extension. C'est possible grâce à la courte discussion qui suit et au lemme 3.8. Ceci étant fait, on est alors exactement dans les hypothèses du théorème 3.9 qui nous dit que  $\Phi$  est bien une conjugaison affine.

On a déjà vu plus haut que tout isomorphisme  $\Phi$  de groupes cristallographiques induit un isomorphisme  $\varphi$  entre leurs réseaux de translations par la formule

$$\Phi(\tau_v) = \tau_{\varphi v}.$$

On sait que  $\varphi = \Phi_{/L_{G_1}} : L_{G_1} \rightarrow L_{G_2}$  et est un isomorphisme de réseau, qu'on peut prolonger à  $E$ . Donc, quitte à conjuguer  $G_1$ , on peut se ramener au cas où  $L_{G_1} = L_{G_2}$  et  $\varphi = \Phi_{/L} = \text{Id}$ . On va montrer qu'en fait, dans ce cas,  $\overrightarrow{\Phi} = \text{Id}$ .

**Lemme 3.8** *Soient  $G_1, G_2$  deux groupes cristallographiques tels que  $L = L_{G_1} = L_{G_2}$  et  $\Phi : G_1 \rightarrow G_2$  un isomorphisme dont la restriction à  $L$  est l'identité. Dans ce cas,  $\overrightarrow{G_1} = \overrightarrow{G_2} = \Gamma$ . De plus, le morphisme induit sur le quotient  $\overrightarrow{\Phi} : \Gamma \rightarrow \Gamma$  est l'identité. Autrement dit,  $\varphi$  est alors un morphisme d'extension de  $G_1$  dans  $G_2$ .*

**Preuve** Soit  $\alpha \in \overrightarrow{G_1}$  et  $\tau \in L$ , il faut d'abord vérifier la compatibilité suivante :

$$\varphi(\alpha \cdot \tau) = \overrightarrow{\Phi}(\alpha) \cdot \tau$$

où l'action de gauche et de droite sont les actions respectives de  $\overrightarrow{G_1}$  et  $\overrightarrow{G_2}$  sur  $L$ .

Les actions sur  $L$  s'écrivent avec des sections ensemblistes  $s_i : \overrightarrow{G}_i \rightarrow G_i$  :

$$\alpha \cdot \tau = s_i(\alpha)\tau s_i(\alpha)^{-1} \in L$$

d'où :

$$\varphi(\alpha \cdot \tau) = \varphi(s_1(\alpha))\tau\varphi(s_1(\alpha))^{-1}$$

or  $\overrightarrow{\varphi(s_1(\alpha))} = \overrightarrow{\varphi}(\alpha)$  donc  $s_2(\overrightarrow{\varphi}(\alpha)) = \varphi(s_1(\alpha)) \pmod L$ , puis :

$$\varphi(\alpha \cdot \tau) = s_2(\overrightarrow{\varphi}(\alpha))\tau s_2(\overrightarrow{\varphi}(\alpha))^{-1}$$

Pour conclure on regarde  $\overrightarrow{G}_1$  et  $\overrightarrow{G}_2$  comme sous-groupes de  $\text{Gl}(E)$  agissant sur  $L$ . Ces deux actions sont libres et compatibles car induites par l'action de  $\text{Gl}(E)$  sur  $L$ . Or, pour tout  $\tau \in L$ ,

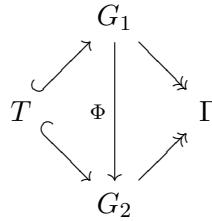
$$\alpha \cdot \tau = \varphi(\alpha \cdot \tau) = \overrightarrow{\varphi}(\alpha) \cdot \tau$$

On a donc  $\alpha = \overrightarrow{\varphi}(\alpha)$ . □

Il est donc possible de se ramener au cas où  $\Phi$  est un isomorphisme d'extension. On termine par le théorème suivant, qu'on pourrait appeler version "faible" de Bieberbach et qui permet de conclure sous ces hypothèses.

**Théorème 3.9** Soient  $G_1, G_2$  deux groupes cristallographiques vérifiant  $T_{G_1} = T_{G_2}$  et  $\overrightarrow{G}_1 = \overrightarrow{G}_2$ , ainsi que  $\Phi : G_1 \rightarrow G_2$  un isomorphisme vérifiant que  $\Phi|_T = \text{Id}$  et  $\overrightarrow{\Phi} = \text{Id}$ . Alors,  $\Phi$  est une conjugaison par une translation de  $E$ .

**Preuve** On est dans la situation suivante :



où on a posé  $T = T_{G_1} = T_{G_2}$  et  $\Gamma = \overrightarrow{G}_1 = \overrightarrow{G}_2$ .

De plus nos deux extensions se plongent dans  $\text{Aff}(E)$  :

$$\begin{array}{ccccc}
 T \hookrightarrow & G_1 \text{ ou } G_2 & \twoheadrightarrow & \Gamma & \\
 \downarrow & \downarrow & & \downarrow & \\
 E \hookrightarrow & \text{Aff}(E) = E \rtimes \text{O}(E) & \twoheadrightarrow & \text{O}(E) & 
 \end{array}$$

Posons  $X$  la préimage de  $\Gamma$  par la flèche quotient  $\text{Aff}(E) \twoheadrightarrow \text{O}(E)$ . On a l'extension de  $E$  par  $\Gamma$  suivante :

$$E \hookrightarrow X \twoheadrightarrow \Gamma$$

où on peut supposer que  $G_1, G_2 \subset X$ .  $X$  est ici, si on le regarde dans  $\text{Aff}(E)$ , simplement le produit  $E \cdot \Gamma$ .

On peut prolonger  $\Phi$  en un automorphisme d'extension  $\tilde{\Phi} : X \rightarrow X$ . Cela se vérifie à la main, mais vient surtout du fait que  $X$  est le *pushout* (voir la remarque plus bas) par  $V$  de  $L \hookrightarrow G_1 \twoheadrightarrow \Gamma$  et que cette construction est unique à isomorphisme près.

On a alors :

$$\begin{array}{ccc}
 & X & \\
 \nearrow & & \searrow \\
 E & & \Gamma \\
 \searrow & & \nearrow \\
 & X & 
 \end{array}$$

$\tilde{\Phi}$  est inscrit sur la flèche verticale descendante.

Or,  $E$  étant un espace vectoriel,  $x \mapsto |\Gamma|x$  est une bijection, on a donc  $H^1(\Gamma, E) = H^2(\Gamma, E) = 0$ .

L'extension  $X$  est alors scindée, et de plus, tout automorphisme est une conjugaison par un élément de  $E$  (à savoir ici une translation). On a alors que  $\tilde{\Phi}$  est une conjugaison affine, et que c'est également le cas de  $\Phi$  qui est la restriction de  $\tilde{\Phi}$  à  $G_1$ .  $\square$

On voit bien au cours de la preuve que les résultats proviennent du fait qu'on a pu regarder nos extensions comme plongées dans une extension plus grande pour laquelle la fibre était plus simple cohomologiquement parlant (ici un espace vectoriel).

**Remarque** (*Pushout*) Lorsque l'on est dans la situation suivante :

$$\begin{array}{ccccc}
 M & \hookrightarrow & G & \twoheadrightarrow & \Gamma \\
 f \downarrow & & & & \\
 M' & & & & 
 \end{array}$$

où la ligne est exacte, il existe  $\xi$ , qu'on note aussi parfois  $f_*G$ , tel que le diagramme suivant commute et que les lignes soient exactes.

$$\begin{array}{ccccc}
 M & \hookrightarrow & G & \twoheadrightarrow & \Gamma \\
 f \downarrow & & \downarrow & & \parallel \\
 M' & \hookrightarrow & \xi & \twoheadrightarrow & \Gamma
 \end{array}$$

Cette opération correspond à changer la fibre au dessus des éléments de  $\Gamma$  de  $M$  à  $M'$ . Sa structure est celle du produit fibré entre  $G$  et  $M'$  au dessus de  $M$ .

La définition exacte de  $\xi$  est la suivante :

$$\xi = M' \rtimes G / \{(f(a), -\iota(a)) \mid a \in M\}$$

On peut démontrer le théorème précédent en utilisant très largement la propriété universelle du *pushout* :

Pour tout  $X$  muni de deux flèches  $z : G \rightarrow X$  et  $x : M' \rightarrow X$  faisant commuter le diagramme précédent et vérifiant, pour  $g \in G$  et  $m \in M'$ ,

$$z(g)x(m)z(g)^{-1} = x(f(g) \cdot f(m))$$

il existe alors un unique  $\xi \rightarrow X$  faisant commuter le grand diagramme.

## 4 Classification

Déterminer tous les groupes cristallographiques à dimension fixée nécessite pour commencer de connaître toutes les classes de cristaux de cette dimension. À savoir, les couples  $(L, \Gamma)$  où  $\Gamma \subset O(E)$  laisse le réseau  $L$  stable.

Il reste ensuite à trouver les classes de conjugaison (affine) d'extensions de  $M$  par  $\Gamma$ .

**Proposition 4.1** *Les classes de conjugaison affines de groupes cristallographiques dans la classe de cristal  $(L, \Gamma)$  sont en bijection avec l'ensemble quotient*

$$H^1(\Gamma, E/L) / N_{\text{Gl}(L)}(\Gamma)$$

où

$$N_{\text{Gl}(L)}(\Gamma) = \{\sigma \in \text{Gl}(L) \mid \sigma\Gamma\sigma^{-1} = \Gamma\}$$

agit de la manière suivante sur  $H^1$  :

$$\sigma \cdot s(\alpha) = \sigma s(\sigma\alpha\sigma^{-1})$$

**Preuve** Moralement, ce résultat vient du fait que  $H^2(\Gamma, L)$  classe les extensions de  $\Gamma$  par  $L$  à conjugaison par un élément de  $E$  près. En effet, si deux extensions sont isomorphes, elles sont, comme on l'a vu dans la preuve du théorème de Bieberbach, conjuguées par une translation. Si deux extensions sont conjuguées par une transformation affine, elle conserve  $L$  et est dans  $N(\Gamma)$ . Le passage de  $H^2$  à  $H^1$  vient de la suite exacte de la proposition 3.5.

Ici, on peut donner une description *ad hoc* de la bijection en se plongeant dans  $\text{Aff}(E)$  (en réalité  $\Gamma \rtimes E$  suffit). Étant donné  $s \in H^1(\Gamma, E/L)$  et  $\tilde{s}$  un relèvement quelconque de  $s$  dans  $E$ , on peut construire :

$$G_s = \{\tau_u \tau_{\tilde{s}(\alpha)} \alpha \mid u \in L, \alpha \in \Gamma\} \subset \text{Aff}(E)$$

Étant donné la définition de  $G_s$ , elle ne dépend pas du choix de  $\tilde{s}$  ce qui justifie la notation. On a alors

$$s \mapsto G_s : Z(\Gamma, E/L) \rightarrow \{\text{extensions de } L \text{ par } \Gamma\}$$



qui est de plus une bijection. En effet, si  $\alpha \in \Gamma$ , il existe un  $s(\alpha) \in E/L$  tel que  $\tau_{s(\alpha)}\alpha \in G$ . Un  $s$  défini de cette manière est bien un cocycle donc  $G = G_s$ . C'est donc bien une surjection. L'injectivité vient du fait qu'étant dans un produit semi-direct, on peut identifier les termes translatifs et linéaires, on a alors, pour  $G_{\tilde{s}} = G_{\tilde{s}'}$ ,  $\tilde{s} - \tilde{s}' \in L$ , donc  $s = s'$ .

L'équivalence suivante est celle de la preuve de Bieberbach, qu'on peut montrer simplement à la main ici

$$H^1(\Gamma, E/L) \simeq \{\text{classes de } E\text{-conjugaison d'extensions de } L \text{ par } \Gamma\}$$

En effet, conjuguer  $G_s$  par une translation, revient à considérer les éléments de la forme :

$$\tau_k \tau_u \tau_{s(\alpha)} \alpha \tau_{-k} = \tau_u \tau_{s(\alpha)+k-\alpha \cdot k} \alpha$$

ce qui exactement la même chose que d'ajouter à  $s$  un cobord.

L'action de  $N$  sur  $H^1(\Gamma, E/L)$  apparaît de la manière suivante. Supposons que  $G_{s'} = \gamma G_s \gamma^{-1}$ . On a alors :

$$\tau_{s'(\alpha')} \alpha' = \gamma \tau_{s(\alpha)} \gamma^{-1} \gamma \alpha \gamma^{-1}$$

d'où  $\alpha' = \vec{\gamma} \alpha \vec{\gamma}^{-1}$  et du coup :

$$\tau_{s'(\vec{\gamma} \alpha \vec{\gamma}^{-1})} = \gamma \tau_{s(\alpha)} \gamma^{-1} = \tau_{\gamma \cdot s(\alpha)}$$

enfin

$$s'(\alpha) = \vec{\gamma} \cdot s(\vec{\gamma}^{-1} \alpha \gamma)$$

□

On peut déjà calculer  $H^1$  pour  $\Gamma$  cyclique :

**Proposition 4.2** *Si  $\Gamma = \langle \gamma \rangle$  est cyclique,*

$$H^1(\Gamma, M) = \ker(N_\gamma) / \text{im}(\gamma - \text{Id})$$

où

$$N_\gamma = \text{Id} + \gamma + \dots + \gamma^{p-1}$$

avec  $p$  l'ordre de  $\gamma$ .

**Preuve** Soit  $s$  un cocycle, on a  $s(\text{Id}) = 0$  et :

$$s(\gamma^i) = (\text{Id} + \gamma + \dots + \gamma^{i-1})s(\gamma)$$

donc, pour  $i = p$ , on a bien  $s(\gamma) \in \ker(N_\gamma)$ . Réciproquement, la formule ci-dessus donne bien un cocycle pour peu qu'on choisisse  $s(\gamma) \in \ker(N_\gamma)$ .

De plus, les cobords correspondent bien aux éléments de la forme  $\gamma k - k$ . □

On a désormais les outils pour prouver le dernier résultat de finitude :

**Théorème 4.3** *Il n'y a qu'un nombre fini, à conjugaison affine près, de groupes cristallographiques.*

**Preuve** Il suffit, par la partie 1, de montrer que chaque cristal ne contient qu'un nombre fini de classes de conjugaison de groupes cristallographiques. Cela revient donc à montrer que  $H^1(\Gamma, E/L)$  est fini.

Montrons que  $H^2(\Gamma, L)$  est un  $\mathbf{Z}$ -module de type fini. C'est le cas, car, comme  $L$  est un  $\mathbf{Z}$ -module de type fini et  $\Gamma$  est fini,  $Z^1(\Gamma, E/L)$  est de type fini comme  $\mathbf{Z}$ -module. C'est donc également le cas de  $H^2(\Gamma, L)$ , qui est de plus de torsion car  $|\Gamma|H^2(\Gamma, L) = 0$ . Or, un  $\mathbf{Z}$ -module de type fini et de torsion est fini par le théorème de structure des modules sur les anneaux principaux.

Enfin,  $H^1(\Gamma, E/L) \simeq H^2(\Gamma, L)$  ce qui conclut.  $\square$

Le dernier obstacle avant de commencer une démarche de description exhaustive de ces groupes est le calcul effectif de  $H^1$  et du normalisateur de  $\Gamma$  sur  $\text{Gl}(L)$ . En utilisant un outil de cohomologie appelé le *transfert cohomologique* on peut ramener le calcul de  $H^1(\Gamma, M)$  à celui de  $H^1(\Gamma_p, M)$  où les  $\Gamma_p$  sont les  $p$ -Sylow de  $\Gamma$ . Nous n'allons pas développer ici les preuves du transfert cohomologique et simplement donner les résultats. Dans toute la suite  $\Lambda \subset \Gamma$  est distingué.

**Proposition 4.4** *La restriction  $\text{res}_\Lambda^\Gamma$  induit une application  $H^1(\Gamma, M) \rightarrow H^1(\Lambda, M)$ .*

*Soit  $s \in H^1(\Lambda, M)$ , on dit que  $s$  est stable par  $\Gamma$  si :*

$$\text{res}_{\Lambda \cap \gamma \Lambda \gamma^{-1}}^\Lambda s = \text{res}_{\Lambda \cap \gamma \Lambda \gamma^{-1}}^{\gamma \Lambda \gamma^{-1}}(\gamma \cdot s)$$

*et on note  $H^1(\Lambda, M)^\Gamma$  les classes de cohomologie stable par  $\Gamma$ .*

*On peut alors définir une application dite de transfert :  $\text{tr}_\Lambda^\Gamma : H^1(\Lambda, M) \rightarrow H^1(\Gamma, M)$  qui vérifie :*

$$\text{tr}_\Lambda^\Gamma \text{res}_\Lambda^\Gamma f = [\Gamma : \Lambda]f \quad \forall f \in H^1(\Gamma, M)$$

*et*

$$\text{res}_\Lambda^\Gamma \text{tr}_\Lambda^\Gamma f = [\Gamma : \Lambda]f \quad \forall f \in H^1(\Lambda, M)^\Gamma$$

Ces applications permettent de prouver l'isomorphisme suivant :

**Proposition 4.5**

$$H^1(\Gamma, M) \simeq \bigoplus_p H^1(\Gamma_p, M)^\Gamma$$

On peut maintenant décrire tous les groupes cristallographiques à condition de bien connaître les sous-groupes finis de  $O(n)$  et d'arriver à calculer leur cohomologie. La classification complète à été faite jusqu'en dimension 4. Il existe un algorithme pour énumérer les groupes cristallographiques.

On va donner une esquisse de la classification en dimension 2 et quelques résultats en dimension 3. Dans ces cas simples on n'aura pas besoin de la décomposition générale que l'on vient de donner. C'est cependant celle-là qui sert pour une classification exhaustive en dimension arbitraire.

## 4.1 Dimension 2

Les groupes d'isométries finis de dimension 2 sont bien connus : ce sont les  $C_n$  et  $D_n$ , les groupes respectivement cycliques et diédraux. On sait par la partie 1 que seul un nombre fini d'entre eux conservent un réseau. Regardons lesquels.

**Proposition 4.6** *Un sous-groupe fini de  $O(2)$  qui laisse un réseau invariant est isomorphe à l'un des dix groupes suivants :*

$$C_1, D_1, C_2, D_2, C_3, D_3, C_4, D_4, C_6, D_6$$

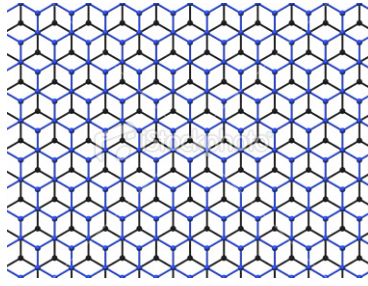
**Preuve** Si  $G \subset O(2)$  contient une rotation  $\sigma$  d'ordre  $p$ . Sa matrice dans une base de  $L$  est entière, donc de trace entière. On en conclut  $2 \cos(2\pi/n) \in \mathbf{Z}$  en conjuguant  $\sigma$ .  $\cos(2\pi/n)$  prend des valeurs entières en 1,2,3,4 et 6. Elle est croissante pour  $n \geq 2$  et tend vers 2.

Ce sont donc les seules rotations autorisées et, réciproquement, les groupes donnés plus haut conviennent tous.  $\square$

Introduisons deux types de réseaux dont on verra qu'ils suffisent :

- Le réseau quadratique engendré par une base orthonormée de  $E_2$ . Il est invariant par
  - le groupe trivial
  - $D_1$  engendré par une réflexion par rapport à un axe du réseau
  - $D_{1*}$  engendré par une réflexion par rapport à une diagonale du réseau
  - $C_2$  engendré par  $x \mapsto -x$
  - $D_2$  engendré par deux réflexions par rapport aux deux axes du réseau
  - $D_{2*}$  engendré par deux réflexions par rapport aux deux diagonales du réseau
  - $C_4$  engendré par une rotation d'ordre 4
  - $D_4$  le groupe de symétries du réseau
- Le réseau hexagonal engendré par deux vecteurs de même longueur formant un angle de  $\frac{\pi}{3}$ . Il est invariant par
  - $C_3$  engendré par une rotation d'ordre 3
  - $D_3$  engendré par des réflexions par rapport à 3 droites passant par les sommets de l'hexagone
  - $D_{3*}$  engendré par des réflexions par rapport à 3 droites passant par les milieux des cotés de l'hexagone
  - $C_6$  engendré par une rotation d'ordre 6
  - $D_6$  le groupe de symétries du réseau

En s'appuyant sur la proposition précédente, on peut classifier, en examinant chaque possibilité de sous-groupe fini de  $O(2)$  parmi les 10, déterminer les différentes classes de



Réseau hexagonal

cristaux ainsi que les réseaux qui les conservent. Ce sont en fait les 13 que nous venons de décrire.

**Théorème 4.7** *Les classes de cristaux (à conjugaison près) en dimension 2 sont les suivantes. Ou encore, de manière équivalente, les classes de conjugaison de sous-groupes finis de  $\text{Gl}_2(\mathbf{Z})$ .*

$$C_1, D_1, D_{1*}, C_2, D_2, D_{2*}, C_3, D_3, D_{3*}, C_4, D_4, C_6, D_6$$

Nous ne prouverons pas ce résultat. Voir [1].

Nous allons maintenant regarder quelques calculs explicites de cohomologie en dimension 2 pour quelques unes des 13 classes de cristaux possibles. Voici la classification complète en dimension 2. Les notations pour les groupes sont standard en cristallographie, voir [1] pour une description.

classe cristalline	#	groupes cristallographiques
$C_1$	1	$1p$
$C_2$	1	$p2$
$C_3$	1	$p3$
$C_4$	1	$p4$
$C_6$	1	$p6$
$D_1$	2	$pm, pg$
$D_{1*}$	1	$cm$
$D_2$	3	$pmm, pmg, pgg$
$D_{2*}$	1	$cmm$
$D_3$	1	$p31m$
$D_{3*}$	1	$p3m1$
$D_4$	2	$p4m, p4g$
$D_6$	1	$p6m$

Par exemple, dans le cas de  $D_4$ , on va calculer  $H^1(D_4, L)$  où  $L$  est le réseau quadratique. On va avoir besoin d'une suite exacte qui relie  $H^1(D_4)$  et  $H^1(D_4/C_4)$ . Dans le cas général, c'est une question complexe, mais ici, les premiers termes de la suite nous suffisent.

**Théorème 4.8** Soit  $\Gamma_1 \triangleleft \Gamma$  un sous groupe distingué. Si  $H^1(\Gamma_1, M) = 0$  alors :

$$H^1(\Gamma/\Gamma_1, M^{\Gamma_1}) \simeq H^1(\Gamma, M)$$

le morphisme en question s'appelle l'inflation.

En réalité, la suite suivante est exacte.

$$H^1(\Gamma/\Gamma_1, M^{\Gamma_1}) \hookrightarrow H^1(\Gamma, M) \rightarrow H^1(\Gamma_1, M)$$

**Preuve** La flèche  $\psi : H^1(\Gamma/\Gamma_1, M^{\Gamma_1}) \rightarrow H^1(\Gamma, M)$  est induite par le foncteur contravariant  $H^1(\cdot, M^{\Gamma_1})$  au morphisme canonique  $\Gamma \rightarrow \Gamma/\Gamma_1$ .

Montrons qu'elle est injective. En effet, si  $s : \Gamma/\Gamma_1 \rightarrow M$  est un cocycle tel que  $\psi(s)(\alpha) = s([\alpha]) = [\alpha] \cdot k - k$  soit un cobord.  $k$  étant  $\Gamma_1$  invariant, l'action de  $\Gamma$  se factorise et donne lieu à une action  $\alpha \cdot k = [\alpha] \cdot k$ . Donc  $s$  est un cobord.

Montrons maintenant qu'elle est surjective. Soit  $s : \Gamma \rightarrow M$  un cocycle. alors on peut trouver  $k \in M$  tel que  $s(\alpha) = \alpha k - k$  pour  $\alpha \in \Gamma_1$ . Posons  $h(\alpha) = \alpha k - k$ . On a  $(s - h)(\Gamma_1) = 0$ . On suppose donc dans la suite que  $s$  est nul sur  $\Gamma_1$ . Si on prend  $\alpha \in \Gamma_1$  et  $\beta \in \Gamma_1$  on a :

$$s(\alpha\beta) = s(\alpha) + \alpha s(\beta) = \alpha s(\beta)$$

et

$$s(\beta) = s(\beta\alpha) = s(\alpha\beta\beta^{-1}\alpha^{-1}\beta\alpha) = s(\alpha\beta)$$

car  $\Gamma_1$  est distingué. Donc  $s(\Gamma) \subset M^{\Gamma_1}$  et  $s$  est constant sur les  $\Gamma_1$ -classes, donc définit bien un cocycle de  $H^1(\Gamma/\Gamma_1, M^{\Gamma_1})$ .  $\square$

Dans notre cas, soit  $\rho \in D_n$  une rotation d'ordre maximal de  $D_n$ . Si  $H^1(\langle \rho \rangle, M) = 0$ , alors

$$H^1(D_n, M) = H^1(\langle \sigma \rangle, M^\rho)$$

où  $\sigma$  est une réflexion de  $D_n$ .

Ici, on a bien  $H^1(C_4) = 0$  par calcul explicite. De plus, on a  $\rho(a) = b$  et  $\rho(b) = -a$ , donc  $M = E/L^\rho = \{0, (a+b)/2\}$ . De plus,  $\sigma$  agit trivialement sur  $M$  donc

$$H^1(D_n, E/L) = H^1(\langle \sigma \rangle, E/L^\rho) = \mathbf{Hom}(\langle \sigma \rangle, M)$$

est de cardinal 2.

La seule classe de cohomologie non nulle est associée au cocycle qui envoie  $\rho$  sur 0 et  $\sigma$  sur  $(a+b)/2$ . Les deux groupes en question sont donc engendrés par :

- $p4m = \langle \tau_a, \tau_b, \sigma, \rho \rangle$ , c'est le produit semi-direct.
- $p4g = \langle \tau_a, \tau_b, \tau_{(a+b)/2}\sigma, \rho \rangle$ .

On peut les réaliser comme groupes de symétrie de deux pavages du plan :

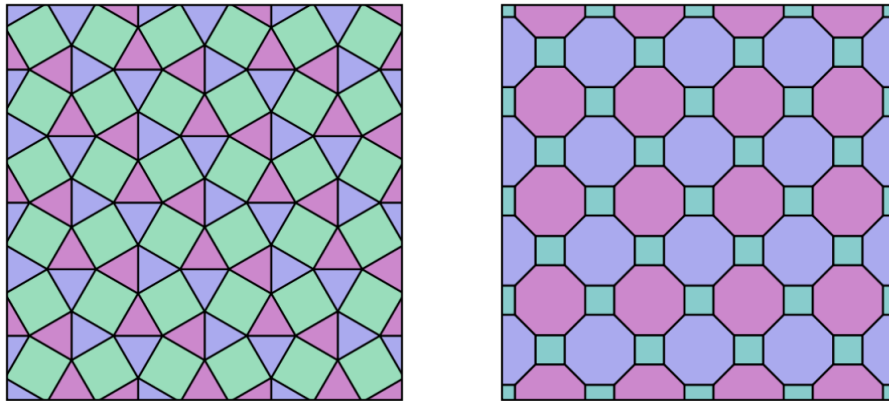


FIGURE 1 – Pavages de groupe  $p4g$  (à gauche) et  $p4m$  (à droite)

## 4.2 Des chiffres sur la dimension 3

On se contente ici de donner quelques chiffres. Il y a 32 classes de conjugaison de sous-groupes finis de  $O(3)$  qui conservent un réseau. On peut dénombrer 219 groupes cristallographiques répartis dans 73 classes de cristaux de dimension 3. La classification complète est disponible, par exemple, dans [1].

\* \* \*

Ainsi, on a vu que la description des groupes cristallographiques, qui est en réalité un problème d'extension de groupes, se simplifie grâce à la structure supplémentaire que leur impose le plongement dans  $E$  ou  $\text{Aff}(E)$ . Ces simplifications apparaissent naturellement d'un point de vue cohomologique. Ce formalisme n'est pas nécessaire, bien qu'il éclaire le déroulement des preuves.

Parmi les applications de cette classification on peut trouver par exemple les théorèmes de compacité d'agencements réguliers. En chimie, bombarder un cristal de rayons X permet d'obtenir des figures de diffraction qui traduisent certaines de ses symétries. On peut souvent en déduire par élimination la maille exacte du cristal et du même coup certaines de ses propriétés physiques.

## Bibliographie

1. Birger Iversen, *Lectures on crystallographic groups*, 1990, (Chapitres I-IV).
2. Jean-Pierre Serre, *Homologie des groupes – Applications arithmétiques*, 1958 (Chapitre I).
3. Charles W.Curtis et Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras*, 1962, (79.12).