Action du groupe de Klein sur une surface K3

Paolo Menegatti

Thèse

Pour l'obtention du Grade de

Docteur de l'Université de Poitiers
Faculté des sciences Fondamentales et Appliquées
(Diplôme National - Arrêté du 25 mai 2016)

École Doctorale Sciences et Ingénierie des Systèmes, Mathématiques, Informatique (ED SISMI)

Spécialité:
Mathématiques

Présentée par:
Paolo Menegatti

Action du groupe de Klein sur une surface K3

Directeur de thèse: Samuel Boissière

Date de la soutenance: le 22 Novembre 2019

Après avis des rapporteurs:

- François Charles (Professeur, Université Paris-Sud)
- Alice Garbagnati (Professore Associato, Université de Milano)

Composition du Jury:

François Charles (Professeur, Université Paris-Sud)	Rapporteur
Alice Garbagnati (Professore Associato, Université de Milano)	Rapporteur
Pascal Autissier (Professeur, Université de Bordeaux)	Examinateur
Enrica Floris (Maître de Conférences, Université de Poitiers)	Examinateur
Jean-Philippe Furter (Maître de Conférences, Université de La Rochelle)	Examinateur
Boris Pasquier (Professeur, Université de Poitiers)	Examinateur
Samuel Boissière (Professeur, Université de Poitiers)	Directeur de thèse

Résumé

L'objet de ce travail est la classification des actions du groupe de Klein $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ sur une surface K3 X, où G contient une involution non-symplectique qui agit trivialement sur le réseau de Neron-Severi de X, ainsi que la détermination du nombre de points qui en composent le lieu fixe.

Cela est accompli avec des méthodes purement algébriques, grâce à la théorie de Smith, qui permet de relier la cohomologie du lieu fixe $H^*\left(X^G, \mathbb{F}_2\right)$ à la G-cohomologie de $H^*(X, \mathbb{F}_2)$.

Nous commençons par déterminer les différentes possibilités pour la cohomologie du G-module $H^2(X, \mathbb{F}_2)$ (et par conséquent la cohomologie du lieu fixe X^G), en donnant aussi des résultats partiels pour le cas plus général $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Ensuite nous étudions l'extension du réseau de cohomologie $H^2(X, \mathbb{Z})$ induite par l'action de G et nous donnons une formule reliant le nombre des point fixes qui composent X^G à certains invariants numériques de l'extension: notamment les dimensions des groupes discriminants des réseaux invariants, mais aussi un nouvel invariant numérique, que nous montrons être indépendant des autres et nécessaire pour le calcul du lieu fixe.

Pour conclure, en utilisant le théorème de Torelli, nous déterminons tous les possibilités pour une action de G sur X et nous donnons aussi des exemples géométriques avec les fibrations elliptiques, confirmant les résultats prouvés.

Abstract

The aim of this work is to classify the actions of the Klein group G on a K3 surface X, where $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ contains a non-symplectic involution which acts trivially on Neron-Severi lattice, as well as computing the number of points composing the fixed locus.

This result is achieved through purely algebraic methods, due to Smith's theory, which relates the cohomology of the fixed locus $H^*(X^G, \mathbb{F}_2)$ to the group cohomology $H^*(X, \mathbb{F}_2)$.

Firstly, we identify all possibilities for the cohomology of the G-module $H^2(X, \mathbb{F}_2)$ (and therefore the cohomology of fixed locus X^G), providing some partial results for the general case $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Thereafter, we study the extension of the cohomology lattice $H^2(X, \mathbb{Z})$ induced by the action of G and we prove a formula giving the number of fixed points composing X^G from some numerical invariants of the extension. Namely the dimensions of discriminant groups of invariant lattices, but also a new numerical invariant, essential for the computation of the fixed locus, which we prove to be unrelated to other ones.

Finally, via Torelli theorem, we find all possibilities for G acting on X and we provide some geometric examples -confirming our results- using elliptic fibrations.

Remerciements

IF YOU DO NOT UNDERSTAND ITALIEN PLEASE ASK YOUR SUPERVISOR OR A FRIEND O YOURS TO KINDLY TRANSLATE THE MAIN POINTS OF THIS ACKNOWLEDGEMENTS

Famiglia, amore, amicizia. Questi sono i tre demoni che bisogna annientare se si vuole avere successo nella stesura di una tesi. Forse è stato proprio il contravvenire a questa regola che mi ha impedito di avere successo nella mia, perché sono numerose le persone che mi hanno accompagnato in questi ~~tre~~ quattro anni e che desidero ringraziare. Per prima cosa vorrei ringraziare i membri della giuria, Pascal Autissier, Enrica Floris, Jean-Philippe Furter, Boris Pasquier per aver accettato di presenziare alla mia tesi e in particolare i valutatori esterni François Charles e Alice Garbagnati, per essersi presi il tempo di leggere e valutare il mio lavoro, oltre a fornire delle utili osservazioni che hanno permesso di correggerlo e migliorarlo. Ringrazio soprattutto il mio direttore di tesi, Samuel Boissière, per avermi accettato come dottorando e avermi proposto un soggetto di tesi interessante. Grazie per la disponibilità e la gentilezza dimostrate nei miei confronti. Ringrazio inoltre Giovanni Mongardi e Alice Garbagnati (una seconda volta) per l'aiuto che mi hanno dato nei punti più difficili del mio lavoro e che mi ha permesso di avanzare in delle situazioni in cui ero davvero rimasto bloccato. Ringrazio tutti membri del labò, personale e docenti, per avermi permesso di lavorare in delle ottime condizioni. Grazie a Nathalie, Jocelyne e Myriam per la disponibilità e l'aiuto che sono sempre state pronte a fornire in biblioteca e in infografica e per aver stampato questa tesi (anche se in questo caso sto parlando al futuro). Grazie a Brigitte per la sua efficacia, a Nathalie per gli ordini di missione, a Benoit per l'eccellente lavoro che ha sempre svolto come tecnico informatico e che mi ha sempre fatto sentire ogni volta che andavo a trovarlo come in un film sugli hacker degli anni novanta. Grazie a Paul, Morgan e tutti gli altri membri della prepà agreg per avermi aiutato nella preparazione all'agrégation. Grazie a Alessandra, Boris, Enrica, Frédéric, Pol e tutti gli altri membri del grup de travai per gli incontri settimanali.

Un ringraziamento speciale va ai miei colleghi dottorandi, che mi hanno accompagnato in questo viaggio, talvolta superandomi. Ringrazio quindi Clément, che è stato un piacevole compagno di cella oltre che di viaggio, Marco, che mi ha aiutato per i miei dubbi di geometria, alla lavagna e

sullo schermo, Meghdad e Nassim, per le grigliate e i capodanni in ritardo, Alberto, che è stato un ottimo compagno a Marsiglia, Wafa, per l'entusiasmo e per avermi fatto conoscere i protestanti carismatici, Shuiran, per avermi fatto un po' conoscere un cultura diversa, Wen, per i numerosi snack e il collegamento al wi-fi, Amine, per il bellissimo lavoro svolto insieme con le ricette genetiche, Fatma, per la gentilezza che ha sempre dimostrato, Carlos, sperando che sopravviva a questo inverno senza prendere un'altra polmonite, Sahar, per aver permesso a Carlos di sopravvivere finora, Alex e Marion, per i numerosi inviti e momenti passati insieme, Angélique, perché senza di lei mi sarei annoiato, François, per il coraggio nella sua scelta, Irene e Pietro, per aver cercato (invano) di convincermi che la geometria algebrica sia bella, Simone, che mi ha permesso di riacquistare fiducia negli italiani, Paul, che mi ha permesso di riacquistare fiducia nei francesi, Antoine, che mi ha mostrato un enigma interessantissimo (sfortunatamente di probabilità) e ovviamente non posso dimenticare Camille, la mia tourangelle preferita. Ora che mi ritrovo a fare l'elenco, mi rendo conto di quanti numerosi siate state e di quanto importante sia stata la vostra compagnia e la vostra amicizia. Spero di non avere dimenticato nessuno, grazie davvero a tutti quanti. Purtroppo esiste un retrogusto amaro nelle amicizie nate durante il dottorato: per la loro stessa natura sono destinate a restare temporanee. Così che dopo aver vissuto insieme dei bellissimi momenti, ci si ritrova da un momento all'altro separati da migliaia di chilometri di distanza, senza molte speranze per un ritorno. Gli addii che ho dovuto dare mi hanno rattristato, così come mi rattristano quelli che so bene che presto arriveranno. Sappiate che conserverò il ricordo di tutti voi.

Ringrazio la mia famiglia e i miei amici che sono rimasti in Italia, per il sostegno che mi hanno dato, nonostante la distanza e le rare occasioni per rivedersi.

Ringrazio gli amici che ho conosciuto qui in Francia: Pierre-Antoine, Audrey et Cédric con i quali ho passato insieme dei momenti bellissimi, tra Mario e Nîmes.

Per finire, grazie a Camille, che mi ha aiutato tantissimo nella correzione del manoscritto, ma che soprattutto è stata la mia compagna di vita durante questi anni e che spero lo sarà in tutti quelli a venire (mbmppasqjapqtac). Grazie a Iris, che a suo modo ha provato anche lei ad aiutarmi nella redazione. Grazie a tutte e due di essere la parte più importante della mia vita.

Table des matières

Introduction

Parmi les types de surfaces complexes qui apparaissent dans la classification de Enriques-Kodaira, les surfaces K3 s'avèrent être parmi les plus étudiées. Pour donner quelques chiffres, la base de données de MathSciNet (le très connu catalogue bibliographique de l'AMS), recense environ 1700 travaux relatifs au sujet (classifiés avec les surfaces d'Enriques par le code MSC 14J28), un nombre qui dépasse tous les autre codes dédiés à des variétés algébriques spécifiques (exception faite par les variétés abéliennes et par les variétés de Calabi-Yau qui sont à égalité, mais qui finalement peuvent aussi être vues comme une des généralisations des surfaces K3).

Cet intérêt trouve sa justification: les surfaces K3 interviennent dans plusieurs branches des mathématiques et se sont révélées être un terrain de test efficace pour la preuve de certains théorèmes importants en géométrie algébrique. Par exemple les conjectures de Weil ont été d'abord démontrées pour les surfaces K3 par Deligne (cf. [De]). Il existe aussi des applications en physique, dans la compréhension de la dualité des cordes et de la supersymétrie, qui ont fait naître un nouveau sujet d'étude, la symétrie miroir.

L'étude de leurs automorphismes est un domaine de recherche qui est aujourd'hui toujours actif, surtout grâce aux possibilités fournies par l'application de la théorie des réseaux, introduite par Nikulin dans [Nik2] et développée aussi par Morrison, Dolgachev et Kondo au cours des années 1980.

Une distinction importante, qui remonte aussi à Nikulin, existe entre automorphismes symplectiques et non symplectiques: pour une surface K3 il existe une seule forme symplectique au scalaire près ($H^0(X, \Omega^2) \simeq \mathbb{C}\omega_X$), on dit donc qu'un automorphisme est symplectique s'il agit comme l'identité sur ω_X et non symplectique sinon.

Comme le groupe des automorphismes d'une surface K3 est discret, l'étude de l'action des groupes finis est d'intérêt central: le cas où G est un groupe abélien avec action symplectique est classifié par Nikulin [Nik2]. Ensuite Mukai [Mu], Xiao [Xi] et Kondo [Ko2], donnent une classification complète pour tous les groupes finis, toujours dans le cas où ceux-ci admettent une action symplectique.

Par rapport à l'étude du lieu fixe X^G, dans le cas d'une action symplectique on a que ce dernier est composé uniquement par des points (cf. [Xi] pour une classification). Dans le cas non-symplectique, où le lieu fixe peut

contenir aussi des courbes lisses, on a que si G est un groupe composé uniquement par des automorphismes non-symplectiques alors G est cyclique d'ordre n (car on a une injection $G \hookrightarrow \mathbb{C}^*$), donc le cas des automorphismes non-symplectiques d'ordre p^n est le plus traité. Dans [Nik3],[Ko],[OZ], [Tak] les cas $p = 2, 3, 11, 13, 17, 19$ sont traités.

Une approche intéressante est utilisée dans [AS] par Artebani, Sarti et Taki: ils appliquent la théorie de Smith en suivant une méthode déjà utilisée par Kharlamov pour le cas $p = 2$ [Kh] pour déterminer en général le lieu fixe d'un automorphisme φ d'ordre $p \geq 3$ premier. Cette technique a été ensuite perfectionnée et réécrite dans [BNS] par Boissière, Nieper-Wisskirchen et Sarti dans un style plus moderne pour pouvoir etre utilisée dans le cas d'un schéma de Hilbert de deux points d'une surface K3.

Un des résultat principal de cet article est l'application d'une formule de Allday et Puppe sur le lieu fixe [AP] au cas des surfaces K3. Dans notre cas X^G sera toujours lisse, car nous avons des automorphismes d'ordre finis. Cela constitue le point de départ de notre travail:

Théorème 0.0.1 ([AP, BNS])**.** *Soit $G = (\mathbb{Z}/p\mathbb{Z})^n$ avec p premier qui agit sur une surface X avec $dim_{\mathbb{F}_p} H^*(X^G, \mathbb{F}_p) < \infty$ et tel que $H^1(X) = H^3(X) = 0$ avec $X^G \neq \emptyset$. Alors :*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) = \begin{cases} \sum_i \left(\sum_{j=0}^{n} \dim_{\mathbb{F}_2} \left((-1)^j \operatorname{Tor}^j_{\mathbb{F}_p[u_1,\dots,u_n]}(\mathbb{F}_2, H^*(G; H^i(X, \mathbb{F}_2))) \right) \right) & si\ p = 2 \\ 2^{-n} \sum_i \left(\sum_{j=0}^{n} \dim_{\mathbb{F}_p} \left((-1)^j \operatorname{Tor}^j_{\mathbb{F}_p[u_1,\dots,u_n]}(\mathbb{F}_p, H^*(G; H^i(X, \mathbb{F}_p))) \right) \right) & si\ p \geq 3 \end{cases}$$

Cette formule résume une procédure capable d'obtenir la dimension totale de la cohomologie du lieu fixe ($\sum_i \dim H^i(X^G, \mathbb{F}_p)$) à partir de l'étude de l'action de G sur la cohomologie de X ($H^*(G; H^i(X, \mathbb{F}_p))$). Elle est peut être excessivement synthétique et une explication est de rigueur.

Soit donc $G = (\mathbb{Z}/p\mathbb{Z})^n$ (dans la suite G sera toujours de cette forme) qui agit sur une surface X qui respecte les hypothèses du théorème, alors pour $0 \leq i \leq 4$, G agit aussi sur $M_i := H^i(X, \mathbb{F}_p)$, la cohomologie de X modulo p. M_i est ainsi un G-module (plus précisément un $\mathbb{F}_p[G]$-module), et on peut en calculer la cohomologie de groupe $H^*(G, M_i)$, qui possède une structure de module gradué sur l'anneau des polynômes $R = \mathbb{F}_p[u_1, \dots, u_n]$.

Nous utiliserons une version simplifiée du Théorème 0.0.1 grâce à deux considérations: premièrement on peut remplacer la somme alternée des Tor avec la localisation dans l'idéal zéro, par le Lemme 1.3.6:

$$\dim_{\mathbb{F}_p(u_1,\dots,u_n)} N_{(0)} = \sum_{j=0}^{n} (-1)^j \dim_{\mathbb{F}_p} \operatorname{Tor}^j(\mathbb{F}_p, N) \text{ pour tout } \mathbb{F}_p[G]\text{-module } N$$

Deuxièmement, dans notre cas X sera une surface K3, en particulier $H^1(X, \mathbb{F}_p) = H^3(X, \mathbb{F}_p) = 0$ et $H^0(X, \mathbb{F}_p) \simeq H^4(X, \mathbb{F}_p) \simeq \mathbb{F}_p$. Il reste donc uniquement à déterminer l'action de G sur $H^2(X, \mathbb{F}_p)$.

On obtient alors:

Théorème. ***1.3.8*** *Soit $G = (\mathbb{Z}/p\mathbb{Z})^n$ qui agit sur X une surface K3 avec $X^G \neq \emptyset$. Alors:*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) = \begin{cases} 2 + \dim_{\mathbb{F}_2(u_1,\dots,u_n)} \left(H^*(G; H^2(X, \mathbb{F}_2))\right)_{(0)} & si\ p = 2 \\ 2 + 2^{-n} \dim_{\mathbb{F}_p(u_1,\dots,u_n)} \left(H^*(G; H^2(X, \mathbb{F}_p))\right)_{(0)} & si\ p \geq 3 \end{cases}$$

L'idée de la thèse est de séparer la procédure qui nous amène à déterminer la cohomologie du lieu fixe en deux étapes:

- Pour tout $\mathbb{F}_p[G]$-module indécomposable M, déterminer la valeur de $\dim H^*(G, M)_{(0)}$;
- À chaque action de G sur une surface K3 associer la décomposition en $\mathbb{F}_p[G]$-modules indécomposables de $H^2(X, \mathbb{F}_p)$.

Dans [BNS] les deux étapes sont accomplies dans le cas $n = 1$ (i.e. $G \simeq \mathbb{Z}/p\mathbb{Z}$), alors que notre travail essaiera de garder un point de vue plus général, en donnant une preuve alternative pour le cas $n = 1$, quelques considérations sur les difficultés relatives aux autres cas, mais surtout notre objectif principal sera de donner un traitement complet du cas $p = n = 2$, donc avec $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ le groupe de Klein.

Une classification pour ce cas est donnée par Garbagnati et Sarti [GaSar] au moyen d'arguments géométriques ad hoc. Dans notre travail on utilisera une stratégie entièrement différente et algébrique, qui révèle un nouvel invariant numérique lié a l'extension des réseaux et surtout fournira aussi des résultats sur le lieu fixe.

Dans le Chapitre 1, nous nous occuperons de la première étape. En utilisant la classification des $\mathbb{F}_p[G]$-modules dans le cas $p = n = 2$ nous montrerons:

Théorème. ***1.3.11*** *Soit $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$, M un $\mathbb{F}_p[G]$-module indécomposable, alors:*

$$\dim_{\mathbb{F}_2(u_1,u_2)}(H^*(G, M))_{(0)} = \begin{cases} 0 & si\ \dim_{\mathbb{F}_2} M\ pair \\ 1 & si\ \dim_{\mathbb{F}_2} M\ impair \end{cases}$$

Malheureusement dans les autres cas il n'existe pas une classification des modules indécomposables, ainsi il n'est pas possible donner des résultats aussi forts. Nous donnerons par contre un résultat partiel: pour un $\mathbb{F}_p[G]$-module M, on définit $\mathrm{leadt}(M) \in \mathbb{Q}$ la constante qui asymptotiquement vérifie $\dim H^i(G, M) \underset{i\to\infty}{\sim} \mathrm{leadt}(M) i^{n-1}$, alors:

Proposition. ***1.4.3*** *Soit M un $\mathbb{F}_p[G]$-module avec $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, alors:*

$$\dim_{\mathbb{F}_p(u_1,\dots,u_n)} H^*(G, M)_{(0)} = \begin{cases} \mathrm{leadt}(M)(n-1)! & si\ p = 2 \\ 2^n\, \mathrm{leadt}(M)(n-1)! & si\ p \geq 3 \end{cases}$$

Dans le Chapitre 2 nous exposerons la théorie des réseaux, dont l'application sera centrale dans le Chapitre 3. Tous les résultats du chapitre ne seront pas utilisés dans la suite, en fait l'objectif sera plutôt de fournir un texte à suivre pour un cours introductif sur le sujet, par exemple dans le cadre d'un cours de master. Mon impression, confirmée à l'occasion de plusieurs échanges entre collègues, est qu'il y a actuellement la nécessité d'un texte simple et riche en exemples qui présente le sujet: je ne peux pas dire si cet objectif a été atteint ou pas, je me suis simplement limité à exposer les arguments de la façon dont j'aurais aimé les écouter la première fois.

Ce chapitre ne contiendra pas de résultats originaux, exception faite pour quelques preuves alternatives de résultats déjà connus (par exemple que E_8 est le seul réseau unimodulaire pair de rang 8). Cependant, sa rédaction a demandé un effort comparable à celui des autres chapitres et pas uniquement à cause du fait qu'il est de loin le plus long des trois.

Dans le Chapitre 3 nous nous occuperons de la deuxième étape, c'est à dire associer à une action de $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ sur une surface K3 X, la décomposition de $H^2(X, \mathbb{F}_2)$ en modules indécomposables. L'outil principal sera la théorie des réseaux, et en particulier la définition d'un nouvel invariant:

Définition. Soit $R \supseteq L_1 \oplus \cdots \oplus L_n$ une extension de réseaux, alors on note:

$$K_R := \frac{R}{L_1^\perp + \cdots + L_n^\perp}$$

Soient donc $\Lambda_{K3} := H^2(X, \mathbb{Z})$, ι et η deux involutions commutant de X telles que ι soit symplectique et η non-symplectique, on note T_{ι^*} et T_{η^*} les parties invariantes du réseau sous l'action respective de ι et η, alors on a l'extension de réseaux:

$$\Lambda_{K3} \supseteq (T_{\iota^*} \cap T_{\eta^*}) \oplus \left(T_{\iota^*}^\perp \cap T_{\eta^*}\right) \oplus \left(T_{\iota^*} \cap T_{\eta^*}^\perp\right) \oplus \left(T_{\iota^*}^\perp \cap T_{\eta^*}^\perp\right)$$

Si on suppose que l'action de η soit triviale sur le groupe de Picard de X on a $T_{\eta^*} = NS(X)$. On obtient alors $T_{\iota^*}^\perp \cap T_{\eta^*}^\perp = 0$ et que les trois autres réseaux sont 2-élémentaires (i.e. leur groupe discriminant est de la forme $\simeq (\mathbb{Z}/2\mathbb{Z})^a$). On pose $a_1, a_3, k \in \mathbb{N}$ tels que pour les groupes discriminants on a $A_{T_\iota \cap T_\eta} \simeq (\mathbb{Z}/2\mathbb{Z})^{a_1}$, $A_{T_\iota \cap T_\eta^\perp} \simeq (\mathbb{Z}/2\mathbb{Z})^{a_3}$ et pour $K_{\Lambda_{K3}}$:

$$K_{\Lambda_{K3}} \simeq (\mathbb{Z}/2\mathbb{Z})^k$$

Selon la définition donné ci-dessus, nous pouvons alors énoncer le résultat principal de ce travail:

Théorème. 3.2.22 *Soit X une surface K3, ι et η deux involutions commutant de X tels que ι soit symplectique et η non-symplectique avec action triviale sur $NS(X)$. Avec les notations expliquées plus haut, si $X^G \neq \emptyset$ alors X^G est une réunion de points (réduits) avec:*

$$\#X^G \;=\; 16 - a_1 - a_3 + 2k$$

Donc le lieu fixe est donné uniquement par les réseaux invariants et leurs orthogonaux, aussi que par la valeur de k, qui nous donne une information supplémentaire sur comment ces réseaux « se recollent » entre eux.

Grâces aux théorèmes dits de Torelli, le parcours inverse est aussi possible: nous avons donc pu déterminer une liste d'invariants de réseaux pour lesquels il existe un couple d'involutions commutant (respectivement symplectique et non symplectique) qui les réalisent et donner le nombre de points fixes prévus par le Théorème 3.2.22. Les différents cas possibles ainsi calculés sont listés dans les Tableaux 3.2.2 et 3.2.3.

Pour conclure, nous revenons à la géométrie, en donnant des exemples de couples d'involutions commutant en utilisant les fibrations elliptiques et en vérifiant géométriquement que le nombre de points fixes est effectivement celui prévu par le Théorème 3.2.22, ce qui confirme l'importance de l'invariant k introduit.

Nous estimons qu'une des principales contributions de ce travail est de montrer, une fois de plus, qu'il est possible d'obtenir des résultats géométriques sur le lieu fixe en utilisant presque exclusivement, grâce à l'action combinée de la théorie de Smith et des théorèmes de Torelli, des arguments algébriques de cohomologie des groupes et de théorie des réseaux. Un sentier qui, peut-être, pourra dans le futur se montrer fructueux.

Je tiens à remercier Alessandra Sarti et Giovanni Mongardi pour les discussions très formatrices sur les surfaces K3 et la théorie des réseaux et Alice Garbagnati pour son aide dans la recherche des exemples géométriques.

Chapitre 1

Cohomologie des groupes

1.1 Qu'est-ce qu'est la cohomologie des groupes ?

L'objectif principal de ce premier chapitre est de prouver le Théorème 1.3.11, qui constitue le premier outil utilisé dans ce travail dans l'étude de l'action du groupe de Klein sur une surface K3.

Nous en profiterons aussi pour introduire quelques résultats de cohomologie des groupe (section 1), ainsi que sur les modules sur l'anneau $\mathbb{F}_p[G]$ (section 2), de façon à donner un cadre que nous espérons être clair et autonome et où enfin prouver les résultats qui nous intéressent (section 3). Dans la section 4 nous présenterons une preuve différente, qui peut être dans certains cas appliquée aussi pour $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec p et n quelconques. Nos efforts ont été particulièrement destinés à essayer de donner une exposition la plus complète possible, en minimisant en même temps les notions introduites, les résultats admis et les pré-requis demandés au lecteur.

Dans ce chapitre tous les anneaux seront sous-entendus commutatifs unitaires et tous les modules seront de type fini.

1.1.1 $\mathbb{F}_p[G]-$modules

Définition 1.1.1. Soit G un groupe, M un ensemble, on appelle *action* de G sur M un morphisme de la forme:

$$\begin{array}{rcl} \psi : G \times M & \longrightarrow & M \\ (g, m) & \longmapsto & g \cdot m \end{array}$$

tel que $\psi(1_G, \bullet) = \mathrm{Id}_M$ et que pour tous $g_1, g_2 \in G$, $m \in M$, $g_1 \cdot (g_2 \cdot m) = (g_1 g_2) \cdot m$.

De plus, si A est un anneau commutatif et M un A-module on dit que l'action est A-linéaire (ou comme on verra dans la suite, que M est un $A[G]$-module) si pour tout $\lambda, \mu \in A$, $m_1, m_2 \in M$, $g \in G$:

$$g \cdot (\lambda m_1 + \mu m_2) = \lambda\,(g \cdot m_1) + \mu\,(g \cdot m_2)$$

Définition 1.1.2. Soit G un groupe, A un anneau. On définit l'*algèbre de groupe* $A[G]$ comme le A-module libre ayant G comme base, $A[G] := A^{(G)} = \bigoplus_{g\in G} Ag$ avec la loi de produit interne donnée par:

$$\begin{array}{rcl} A[G]\times A[G] & \longrightarrow & A[G] \\ (\sum_{i=1}^{n}\lambda_i g_i, \sum_{j=1}^{m}\mu_j h_j) & \longmapsto & \sum_{j=1}^{m}\sum_{i=1}^{n}\lambda_i\mu_j g_i h_j \end{array}$$

Remarque 1.1.3. On vérifie facilement que pour un A-module M, avoir une action A-linéaire de G et avoir une structure de $A[G]$-module sont deux notions complètement équivalentes. Parfois un tel module est appelé aussi plus simplement « G-module ».

Remarque 1.1.4. Tous les $\mathbb{F}_p$-espaces vectoriels ont une structure naturelle de $\mathbb{F}_p[G]$-module, donnée par l'action triviale de G.

Dans la suite G sera toujours de la forme $G\simeq\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n$, p premier, avec une action $\mathbb{F}_p$-linéaire sur M, où M sera un $\mathbb{F}_p$-espace vectoriel de dimension finie. Donc on pourra voir M comme un $\mathbb{F}_p[G]$-module.

Lemme 1.1.5. *Soit $G\simeq\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n$, p premier, avec une action $\mathbb{F}_p$-linéaire sur $M\simeq\mathbb{F}_p$. Alors l'action de G sur M est triviale.*

Démonstration. Il suffit de prouver le résultat dans le cas cyclique, donc pour $n = 1$. Soit g un générateur de G, $\langle g\rangle = G$, comme M est un $\mathbb{F}_p$-espace de dimension un l'action de g sur $M\simeq\mathbb{F}_p$ est donnée par le produit par une constante $k \in \mathbb{F}_p$, donc $g\cdot m = km$ pour tout $m \in M\simeq\mathbb{F}_p$. Comme G a ordre p, on a $g^p\cdot m = 1_G\cdot m = m$, mais $g^p\cdot m = k^p m = km = g\cdot m$. En conclusion $g\cdot m = m$ et l'action de G est triviale. □

1.1.2 Résolution libre

Définition 1.1.6. Soit M un R-module, une *résolution libre* de M est une suite exacte:

$$\ldots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \ldots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon_0} M \to 0$$

avec F_i un R-module libre. L'application ε_0 est dit *morphisme d'augmentation.*

Dans la suite, pour les calculs de la cohomologie, on aura besoin d'une résolution libre de $\mathbb{F}_p$ en tant que $\mathbb{F}_p[G]$-module. On commence par le cas où G cyclique:

Proposition 1.1.7. *Soit p un nombre premier, $G = \mathbb{Z}/p\mathbb{Z} = \langle g\rangle$. Soit $\varepsilon : \mathbb{F}_p[G] \to \mathbb{F}_p$ le morphisme de $\mathbb{F}_p[G]$-module donné par $\varepsilon(1) = 1$ (donc*

$\varepsilon(g^i) = g^i \cdot 1 = 1$ pour tout i) et soit $\tau = g - 1 \in \mathbb{F}_p[G]$. Alors on a la suite exacte longue:

$$\ldots \overset{\cdot\tau^{p-1}}{\to} \mathbb{F}_p[G] \overset{\cdot\tau}{\to} \mathbb{F}_p[G] \overset{\cdot\tau^{p-1}}{\to} \mathbb{F}_p[G] \overset{\cdot\tau}{\to} \mathbb{F}_p[G] \overset{\varepsilon}{\twoheadrightarrow} \mathbb{F}_p \tag{1.1.1}$$

qui est une résolution libre de $\mathbb{F}_p$.

Démonstration. Le morphisme ε est clairement surjectif, avec le noyau donné par $\ker(\varepsilon) \subsetneq \mathbb{F}_p[G]$. Comme $\langle g-1\rangle \in \ker(\varepsilon)$ et $\langle g-1\rangle$ est un idéal maximal, on a $\ker(\varepsilon) = \langle g-1\rangle = \langle\tau\rangle$.

Ensuite, soient φ_τ et $\varphi_{\tau^{p-1}}$ les morphismes donnés respectivement par le produit par τ et τ^{p-1}:

$$\begin{array}{rcl} \varphi_\tau : \mathbb{F}_p[G] & \longrightarrow & \mathbb{F}_p[G] \\ a & \mapsto & a\tau \\ \varphi_{\tau^{p-1}} : \mathbb{F}_p[G] & \longrightarrow & \mathbb{F}_p[G] \\ a & \mapsto & a\tau^{p-1} \end{array}$$

Alors on vérifie facilement que $\mathrm{Im}(\varphi_\tau) = \langle\tau\rangle$, $\mathrm{Im}(\varphi_{\tau^{p-1}}) = \langle\tau^{p-1}\rangle$. On a aussi:

$$\begin{array}{rcl} \varphi_{\tau^{p-1}}(\tau) & = & \tau^{p-1}\tau \\ & = & (g-1)^p \\ & = & (g^p - 1) = 0 \end{array}$$

et donc $\ker(\varphi_{\tau^{p-1}}) = \langle\tau\rangle$ (car $\langle\tau\rangle$ est idéal maximal).

Il reste à montrer que $\ker(\varphi_\tau) = \langle\tau^{p-1}\rangle$: on a que $\tau^{p-1} \in \ker(\varphi_\tau)$ car $\varphi_\tau(\tau^{p-1}) = \varphi_{\tau^{p-1}}(\tau) = 0$ et $\mathrm{Im}(\varphi_\tau)$ a dimension $p-1$ comme $\mathbb{F}_p$-espace vectoriel, donc $\ker(\varphi_\tau)$ a dimension 1 et on peut donc conclure. □

En appliquant la formule de Künneth ([Br, V]) on obtient la résolution de $\mathbb{F}_p$ dans le cas général:

Proposition 1.1.8. *Soit p un nombre premier, $G = (\mathbb{Z}/p\mathbb{Z})^n = \langle g_1, \ldots, g_n\rangle$. Soit $\varepsilon : \mathbb{F}_p[G] \to \mathbb{F}_p$ le morphisme* de $\mathbb{F}_p[G]$-modules *tel que $\varepsilon(1) = 1$, et $\tau_i = g_i - 1 \in \mathbb{F}_p[G]$ pour $1 \le i \le n$. Alors la suite:*

$$\ldots \overset{d_n}{\to} \mathbb{F}_p[G]^{\alpha_n} \overset{d_{n-1}}{\to} \ldots \overset{d_3}{\to} \mathbb{F}_p[G]^{\alpha_3} \overset{d_2}{\to} \mathbb{F}_p[G]^{\alpha_2} \overset{d_1}{\to} \mathbb{F}_p[G]^{\alpha_1} \overset{\varepsilon}{\to} \mathbb{F}_p$$

avec:

$$\alpha_i = \binom{n+i-1}{n-1}$$

$$\begin{array}{rcl} d_i : \mathbb{F}_p[G]^{\alpha_{i+1}} & \longrightarrow & \mathbb{F}_p[G]^{\alpha_i} \\ \displaystyle\sum_{i_1+\cdots+i_n=m+1} f_{i_1,\ldots,i_n} & \longmapsto & \displaystyle\sum_{i_1+\cdots+i_n=m} h_{i_1,\ldots,i_n} \end{array}$$

et:

$$\begin{aligned} h_{i_1,\dots,i_n} &= (-1)^{(i_1+1)\cdots i_n} f_{i_1+1,i_2,\dots,i_{n-1},i_n} \tau_1^{\epsilon_{i_1}} + (-1)^{i_1\cdots i_n} f_{i_1,i_2+1,\dots,i_{n-1},i_n} \tau_2^{\epsilon_{i_2}} + \cdots + \\ &\quad + (-1)^{i_1\cdots i_n} f_{i_1,i_2,\dots,i_{n-1}+1,i_n} \tau_{n-1}^{\epsilon_{i_{n-1}}} + (-1)^{i_1\cdots(i_n+1)} f_{i_1,i_2,\dots,i_{n-1},i_n+1} \tau_n^{\epsilon_{i_n}} \end{aligned}$$

$$\epsilon_j = \begin{cases} 1 & si\ j\ pair \\ p-1 & si\ j\ impair \end{cases}$$

est une résolution libre de $\mathbb{F}_p$.

Remarque 1.1.9 (Cas $n = 2$). On examine de manière détaillée le cas $n = 2$ en le prouvant indépendamment du résultat précédent, en utilisant les complexes doubles. Soit donc $G = (\mathbb{Z}/p\mathbb{Z})^2 = \langle g_1, g_2 \rangle$ où g_1 et g_2 sont deux générateurs de G, donc $G = G_1 \times G_2$ avec $G_i =< g_i >$. Alors on a:

$$\begin{array}{ccc} \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xrightarrow{\simeq} & \mathbb{F}_p[G] \\ f \otimes h & \mapsto & fh \end{array}$$

On définit $\tau_i = g_i - 1$ et on considère maintenant le complexe double suivant:

$$\begin{array}{ccccccc} \vdots & & \vdots & & \vdots & & \vdots \\ \downarrow{\scriptstyle \cdot\tau_2} & & \downarrow{\scriptstyle \cdot(-\tau_2)} & & \downarrow{\scriptstyle \cdot\tau_2} & & \\ \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1} & \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1^{p-1}} & \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1} & \dots \\ \downarrow{\scriptstyle \cdot\tau_2^{p-1}} & & \downarrow{\scriptstyle \cdot(-\tau_2^{p-1})} & & \downarrow{\scriptstyle \cdot\tau_2^{p-1}} & & \\ \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1} & \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1^{p-1}} & \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot(-\tau_1)} & \dots \\ \downarrow{\scriptstyle \cdot\tau_2} & & \downarrow{\scriptstyle \cdot(-\tau_2)} & & \downarrow{\scriptstyle \cdot\tau_2} & & \\ \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1} & \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1^{p-1}} & \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] & \xleftarrow{\cdot\tau_1} & \dots \end{array}$$

Sur chaque ligne la différentielle agit comme dans la Proposition 1.1.7 sur le premier terme du produit tensoriel et l'identité sur le deuxième, donc chaque ligne est exacte (également pour chaque colonne). Donc le complexe total:

$$\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] \xleftarrow{d_1} \Big(\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2]\Big)^2 \xleftarrow{d_2} \Big(\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2]\Big)^3 \quad \dots \tag{1.1.2}$$

défini par les morphismes:

• pour i impair:

$$\begin{array}{rccl} d_i : \Big(\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2]\Big)^{i+1} & \longrightarrow & \Big(\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2]\Big)^i \\ (f_1, ..., f_{i+1}) & \mapsto & (f_1\tau_1 + f_2\tau_2, f_2\tau_1^{p-1} - f_3\tau_2^{p-1}, \dots, f_i\tau_1 + f_{i+1}\tau_2) \end{array}$$

• pour i pair:

$$\begin{array}{rccl} d_i : \Big(\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2]\Big)^{i+1} & \longrightarrow & \Big(\mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2]\Big)^i \\ (f_1, ..., f_{i+1}) & \mapsto & (f_1\tau_1^{p-1} - f_2\tau_2, f_2\tau_1 + f_3\tau_2^{p-1}\tau_2, \dots, f_i\tau_1 + f_{i+1}\tau_2^{p-1}) \end{array}$$

est aussi une suite exacte.

Pour conclure, on a que $\mathrm{Im}(d_1) = \langle g_1 - 1, g_2 - 1\rangle$ correspond au noyau du morphisme d'augmentation ε:

$$\begin{aligned} \varepsilon : \mathbb{F}_p[G_1] \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_2] &\to \mathbb{F}_p \\ g_i &\to 1 \end{aligned}$$

1.1.3 Cohomologie des $\mathbb{F}_p[G]$-modules

Maintenant on peut utiliser une résolution libre de $\mathbb{F}_p$ pour calculer la cohomologie d'un $\mathbb{F}_p[G]$-module. Soit donc M un $\mathbb{F}_p[G]$-module et $F^\bullet \to \mathbb{F}_p$ une résolution libre de $\mathbb{F}_p$:

$$\ldots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \ldots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon_0} \mathbb{F}_p \to 0$$

On applique le foncteur $\mathrm{Hom}(\bullet, M)$ à la résolution:

$$\ldots \xleftarrow{d_{n+1}^*} \mathrm{Hom}(F_n, M) \xleftarrow{d_n^*} \ldots \xleftarrow{d_1^*} \mathrm{Hom}(F_0, M) \xleftarrow{\varepsilon_0^*} \mathrm{Hom}(\mathbb{F}_p, M) \longleftarrow 0 \tag{1.1.3}$$

A priori le résultat n'est pas une suite exacte, mais il satisfait $d_{n+1}^* \circ d_n^* = 0$. On peut donc en prendre la cohomologie, qu'on note:

$$H^n(G, M) := \frac{\ker(d_{n+1}^*)}{\mathrm{Im}(d_n^*)}$$

Définition 1.1.10. Soit $F^\bullet \to \mathbb{F}_p$ une résolution libre de $\mathbb{F}_p$ en tant que $\mathbb{F}_p[G]$-module, on appelle $H^n(G, M) := H^n(\mathrm{Hom}(F^\bullet, M))$ le n-ième groupe de cohomologie de G à coefficients dans M.

Remarque 1.1.11. Comme une résolution libre est aussi une résolution projective, la G-cohomologie peut etre calculée en appliquant le foncteur Ext:

$$\begin{aligned} H^*(G, M) &= H^*(\mathrm{Hom}_{\mathbb{F}_p[G]}(F^\bullet, M)) \\ &= \mathrm{Ext}^*_{\mathbb{F}_p[G]}(\mathbb{F}_p, M) \end{aligned}$$

Le résultat suivant [Br, I.7.5] assure que la cohomologie d'un module est définie indépendamment de la résolution choisie:

Théorème 1.1.12. *Soient $F^\bullet \to M$ et $F'^\bullet \to M$ deux résolutions libres d'un module M, alors il existe un morphisme $f : F^\bullet \to F'^\bullet$ compatible avec les applications différentielles et qui induit un isomorphisme $\tilde{f}$ entre les groupes d'homologie.*

En plus, $\tilde{f}$ est unique et ne dépend pas du choix de f.

L'exactitude à gauche du foncteur Hom implique que $\ker(d_0^*) = \ker(\varepsilon_0^*)$, donc:

$$H^0(G, M) = \ker(\varepsilon_0^*) \simeq \mathrm{Hom}(\mathbb{F}_p, M)$$

On a une définition alternative pour $H^0(G,M)$. On définit $M^G \subseteq M$ les *invariants* de M de la façon suivante:

$$M^G := \{m \in M | g \cdot m = m \, \forall g \in G\}$$

On a le résultat suivant:

Lemme 1.1.13. *Soit M un $\mathbb{F}_p[G]$-module, alors:*

$$H^0(G,M) \simeq \mathrm{Hom}(\mathbb{F}_p, M) \simeq M^G$$

Démonstration. On considère le morphisme injectif:

$$\begin{array}{rccc} \nu_1 : \mathrm{Hom}(\mathbb{F}_p, M) & \longrightarrow & M \\ \varphi & \mapsto & \varphi(1) \end{array}$$

Alors $\mathrm{Im}(\nu_1) \subseteq M^G$ car pour tout $g \in G$ $g \cdot \varphi(1) = \nu_1(g \cdot \varphi) = \varphi(g \cdot 1) = \varphi(1)$ et pour tout $m \in M^G$ $\mathbb{F}_p[G] \cdot m = \mathrm{span}(m) \simeq \mathbb{F}_p$ et définit donc un plongement $\mathbb{F}_p \to M$ donc $M^G \subseteq \mathrm{Im}(\nu_1)$. □

Cas $n = 1$

On considère le cas $G = \mathbb{Z}/p\mathbb{Z} = \langle g \rangle$, $\tau = g - 1$, on rappelle qu'on a la résolution libre:

$$\ldots \xrightarrow{\varphi_\tau} \mathbb{F}_p[G] \xrightarrow{\cdot\tau} \mathbb{F}_p[G] \xrightarrow{\varphi_{\tau^{p-1}}} \mathbb{F}_p[G] \xrightarrow{\varphi_\tau} \mathbb{F}_p[G] \xrightarrow{\varepsilon} \mathbb{F}_p \to 0$$

avec $\varphi_\tau(m) = \tau \cdot m$ et $\varphi_{\tau^{p-1}}(m) = \tau^{p-1} \cdot m$. Soit M un $\mathbb{F}_p[G]$-module, on veut en calculer les groupes de cohomologie. On applique d'abord le foncteur $\mathrm{Hom}(\bullet, M)$:

$$\ldots \xleftarrow{\varphi_\tau^*} \mathrm{Hom}_G(\mathbb{F}_p[G], M) \xleftarrow{\varphi_{\tau^{p-1}}^*} \mathrm{Hom}_G(\mathbb{F}_p[G], M) \xleftarrow{\varphi_\tau^*} \mathrm{Hom}_G(\mathbb{F}_p[G], M)$$

$$\begin{array}{ccccccccc} \ldots & & \mathbb{F}_p[G] & \xrightarrow{\varphi_\tau} & \mathbb{F}_p[G] & \xrightarrow{\varphi_{\tau^{p-1}}} & \mathbb{F}_p[G] & \xrightarrow{\varphi_\tau} & \mathbb{F}_p[G] \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \ldots & & M & & M & & M & & M \end{array}$$

On rappelle que si $f \in \mathrm{Hom}_G(\mathbb{F}_p[G], M)$ alors $\varphi_\tau^*(f) = f \circ \varphi_\tau$ et qu'on a l'identification:

$$\begin{array}{rccc} \nu_1 : \mathrm{Hom}(\mathbb{F}_p[G], M) & \xrightarrow{\simeq} & M \\ f & \mapsto & f(1) \end{array}$$

Donc on obtient le diagramme commutatif suivant:

$$\begin{array}{ccccccccc} \ldots & \xleftarrow{\varphi_\tau^*} & \mathrm{Hom}_G(\mathbb{F}_p[G], M) & \xleftarrow{\varphi_{\tau^{p-1}}^*} & \mathrm{Hom}_G(\mathbb{F}_p[G], M) & \xleftarrow{\varphi_\tau^*} & \mathrm{Hom}_G(\mathbb{F}_p[G], M) \\ & & \downarrow{\scriptstyle \nu_1} & & \downarrow{\scriptstyle \nu_1} & & \downarrow{\scriptstyle \nu_1} \\ \ldots & \xleftarrow{\varphi_\tau} & M & \xleftarrow{\varphi_{\tau^{p-1}}} & M & \xleftarrow{\varphi_\tau} & M \end{array}$$

Et donc les groupes de cohomologie de M sont donnés par la cohomologie de la suite:

$$\cdots \leftarrow M \xleftarrow{\varphi_\tau} M \xleftarrow{\varphi_{\tau^{p-1}}} M \xleftarrow{\varphi_\tau} M \tag{1.1.4}$$

Lemme 1.1.14. *Soit $M = \langle \tau^j \rangle$ un idéal de $\mathbb{F}_p[G]$, avec $0 \leq j \leq p-1$, alors les groupes de cohomologie de M sont de la forme:*

$$H^i(G, M) \simeq \mathbb{F}_p \text{ si } j \geq 1$$

$$H^0(G, M) \simeq \mathbb{F}_p \text{ et } H^i(G, M) \simeq 0 \text{ pour } i \geq 1 \text{ si } j = 0$$

Démonstration. Il s'agit donc de calculer la cohomologie de la séquence (1.1.4):

$$\left\langle \tau^j \right\rangle \xrightarrow{\varphi_\tau} \left\langle \tau^j \right\rangle \xrightarrow{\varphi_{\tau^{p-1}}} \left\langle \tau^j \right\rangle \xrightarrow{\varphi_\tau} \left\langle \tau^j \right\rangle \xrightarrow{\varphi_{\tau^{p-1}}} \left\langle \tau^j \right\rangle \ldots$$

• Pour $j \geq 1$ on a $\ker(\varphi_{\tau^{p-1}}) = M = \langle \tau^j \rangle$, $\mathrm{Im}(\varphi_{\tau^{p-1}}) = 0$, $\ker(\varphi_\tau) = \langle \tau^{p-1} \rangle$, $\mathrm{Im}(\varphi_\tau) = \langle \tau^{j+1} \rangle$, donc:

$$H^i(G, M) = \frac{\ker(\varphi_{\tau^{p-1}})}{\mathrm{Im}(\varphi_\tau)} = \frac{\langle \tau^j \rangle}{\langle \tau^{j+1} \rangle} \simeq \mathbb{F}_p \text{ pour } i \text{ impair}$$

$$H^i(G, M) = \frac{\ker(\varphi_\tau)}{\mathrm{Im}(\varphi_{\tau^{p-1}})} = \frac{\langle \tau^{p-1} \rangle}{\langle 0 \rangle} \simeq \mathbb{F}_p \text{ pour } i \text{ pair}$$

• Pour $j = 0$ on a $M \simeq (1) \simeq \mathbb{F}_p[G]$ et donc la suite coïncide avec la résolution exacte de $\mathbb{F}_p$, donc la cohomologie est nulle sauf pour $H^0(G, \mathbb{F}_p[G]) = \ker(\varphi_\tau) \simeq \mathbb{F}_p$. □

Remarque 1.1.15. Choisir M comme idéal de $\mathbb{F}_p[G]$ est en réalité la seule possibilité si on demande que M soit indécomposable (comme on verra dans le Corollaire 1.2.22).

1.1.4 Structure d'algèbre

1.1.4.1 Cup-produit

Nous avons donc vu qu'à un $\mathbb{F}_p[G]$-module M on peut associer une suite de groupes de cohomologie, qui par contre pour l'instant sont « non liés » entre eux. On verra dans cette section qu'il est possible de regrouper la cohomologie de M dans une algèbre graduée.

Évidemment pour cela on a besoin d'un produit, que nous définirons en deux étapes.

Soit donc M un $\mathbb{F}_p[G]$-modules, et $F^\bullet$ une résolution libre de $\mathbb{F}_p$ en tant que $\mathbb{F}_p[G]$-module. Par la formule de Kunneth [Br, V] $F^\bullet \otimes F^\bullet$ est une résolution de $\mathbb{F}_p$ en tant que G^2-module.

On peut donc définir un morphisme de complexes:

$$(\bullet \times \bullet) : \mathrm{Hom}_G(F^\bullet, M) \times \mathrm{Hom}_G(F^\bullet, \mathbb{F}_p) \to \mathrm{Hom}_{G^2}((F^\bullet)^{\otimes 2}, M)$$

qui pour chaque couple d'éléments est défini de la façon suivante:

$$\begin{array}{rcl}(\bullet \times \bullet) : \mathrm{Hom}_G(F_r, M) \times \mathrm{Hom}_G(F_s, \mathbb{F}_p) & \to & \mathrm{Hom}_{G^2}\left(F_r \otimes F_s, M\right) \\ (u, v) & \mapsto & (-1)^{rs} u \otimes v\end{array}$$

Ce morphisme se révèle être compatible avec les différentielles [Br, V.2] et donc il induit un produit (appelé *cross-product*) entre les groupes de cohomologie:

$$(\bullet \times \bullet) : H^r(G, M) \times H^s(G, \mathbb{F}_p) \to H^{r+s}(G^2, M)$$

Le cross-product ne suffit pas à définir une structure d'algèbre sur la cohomologie de M, car il prend ses valeurs sur la cohomologie de M vu comme $\mathbb{F}_p[G^2]$-module: il faut donc revenir à la cohomologie sur G.

D'abord on remarque que tous les $\mathbb{F}_p[G^2]$-module possèdent aussi une structure naturelle de G-module, induite par l'application diagonale $G \to G \times G$, $g \mapsto (g, g)$. Donc, si $F^\bullet \otimes F^\bullet$ est une résolution libre de $\mathbb{F}_p$ en tant que $\mathbb{F}_p[G^2]$-module, elle est aussi une résolution libre de $\mathbb{F}_p$ en tant que $\mathbb{F}_p[G]$-module.

Donc $F^\bullet \to \mathbb{F}_p$ et $F^\bullet \otimes F^\bullet \to \mathbb{F}_p$ sont deux résolutions de $\mathbb{F}_p$: par le Théorème 1.1.12 il existe alors un morphisme $\Delta : F^\bullet \to F^\bullet \otimes F^\bullet$ compatible avec les différentielles et qui induit un isomorphisme entre les groupes d'homologie: on appelle *approximation diagonale* un choix de Δ.

Déterminer une formulation explicite de Δ n'est pas en général un problème trivial, en tout cas pour G cyclique d'ordre premier on a le lemme suivant [Br]:

Lemme 1.1.16. *Soit $G \simeq \mathbb{Z}/p\mathbb{Z}$, alors une approximation diagonale est donnée par les morphismes $\Delta_{r,s} : F_{r+s} \to F_r \otimes F_s$ définis comme:*

$$\Delta_{r,s}(1) = \begin{cases} 1 \otimes 1 & \text{pour } r \text{ pair} \\ 1 \otimes g & \text{pour } r \text{ impair, } s \text{ pair} \\ \sum_{0 \le i < j \le p-1} g^i \otimes g^j & \text{pour } r \text{ impair, } s \text{ impair} \end{cases}$$

A partir de Δ on obtient l'application duale:

$$\begin{array}{rcl}\Delta^*_{r,s} : \mathrm{Hom}_{G^2}(F_r \otimes F_s, M) & \longrightarrow & \mathrm{Hom}_G(F_{r+s}, M) \\ f & \mapsto & f \circ \Delta_{r,s}\end{array}$$

Δ^* commute avec les applications différentielles et passe donc à la cohomologie. On peut alors la composer avec le cross-product afin d'obtenir une action sur la cohomologie:

Définition 1.1.17. Soit M un $\mathbb{F}_p[G]$-module, on appelle *cup-produit* le morphisme:

$$\begin{array}{rcl}\bullet \cup \bullet : H^r(G, M) \times H^s(G, \mathbb{F}_p) & \longrightarrow & H^{r+s}(G, M) \\ (u, v) & \mapsto & \Delta^*\left(u \times v\right)\end{array}$$

Le cup-produit définit un produit interne sur le $\mathbb{F}_p$-module $H^*(G,\mathbb{F}_p) = \bigoplus_{i\geq 0} H^i(G,\mathbb{F}_p)$ qui lui donne une structure d'algèbre graduée.

De plus, si M est un $\mathbb{F}_p[G]$-module, le cup-produit induit sur $H^*(G,M)$ une structure de $H^*(G,\mathbb{F}_p)$-module. C'est cette structure qui sera notre sujet d'intérêt dans la suite.

1.1.4.2 Cas $n = 1$

Comme d'habitude on commence par étudier le cas cyclique, $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Soit $F^\bullet \to \mathbb{F}_p$ la résolution libre vue dans (1.1.1). On rappelle qu'il existe un isomorphisme entre M et $\mathrm{Hom}(\mathbb{F}_p[G], M)$ donné par $\nu_1 : \varphi \mapsto \varphi(1)$, donc on peut identifier $a_r \in \mathrm{Hom}(F_r, \mathbb{F}_p)$, $m_s \in \mathrm{Hom}(F_s, M)$ avec $\nu_1(a_r) := a_r(1) \in \mathbb{F}_p$ et $\nu_1(m_s) := m_s(1) \in M$. Avec cette identification le cup-produit devient:

$$\begin{array}{ccc} H^r(G,\mathbb{F}_p) \times H^s(G,M) & \longrightarrow & H^{r+s}(G,M) \\ \downarrow & & \downarrow \\ \mathbb{F}_p \times M & \longrightarrow & M \end{array} \tag{1.1.5}$$

$$\begin{array}{ccc} (a_r, m_s) & \longmapsto & a_r \cup m_s \\ \downarrow & & \downarrow \\ (\nu_1(a_r), \nu_1(m_s)) & \longmapsto & (-1)^{rs}\Delta^*_{r,s}(1\otimes 1)\nu_1(a_r)\nu_1(m_s) \end{array}$$

où on peut réécrire l'application diagonale sous la forme:

$$\Delta^*_{r,s}(1\otimes 1) = \begin{cases} 1 & \text{pour } r \text{ pair} \\ g = \tau + 1 & \text{pour } r \text{ impair, } s \text{ pair} \\ -g\tau^{p-2} = -\tau^{p-2} - \tau^{p-1} & \text{pour } r \text{ impair, } s \text{ impair} \end{cases}$$

où la dernière équivalence vient de:

$$\sum_{0\leq i<j\leq p-1} g^{i+j} = g + 2g^2 + ... + (p-1)g^{p-1} = -g\tau^{p-2}$$

Passons maintenant à la cohomologie, soit donc $M = \langle \tau^j \rangle$ avec $1 \leq j \leq p-1$ (si $j = 0$ alors $M \simeq \mathbb{F}_p[G]$ et la cohomologie est nulle exception faite pour H^0). On rappelle que:

$$H^i(G,M) = \frac{\ker(\varphi_{\tau^{p-1}})}{\mathrm{Im}(\varphi_\tau)} = \frac{\langle \tau^j \rangle}{\langle \tau^{j+1} \rangle} \simeq \mathbb{F}_p \text{ pour } i \text{ impair}$$

$$H^i(G,M) = \frac{\ker(\varphi_\tau)}{\mathrm{Im}(\varphi_{\tau^{p-1}})} = \frac{\langle \tau^{p-1} \rangle}{(0)} \simeq \mathbb{F}_p \text{ pour } i \text{ pair}$$

Pour tout i, on choisit $\beta_i \in H^i(G,M)$ de la forme $\beta_i := \overline{\tau^j}$ si i impair et $\beta_i := \overline{\tau^{p-1}}$ si i pair, en particulier $\text{span}(\beta_i) = H^i(G,M)$. De la même façon, on note $\alpha_i \in H^i(G,\mathbb{F}_p)$ de la forme $\alpha_i := \overline{1}$ (on remarque que si $M \simeq \langle \tau^{p-1} \rangle \simeq \mathbb{F}_p$ alors $\alpha_i = \beta_i$)

En appliquant (1.1.5) on trouve:

$$\begin{aligned} \alpha_r \cup \beta_s &= (-1)^{rs}\Delta^*(\alpha_r \otimes \beta_s) \\ &= (-1)^{rs}\Delta^*(1 \otimes 1)\beta_s \end{aligned}$$

On considère les différents cas séparément:

- Si r pair et s pair, alors $a_r \cup \beta_s = 1 \cdot 1 \cdot \overline{\tau^{p-1}} = \overline{\tau^{p-1}} = \beta_{r+s}$ car $r+s$ est pair et donc $\overline{\tau^{p-1}}$ est un représentant de β_{r+s} ;
- Si r pair et s impair, alors $a_r \cup \beta_s = 1 \cdot 1 \cdot \overline{\tau^j} = \overline{\tau^j} = \beta_{r+s}$ car $r+s$ est impair et donc $\overline{\tau^j}$ est un représentant de β_{r+s} ;
- Si r impair et s pair, alors: $a_r \cup \beta_s = 1 \cdot (\tau+1) \cdot \overline{\tau^{p-1}} = \overline{\tau^{p-1}} + \overline{\tau^p} = \overline{\tau^{p-1}}$ car $\overline{\tau^p} = \overline{0}$. On a deux cas:
  — $\overline{\tau^{p-1}} = \beta_{r+s}$ si $j = p-1$;
  — $\overline{\tau^{p-1}} = \overline{0}$ si $j < p-1$.
- Si r impair et s impair, alors: $a_r \cup \beta_s = (-1) \cdot (-\tau^{p-1} - \tau^{p-2}) \cdot \overline{\tau^j} = \overline{\tau^{p-1+j}} + \overline{\tau^{p-2+j}} = \overline{\tau^{p-2+j}}$ où le dernier passage descend de $j > 0$. On a aussi deux cas:
  — $\overline{\tau^{p-2+j}} = \beta_{r+s}$ si $j = 1$;
  — $\overline{\tau^{p-2+j}} = 0$ si $j > 1$.

Donc en résumant:

$\alpha_r \cup \beta_s$	s pair	s impair
r pair	β_{r+s}	β_{r+s}
r impair	β_{r+s} si $j = p-1$	β_{r+s} si $j = 1$
	0 sinon	0 sinon

TABLE 1.1.1 – Cup produit sur les modules de cohomologie

Il suffit maintenant d'utiliser le Tableau 1.1.1 pour déterminer la structure d'algèbre/module de $H^*(G,M)$ dans les différents cas:

Proposition 1.1.18. *Soit $G = \mathbb{Z}/2\mathbb{Z}$, $M \simeq \mathbb{F}_2$ vu comme $\mathbb{F}_2[G]$-module. Alors sur $H^*(G,\mathbb{F}_2)$ le cup-produit induit une structure d'anneau:*

$$\begin{aligned} \psi : \mathbb{F}_2[u] &\xrightarrow{\simeq} H^*(G,\mathbb{F}_2) \\ u^i &\mapsto \beta_i \end{aligned}$$

Démonstration. On a $M \simeq \langle \tau \rangle \simeq \mathbb{F}_2$, c'est alors le cas $j = 1 = p-1$, donc pour toute valeur de r,s on a $\alpha_r = \beta_r$ et $\beta_r \cup \beta_s = \beta_{r+s}$, ce qui correspond à la loi du produit dans l'anneau des polynômes à une variable $\mathbb{F}_2[u]$. □

Proposition 1.1.19. *Soit $G = \mathbb{Z}/p\mathbb{Z}$ avec $p > 2$, $M \simeq \mathbb{F}_p$ vu comme $\mathbb{F}_p[G]$-module. Alors sur $H^*(G, \mathbb{F}_p)$ le cup-produit induit une structure d'anneau de la forme:*

$$\begin{array}{rcl} \psi : \bigwedge(\sigma) \otimes_{\mathbb{F}_p} \mathbb{F}_p[z^2] & \xrightarrow{\simeq} & H^*(G, \mathbb{F}_p) \\ 1 \otimes z^{2i} & \mapsto & \beta_{2i} \\ \sigma \otimes z^{2i} & \mapsto & \beta_{2i+1} \end{array}$$

où $\bigwedge(\sigma)$ est l'algèbre extérieure engendrée par σ, i.e. $\bigwedge(\sigma) \simeq \frac{\mathbb{F}_p[\sigma]}{\langle \sigma^2 \rangle}$.

Démonstration. On a $M \simeq \langle \tau^{p-1} \rangle \simeq \mathbb{F}_p$, c'est alors le cas $j = p - 1 \neq 1$ donc pour toute valeur de r,s on a $\alpha_r = \beta_r$ et:

- $\beta_r \cup \beta_s = 0$ si r et s sont impairs ;
- $\beta_r \cup \beta_s = \beta_{r+s}$ sinon.

ψ est donc un isomorphisme d'anneaux. □

Remarque 1.1.20. L'utilisation de la variable z^2 (en lieu de u) dans l'anneau de polynômes $\mathbb{F}_p[z^2]$ est pour rendre plus lisible la correspondance entre le degré en cohomologie et le degré dans l'anneau des polynômes.

Proposition 1.1.21. *Soit $G = \mathbb{Z}/p\mathbb{Z}$ avec $p > 2$, $M \simeq \langle \tau^j \rangle$ avec $1 < j < p - 1$, si on identifie $H^*(G, \mathbb{F}_p)$ avec $\bigwedge(\sigma) \otimes_{\mathbb{F}_p} \mathbb{F}_p[z^2]$ alors le cup-produit induit sur $H^*(G, M)$ une structure de $H^*(G, \mathbb{F}_p)$-module de la forme:*

$$\begin{array}{rcl} \psi : \sigma \otimes \left(\mathbb{F}_p[z^2] \oplus \mathbb{F}_p[z^2] \right) & \xrightarrow{\simeq} & H^*(G, M) \\ \sigma \otimes (z^{2i}, 0) & \mapsto & \beta_{2i} \\ \sigma \otimes (0, z^{2i}) & \mapsto & \beta_{2i+1} \end{array}$$

Démonstration. Par la proposition précédente on peut voir $H^*(G, M)$ comme un $\left(\bigwedge(\sigma) \otimes_{\mathbb{F}_p} \mathbb{F}_p[z^2] \right)$-anneau. Comme $1 < j < p-1$ l'action est donnée par:

- Si r impair et s pair alors $\alpha_r \cup \beta_s = 0$, qui au travers de ψ devient: $(\sigma \otimes z^{r-1})(\sigma \otimes (z^s, 0)) = 0$;
- Si r impair et s impair alors $\alpha_r \cup \beta_s = \beta_{r+s}$, qui au travers de ψ devient: $(\sigma \otimes z^{r-1})(\sigma \otimes (0, z^{s-1})) = 0$;
- Si r pair et s pair alors $\alpha_r \cup \beta_s = \beta_{r+s}$, qui au travers de ψ devient: $(1 \otimes z^r)(\sigma \otimes (z^s, 0)) = \sigma \otimes (z^{s+r}, 0)$;
- Si r pair et s impair alors $\alpha_r \cup \beta_s = \beta_{r+s}$, qui au travers de ψ devient: $(1 \otimes z^r)(\sigma \otimes (0, z^{s-1})) = \sigma \otimes (0, z^{s+r-1})$.

□

Proposition 1.1.22. *Soit $G = \mathbb{Z}/p\mathbb{Z}$ avec $p > 2$, $M \simeq \langle \tau \rangle$, si on identifie $H^*(G, \mathbb{F}_p)$ avec $\bigwedge(s) \otimes_{\mathbb{F}_p} \mathbb{F}_p[z^2]$ alors avec le cup-produit $H^*(G, M)$ est isomorphe à l'idéal $(1 \otimes z^2, \sigma \otimes 1) \leq \bigwedge(\sigma) \otimes_{\mathbb{F}_p} \mathbb{F}_p[z^2]$, dans le détail:*

$$\begin{array}{rcl} \psi : \left\langle 1 \otimes u^2, \sigma \otimes 1 \right\rangle & \xrightarrow{\simeq} & H^*(G, M) \\ 1 \otimes z^{2i} & \mapsto & \beta_{2i-1} \\ \sigma \otimes z^{2i} & \mapsto & \beta_{2i} \end{array}$$

Démonstration. En suivant le Tableau 1.1.1 on obtient pour $j = 1$:

- Si r impair et s pair alors $\alpha_r \cup \beta_s = 0$, qui au travers de ψ devient: $(\sigma \otimes z^{r-1})(\sigma \otimes z^s)) = 0$;
- Si r impair et s impair alors $\alpha_r \cup \beta_s = \beta_{r+s}$, qui au travers de ψ devient: $(\sigma \otimes z^{r-1})(1 \otimes z^{s+1}) = \sigma \otimes z^{s+r}$;
- Si r pair et s pair alors $\alpha_r \cup \beta_s = \beta_{r+s}$, qui au travers de ψ devient: $(1 \otimes z^r)(\sigma \otimes z^s) = \sigma \otimes z^{s+r}$;
- Si r pair et s impair alors $\alpha_r \cup \beta_s = \beta_{r+s}$, qui au travers de ψ devient: $(1 \otimes z^r)(1 \otimes z^{s+1}) = 1 \otimes z^{s+r+1}$.

□

En résument on obtient:

$H^*(G, \langle\tau^j\rangle)$	$j = 0$	$j = 1$	$1 < j < p-1$	$j = p-1$
$p = 2$	$\mathbb{F}_2$	$\mathbb{F}_2[u]$	/	$\mathbb{F}_2[u]$
$p \geq 3$	$\mathbb{F}_p$	$\langle s, z^2\rangle$	$\langle s\rangle \oplus \langle s\rangle$	$\mathbb{F}_p[z^2] \oplus \bigwedge(s)$

Remarque 1.1.23. Dans [BNS, Prop. 2.3] on affirme que si $j \geq 1$ alors $H^*(G, \langle\tau^j\rangle) \simeq H^*(G, \mathbb{F}_p)$. D'après les Propositions 1.1.21, 1.1.22 cela n'est pas complètement exact, mais ça reste vrai que $H^*(G, \langle\tau^j\rangle)$ est un $\mathbb{F}_p[z^2]$-module libre, donc le calcul des modules de torsion associés reste inchangé. En plus le cas $1 \leq j \leq p-2$ n'intervient jamais dans le calcul du lieu fixe.

En appliquant la formule de Kunneth au cas cyclique on peut obtenir l'anneau de cohomologie dans le cas général (voir [CTVZ, Prop. 4.5.4]):

Proposition 1.1.24. *Soit* $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$*, alors:*

$$H^*(G, \mathbb{F}_p) \simeq \begin{cases} \mathbb{F}_2[u_1, \ldots, u_n] & \text{si } p = 2 \\ \mathbb{F}_p[z_1^2, \ldots, z_n^2] \otimes \bigwedge(s_1, \ldots, s_n) & \text{si } p \geq 3 \end{cases}$$

où z_1, u_i, s_2 *interviennent en degré* 1 *dans la cohomologie.*

Remarque 1.1.25. Soit R la partie polynomiale de $H^*(G, \mathbb{F}_p)$, donc $R = \mathbb{F}_p[u_1, \ldots, u_n]$ (avec $u_i = z_i^2$ si $p \geq 3$), alors $H^*(G, \mathbb{F}_p)$ est une R-algèbre et en particulier pour tout $\mathbb{F}_p[G]$-module M, $H^*(G, M)$ est un R-module. Attention que dans ce cas le degré en cohomologie de u_i sera 2 si $p \geq 3$.

1.2 L'anneau $\mathbb{F}_p[G]$

1.2.1 Propriétés principales

Vu qu'une action de G sur un $\mathbb{F}_p$-espace vectoriel est équivalent à un module sur l'anneau $\mathbb{F}_p[G]$, il s'avère fondamental de mieux détailler les propriétés de cet anneau.

D'abord on fait un changement de notation, pour alléger les calculs dans la suite:

Définition 1.2.1. Soit p premier, $n \in \mathbb{N}^*$, on note:

$$A_p^n \simeq \frac{\mathbb{F}_p[x_1, \ldots, x_n]}{\langle x_1^p, \ldots, x_n^p \rangle}$$

et $A_p := A_p^1$.

On vérifie facilement que $A_p^n \simeq A_p^{\otimes n}$ et que:

Lemme 1.2.2. *Soit $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec p premier, alors:*

$$\mathbb{F}_p[G] \simeq A_p^n$$

Démonstration. Comme $\mathbb{F}_p[G]$ a caractéristique p on a:

$$\begin{aligned} \mathbb{F}_p[G] &\simeq \frac{\mathbb{F}_p[g_1, \ldots g_n]}{\langle g_1^p - 1, \ldots g_n^p - 1 \rangle} \\ &\simeq \frac{\mathbb{F}_p[g_1, \ldots g_n]}{\langle (g_1 - 1)^p, \ldots (g_n - 1)^p \rangle} \end{aligned}$$

et on pose $x_i = g_i - 1$ pour obtenir l'isomorphisme recherché. □

Dans la suite on utilisera parfois, selon le contexte, A_p^n au lieu de $\mathbb{F}_p[G]$, surtout quand une notation différente sera plus pratique.

Lemme 1.2.3. *A_p^n est un anneau artinien local avec idéal maximal $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$ avec $\dim_{\mathbb{F}_p} A_p^n = p^n$.*

Démonstration. $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$ est un idéal maximal car $A_p^n/\mathfrak{m} \simeq \mathbb{F}_p$. Soit $\mathfrak{p} \subset A_p^n$ un idéal premier, pour tout i on a $x_i \in \mathfrak{p}$ car élément nilpotent, alors $\mathfrak{m} \subseteq \mathfrak{p}$ mais $\mathfrak{m}$ est idéal maximal et on a donc l'égalité et A_p^n est local. Une base de A_p^n en tant que $\mathbb{F}_p$ espace vectoriel est donnée par les monômes du type $x_1^{i_1} \ldots x_n^{i_n}$ avec $0 \leq i_j \leq p-1$, donc on a un total de p^n choix possibles pour les indices $(i_1, \ldots, i_n)$. A_p^n a alors dimension finie p^n et en particulier est artinien. □

Remarque 1.2.4. Soit M un A_p^n-module, alors $\mathrm{Hom}_{\mathbb{F}_p}(M, \mathbb{F}_p)$ hérite aussi une structure de A_p^n-module donné par $(a \cdot \varphi)(m) = \varphi(a \cdot m)$ pour tout $m \in M$, $a \in A_p^n$, $\varphi \in \mathrm{Hom}_{\mathbb{F}_p}(M, \mathbb{F}_p)$. On peut donc voir, avec abus de notation, $\mathrm{Hom}_{\mathbb{F}_p}(\bullet, \mathbb{F}_p)$ comme un foncteur de $A_p^n - \mathrm{Mod}$ contravariant dans lui même.

Lemme 1.2.5. *On a l'isomorphisme de A_p^n-modules:*

$$A_p^n \simeq \mathrm{Hom}_{\mathbb{F}_p}(A_p^n, \mathbb{F}_p)$$

Démonstration. Soit $B = (f_1, \ldots, f_{p^n})$ une base de A_p^n donnée par les monômes en degré croissant (par exemple dans un ordre lexicographique gradué $(x_n, x_{n-1}, \ldots, x_1, x_n^2, x_n x_{n-1}, \ldots, x_n^{p-1} \ldots x_1^{p-1})$) alors $f_{p^n} = x_1^{p-1} x_2^{p-1} \ldots x_n^{p-1}$.

On considère l'application $\xi : A_p^n \longrightarrow \mathbb{F}_p$ donnée par la projection sur $\mathrm{span}(f_{p^n})$ (par exemple si $n = 2$ et $p = 5$ on a $\xi(x_1 + 2x_2 + 3x_1^4 x_2^4) = 3$), on définit:

$$\begin{array}{rcl} \sigma : A_p^n \times A_p^n & \longrightarrow & \mathbb{F}_p \\ (r, s) & \mapsto & \xi(rs) \end{array}$$

Comme ξ est une application linéaire et A_p^n une $\mathbb{F}_p$-algèbre commutative, on obtient que σ est une forme bilinéaire symétrique. Donc on a une application linéaire:

$$\begin{array}{rcl} \psi : A_p^n & \longrightarrow & \mathrm{Hom}(A_p^n, \mathbb{F}_p) \\ r & \mapsto & \sigma(r, \bullet) \end{array}$$

On vérifie facilement que ψ est aussi un morphisme de A_p^n-modules, il reste donc à montrer que ψ est une bijection.

Comme ψ est un morphisme entre espaces de la même dimension, il suffit de montrer que ψ est injective: soit donc $0 \neq r \in A_p^n$, on veut montrer que $\psi(r) \neq 0$, i.e. il existe $s \in A_p^n$ tel que $\psi(r)(s) = \sigma(r, s) = \xi(rs) \neq 0$.

Soit $r = \lambda_1 f_1 + \cdots + \lambda_n f_{p^n}$ avec $\lambda_i \in \mathbb{F}_p$ la décomposition de r en monômes et i tel que $\lambda_i \neq 0$, $f_i = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. Si on pose $\tilde{f}_i := f_{p^n}/f^i = x_1^{p-i_1-1} x_2^{p-i_2-1} \ldots x_n^{p-i_n-1}$ on a $f_i \tilde{f}_i = x_1^{p-1} \ldots x_n^{p-1} = f_{p^n}$ et pour $j \neq i$ soit $\tilde{f}_i f_j = 0$, soit $\tilde{f}_i f_j = f_k \neq f_{p^n}$. Donc $\tilde{f}_i r = \mu_1 f_1 + \cdots + \mu_n f_{n^p}$ avec $\mu_n = \lambda_i \neq 0$ et en particulier $\xi(\tilde{f}_i r) \neq 0$. □

Définition 1.2.6. Un anneau R est dit injectif (ou auto-injectif) si R est injectif en tant que R-module.

On énumère dans la suite quelques propriétés des A_p^n-modules [La, §15-16]:

Proposition 1.2.7. *Soit M un A_p^n-module, on note $M^* := \mathrm{Hom}_{A_p^n}(M, A_p^n)$. On a les résultats suivants:*

1. $M^* \simeq \mathrm{Hom}_{\mathbb{F}_p}(M, \mathbb{F}_p)$
2. $M \simeq M^{**}$;
3. $\dim_{\mathbb{F}_p} M = \dim_{\mathbb{F}_p} M^*$;
4. *Le foncteur* $(\bullet)^* = \mathrm{Hom}_{A_p^n}(\bullet, A_p^n)$ *est exact*
5. $\mathbb{F}_p^* \simeq \mathbb{F}_p$
6. $A_p^{n*} \simeq A_p^n$
7. *M indécomposable si et seulement si M^* est indécomposable ;*
8. *A_p^n est injectif*
9. *M plat $\iff$ M projectif $\iff$ M libre $\iff$ M injectif.*

Démonstration. 1) Par le Lemme 1.2.5 et l'adjonction tensor-hom on a:

$$\begin{aligned} M^* &\simeq \mathrm{Hom}_{A_p^n}(M, A_p^n) \\ &\simeq \mathrm{Hom}_{A_p^n}(M, \mathrm{Hom}_{\mathbb{F}_p}(A_p^n, \mathbb{F}_p)) \\ &\simeq \mathrm{Hom}_{\mathbb{F}_p}(M \otimes_{A_p^n} A_p^n, \mathbb{F}_p) \\ &\simeq \mathrm{Hom}_{\mathbb{F}_p}(M, \mathbb{F}_p) \end{aligned}$$

dans la troisième équivalence l'anneau relatif au produit tensoriel et l'anneau relatif à Hom s'échangent grâce à l'adjonction. On obtient donc un isomorphisme de A_p^n-modules.

2-4) Viennent directement du fait que par le point 1) les foncteurs $\mathrm{Hom}_{A_p^n}(\bullet, A_p^n)$ et $\mathrm{Hom}_{\mathbb{F}_p}(\bullet, \mathbb{F}_p)$ sont naturellement équivalents (on rappelle la Remarque 1.2.4) et que M est un $\mathbb{F}_p$-espace vectoriel de dimension finie.

5) On a $\mathbb{F}_p^* \simeq \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p, \mathbb{F}_p)$ donc c'est un A_p^n-module de dimension un sur $\mathbb{F}_p$ avec action trivial de A_p^n.

6) En appliquant le Lemme 1.2.5 et le point 1) on obtient:
$A_p^n \simeq \mathrm{Hom}_{\mathbb{F}_p}(A_p^n, \mathbb{F}_p) \simeq A_p^{n*}$.

7) Soit $M \simeq U_1 \oplus U_2$ avec $U_i \neq 0$, alors $M^* \simeq U_1^* \oplus U_2^*$ est aussi une décomposition avec $\dim_{\mathbb{F}_p} U_i^* = \dim_{\mathbb{F}_p} U_i \neq 0$. Donc M^* indécomposable implique M indécomposable, mais par le point 2) on a aussi $M^{**} \simeq M$ indécomposable implique M^* indécomposable.

8) Conséquence immédiate du point 4.

9) On a M plat $\iff$ M projectif $\iff$ M libre car A_p^n est un anneau artinien local. Comme A_p^n est injectif alors M libre $\implies$ M injectif. Réciproquement, soit M un module injectif, alors par dualité M^* est un module projectif et donc libre, donc $M \simeq M^{**}$ est libre aussi. □

On donne quelques résultats simples qui nous seront utiles dans la suite:

Lemme 1.2.8. *Soit M un A_p^n-module, on identifie $x_i \in A_p^n$ avec l'action induite sur M, $x_i : M \to M$, $x_i(m) = x_i m$, alors:*

1. $\mathfrak{m}M \simeq \mathrm{Im}(x_1) + \cdots + \mathrm{Im}(x_n)$
2. $M^G \simeq \ker(x_1) \cap \cdots \cap \ker(x_n)$
3. $\frac{M}{\mathfrak{m}M} \simeq M \otimes \mathbb{F}_p$
4. $\left(\frac{M}{\mathfrak{m}M}\right)^* \simeq (M^*)^G$
5. $\frac{M^*}{\mathfrak{m}M^*} \simeq \left(M^G\right)^*$

Démonstration. 1-2) viennent directement de la définition de
$\mathfrak{m}M := (x_1, \ldots, x_n)M$ et de $M^G := \{m \in M | (x_i - 1)m = m,\ 1 \leq i \leq n\}$.

3) Comme A_p^n est un anneau local avec corps résiduel $\mathbb{F}_p$ on a:

$$\begin{aligned} \frac{M}{\mathfrak{m}M} &\simeq M \otimes \frac{A_p^n}{\mathfrak{m}M} \\ &\simeq M \otimes \mathbb{F}_p \end{aligned}$$

4) En appliquant l'adjonction tensor-hom sur le point 3) on obtient:

$$\begin{aligned}\left(\frac{M}{\mathfrak{m}M}\right)^* &\simeq (\mathbb{F}_p \otimes M)^* \\ &\simeq \mathrm{Hom}_{A_p^n}(\mathbb{F}_p \otimes_{A_p^n} M, A_p^n) \\ &\simeq \mathrm{Hom}_{A_p^n}(\mathbb{F}_p, \mathrm{Hom}_{A_p^n}(M, A_p^n)) \\ &\simeq \mathrm{Hom}(\mathbb{F}_p, M^*) \\ &\simeq (M^*)^G\end{aligned}$$

5) On le montre en remplaçant M par M^* dans le point 4) □

1.2.2 Modules de syzygie

Définition 1.2.9. Soit R un anneau local et M un R-module fini. Soit $(m_1, \ldots, m_b)$ un ensemble minimal de générateurs de M (par le lemme de Nakayama $b = \mathrm{rang}\,(M/\mathfrak{m}M)$) et on considère le morphisme $\epsilon : R^b \twoheadrightarrow M$ qui envoie la base canonique sur l'ensemble des générateurs de M. Alors $\Omega^1 M := \ker(\epsilon)$ est le (premier) module de syzygie de M:

$$0 \to \Omega^1 M \to R^b \xrightarrow{\epsilon} M \to 0$$

Plus généralement, pour tout $i \in \mathbb{N}$, si $\Omega^i M$ est le i-ème module de syzygie alors on note:

$$\Omega^{i+1} := \Omega\left(\Omega^i M\right)$$

le module de syzygie successif. Par convention on pose $\Omega^0 M = M$.

A priori la définition semblerait dépendre du choix du système de générateurs, mais en fait cela n'a aucune importance:

Proposition 1.2.10. *Soit R un anneau local et M un R-module fini, alors $\Omega^1 M$ est indépendant du choix des générateurs.*

Démonstration. Soient $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_m)$ deux ensembles de générateurs minimaux de M associés respectivement aux modules de syzygie $\Omega^1 M$ et $\widetilde{\Omega^1 M}$, on montre qu'ils sont isomorphes.

Si les (x_i) sont des générateurs, alors les (y_j) sont obtenus par combinaisons linéaires, donc il existe une matrice A à coefficients dans R tel que $A \cdot (x_1, \ldots, x_n) = (y_1, \ldots, y_m)$, et le produit par A définit alors une surjetion $M \twoheadrightarrow M$. Soit p la projection sur $M/\mathfrak{m}M$, alors le morphisme passe au quotient et il est défini par le produit par la matrice $\overline{A}$ à coefficients dans $k = R/\mathfrak{m}$.

Par le lemme de Nakayama $(\overline{x_i})$ et $(\overline{y_j})$ sont deux bases de $M/\mathfrak{m}M$, donc $m = n = \dim_k(M/\mathfrak{m}M)$ et le rang implique que le produit par $\overline{A}$ est un isomorphisme.

$$\begin{array}{ccc} M & \xrightarrow[\cdot A]{\simeq} & M \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ k^n \simeq \frac{M}{\mathfrak{m}M} & \xrightarrow[\cdot \overline{A}]{\simeq} & k^n \simeq \frac{M}{\mathfrak{m}M} \end{array}$$

La matrice $\overline{A}$ est alors inversible, donc $\det(\overline{A}) = \overline{\det(A)} \neq \overline{0}$ ce qui implique que $\det(A) \in R\backslash\mathfrak{m}$ est inversible dans R car c'est un anneau local. A est donc inversible aussi et définit un isomorphisme entre $\Omega^1 M$ et $\widetilde{\Omega^1 M}$. □

Si R est auto-injectif, c'est intéressant de définir le module de co-syzygie aussi:

Définition 1.2.11. Soit R un anneau local injectif et M un R-module fini. Soit $\eta : M \hookrightarrow R^c$ une injection telle que que $c \in \mathbb{N}$ soit minimal (par la Remarque 1.2.12 $c = \text{rang}\left(M^G\right)$). Alors $\Omega^{-1}M := \text{coker}(\eta)$ est le module de co-syzygie de M.

$$0 \to M \xrightarrow{\eta} R^c \to \Omega^{-1}M \to 0$$

Pour tout $i \in \mathbb{N}$, si $\Omega^{-i}M$ est le i-ième module de co-syzygie alors on note:

$$\Omega^{-i-1} := \Omega^{-1}\left(\Omega^{-i}M\right)$$

le module de co-syzygie suivant.

Remarque 1.2.12. Soit $c \in \mathbb{N}$ valeur minimale telle qu'il existe une injection $\eta : M \hookrightarrow R^c$, alors par dualité c est la valeur minimale pour laquelle il existe une surjection $\eta^* : R^c \twoheadrightarrow M^*$, donc $c = \dim\left(M^*/\mathfrak{m}M^*\right) = \dim\left(M^G\right)$ par le Lemme 1.2.8.

On énonce quelques propriétés du module de (co-)syzygie [Cr]:

Lemme 1.2.13. *Soit M un module sur un anneau R local injectif (dans notre cas $R = A_n^p$). Alors pour tout $i \in \mathbb{Z}$:*

1 $\left(\Omega^i M\right)^* = \Omega^{-i}M^*$;

2 $\Omega^i(M \oplus N) \simeq \Omega^i(M) \oplus \Omega^i(N)$;

3 $M \simeq \Omega^i(\Omega^{-i}M) \oplus F$ *où* F *est un module libre ;*

4 $\Omega^i(M) = 0$ *si et seulement si* M *est un module libre ;*

Démonstration. 1) On procède par récurrence. Si $i = 0$ l'énoncé est trivial, pour $i > 0$ soit $R^{b_i} \xrightarrow{\epsilon_i} \Omega^i M$ avec b_i minimal, on a alors la suite:

$$0 \to \Omega^{i+1}M \to R^{b_i} \xrightarrow{\epsilon_i} \Omega^i M \to 0$$

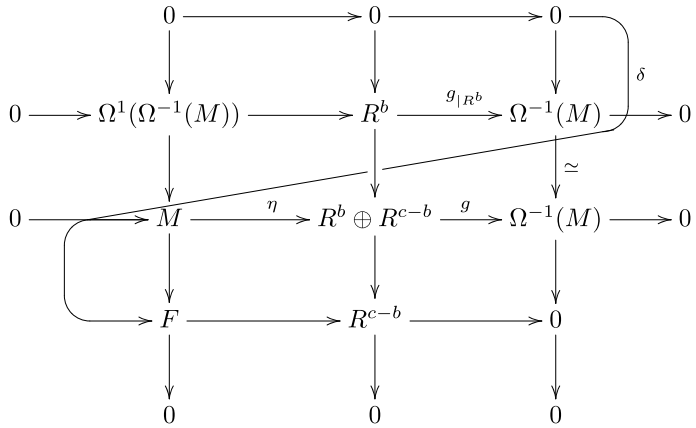
en dualisant on obtient la suite:

$$0 \to \left(\Omega^i M\right)^* \xrightarrow{\epsilon_i^*} R^{b_i} \to \left(\Omega^{i+1}M\right)^* \to 0$$

mais comme b_i est minimal on a $\left(\Omega^{i+1}M\right)^* \simeq \Omega^{-1}\left(\left(\Omega^i M\right)^*\right)$. Par hypothèse de récurrence $\left(\Omega^i M\right)^* \simeq \Omega^{-i}M^*$ donc $\left(\Omega^{i+1}M\right)^* \simeq \Omega^{-i-1}M^*$ ce qui prouve l'énoncé pour $i \geq 0$. Il suffit de dualiser pour le cas $i < 0$.

2) Le résultat découle immédiatement de l'indépendance du choix des générateurs dans le calcul du module de syzygie.

3) Il suffit de prouver le résultat pour $i = 1$. Soit c valeur minimale telle qu'il existe une injection $M \overset{\eta}{\twoheadrightarrow} R^c$, on a donc la suite $0 \to M \overset{\eta}{\to} R^c \overset{g}{\to} \Omega^{-1}M \to 0$. Si $(e_1, \ldots, e_c)$ est la base canonique de R^c, alors $(g(e_1), \ldots, g(e_c))$ est un ensemble de générateurs de $\Omega^{-1}M$. Par le lemme de Nakayama il existe un sous-ensemble de générateurs $(g(e_{i_1}), \ldots, g(e_{i_b}))$ de cardinalité minimale b avec $b = \dim(\Omega^{-1}M/\mathfrak{m}\Omega^{-1}M)$. Donc il existe une décomposition $R^c \simeq R^b \oplus R^{c-b}$ avec $g_{|R^b} \twoheadrightarrow \Omega^{-1}M$ surjectif. Par le lemme du serpent on obtient le diagramme commutatif:



avec $F \simeq R^{c-b}$ module libre. Donc $0 \to \Omega^1(\Omega^{-1}M) \to M \to F \to 0$, mais F libre implique F projectif, donc la suite scinde et $M \simeq \Omega^1(\Omega^{-1}M) \oplus F$.

4) Si M est un module libre alors $M \simeq R^a$ et on vérifie facilement que $\Omega^i R^a = \Omega^i R^a = 0$. Réciproquement, soit M tel que $\Omega^i(M) = 0$, alors $\Omega^1(\Omega^{i-1}M) = 0$ et il existe donc une surjection $R^b \overset{\epsilon}{\twoheadrightarrow} \Omega^{i-1}M$ avec $\ker(\epsilon) = 0$, donc $\Omega^{i-1}(M) \simeq R^b$ et donc soit $M = 0$ soit M est un module libre. □

Définition 1.2.14. Soit R un anneau artinien local injectif, un R-module M est dit *libre de projectifs* s'il n'existe aucun morphisme injectif $R \hookrightarrow M$.

Remarque 1.2.15. Comme R est injectif, s'il existe une injection $R \hookrightarrow M$ alors il existe un R-module M' tel que $M \simeq R \oplus M'$. Comme on verra plus tard, la décomposition en modules indécomposables est unique, donc un module est libre de projectifs si et seulement si R n'apparaisse pas dans sa décomposition.

Si M est un module libre de projectif, alors $\Omega^{-1}(\Omega^1(M)) \simeq M$, donc le syzygie et le co-syzygie deviennent deux opérations inverse l'une de l'autre. De plus, comme on peut prendre les modules de syzygie successifs, on peut associer à M une famille infinie de modules sur le même anneau. Donc on peut affirmer que pour un anneau R artinien local injectif, les syzygies et le co-syzygies définissent une relation d'équivalence sur les R-modules libres de projectif (en fait on peut facilement étendre cette relation à tous les

R-modules, en posant comme équivalent deux modules qui ont la même décomposition aux termes libres près).

Deux modules qui partagent la même classe d'équivalence partagent aussi des autres propriétés, comme:

Lemme 1.2.16. *Soit R un anneau artinien local injectif et M un R-module libre de projectif. Alors pour tout $i \in \mathbb{Z}$, M est indécomposable si et seulement si $\Omega^i M$ est indécomposable.*

Démonstration. Soit $M \simeq U_1 \oplus U_2$ avec U_1 et U_2 non libres et non nuls, alors par le Lemme 1.2.13 $\Omega^i M \simeq \Omega^i(U_1) \oplus \Omega^i(U_2)$ avec $\Omega^i(U_i) \neq 0$ et non libre, donc $\Omega^i M$ indécomposable implique que M est indécomposable aussi. Pour l'implication inverse, on a $M \simeq \Omega^{-i}(\Omega^i M)$ car M est libre de projectif, donc $\Omega^{-i}(\Omega^i M) \simeq M$ indécomposable implique que $\Omega^{-i} M$ est indécomposable. □

Pour conclure on énonce une dernière propriété qui constitue la raison principale (mais pas la seule) de s'intéresser aux modules de (co-)syzygie d'un $\mathbb{F}_p[G]$-module.

Lemme 1.2.17. *Soit M un $\mathbb{F}_p[G]$-module, alors pour tout $0 \leq j \leq i$:*

$$H^i(G, M) \simeq H^{i-j}(G, \Omega^{-j} M)$$

En particulier:

$$H^i(G, M) \simeq \left(\Omega^{-i} M\right)^G$$

Démonstration. Il suffit de prouver l'énoncé pour $j = 1$. Soit c minimale telle qu'il existe $M \overset{\eta}{\twoheadrightarrow} R^c$. On considère la suite exacte:

$$0 \to M \to \mathbb{F}_p[G]^c \to \Omega^{-1} M \to 0$$

En appliquant le foncteur $H^*(G, \bullet)$ on obtient la suite exacte:

$$0 \to H^0(G, M) \to H^0(G, \mathbb{F}_p[G]^c) \to H^0(G, \Omega^{-1} M) \to H^1(G, M) \to H^1(G, \mathbb{F}_p[G]^c)$$

mais $H^0(G, M) \simeq H^0(G, \mathbb{F}_p[G]^c) \simeq \mathbb{F}_p^c$ par le Lemme 1.2.12 et $H^s(G, \mathbb{F}_p[G]^c) = 0$ pour $s \geq 1$ car $\mathbb{F}_p[G]^c$ est un module libre. Donc pour tout $i \geq 1$ il ne reste que:

$$H^{i-1}(G, \Omega^{-1} M) \simeq H^i(G, M)$$

En particulier si $j = i$ on obtient $H^i(G, M) \simeq H^0(G, \Omega^{-i} M) \simeq (\Omega^{-i} M)^G$ où on applique le Lemme 1.2.12 pour la dernière équivalence.

□

1.2.3 Classification des modules sur $\mathbb{F}_p[G]$

On s'intéresse à déterminer les différentes possibilités pour un module de type fini sur A_p^n dans l'objectif de pouvoir idéalement en donner une liste.

Soit M un $\mathbb{F}_p[G]$-module fini, alors on a deux cas: soit M se décompose comme une somme de deux modules non nuls, soit M est indécomposable. En répétant la procédure, comme M est aussi un $\mathbb{F}_p$-espace vectoriel de dimension finie, il s'ensuit que tout $\mathbb{F}_p[G]$-module fini se décompose comme une somme finie de $\mathbb{F}_p[G]$-modules indécomposables.

Mais cette décomposition est-elle unique ? Pour un anneau R dont les modules ont une décomposition unique on dit que R a la propriété de Krull–Schmidt, plus précisément [Ben, 1.4.2]:

Définition 1.2.18. Un anneau R possède la propriété de Krull–Schmidt si pour tout choix de (M_i),(N_j) familles finies de modules indécomposables sur R telles que:

$$\bigoplus_{i=1}^{n} M_i \simeq \bigoplus_{j=1}^{m} N_j$$

alors $n = m$ et il existe un ré-arrangement des N_j tels que $M_i \simeq N_i$ pour tout i.

Il se trouve que tous anneaux artiniens possèdent la propriété de Krull–Schmidt pour les modules de type fini [Ben, 1.4.6]. Comme $\mathbb{F}_p[G]$ est un anneau artinien, cela s'applique à notre cas.

Par conséquent, le problème de déterminer tous les $\mathbb{F}_p[G]$-modules se réduit à la classification uniquement des $\mathbb{F}_p[G]$-modules indécomposables en classes d'isomorphisme, ce qu'on appelle la *représentation de* $\mathbb{F}_p[G]$. Malheureusement une telle classification n'est pas toujours réalisable. Plus précisément, pour un anneau de la forme $k[G]$ (avec k infini) trois cas se présentent [Ben, 4.4.1]:

- Il existe un nombre fini de modules indécomposables sur $k[G]$ qu'on peut énumérer. Dans ce cas, qui est généralement le cas plus simple, on dit que $k[G]$ *a représentation finie* ;
- Sinon $k[G]$ *a représentation infinie* et on a deux sous-cas:
  — Pour chaque $d \geq 1$, le modules indécomposables de dimension d sont classifiés par un nombre fini de familles a un paramètre. Plus précisément, une famille à un paramètre est un ensemble de $k[G]$-modules de la forme:

$$\mathcal{M} = \left\{ \frac{M}{(T-\lambda)M},\ \lambda \in k \right\}$$

avec M un $k[G] - k[T]$-bimodule de type fini et libre en tant que $k[T]$-module. En simplifiant, un module est donc identifié pour quelque paramètres discrets et un paramètre continu (comme par

exemple dans la réduction de Jordan). Dans ce cas, qui est généralement plus compliqué, mais traitable, on dit que $k[G]$ *a représentation modérée* ;

— La classification demande au moins une famille a deux paramètres ou plus. Dans ce cas classifier le modules indécomposables sur $\mathbb{F}_p[G]$ est au moins aussi complexe que donner une classification des modules sur l'algèbre libre $k\langle X, Y\rangle$. Plus précisément, il existe un $k[G]-k\langle T_1, T_2\rangle$-bimodule M libre en tant que $k\langle X, Y\rangle$-module tel que le foncteur $M\otimes_{k\langle X,Y\rangle}\bullet$ de la catégorie de $k\langle X, Y\rangle$-modules de type fini à celle de $k[G]$-modules préserve l'indécomposabilité et la classe d'isomorphisme.
Dans ce cas, qui est dans un certain sens « sans espoir », on dit que $k[G]$ *a représentation sauvage.*

Comme $\mathbb{F}_p$ est un corps fini, il s'ensuit par une simple considération de cardinalité qu'il existe au plus un nombre fini de $\mathbb{F}_p[G]$-modules de dimension donnée, mais pourtant aucune classification est connue pour $n \geq 2$ (sauf pour le cas $p = 2$ et $n = 2$).

La raison est plus claire si on remplace $\mathbb{F}_p$ par un corps k toujours de caractéristique p mais cardinalité infinie. En fait, dans ce cas on a le résultat suivant [Ben, 4.4.4]:

Théorème 1.2.19. *Soit k un corps de cardinalité infinie et caractéristique p et $G\simeq(\mathbb{Z}/p\mathbb{Z})^n$, alors:*

- *$k[G]$ a représentation finie si $n = 1$;*
- *$k[G]$ a représentation modérée si $p = 2$ et $n = 2$;*
- *$k[G]$ a représentation sauvage sinon.*

Apparemment, dans le cas « sauvage », l'avantage d'une cardinalité finie, même si théoriquement elle rend possible de donner une classification en un temps fini, ne simplifie pas le problème conceptuellement, qui reste donc aussi insurmontable que dans le cas infini.

C'est donc la raison pour laquelle on se limitera dans notre travail au cas $n = 1$ (qui est déjà présent dans [BNS]) et au cas $G\simeq(\mathbb{Z}/2\mathbb{Z})^2$ (groupe de Klein).

Une éventuelle généralisation aux autre cas serait difficilement réalisable en passant par une classification de $\mathbb{F}_p[G]$-modules, elle devrait d'une façon ou d'une autre passer cette étape.

1.2.3.1 Cas $n = 1$

Proposition 1.2.20. *Soit M un A_p-module indécomposable, $A_p\simeq\frac{\mathbb{F}_p[x]}{\langle x^p\rangle}$. Alors M est de la forme $M\simeq\mathbb{F}_p[x]/\langle x^j\rangle$ avec $0 \leq j \leq p$.*

Démonstration. Soit M un A_p-module indécomposable, alors M est aussi un module indécomposable sur l'anneau des polynômes $\mathbb{F}_p[x]$ et par la clas-

sification des modules sur les anneaux principaux, M est de la forme:

$$M \simeq \frac{\mathbb{F}_p[x]}{\langle \alpha \rangle}$$

Comme M est un A_p-module, on a $x^p M = 0$ qui implique que $\alpha | x^p$, donc $\alpha = x^j$ avec $0 \leq j \leq p$. □

De façon équivalente on peut voir M comme un idéal de A_p, qui est la forme utilisée dans la sous-section 1.1.4.2:

Lemme 1.2.21. *Soit $0 \leq j \leq p$, alors:*

$$\frac{\mathbb{F}_p[x]}{\langle x^j \rangle} \simeq \frac{\langle x^{p-j} \rangle}{\langle x^p \rangle}$$

Démonstration. Soit π la projection:

$$\begin{array}{rccc} \pi : \mathbb{F}_p[x] & \longrightarrow & \dfrac{(x^{p-j})}{(x^p)} \\ a & \mapsto & ax^{p-j} \end{array}$$

alors $\ker(\pi) = \langle x^j \rangle$ et le résultat vient du premier théorème d'isomorphisme. □

Corollaire 1.2.22. *Soit M un A_p-module indécomposable, $A_p \simeq \frac{\mathbb{F}_p[x]}{\langle x^p \rangle}$. Alors M est de la forme $M \simeq \langle x^j \rangle$, où $\langle x^j \rangle \leq A_p$ avec $0 \leq j \leq p$.*

1.2.3.2 Cas $n = 2$, $p = 2$

Dans la suite on considère le cas $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$, le groupe de Klein. La classification des modules dans ce cas est le résultat du travail de plusieurs personnes, qui ont affronté le problème dans des époques et avec des points de vue différents entre eux (dans [CB] où l'histoire de la preuve est retracée, les auteurs attribués sont Kronecker, Weierstrass, Basev, Gelfand, Ponomarev, Conlon, Heller, Reiner et Benson).

Dans la suite nous nous limiterons à donner la preuve uniquement dans le cas des modules impairs, renvoyant le lecteur intéressé à [Ben] ou [CB] pour le cas pair.

On commence par lister les cas les plus simples:

- $\mathbb{F}_2$ est le seul module de dimension un ;
- A_2^2 est le seul module indécomposable libre et a dimension 4.

On peut donc exclure ces deux cas dans la suite et en particulier choisir M libre de projectif:

Lemme 1.2.23. *Soit M un A_2^2-module. Alors M est libre de projectifs si et seulement si $\forall\, m \in M$, $xy \cdot m = 0$*

Démonstration. Soit $m \in M$ tel que $xy \cdot m \neq 0$, alors l'application $f : A_2^2 \to M$ tel que $f(1) = m$ est injective, car pour tout $a \in A_2^2$, $a \mid xy$ et donc $f(1) \neq 0$ implique que $f(a) \neq 0$ aussi.

Réciproquement si M n'est pas libre de projectifs alors il existe une injection $f : A_2^2 \hookrightarrow M$, donc $xy \cdot f(1) = f(xy) \neq 0$.

□

On peut voir un module M comme un $\mathbb{F}_2$-espace vectoriel et $x, y : M \to M$ des endomorphismes tels que $x \circ y = y \circ x = 0$. Donc si M est libre de projectifs on a $\mathrm{Im}(y) \subseteq \ker(x)$ et $\mathrm{Im}(x) \subseteq \ker(y)$ (on a aussi $\mathrm{Im}(x) \subseteq \ker(x)$ et $\mathrm{Im}(y) \subseteq \ker(y)$ car $x^2 = y^2 = 0$). On rappelle que par le Lemme 1.2.8 $\mathfrak{m}M = \mathrm{Im}(x) + \mathrm{Im}(y)$ et $M^G = \ker(x) \cap \ker(y)$, donc en particulier on a $\mathfrak{m}M \subseteq M^G$. Par conséquent les morphismes x, y passent au quotient et on obtient:

$$\frac{M}{\mathfrak{m}M} \underset{\overline{y}}{\overset{\overline{x}}{\rightrightarrows}} \mathfrak{m}M$$

Donc on peut toujours associer à un module libre de projectifs un couple de morphismes entre deux $\mathbb{F}_2$-espaces vectoriels. Réciproquement, si $f, g : V \to W$ sont deux applications linéaires, on peut se ramener au module $V \oplus W$ où l'action de A_2^2 est donnée par $x \cdot (v, w) = (0, f(v))$ et $y \cdot (v, w) = (0, g(v))$. Pour résumer:

Proposition 1.2.24. *Soit M un A_2^2-module libre de projectif, alors M est complètement identifié par le couple d'applications linéaires $\overline{x}, \overline{y} : M/\mathfrak{m}M \to \mathfrak{m}M$, et pour tout couple d'applications linéaires $f, g : V \to W$ il existe un module M identifié par f et g.*

Classifier les modules sur A_2^2 est alors un problème complètement équivalent à celui de classifier les paires de matrices à valeur dans $\mathbb{F}_2$ par équivalence simultanée. C'est d'ailleurs dans ce contexte que Kronecker avait originairement approché le problème.

On donne ici une reformulation légèrement différente de la Proposition 1.2.24 qu'on utilisera dans le Chapitre 3:

Corollaire 1.2.25. *Soit M un A_2^2-module libre de projectif, $I, K \subseteq M$ deux sous-modules tels que:*

$$\mathfrak{m}M \subseteq I \subseteq K \subseteq M^G \tag{1.2.1}$$

alors M se décompose partiellement comme:

- *Une somme de modules simples de la forme $\mathbb{F}_2^{\oplus(\dim(K)-\dim(I))}$;*
- *Un module libre de projectifs (a priori non-indécomposable) décrit par les morphismes $\frac{M}{K} \underset{g}{\overset{f}{\rightrightarrows}} I$ avec $f \circ \pi_K = x$ et $g \circ \pi_K = y$, $\pi_K : M \twoheadrightarrow \frac{M}{K}$ la projection sur le quotient par K, c'est-à-dire f et g*

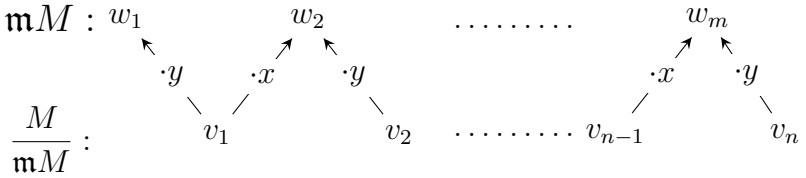
tels que les diagrammes suivants commutent:

Démonstration. On rappelle que $\mathfrak{m}M = \mathrm{Im}(x) + \mathrm{Im}(y)$ et $M^G = \ker(x) \cap \ker(y)$, donc en raisonnant comme dans la Proposition 1.2.24, M est identifié par le couple de morphismes $f, g : M/K \to K$. Soit J un supplémentaire" de I dans K, $K = I \oplus J$, alors les morphismes f et g se décomposent comme:

$$f, g : M/K \to I \oplus J \implies (M/K \to I) \oplus (0 \to J)$$

Le morphisme nul $0 \to J$ est identifié avec un module avec action de A_2^2 triviale, donc $\mathbb{F}_2^{\dim(J)}$, et $f, g : M/K \to I$ sont identifiés avec un module libre de projectifs. □

La Proposition 1.2.24 suggère aussi une façon intuitive de représenter graphiquement les A_2^2-modules: les diagrammes à zigzag. L'idée est de choisir $(v_1, \ldots, v_n)$ base de $M/\mathfrak{m}M$ et $(w_1, \ldots, w_m)$ base de $\mathfrak{m}M$, et de les représenter sur deux lignes horizontales. Ensuite on marque l'action donnée par le produit par x ou y par des flèches avec orientations différentes:



A priori il n'y a aucune raison pour laquelle l'image d'un éléments (v_i) corresponde à un des éléments (w_j) et donc un tel diagramme peut sembler d'utilité limitée, mais comme on verra dans la suite, si M est un module indécomposable alors on peut toujours choisir les bases (v_i) et (w_i) de façon que pour tous les v_i (sauf au plus un), $x(v_i) \in \{w_j\}$ et $y(v_i) \in \{w_j\}$.

Les diagrammes à zigzag se révèlent donc une façon pratique de représenter et même de faire des calculs sur les modules. Par exemple, pour représenter le dual d'un module à partir de son diagramme il suffit d'inverser le sens des flèches.

En vérité nous ne sommes pas obligés de nous limiter uniquement au cas des A_2^2-modules libres de projectif. À condition d'utiliser cette représentation sur plusieurs lignes (représentant une filtration de M du type $M \supseteq \mathfrak{m}M \supseteq \mathfrak{m}^2M \supseteq \cdots \supseteq \mathfrak{m}^{n(p-1)+1}M \supseteq \mathfrak{m}^{n(p-1)+2}M = 0$) elle peut être utilisée de manière plus générale à condition que $n = 2$ (voir par exemple [**CFS**]). Par exemple les diagrammes pour A_2^2 et A_3^2 sont:

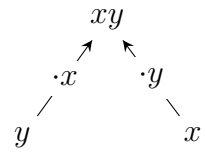
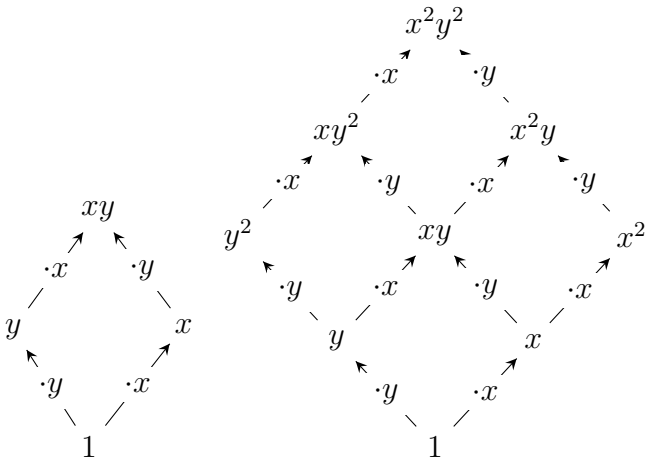


FIGURE 1.2.1 – Diagramme à zigzag du module $M = \mathfrak{m} = (x, y) \leq A_2^2$. Les espaces vectoriels sont $W = \mathfrak{m}M = \langle xy \rangle$ et $V = M/\mathfrak{m}M = \langle x, y \rangle$.



Avant de donner la classification pour le cas impair, on aura besoin du résultat suivant:

Lemme 1.2.26. *Soit M un A_2^2-module indécomposable différent de $\mathbb{F}_2$ et de A_2^2, $b, c \in \mathbb{N}$ les valeurs minimales pour lesquelles il existe respectivement des morphismes $(A_2^2)^b \twoheadrightarrow M$ et $M \hookrightarrow (A_2^2)^c$, alors $b + c = \dim_{\mathbb{F}_2} M$.*

Démonstration. On rappelle que $b = \dim(M/\mathfrak{m}M)$ et $c = \dim(M^G)$, comme $\mathfrak{m}M \subseteq M^G$, pour conclure on doit montrer que $\mathfrak{m}M = M^G$.

Soit donc $m \in M^G \backslash \mathfrak{m}M$, alors $x \cdot m = y \cdot m = 0$ et pour tout $m' \in M$, $x \cdot m' \neq m \neq y \cdot m'$. Soit $\overline{N}$ un supplémentaire de $\langle m \rangle$ dans $M/\mathfrak{m}M$, et (avec un abus de notation) $N = A_2^2\overline{N}$ le sous-module de M engendré par les éléments de $\overline{N}$, alors M libre de projectifs implique que les éléments de $\mathfrak{m}M$ sont tous images d'un élément de $M/\mathfrak{m}M$, mais comme m n'a pas d'image on a $\mathfrak{m}\overline{N} = \mathfrak{m}M$. De plus, m n'est dans l'image d'aucun élément, donc $M = N \oplus \langle m \rangle$ est une décomposition, mais M indécomposable implique que $M \simeq \langle m \rangle \simeq \mathbb{F}_2$, ce qui contredit les hypothèses. □

Voyons maintenant comment on peut utiliser les modules de syzygie successifs pour obtenir tous les modules impairs. Dans la sous-section 1.1.2 nous avons vu une résolution libre de A_2^2 de la forme:

$$... \to \left(A_2^2\right)^4 \xrightarrow{d_3} \left(A_2^2\right)^3 \xrightarrow{d_2} \left(A_2^2\right)^2 \xrightarrow{d_1} A_2^2 \to \mathbb{F}_p$$

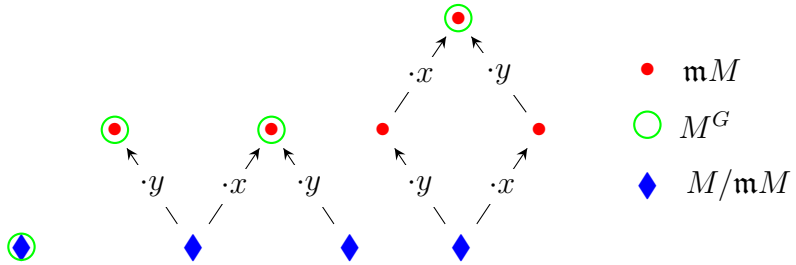


FIGURE 1.2.2 – Représentation de certains sous-modules remarquables d'un A_2^2-module M à l'aide d'un diagramme à zigzag

où les morphismes d_i ont la forme:

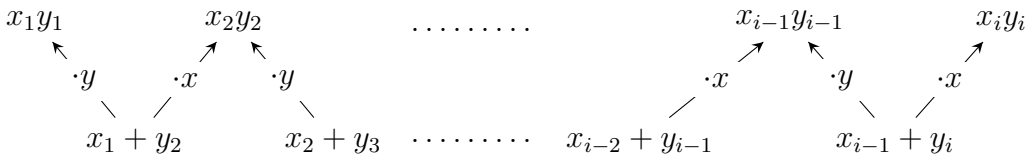
$$\begin{array}{rcl} d_i : \left(A_2^2\right)^{i+1} & \longrightarrow & \left(A_2^2\right)^i \\ (f_1, \ldots, f_{i+1}) & \mapsto & (f_1x + f_2y, f_2x + f_3y, f_3x + f_4y, \ldots, f_ix + f_{i+1}y) \end{array}$$

donc $\Omega^i\mathbb{F}_2 \simeq \ker(d_i) \simeq \mathrm{Im}(d_{i+1})$ pour tout i et on a la suite exacte courte:

$$0 \to \Omega^i\mathbb{F}_2 \xrightarrow{d_i} \left(A_2^2\right)^i \xrightarrow{d_{i-1}} \Omega^{i-1}\mathbb{F}_2 \to 0$$

En connaissant les morphismes d_i on peut reconstruire le diagramme à zigzag de $\Omega^i\mathbb{F}_2$:

On inverse le sens des flèches pour obtenir le diagramme de $\Omega^{-i}\mathbb{F}_2$:



Théorème 1.2.27 ([Ben, 4.3]). *Les A_2^2-modules impairs de dimension $2i+1$ avec $i \geq 1$, sont de la forme $\Omega^i\mathbb{F}_2$ (noté aussi M_{2i+1}) ou $\Omega^{-i}\mathbb{F}_2$ (noté aussi W_{2i+1}). En plus $\Omega^i\mathbb{F}_2 \not\simeq \Omega^{-i}\mathbb{F}_2$.*

Démonstration. Par les Lemmes 1.2.16 et 1.2.26 $\Omega^i\mathbb{F}_2$ est un module indécomposable de dimension $\dim_{\mathbb{F}_2} \Omega^i\mathbb{F}_2 = 2i + 1$.

Le même résultat est donc vrai pour son dual $\Omega^{-i}\mathbb{F}_2 = (\Omega^i\mathbb{F}_2^*)^* = (\Omega^i\mathbb{F}_2)^*$ et en plus $\Omega^i\mathbb{F}_2 \not\simeq \Omega^{-i}\mathbb{F}_2$ car leurs modules de syzygie ont des dimensions différentes:

$$\begin{aligned}\dim_{\mathbb{F}_2}\Omega\left(\Omega^i\mathbb{F}_2\right) &= \dim_{\mathbb{F}_2}\Omega^{i+1}\mathbb{F}_2 = 2i+3\\ \dim_{\mathbb{F}_2}\Omega\left(\Omega^{-i}\mathbb{F}_2\right) &= \dim_{\mathbb{F}_2}\Omega^{-i+1}\mathbb{F}_2 = 2i-1\end{aligned}$$

Donc pour tout $k = 2i+1$, $\Omega^i\mathbb{F}_2$ et $\Omega^{-i}\mathbb{F}_2$ sont deux A_2^2-modules indécomposables différents de dimension k. Il reste à montrer qu'il n'en n'existe pas d'autres.

Soit M un module indécomposable de dimension $2i+1$, $i \geq 1$, et $b, c \in \mathbb{N}$ les valeurs minimales telles qu'il existe les morphismes $(A_2^2)^b \twoheadrightarrow M$ et $M \hookrightarrow (A_2^2)^c$, alors par le Lemme 1.2.26 soit $b \leq i$, soit $c \leq i$. Supposons sans perte de généralité que $b \leq i$ (si $c \leq i$ le restant de la preuve est identique en échangeant les modules de syzygie par les modules de co-syzygie), alors on a la suite exacte:

$$0 \to \Omega M \to \left(A_2^2\right)^b \to M \to 0$$

avec $\dim \Omega M \leq 4b - 2i - 1 \leq 2i - 1$. Donc $\dim \Omega M < \dim M$ et en itérant le raisonnement, en prenant les modules de syzygie successifs on obtiendra une suite de modules de dimension décroissante, jusqu'à obtenir que pour un certain $j \in \mathbb{N}$, $\Omega^j M = \mathbb{F}_2$ et donc M est de la forme $M \simeq \Omega^{-j}\mathbb{F}_2$. □

Pour les modules de dimension paire on a la classification suivante [Ben, 4.3]:

Théorème 1.2.28. *Soit M un A_2^2-module pair non libre de dimension $2i$ avec $i \geq 1$, $W := \mathfrak{m}M$ et V un supplémentaire de W, donc $M \simeq V \oplus W$. Alors $\dim_{\mathbb{F}_2} V = \dim_{\mathbb{F}_2} W = i$ et pour M on a trois cas différents, classifiés par les morphismes $x, y : V \to W$:*

- *$M \simeq E_{0,2i}$, avec $x = Id$ et y avec matrice:*

$$J = \begin{pmatrix} 0 & & & & 0 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & \\ 0 & & & 1 & 0 \end{pmatrix}$$

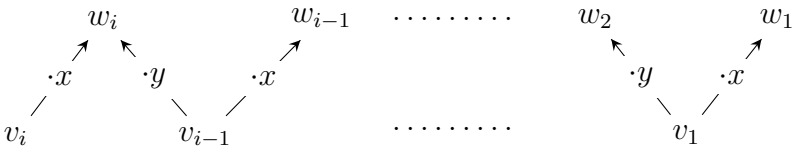
- *$M \simeq E_{\infty,2i}$ avec $y = Id$ et x avec matrice égale à J ;*
- *$M \simeq E_{f,2i}$ avec $f(a) = a^i + \sum_{j=0}^{i-1}\lambda_j a^j = (g(a))^m$ où $g(a)$ est un poly-*

nôme unitaire irréductible non nul, $x = Id$ et y avec matrice:

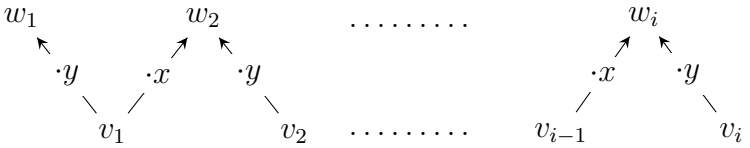
$$\begin{pmatrix} 0 & & & 0 & \lambda_0 \\ 1 & 0 & & & \lambda_1 \\ & 1 & 0 & & \vdots \\ & & \ddots & 0 & \lambda_{i-2} \\ 0 & & & 1 & \lambda_{i-1} \end{pmatrix}$$

Remarque 1.2.29. Pour les modules pairs on a les diagrammes à zigzag suivants:

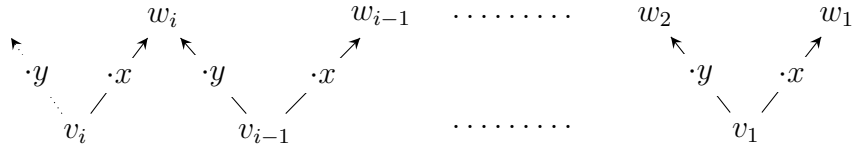
- $E_{0,2i}$:



- $E_{\infty,2i}$:



- $E_{f,2i}$ (la première flèche représente le morphisme donné par $y \cdot v_i = \sum \lambda_j w_j$):



Dans la suite on aura besoin du résultat suivant:

Lemme 1.2.30. *Soit M un A_2^2-module indécomposable non libre de dimension paire. Alors pour tout $i \in \mathbb{Z}$:*

$$\dim_{\mathbb{F}_2} M = \dim_{\mathbb{F}_2} \Omega^i M$$

Démonstration. Il suffit de prouver l'énoncé pour $i = \pm 1$. On procède par récurrence sur $\dim_{\mathbb{F}_2}(M) = 2n$, si $n = 0$ la preuve est triviale, sinon par le Lemme 1.2.26 il existe les morphismes $(A_2^2)^b \twoheadrightarrow M$ et $M \hookrightarrow (A_2^2)^c$ avec b, c minimales et $b + c = 2n$.

On affirme que $b = c = n$ et donc on a la suite exacte:

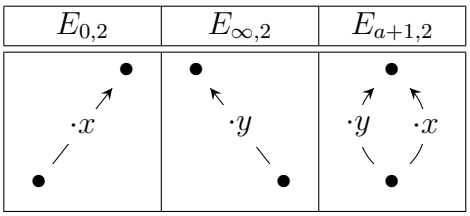
$$0 \to \Omega M \to \left(A_2^2\right)^b \twoheadrightarrow M \hookrightarrow \left(A_2^2\right)^c \to \Omega^{-1} M \to 0$$

avec $\dim \Omega^1 M = \dim \Omega^{-1} M = 4n - 2n = 2n$ ce qui prouve le Lemme.

Sinon dans le cas contraire on aurait que soit $b < n$, soit $c < n$. Supposons sans perte de généralité que $b < n$, alors $\dim \Omega M \leq 4b - 2n < 2n$. Donc $\Omega^{-1}(\Omega^1 M) = M$ est un module de dimension différent de $\Omega^1 M$, en contradiction avec l'hypothèse de récurrence. □

En fait l'équivalence n'est pas uniquement sur la dimension, puisque plus généralement on a $M \simeq \Omega^i M$. Mais dans le cadre de ce travail montrer qu'ils ont la même dimension est suffisant pour nos besoins.

Remarque 1.2.31. Si M est un module de dimension 2 (cas qui nous intéressera le plus dans le Chapitre 3) le seul polynôme $f(a)$ unitaire non nul avec $\deg(f) \leq 1$ est $a + 1$. Il existe donc uniquement trois modules irréductibles de dimension 2, c'est-à-dire:



1.3 Structure d'algèbre de $H^*(G, M)$

1.3.1 Résultats techniques

Les résultats suivants s'appliquent à n'importe quel $\mathbb{F}_p[G]$-module, même si nous les utiliserons uniquement dans le cas de $\mathbb{F}_p[G] = A_2^2$.

On cite d'abord les deux lemmes suivants [Br, V.3]:

Lemme 1.3.1. *Soit $f : M \to N$ morphisme de $\mathbb{F}_p[G]$-modules, et $u \in H^*(G, M)$, $v \in H^*(G, \mathbb{F}_p)$. Alors:*

$$f^*(u \cup v) = f^* u \cup v$$

Lemme 1.3.2. *Soit $0 \to M \to N \to P \to 0$ une suite exacte de $\mathbb{F}_p[G]$-modules i. Alors $\delta(u \cup v) = \delta(u) \cup v$ pour tout $u \in H^p(G, P)$, $v \in H^q(G, \mathbb{F}_p)$ où δ est le morphisme de bord, i.e. le diagramme suivant commute:*

$$\begin{array}{ccc} H^p(G,P) & \xrightarrow{\delta} & H^{p+1}(G,M) \\ {\scriptstyle -\cup v}\downarrow & & \downarrow{\scriptstyle -\cup v} \\ H^{p+q}(G,P) & \xrightarrow{\delta} & H^{p+q+1}(G,M) \end{array}$$

Le premier lemme permet d'établir le lien entre un morphisme de module et son action sur la cohomologie, alors que le deuxième est utile dans les arguments de type « dimension-shifting ». En particulier nous l'utiliserons pour établir le lien entre la cohomologie d'un groupe et son module de syzygie.

Proposition 1.3.3. *Soit:*

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

une suite exacte de $\mathbb{F}_p[G]$-modules, alors f et g induisent respectivement deux morphismes $\tilde{f} : H^*(G, M) \to H^*(G, N)$ et $\tilde{g} : H^*(G, N) \to H^*(G, P)$ de $H^*(G, \mathbb{F}_p)$-modules entre les modules de cohomologie associés.

De plus, si pour tout i, le morphisme induit sur la i-ème cohomologie $f^i : H^i(G, M) \to H^i(G, N)$ [ou $g^i : H^i(G, N) \to H^i(G, P)$] est injectif [ou surjectif] alors $\tilde{f}$ [ou $\tilde{g}$] est aussi injectif [ou surjectif].

Démonstration. En appliquant le foncteur $H^*(G, \bullet)$ on obtient la suite exacte longue:

$$0 \to H^0(G, M) \xrightarrow{f^0} H^0(G, N) \xrightarrow{g^0} H^0(G, P) \xrightarrow{\partial^0} H^1(G, M) \xrightarrow{f^1} H^1(G, N) \xrightarrow{g^1} \dots$$

comme $H^*(G, M) \simeq \bigoplus_i H^i(G, M)$ et $H^*(G, N) \simeq \bigoplus_i H^i(G, N)$, si on pose $\tilde{f} := \bigoplus f^i$ on obtient que:

$$\tilde{f} : H^*(G, M) \to H^*(G, N)$$

est un morphisme de $\mathbb{F}_p$-espaces vectoriels, qui est injectif [ou surjectif] si f^i est injectif [ou surjectif] pour tout i. Pour conclure $\tilde{f}$ est un morphisme de $H^*(G, \mathbb{F}_p)$-modules grâce au Lemme 1.3.1. L'argument est le même pour g. □

Corollaire 1.3.4. *Soit:*

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

une suite exacte de $\mathbb{F}_p[G]$-modules, tels que pour tout $i \in \mathbb{N}$ on a:

$$\dim_{\mathbb{F}_p}\left(\left(\Omega^{-i}N\right)^G\right) = \dim_{\mathbb{F}_p}\left(\left(\Omega^{-i}M\right)^G\right) + \dim_{\mathbb{F}_p}\left(\left(\Omega^{-i}P\right)^G\right)$$

Alors f et g induisent une suite exacte de $H^*(G, \mathbb{F}_p)$-modules gradués:

$$0 \to H^*(G, M) \xrightarrow{\tilde{f}} H^*(G, N) \xrightarrow{\tilde{g}} H^*(G, P) \to 0$$

Démonstration. En appliquant le foncteur $H^*(G, \bullet)$ on obtient la suite exacte longue:

$$0 \to H^0(G, M) \xrightarrow{f^0} H^0(G, N) \xrightarrow{g^0} H^0(G, P) \xrightarrow{\partial^0} H^1(G, M) \xrightarrow{f^1} H^1(G, N) \xrightarrow{g^1} \dots$$

Par le Lemme 1.2.17 on a:

$$\dim_{\mathbb{F}_p}\left(H^i(G, N)\right) = \dim_{\mathbb{F}_p}\left(H^i(G, M)\right) + \dim_{\mathbb{F}_p}\left(H^i(G, P)\right)$$

En raisonnant sur les dimensions on obtient alors que pour tout i la suite suivante est exacte:

$$0 \to H^i(G, M) \xrightarrow{f^i} H^i(G, N) \xrightarrow{g^i} H^i(G, P) \to 0$$

On conclut alors par la Proposition 1.3.3. □

Proposition 1.3.5. *Soit M un $\mathbb{F}_p[G]$-module libre de projectif, alors $H^*(G,M) \simeq H^{\geq 1}(G, \Omega^1 M)$ comme $H^*(G,\mathbb{F}_p)$-modules.*

Démonstration. On a la suite exacte courte:

$$0 \to \Omega^1 M \xrightarrow{f} \mathbb{F}_p[G]^b \xrightarrow{g} M \to 0$$

et en appliquant le foncteur $H^*(G,\bullet)$ on obtient la suite exacte longue:

$$0 \to H^0(G,\Omega^1 M) \xrightarrow{f^0} H^0(G,\mathbb{F}_p[G]^b) \xrightarrow{g^0} H^0(G,M) \xrightarrow{\partial^0} H^1(G,\Omega^1 M) \xrightarrow{f^1} H^1(G,\mathbb{F}_p[G]^b) \xrightarrow{g^i} \dots$$

Par le Lemme 1.2.17 $\dim\left(H^0(G,\Omega^1 M)\right) = \dim\left((\Omega^1 M)^G\right) = b$ donc f^0 est une bijection et $g^0 = 0$. Comme un module libre a cohomologie nulle, il s'ensuit que pour tout i, $f^i = 0$, $g^i = 0$ et $\partial^i : H^i(G,M) \xrightarrow{\simeq} H^{i+1}(G,\Omega^1 M)$ est un isomorphisme.

Alors $H^*(G,M) \simeq H^{\geq 1}(G,\Omega^1 M)$ en tant que $\mathbb{F}_p$-espaces vectoriels et par le Lemme 1.3.2 ils sont isomorphes aussi en tant que $H^*(G,\mathbb{F}_p)$-modules. □

On a vu dans le Lemme 1.1.24 que pour $G \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ la structure d'algèbre est $H^*(G,\mathbb{F}_2) \simeq \mathbb{F}_2[u,v]$, donc en appliquant la Proposition 1.3.5 on obtient que $H^*(G,\Omega^{-1}) \simeq H^{\geq 1}(G,\mathbb{F}_p) \simeq \mathbb{F}_2[u,v]_{\geq 1}$ et donc plus en général $H^*(G,\Omega^{-i}) \simeq \mathbb{F}_2[u,v]_{\geq i}$.

On a clairement $H^*(G,\mathbb{F}_2[G]) = \mathbb{F}_p$, donc il ne reste qu'à déterminer la structure de $H^*(G,\mathbb{F}_2)$-module de $H^*(G,\Omega^{-1})$ et de $H^*(G,E_{f,2i})$. Cependant, même si initialement cela avait été la solution adoptée, on utilisera ici une approche différente, qui, en faisant utilisation des Lemmes 1.2.17 et 1.3.4 permet de déterminer les invariants qui nous intéressent sans avoir besoin de passer par un calcul explicite de la structure de module, qui finalement se révèle ne pas etre nécessaire dans le cadre de ce travail.

1.3.2 Calcul de $H^*(G,M)_{(0)}$

1.3.2.1 Réduction de l'énoncé

Nous avons maintenant tous les outils nécessaires pour pouvoir finalement appliquer le Théorème 0.0.1 qu'on rappelle ici.

Théorème. *0.0.1 Soit $G = (\mathbb{Z}/p\mathbb{Z})^n$ avec p premier qui agit sur une surface X avec $dim_{\mathbb{F}_p} H^*(X^G,\mathbb{F}_p) < \infty$ et tel que $H^1(X) = H^3(X) = 0$ avec $X^G \neq \emptyset$. Alors :*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G,\mathbb{F}_p) = \begin{cases} \sum\limits_i \left(\sum\limits_{j=0}^{n} \dim_{\mathbb{F}_2} \left((-1)^j \operatorname{Tor}^j_{\mathbb{F}_p[u_1,\dots,u_n]}(\mathbb{F}_2, H^*(G; H^i(X,\mathbb{F}_2))) \right) \right) & si\ p = 2 \\ 2^{-n} \sum\limits_i \left(\sum\limits_{j=0}^{n} \dim_{\mathbb{F}_p} \left((-1)^j \operatorname{Tor}^j_{\mathbb{F}_p[u_1,\dots,u_n]}(\mathbb{F}_p, H^*(G; H^i(X,\mathbb{F}_p))) \right) \right) & si\ p \geq 3 \end{cases}$$

Nous allons réduire cet énoncé en une forme simplifiée.

Soit M un $\mathbb{F}_p[G]$-module, par le Théorème 1.4.6 $H^*(G,M)$ est un $\mathbb{F}_p[u_1,\dots,u_n]$-module de type fini et on est dans les hypothèses du lemme suivant:

Lemme 1.3.6. *Soit k un corps, N un $k[x_1, \ldots, x_n]$-module fini, alors pour $N_{(0)} \simeq N \otimes_{k[u_1,\ldots,u_n]} k(u_1, \ldots, u_{m,})$ on a:*

$$\dim_{k(u_1,\ldots,u_n)} N_{(0)} = \sum_{j=0}^{n} (-1)^j \dim_k Tor^j(k, N)$$

Démonstration. N est de type fini, donc il admet une résolution libre $F^\bullet \to N$ de longueur au plus n (cf. Sous-section 1.4.1):

$$0 \to F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \ldots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \to N \to 0 \tag{1.3.1}$$

avec $F_j \simeq (k[x_1, \ldots, x_n])^{i_j}$ et $\mathrm{Im}(d_j) = \ker(d_{j-1})$. Si on applique le foncteur $\bullet \otimes k$, alors $F_j \otimes k \simeq k^{i_j}$ et on obtient le complexe:

$$0 \to k^{i_n} \xrightarrow{d_n \otimes k} k^{i_{n-1}} \xrightarrow{d_{n-1} \otimes k} \ldots \xrightarrow{d_2 \otimes k} k^{i_1} \xrightarrow{d_1 \otimes k} k^{i_0} \to 0$$

avec $\mathrm{Im}(d_j \otimes k) \subseteq \ker(d_{j-1} \otimes k)$. Par définition l'homologie du complexe donne les modules du foncteur dérivé $\mathrm{Tor}^j(k, \bullet)$:

$$\mathrm{Tor}^j(k, H^*(G, M)) \simeq \frac{\ker(d_j \otimes k)}{\mathrm{Im}(d_{j+1} \otimes k)}$$

En appliquant la formule du rang et en réarrangeant le terme de la somme on obtient:

$$\begin{aligned}
& \sum_{j=0}^{n} (-1)^j \dim_k \mathrm{Tor}^j(k, H^*(G, M)) \\
= & \sum_{j=0}^{n} (-1)^j \left(\dim_k \ker(d_j \otimes k) - \dim_k \mathrm{Im}(d_{j+1} \otimes \mathbb{F}_p)\right) \\
= & \sum_{j=0}^{n} (-1)^j \left(i_j - \dim_k \mathrm{Im}(d_j \otimes \mathbb{F}_p) - \dim_k \mathrm{Im}(d_{j+1} \otimes \mathbb{F}_p)\right) \\
= & \sum_{j=0}^{n} (-1)^j i_j
\end{aligned}$$

Le même résultat apparaît si on applique la localisation dans l'idéal zéro (ce qui est équivalent au produit tensoriel par le corps des fractions rationnelles $\otimes_{k[x_1,\ldots,x_n]} k(x_1, \ldots, x_n)$) à la suite (1.3.1). Comme la localisation est un foncteur exact (et de façon équivalente le corps des fractions est un module plat) on obtient la suite exacte d'espaces vectoriels:

$$0 \to (k(x_1, \ldots, x_n))^{i_n} \to \ldots \to (k(x_1, \ldots, x_n))^{i_0} \to N_{(0)}$$

Et pour la dimension sur le corps $k(x_1, \ldots, x_n)$ on a:

$$\begin{aligned}
\dim_{k(x_1,\ldots,x_n)} N_{(0)} &= \sum_{j=0}^{n} (-1)^j i_j \\
&= \sum_{j=0}^{n} (-1)^j \dim_k \mathrm{Tor}^j(k, N)
\end{aligned}$$

□

On peut donc réécrire le Théorème 0.0.1 de la façon suivante:

Théorème 1.3.7. *Soit $G = (\mathbb{Z}/p\mathbb{Z})^n$ qui agit sur une surface X avec $dim_{\mathbb{F}_p} H^*(X^G, \mathbb{F}_p) < \infty$ et tel que $H^1(X) = H^3(X) = 0$ avec $X^G \neq \emptyset$. Alors :*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) = \begin{cases} \sum_i \dim_{\mathbb{F}_2(u_1,\dots,u_n)} \left(H^*(G; H^i(X, \mathbb{F}_2))\right)_{(0)} & si\ p = 2 \\ \sum_i 2^{-n} \dim_{\mathbb{F}_p(u_1,\dots,u_n)} \left(H^*(G; H^i(X, \mathbb{F}_p))\right)_{(0)} & si\ p \geq 3 \end{cases}$$

La deuxième simplification apportée vient du fait que dans notre cas X est une surface $K3$, donc les conditions sur la cohomologie sont automatiquement satisfaites, et il ne reste qu'à vérifier que le lieu fixe soit non-vide. En plus si on pose:

$$M_i := H^i(X, \mathbb{F}_p)$$

alors pour $M_0 \simeq M_4 \simeq \mathbb{F}_p$ on a que la dimension sur le corps $\mathbb{F}_p(u_1, \dots, u_n)$ est:

$$\dim \left(H^*(G, \mathbb{F}_p)\right)_{(0)} = \begin{cases} \dim \mathbb{F}_2(u_1, \dots, u_n) = 1 & \text{si } p = 2 \\ \dim \mathbb{F}_p(u_1, \dots, u_n) \otimes \bigwedge(s_1, \dots, s_n) = 2^n & \text{si } p \geq 3 \end{cases}$$

et en remplaçant dans le Théorème 1.3.7 on obtient:

Théorème 1.3.8. *Soit $G = (\mathbb{Z}/p\mathbb{Z})^n$ qui agit sur X une surface $K3$ avec $X^G \neq \emptyset$. Alors:*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) = \begin{cases} 2 + \dim_{\mathbb{F}_2(u_1,\dots,u_n)} \left(H^*(G; H^2(X, \mathbb{F}_2))\right)_{(0)} & si\ p = 2 \\ 2 + 2^{-n} \dim_{\mathbb{F}_p(u_1,\dots,u_n)} \left(H^*(G; H^2(X, \mathbb{F}_p))\right)_{(0)} & si\ p \geq 3 \end{cases}$$

Soit $M_2 = N_1 \oplus \cdots \oplus N_k$ une décomposition en modules indécomposables, donc pour tout i, $H^*(G, N_i)$ est un $H^*(G, \mathbb{F}_p)$-module et par le Lemme 1.1.24 $H^*(G, N_i)$ est aussi un $\mathbb{F}_p[u_1, \dots, u_n]$-module.

Si on pose $d_i = \dim_{\mathbb{F}_p(u_1,\dots,u_n)} \left(H^*(G, N^i)\right)_{(0)}$ et on applique le Théorème 1.3.8 on obtient:

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) = \begin{cases} 2 + \sum d_i & \text{si } p = 2 \\ 2 + 2^{-n} \sum d_i & \text{si } p \geq 3 \end{cases} \tag{1.3.2}$$

La dernière étape de ce chapitre est de déterminer les valeurs d_i associées aux différents modules N_i indécomposables qui interviennent dans la décomposition de $H^2(X, \mathbb{F}_p)$. Comme nous l'avons déjà anticipé, il nous est possible de donner une telle liste uniquement pour les cas $n = 1$ et $n = p = 2$, car ce sont les seuls cas où une classification des modules indécomposables existe.

1.3.2.2 Cas $n = 1$

Ce cas est déjà résolu dans [BNS], mais on le présente ici pour exhaustivité et aussi pour en donner une preuve différente. On rappelle que par le Corollaire 1.2.22 les A_p-modules sont tous de la forme $\langle x^j \rangle$ et les modules de cohomologie sont décrits dans la sous-section 1.1.4.2.

Cas $p = 2$: Soit M un A_2-module, alors on a deux possibilités:

- $M \simeq (1) \simeq A_2$, donc $H^*(G, A_2) = \mathbb{F}_2$, mais $\mathbb{F}_2 \otimes_{\mathbb{F}_2[u]} \mathbb{F}_2(u) = 0$ qui a dimension nulle ;
- $M \simeq (x) \simeq \mathbb{F}_2$, donc $H^*(G, \mathbb{F}_2) = \mathbb{F}_2[u]$ et $\mathbb{F}_2[u] \otimes_{\mathbb{F}_2[u]} \mathbb{F}_2(u) = \mathbb{F}_2(u)$ qui a dimension un.

Cas $p \geq 3$: Soit M un A_p-module avec $p \geq 3$, alors on a les possibilités suivantes:

- $M \simeq (1) \simeq A_p$, donc $H^*(G, A_p) = \mathbb{F}_p$, mais $\mathbb{F}_p \otimes_{\mathbb{F}_p[u]} \mathbb{F}_p(u) = 0$ qui a dimension nulle ;
- $M \simeq (x^{p-1}) \simeq \mathbb{F}_p$, donc $H^*(G, \mathbb{F}_p) = \mathbb{F}_p[u] \otimes \bigwedge(s) \simeq \mathbb{F}_p[u]^2$ en tant que $\mathbb{F}_p[u]$-module, donc $\mathbb{F}_p[u]^2 \otimes_{\mathbb{F}_p[u]} \mathbb{F}_p(u) = \mathbb{F}_p(u)^2$ qui a dimension deux ;
- $M \simeq (x)$, $H^*(G, M) = (1 \otimes u^2, \sigma \otimes 1) \simeq \mathbb{F}_p[u]^2$ en tant que $\mathbb{F}_p[u]$-module, donc on a encore $\dim_{\mathbb{F}_p(u)} H^*(G, M)_{(0)} = 2$;
- $M \simeq (x^j)$ avec $2 \leq j \leq p-2$, $H^*(G, M) = \sigma \otimes (\mathbb{F}_p[u^2] \oplus \mathbb{F}_p[u^2]) \simeq \mathbb{F}_p[u]^2$ en tant que $\mathbb{F}_p[u]$-module et on obtient encore $\dim_{\mathbb{F}_p(u)} H^*(G, M)_{(0)} = 2$.

Ce qui prouve:

Théorème 1.3.9. *Soit $G \simeq \mathbb{Z}/p\mathbb{Z}$, M un $\mathbb{F}_p[G]$-module indécomposable, alors:*

$$\dim_{\mathbb{F}_p(u_1,\ldots,u_n)}(H^*(G, M))_{(0)} = \begin{cases} 0 & \textit{si } M \textit{ est libre} \\ 1 & \textit{sinon} \end{cases}$$

En appliquant le Théorème 1.3.7 on obtient pour le cas $n = 1$:

Théorème 1.3.10. *Soit X un surface K3, G cyclique qui agit sur X avec lieu fixe non vide. Alors:*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) = \# \left\{ \begin{array}{l} \textit{modules non libres indécomposables} \\ \textit{dans la décomposition de } H^2(X, \mathbb{F}_p) \end{array} \right\} + 2$$

1.3.2.3 Cas $n = 2$, $p = 2$

Dans cette section on prouvera le résultat suivant:

Théorème 1.3.11. *Soit $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$, M un $\mathbb{F}_p[G]$-module indécomposable de type fini, alors:*

$$\dim_{\mathbb{F}_2(u_1,u_2)}(H^*(G, M))_{(0)} = \begin{cases} 0 & \textit{si } \dim_{\mathbb{F}_2} M \textit{ pair} \\ 1 & \textit{si } \dim_{\mathbb{F}_2} M \textit{ impair} \end{cases}$$

On considère séparément les différents cas possibles pour M en montrant qu'ils vérifient l'énoncé du théorème. D'abord pour les deux cas les plus simples on a:

- si $M \simeq A_2^2$, alors $H^*(G, A_2^2) = \mathbb{F}_2$ et $\mathbb{F}_2 \otimes_{\mathbb{F}_2[u,v]} \mathbb{F}_2(u, v) = 0$ qui a dimension nulle.

- si $M \simeq \mathbb{F}_2$, alors $H^*(G,\mathbb{F}_2) = \mathbb{F}_2[u,v]$ et $\mathbb{F}_2[u,v] \otimes_{\mathbb{F}_2[u,v]} \mathbb{F}_2(u,v) \simeq \mathbb{F}_2(u,v)$ qui a dimension un.

Pour les autres cas on utilisera les résultats suivants, qui sont aussi valides dans le cas générique d'un anneau A_p^n mais que nous utiliserons uniquement ici.

Lemme 1.3.12. *Soit $0 \to M \to N \to P \to 0$ une suite exacte telle que pour tout $i \in \mathbb{N}$ on a:*

$$\dim_{\mathbb{F}_p}\left(\left(\Omega^{-i}N\right)^G\right) = \dim_{\mathbb{F}_p}\left(\left(\Omega^{-i}M\right)^G\right) + \dim_{\mathbb{F}_p}\left(\left(\Omega^{-i}P\right)^G\right)$$

alors:

$$H^*(G,N)_{(0)} \simeq H^*(G,M)_{(0)} \oplus H^*(G,P)_{(0)}$$

Démonstration. Par le Corollaire 1.3.4 on a la suite exacte:

$$0 \to H^*(G,M) \to H^*(G,N) \to H^*(G,P) \to 0$$

comme la localisation est un foncteur exact, on obtient:

$$0 \to H^*(G,M)_{(0)} \to H^*(G,N)_{(0)} \to H^*(G,P)_{(0)} \to 0$$

qui est une suite exacte de $\mathbb{F}_2(u,v)$-espaces vectoriels et donc scinde. □

Lemme 1.3.13. *Soit M un $\mathbb{F}_p[G]$-module libre de projectifs, alors:*

$$H^*(G,M)_{(0)} \simeq H^*(G,\Omega^{-1}M)_{(0)}$$

Démonstration. Par la Proposition 1.3.5 on a $H^*(G,M) \simeq H^{\geq 1}(G,\Omega^{-1}M)$, il existe donc une suite exacte:

$$0 \to H^*(G,M) \to H^*(G,\Omega^{-1}M) \to H^0(G,\Omega^{-1}M) \to 0$$

où $H^0(G,\Omega^{-1}M) \simeq \frac{H^*(G,\Omega^{-1}M)}{H^{\geq 1}(G,\Omega^{-1}M)} \simeq \mathbb{F}_2^{h_0}$ avec $h^0 = \dim_{\mathbb{F}_2} H^0(G,\Omega^{-1}M)$. Comme la localisation est un foncteur exact, on obtient:

$$H^*(G,\Omega^{-1}M)_{(0)} \simeq H^*(G,M)_{(0)} \oplus \left(\mathbb{F}_2^{h_0}\right)_{(0)}$$

mais $\left(\mathbb{F}_2^{h_0}\right)_{(0)} = 0$ et on obtient l'isomorphisme cherché. □

En appliquant le Lemme 1.3.13 on obtient directement que:

$$H^*(G,\Omega^i\mathbb{F}_2)_{(0)} \simeq H^*(G,\mathbb{F}_2)_{(0)} \simeq \mathbb{F}_2(u,v)$$

pour tout $i \in \mathbb{Z}$.

Pour terminer la preuve du Théorème 1.3.11 il ne reste donc qu'à vérifier le cas M de dimension paire.

Soit $M \simeq E_{f,2i}$ où $M = E_{\infty,2i}$. Par la Proposition 1.2.24 on peut représenter $\Omega^{-i}\mathbb{F}_p$ par un couple de matrices, $x_1, y_1 : V_1 \to W_1$ avec $\dim(V_1) = i$ et $\dim(W_1) = i+1$:

$$x_1 = \begin{pmatrix} 1 & & & 0 \\ 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \qquad y_1 = \begin{pmatrix} 0 & & & 0 \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & \ddots & 0 \\ 0 & & & 1 \end{pmatrix}$$

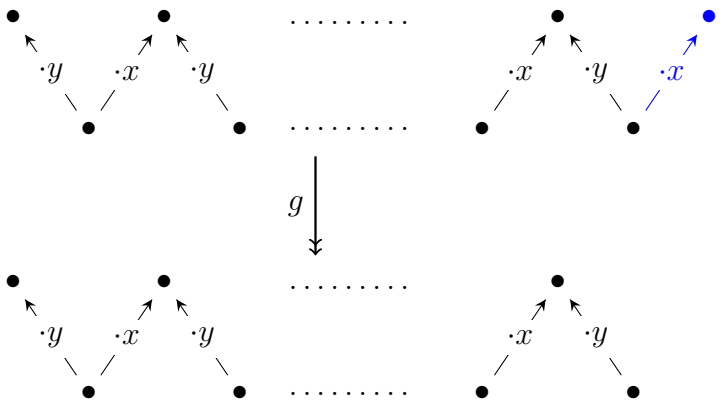
D'ailleurs M est aussi représenté par un couple de matrices $x_2, y_2 : V_2 \to W_2$, figurant dans le Théorème 1.2.28. Soit (v_j^k) une base de V_2 et (w_j^k) une base de W_2, alors il existe un morphisme surjectif $g : \Omega^{-i}(\mathbb{F}_2) \twoheadrightarrow M$ donné par les applications:

$$\text{si } M \simeq E_{0,2i} : \quad \begin{array}{ccc} g_V : V_1 & \longrightarrow & V_2 \\ v_j^1 & \mapsto & v_j^2 \end{array} \qquad \begin{array}{ccc} g_W : W_1 & \longrightarrow & W_2 \\ w_j^1 & \mapsto & w_j^2 \text{ si } j \leq i \\ w_{i+1}^1 & \mapsto & 0 \end{array}$$

$$\text{si } M \simeq E_{f,2i} : \quad \begin{array}{ccc} g_V : V_1 & \longrightarrow & V_2 \\ v_j^1 & \mapsto & v_j^2 \end{array} \qquad \begin{array}{ccc} g_W : W_1 & \longrightarrow & W_2 \\ w_j^1 & \mapsto & w_j^2 \text{ si } j \leq i \\ w_{i+1}^1 & \mapsto & \sum_{k=1}^{i} \lambda_k w_k \end{array}$$

$$\text{si } M \simeq E_{\infty,2i} : \quad \begin{array}{ccc} g_V : V_1 & \longrightarrow & V_2 \\ v_j^1 & \mapsto & v_{i-j+1}^2 \end{array} \qquad \begin{array}{ccc} g_W : W_1 & \longrightarrow & W_2 \\ w_j^1 & \mapsto & w_{i-j+2}^2 \text{ si } j \geq 2 \\ w_1^1 & \mapsto & 0 \end{array}$$

Remarque 1.3.14. Suivre la représentation matricielle peut être un peu compliqué, il est sûrement plus simple de comprendre l'isomorphisme en pensant aux diagrammes à zigzag. Par exemple, pour $g : \Omega^{-i}(k) \twoheadrightarrow E_{0,2i}$ on a la représentation suivante:



Les diagrammes se superposent, à l'exception de w_{i+1} (représenté par le cercle bleu) qui est envoyé en zéro.

Comme $\dim_{\mathbb{F}_2}(\ker(k)) = 1$ on a $\ker(g) \simeq \mathbb{F}_2$, donc on a la suite exacte:

$$0 \to \mathbb{F}_2 \to \Omega^{-i}\mathbb{F}_2 \to N \to 0$$

En regardant les preuves du Lemme 1.2.30 et du Théorème 1.2.27 pour tout j on a $\dim_{\mathbb{F}_p}\left((\Omega^{-j}N)^G\right) = i$, $\dim_{\mathbb{F}_p}\left((\Omega^{-i-j}\mathbb{F}_2)^G\right) = i+j+1$ et $\dim_{\mathbb{F}_p}\left((\Omega^{-j}\mathbb{F}_2)^G\right) = j+1$. On est donc dans les hypothèses du Lemme 1.3.12 et on obtient:

$$\begin{aligned}\dim_{\mathbb{F}_2} H^*(G,M)_{(0)} &= \dim_{\mathbb{F}_2} H^*(G,\Omega^{-i}\mathbb{F}_2)_{(0)} - \dim_{\mathbb{F}_2} H^*(G,\Omega^{-i}\mathbb{F}_2)_{(0)} \\ &= 1-1=0\end{aligned}$$

Ce qui conclut la preuve du Théorème 1.3.11.

Finalement en appliquant le Théorème 1.3.7 on obtient pour le cas $n = p = 2$:

Théorème 1.3.15. *Soit X une surface K3, $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ qui agit sur X avec lieu fixe non vide. Alors*

$$\sum_i \dim_{\mathbb{F}_2} H^i(X^G,\mathbb{F}_2) = \#\left\{\begin{array}{c}\textit{modules impairs indécomposables} \\ \textit{dans la décomposition de } H^2(X,\mathbb{F}_2)\end{array}\right\} + 2$$

1.4 Méthode alternative

Dans ce chapitre, nous avons vu une solution complète pour les cas $n = 1$ et $n = p = 2$, par contre, en ce qui concerne les autres cas, nous avons très peu de résultats. Comme nous avons vu dans la sous-section 1.2.3, dans le cas général il n'existe aucune classification, et nous ne pouvons pas espérer en obtenir une, donc la stratégie de calculer le module de cohomologie $H^*(G,M)$ pour chaque module M indécomposable ne semble pas être une solution envisageable.

Par contre, est-il possible de donner un algorithme tel que pour un $\mathbb{F}_p[G]$-module M donné, il calcule la valeur de $\dim_{\mathbb{F}_p} H^*(G,M)_{(0)}$?

Pour l'instant la réponse est plutôt non, vu que c'est d'abord nécessaire de déterminer la structure de $H^*(G,\mathbb{F}_p)$-module de $H^*(G,M)$ (et donc le cup-produit), ce qui même pour le cas $n = 1$ n'est pas immédiat et que pour le cas $n = p = 2$ a demandé une approche *ad hoc.*

Dans cette section, même si finalement nous ne serons pas capables de satisfaire pleinement nos attentes, nous verrons qu'en général on peut se passer du calcul du cup-produit, et que le comportement asymptotique de $\dim_{\mathbb{F}_p}(H^i(G,M))$ pour $i \gg 0$ est une donnée suffisante.

Soit donc M un $\mathbb{F}_p[G]$-module, on considère une résolution injective (avec c_i minimales):

$$M \to \mathbb{F}_p[G]^{c_0} \to \mathbb{F}_p[G]^{c_1} \to \mathbb{F}_p[G]^{c_2} \to \mathbb{F}_p[G]^{c_3} \to \dots$$

alors par le Lemme 1.2.17 $c_i = \dim_{\mathbb{F}_p} H^i(G, M) = \dim_{\mathbb{F}_p} \left((\Omega^{-i}M)^G\right)$. Pour un module M, on appelle $c_i(M) := c_i$ le i-ème *nombre de Bass* [Av].

Remarque 1.4.1. Les nombres de Bass sont le concept dual des plus connus *nombres de Betti*, qui dans ce cas peuvent être définis comme $b_i(M) := \dim_{\mathbb{F}_p} \left((\Omega^i M) \otimes_{\mathbb{F}_p[G]} \mathbb{F}_p\right)$. En particulier on a $c_i(M) = b_i(M^*)$.

On a le résultat suivant [Av, 4.1]:

Théorème 1.4.2. *Soit M un $\mathbb{F}_p[G]$-module avec $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, alors il existe $A \in \mathbb{Q}$ tel que pour $i \to \infty$:*

$$c_i(M) = Ai^{n-1} + O(i^{n-2})$$

On notera $\mathrm{leadt}(M) := A$, le coefficient du terme de degré $n-1$.

La preuve du résultat suivant sera l'objet des deux sous-sections suivantes:

Proposition 1.4.3. *Soit M un $\mathbb{F}_p[G]$-module avec $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, alors:*

$$\dim_{\mathbb{F}_p(u_1,\dots,u_n)} H^*(G, M)_{(0)} = \begin{cases} \mathrm{leadt}(M)(n-1)! & \text{si } p = 2 \\ 2^n \,\mathrm{leadt}(M)(n-1)! & \text{si } p \geq 3 \end{cases}$$

Et en appliquant le Théorème 1.3.7 on obtient immédiatement comme conséquence:

Théorème 1.4.4. *Soit X une surface K3, $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ qui agit sur X avec lieu fixe non vide. Alors:*

$$\sum_i \dim_{\mathbb{F}_2} H^i(X^G, \mathbb{F}_2) = \mathrm{leadt}\left(H^2(X, \mathbb{F}_p)\right)(n-1)! + 2$$

1.4.1 Rappels sur les polynômes de Hilbert

Soit k un corps, N un module gradué de type fini sur l'anneau des polynômes à n variables $R = k[x_1, \dots, x_n]$, alors par un résultat très connu de Hilbert (voir par exemple [BH, 2.2.14]), N admet une résolution libre de longueur au plus n:

$$0 \to F_n \to \cdots \to F_1 \to F_0 \to N \to 0 \tag{1.4.1}$$

où les morphismes ont degré zéro (i.e. l'image d'un élément de degré d a degré d). Chaque module libre peut être écrit sous la forme:

$$F_i = \bigoplus_{j=1}^{r_i} R(-a_{ij})$$

où $R(-a_{ij})$ est le *shifting* du module R d'un facteur a_{ij}:

$$R(-a_{ij})_d = R_{d-a_{ij}}$$

i.e. les éléments de degré d en R deviennent de degré $d+a_{ij}$ ($\deg 0 \mapsto \deg a_{ij}$). On rappelle que le nombre des monômes de degré d à n variables est $\binom{n+d-1}{n-1}$, donc pour chaque $R[a_{ij}]$ on a :

$$\dim_k R(-a_{ij})_d = \dim_k R_{d-a_{ij}} = \begin{cases} \binom{n+d-a_{ij}-1}{n-1} & \text{si } d \geq a_{ij} \\ 0 & \text{sinon} \end{cases} \tag{1.4.2}$$

La suite (1.4.1) se décompose comme une somme de suites exactes entre les termes de degrés d pour tout d:

$$0 \to (F_n)_d \to \cdots \to (F_1)_d \to (F_0)_d \to N_d \to 0$$

Les termes de la suite sont des k-espaces vectoriels, donc pour la dimension de N_d on a:

$$\dim_k N_d = \sum_{i=0}^{n} (-1)^i \dim_k (F_i)_d$$

Si on remplace avec (1.4.2) on obtient qu'il existe un polynôme H_N (dit polynôme d'Hilbert de N) tel que $\dim_k (N_d) = H_N(d)$ pour $d \geq \max\{a_{ij}\}$ (cf. [BH, 4.1.13]), avec:

$$H_N(d) = \sum_{i=0}^{n} (-1)^i \sum_{j=1}^{r_i} \binom{n+d-a_{ij}-1}{n-1}$$

Après quelques simplifications, pour le terme principal de H_N on trouve:

$$\begin{aligned} H_N(d) &= \sum_{i=0}^{n} (-1)^i \sum_{j=1}^{r_i} \frac{1}{(n-1)!} d^{n-1} + \text{termes de degré} \leq n-2 \\ &= \frac{1}{(n-1)!} \sum_{i=0}^{n} (-1)^i r_i d^{n-1} + \text{termes de degré} \leq n-2 \end{aligned}$$

De l'autre coté, en localisant (1.4.1) en 0 on obtient la suite exacte de $k(x_1, \ldots, x_n)$-espaces vectoriels:

$$0 \to (F_n)_{(0)} \to \cdots \to (F_1)_{(0)} \to (F_0)_{(0)} \to N_{(0)} \to 0$$

Comme $(F_i)_{(0)} \simeq \bigoplus_{j=1}^{r_i} R(-a_{ij})_{(0)} \simeq k(x_1, \ldots, x_n)^{r_i}$, on a:

$$\dim_{k(x_1,\ldots,x_n)} N_{(0)} = \sum_{i=0}^{n} (-1)^i r_i$$

Donc on a prouvé:

Lemme 1.4.5. *Soit k un corps, N un $k[x_1, \ldots, x_n]$-module gradué de type fini. Si A est le coefficient du terme de degré $d-1$ du polynôme d'Hilbert H_N, alors:*

$$\dim_{k(x_1,\ldots,x_n)} N_{(0)} = A(n-1)!$$

1.4.2 Preuve de la Proposition 1.4.3

Soit M un $\mathbb{F}_p[G]$-module, nous avons vu que $H^*(G,M)$ est un $\mathbb{F}_p[u_1,\dots,u_n]$-module gradué (où dans le cas $p \geq 3$ on a $u_i = z_i^2$ de degré 2 en cohomologie). De plus, on a que $H^*(G,M)$ est de type fini [Av, 2.1]:

Théorème 1.4.6. *Soit $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, M un $\mathbb{F}_p[G]$-module de type fini, alors $H^*(G,M)$ est un $\mathbb{F}_p[u_1,\dots,u_n]-$module gradué de type fini.*

Nous avons maintenant tous les éléments pour conclure, il reste uniquement la question du degré différent en cohomologie dans le cas $p \geq 3$, ce qui n'est pas vraiment un problème, mais demande juste un peu d'attention. On sépare donc les deux cas:

Cas $p = 2$ Ce cas est immédiat: en résumant $H^*(G,M)$ est un module gradué de type fini sur $\mathbb{F}_2[u_1,\dots,u_n]$, avec $\dim H^*(G,M)_d = c_d(M)$. Soit $H_{H^*(G,M)}(d) = Ad^{n-1} + \text{termes de degré} \leq n-2$ le polynôme d'Hilbert associé, alors pour $d \gg 0$ on a $c_d(M) = H_{H^*(G,M)}(d)$, donc $A = \text{leadt}(M)$ et par le Lemme 1.4.5:

$$\text{leadt}(M)(n-1)! = A(n-1)! = \dim_{\mathbb{F}_2(u_1,\dots,u_n)} N_{(0)}$$

ce qui montre la Proposition 1.4.3 dans le cas $p = 2$.

Cas $p \geq 3$ Dans ce cas $H^*(G,M)$ est un $R = \mathbb{F}_p[z_1^2,\dots,z_n^2]$-module gradué, donc R agit séparément sur les termes pairs et impairs de la cohomologie, on a alors la décomposition:

$$H^*(G,M) \simeq H^{\text{pair}}(G,M) \oplus H^{\text{impair}}(G,M)$$

On considère d'abord le cas pair. Soit N le module obtenu en divisant par 2 les degrés des termes de $H^{\text{pair}}(G,M)_{2d}$:

$$N_d = H^{\text{pair}}(G,M)_{2d}$$

alors N est un module gradué sur l'anneau $\mathbb{F}_p[z_1,\dots,z_n]$ avec $\dim N_d = c_{2d}(M)$. Soit $H_N(d) = Ad^{n-1} + \text{termes de degré} \leq n-2$ le polynôme de Hilbert associé, alors pour $d \gg 0$ on a $c_{2d} = H_N(d)$, donc asymptotiquement:

$$\begin{aligned} c_{2d} &\sim H_N(d) \\ \text{leadt}(M)(2d)^{n-1} + O(t^{n-2}) &\sim Ad^{n-1} + O(t^{n-2}) \end{aligned}$$

et donc $A = 2^{n-1}\,\text{leadt}(M)$ et par le Lemme 1.4.5 $\dim N_{(0)} = 2^{n-1}\,\text{leadt}(M)$.

Le même argument peut être appliqué à N' obtenu à partir des termes de degré impairs, $N'_d = H^{\text{impair}}(G,M)_{2d+1}$, donc finalement:

$$\begin{aligned} \dim H^*(G,M)_{(0)} &= \dim H^{\text{pair}}(G,M)_{(0)} + \dim H^{\text{impair}}(G,M)_{(0)} \\ &= 2 \cdot 2^{n-1}\,\text{leadt}(M) \end{aligned}$$

ce qui conclut la preuve de la Proposition 1.4.3.

1.4.3 Applications

1.4.3.1 Preuves alternatives

La Proposition 1.4.3 donne un raccourci pratique pour une preuve alternative à celles de la section 1.3 des Théorèmes 1.3.9 et 1.3.11, ainsi qu'une stratégie pour déterminer l'invariant $\dim H^*(G,M)_{(0)}$ dans le cas général.

Cas $n = 1$ Pour tout M indécomposable non libre, d'après le Lemme 1.1.14 on a $\dim H^i(G,M) = 1$, en particulier $\dim H^*(G,M)_{(0)} = \text{leadt}(M) = 1$.

Cas $n = p = 2$ Si M est indécomposable non libre de dimension paire $2m$, alors par le Lemme 1.2.30 on a $c_i(M) = m$ pour tout $i \geq 0$, donc $\dim H^*(G,M)_{(0)} = \text{leadt}(M) = 0$.

Si M est indécomposable de dimension impaire $2m+1$, alors par le Théorème 1.2.27 $M \simeq \Omega^j(\mathbb{F}_p)$ avec $j = \pm m$ et $\dim H^i(G,M) = |i-j|+1$. Donc $\dim H^*(G,M)_{(0)} = \text{leadt}\, M = 1$.

Cas général Soit M un $\mathbb{F}_p[G]$-module, $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec p, n quelconques. D'après la preuve de la la Proposition 1.4.3 il existe un polynôme $P(d)$ de degré au plus $n-1$ et une constante $D_M \in \mathbb{N}$ tel que pour $d = 2i > D_M$:

$$c_d(M) = P(d)$$

et l'égalité est vérifiée aussi pour les valeurs impaires de d si $p = 2$.

Le calcul de la suite des valeurs de $c_d(M)$ peut être facilement accompli avec l'aide d'un ordinateur, théoriquement il suffirait donc de calculer les valeurs de $c_d(M)$ pour au moins n valeurs (pour d pair si $p \geq 3$) plus grandes que D_M pour déterminer l'expression de $P(d)$ et en particulier le terme principal $\text{leadt}(M)$.

L'obstacle à l'application de cette méthode est que nous ne connaissons aucune borne supérieure pour la valeur de D_M, donc même si heuristiquement on peut raisonnablement considérer fiable une estimation de $\text{leadt}(M)$ donnée par le calcul d'un grand nombre de valeurs de $c_d(M)$, dans la pratique cela ne constitue d'aucune façon une preuve.

Cependant, une estimation de la valeur de D_M pourrait effectivement résoudre ce problème et rendre cette option viable.

Sinon il est quand même nécessaire de déterminer, au moins asymptotiquement, la valeur de $c_d(M)$ pour tout d, ce qui en tout cas reste plus simple que de déterminer la structure de $H^*(G,\mathbb{F}_p)$-module de $H^*(G,M)$.

1.4.3.2 Bornes pour $\text{leadt}(M)$

Une deuxième application de la Proposition 1.4.3 est la possibilité de donner des bornes, maximales et minimales, pour la valeur de $\dim H^*(G,M)_{(0)}$.

Borne supérieure Soit M un $\mathbb{F}_p[G]$-module avec $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, d'après la Proposition 1.1.8 il existe une résolution libre de $\mathbb{F}_p$ de la forme :

$$... \to \mathbb{F}_p[G]^{\alpha_n} \to \ldots \to \mathbb{F}_p[G]^{\alpha_3} \to \mathbb{F}_p[G]^{\alpha_2} \to \mathbb{F}_p[G]^{\alpha_1} \to \mathbb{F}_p$$

avec:

$$\alpha_i = \binom{n+i-1}{n-1}$$

On rappelle que les groupes de cohomologie $H^i(G, M)$ sont donnés par la cohomologie de la suite obtenue en appliquant le foncteur $\mathrm{Hom}(\bullet, M)$, donc:

$$... \to \mathrm{Hom}\left(\mathbb{F}_p[G]^{\alpha_n}, M\right) \to \ldots \to \mathrm{Hom}\left(\mathbb{F}_p[G]^{\alpha_2}, M\right) \to \mathrm{Hom}\left(\mathbb{F}_p[G]^{\alpha_1}, M\right) \to \mathbb{F}_p$$

en particulier $H^i(G, M) \leq \mathrm{Hom}\left(\mathbb{F}_p[G]^{\alpha_i}, M\right) \simeq M^{\alpha_i}$, donc:

$$\begin{aligned} c_i(M) &= \dim H^i(G, M) \\ &\leq \alpha_i \dim M \\ &= \binom{n+i-1}{n-1} \dim M \\ &= \frac{\dim M}{(n-1)!} i^{n-1} + \text{termes de degré} \leq n-2 \end{aligned}$$

et en appliquant la Proposition 1.4.3 on obtient:

Lemme 1.4.7. *Soit M un $\mathbb{F}_p[G]$-module avec $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, alors:*

$$\dim_{\mathbb{F}_p(u_1,\ldots,u_n)} H^*(G, M)_{(0)} \leq \dim_{\mathbb{F}_p} M$$

D'ailleurs il s'agit d'une borne optimale, vu qu'elle est atteinte pour $M \simeq \mathbb{F}^{\oplus m}$ avec $m \in \mathbb{N}$. En remplaçant dans le Théorème 1.3.7 on obtient une borne pour la cohomologie du lieu fixe (cf. [BCS] pour d'autres inégalités similaires) :

Proposition 1.4.8. *Soit $G = (\mathbb{Z}/p\mathbb{Z})^n$ qui agit sur une surface X avec $\dim H^*(X^G, \mathbb{F}) < \infty$ et tel que $H^1(X) = H^3(X) = 0$. Alors :*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) \leq \sum_i \dim_{\mathbb{F}_p} H^i(X, \mathbb{F}_p)$$

Borne inférieure Déterminer une borne inférieure pour $\dim H^*(G, M)_{(0)}$ est sans doute plus compliqué, mais le résultat suivant nous aide dans la tâche [Av, 7.2]:

Théorème 1.4.9. *Soit M un $\mathbb{F}_p[G]$-module, $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Si $\mathrm{leadt}(M) = 0$ alors $p \mid \dim M$.*

Dans le cas d'une surface K3 on obtient par exemple:

Proposition 1.4.10. *Soit X un surface K3, $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec $p \neq 2, 11$, qui agit sur X avec lieu fixe non vide. Alors:*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) \geq 3$$

Démonstration. Soit $M = H^2(X, \mathbb{F}_p)$, si $p \neq 2, 11$ alors $p \nmid \dim M = 2$, donc $\operatorname{lead}(M) > 0$. Par le Théorème 1.4.4 on a $\sum_i \dim_{\mathbb{F}_p} H^i(X^G, \mathbb{F}_p) \geq 2 + \operatorname{leadt} M(n-1)! > 2$. □

Chapitre 2

Réseaux

2.1 Qu'est-ce qu'un réseau ?

Nous donnerons dans ce chapitre une exposition (qu'on espère) simple de certains résultats concernant la théorie des réseaux.

Bien sûr, il existe déjà plusieurs ouvrages sur ce sujet, comme ceux qui ont été utilisés comme référence principale dans la rédaction de ce chapitre : [Dol, MM, Nik, Con, CS].

Cependant, nous trouvions qu'il manquait un texte avec les caractéristiques suivantes:

- Facilement accessible pour celui qui aborde la théorie des réseaux pour la premier fois, donc:
  - contenant une introduction sur les concepts de base accompagnée de plusieurs exemples ;
  - utilisant des techniques le plus simple possible et bien expliquées ;
  - qui ne tombe pas trop dans les détails techniques et qui garde un point de vue « pratique »
- Qui ne soit pas focalisé sur les réseaux définis, mais au contraire pensé pour celui qui devra utiliser les réseaux en géométrie algébrique, donc:
  - qui parle des réseaux indéfinis ;
  - qui développe le discours sur le groupe discriminant ;
  - qui parle des extensions primitives et des actions d'un groupe sur un réseau ;

Cela a été notre objectif de donner une présentation qui puisse être utilisée comme première introduction à cette théorie. On n'a donc pas hésité à ajouter plusieurs exemples, qui parfois peuvent paraître répétitifs, mais dans une première approche, ils peuvent être utiles à une meilleure compréhension du sujet.

2.1.1 Libre de torsion et libre tout court

En premier lieu, un réseau L est un $\mathbb{Z}$-module libre de type fini. On rappelle que:

- « $\mathbb{Z}$-module » est un synonyme de « groupe abélien » (mais on préférera utiliser le premier terme, car la structure de module jouera un rôle important) ;
- Si M est un module sur un anneau A, alors M est:
  - un *A-module libre* si on peut écrire M comme une somme de copies de A indexées par un ensemble G quelconque:
$$M \simeq \bigoplus_{g \in G} A$$
  - *de type fini* s'il existe un ensemble fini $g_1, \ldots, g_r \in M$ dit « de générateurs » tel que tout élément $m \in M$ peut être écrit sous la forme $m = a_1 g_1 + \cdots + a_r g_r$ avec $a_1, \ldots, a_r \in A$;

Donc dire que L est un $\mathbb{Z}$-module libre de type fini est équivalent à dire qu'il existe $r \in \mathbb{N}$ (le *rang* du réseau, $\mathrm{rang}(L)$) tel que $L \simeq \mathbb{Z}^r$.

Les modules libres ont aussi une autre propriété, similaire mais généralement plus faible: l'absence de torsion. Un A-module M est dit *sans torsion* si pour tout $a \in A\backslash\{0\}$, $m \in M\backslash\{0\}$, $am \neq 0$. On a que dans notre cas, les deux propriétés sont équivalentes:

Lemme 2.1.1. *Soit L un $\mathbb{Z}$-module de type fini, alors L est libre $\iff$ L est sans torsion.*

Démonstration. Tout module libre est aussi sans torsion, donc il faut montrer uniquement " $\Leftarrow$ ". Par le Théorème de structure des groupes abéliens de type fini on peut écrire:

$$M \simeq \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{n_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{n_s\mathbb{Z}}$$

avec $n_1, \ldots, n_s \in \mathbb{Z}\backslash\{0\}$. Comme $\mathbb{Z}/n_i\mathbb{Z}$ *est de torsion* on obtient que $s = 0$ et $M \simeq \mathbb{Z}^r$. □

Exemple 2.1.2. Sans l'hypothèse de finitude le résultat est faux, par exemple $\mathbb{Q}$ est un $\mathbb{Z}$-module sans torsion, mais ce n'est pas un $\mathbb{Z}$-module libre.

En effet, si $\mathbb{Q}$ était libre alors on pourrait écrire $\mathbb{Q} \simeq \bigoplus_{g \in G} \mathbb{Z}$ et en particulier $\mathbb{Z}^2 \hookrightarrow \mathbb{Q}$, mais cela est impossible, car pour n'importe quel couple de rationnels $q_1, q_2 \in \mathbb{Q}\backslash\{0\}$ il existe $z_1, z_2 \in \mathbb{Z}$ tel que $z_1 q_1 = z_2 q_2$.

Exemple 2.1.3. Même si les analogies avec les espaces vectoriels sont nombreuses, il faut se souvenir que le $\mathbb{Z}$-modules libres ont aussi plusieurs différences, surtout en ce qui concerne le choix d'une base. Par exemple, soit $L \subset \mathbb{Q}^2$ le $\mathbb{Z}$-module engendré par les vecteurs $v_1 = (1, 0)$, $v_2 = (1, 2)$, $v_3 = (1, 5)$. Comme L est de rang 2, il est toujours possible de déterminer une

base de cardinalité 2 (par exemple $(1,0)$ et $(0,1)$), par contre, à la différence des espace vectoriels, pour un ensemble de générateurs donné, en général il n'est pas toujours possible de choisir une base parmi ses sous-ensembles (aucun choix de deux vecteurs parmi v_1, v_2, v_3 n'engendre le troisième).

2.1.2 Plongement dans un espace vectoriel

À l'origine, les « points du réseau » étaient les points à coordonnées entières de $\mathbb{R}^2$. Aujourd'hui la définition qu'on utilise est plus abstraite, mais cette connotation géométrique du réseau vu comme « grille de points dans $\mathbb{R}^n$ » représente une intuition toujours valide. C'est donc bien de s'interroger sur les plongements possibles de $\mathbb{Z}$-modules libres dans $\mathbb{R}^n$ et $\mathbb{Q}^n$.

Remarque 2.1.4. Pour un ensemble S de vecteurs, dans la suite on notera avec $\mathrm{span}_{\mathbb{Z}} S$ et $\mathrm{span}_{\mathbb{Q}} S$ respectivement le $\mathbb{Z}$-module engendré par les combinaisons à coefficients entiers et l'espace engendré par les combinaisons à coefficient rationnels. Parfois on omettra l'indice quand il n'y aura pas d'ambiguïté sur l'espace ambiant.

Lemme 2.1.5. *Soit $L \subset \mathbb{Q}^n$ un $\mathbb{Z}$-module libre. Alors* $\mathrm{rang}(L) \leq n$.

Démonstration. On suppose, sans perte de généralité, que les points de L engendrent $\mathbb{Q}^n$ comme $\mathbb{Q}$-espace vectoriel. Si $\mathrm{rang}(L) = r > n$, il existe $l_1, \ldots, l_r \in L$ $\mathbb{Z}$-base de L, mais comme $\dim_{\mathbb{Q}} \mathbb{Q}^n = n < r$ on a l'existence de $\lambda_1, \ldots, \lambda_r \in \mathbb{Q}$ (non tous nuls) tels que $\lambda_1 l_1 + \cdots + \lambda_r l_r = 0$. Pour tout $1 \leq i \leq r$ on peut écrire $\lambda_i = p_i/q_i$ avec $p_i, q_i \in \mathbb{Z}$, $(p_i, q_i) = 1$, donc si on pose $q = \text{p.p.c.m.}(q_1, \ldots, q_r)$ on a $q\lambda_1 l_1 + \cdots + q\lambda_r l_r = 0$ avec $q\lambda_i \in \mathbb{Z}$, impossible car $(l_1, \ldots, l_r)$ est une $\mathbb{Z}$-base de L, donc $k \leq n$. □

On rappelle le résultat suivant:

Proposition 2.1.6 (Forme normale de Smith pour les $\mathbb{Z}$-modules)**.** *Soit $f : L_1 \to L_2$ un morphisme de $\mathbb{Z}$-modules libres de type fini, alors il existe des bases B_1, B_2 de L_1 et L_2 telles que la matrice de f dans ces bases soit de la forme:*

$$\mathrm{mat}_{B_1,B_2}(f) = \begin{pmatrix} \lambda_1 & & & & & \\ & \cdots & & & & \\ & & \lambda_n & & & \\ & & & 0 & \cdots & 0 \\ & & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 0 \end{pmatrix}$$

Définition 2.1.7. Soit M un A-module avec A anneau commutatif, $N \subset M$ un sous-module. On dira que N est un sous-module *primitif* si $N \hookrightarrow M$ scinde, (i.e. si $M \simeq N \oplus \frac{M}{N}$ où l'injection $N \hookrightarrow M$ est réalisée par l'isomorphisme sur le premier terme de la somme). De la même façon, on dira que $v \in L$ est un *élément primitif* si $\mathrm{span}_A(v)$ est primitif.

Dans le cas où L est un $\mathbb{Z}$-module libre fini, en appliquant la forme normale de Smith, on a aussi que $L' \subset L$ est un sous-module primitif (ou un *sous-réseau primitif* après qu'on aura introduit les forme bilinéaires) si pour tout $v \in L$, $\lambda \in \mathbb{Z}$ et $\lambda v \in L' \backslash \{0\}$ alors $v \in L'$, ce qui est équivalent à affirmer que $\frac{L}{L'}$ est sans torsion. De plus, $v \in L$ est primitif si les coordonnées de v dans une base de L sont $v = (a_1, \ldots, a_n)$ avec $\text{pgcd}(a_1, \ldots, a_n) = 1$.

Exemple 2.1.8. Soit $f : L_1 \to L_2$ un morphisme de $\mathbb{Z}$-modules libres finis et $L' \subset L_2$ un sous-module primitif. Alors $f^{-1}(L')$ est aussi un sous-module primitif de L_1: en effet, si $\lambda v \in f^{-1}(L') \backslash \{0\}$, alors $\lambda f(v) \in L'$ et comme L' est primitif, $f(v) \in L'$ et donc $v \in f^{-1}(L')$. En particulier, $\ker(f)$ est un sous-module primitif de L_1.

Exemple 2.1.9. Soit $L = \mathbb{Z}^2$, alors:

- $L_1 = \text{span}_{\mathbb{Z}}((1,1))$ est un sous-module primitif ;
- $L_2 = \text{span}_{\mathbb{Z}}((2,0))$ n'est pas un sous-module primitif.

Remarque 2.1.10. De façon plus géométrique, pour un $\mathbb{Z}$-module de type fini L on peut considérer le plongement canonique $L \subset L \otimes \mathbb{Q} = V$. Si W est un sous-espace vectoriel de V, on peut considérer le sous-module $L' := W \cap L$, qui est primitif. De plus, pour tout $x \in W$, il existe $\lambda \in \mathbb{Z}$ tel que $\lambda x \in L'$, donc $\text{span}_{\mathbb{Q}}(L') = W$ et donc $\text{rang}(L') = \dim(W)$.

Si $L' \subset L$ est un sous-module, alors on appelle la *saturation* de L' dans L le sous-module de L donné par $\text{span}_{\mathbb{Q}}(L') \cap L$, il s'agit donc du plus petit sous-module primitif de L qui contient L', car il a la même dimension, et donc L' est primitif si et seulement si il coïncide avec sa saturation dans L, $L' = \text{span}_{\mathbb{Q}}(L') \cap L$.

Lemme 2.1.11. *Soit L un $\mathbb{Z}$-module libre de type fini, $L_1, L_2 \subseteq L$ sous-modules primitifs, alors $L_1 \cap L_2$ est primitif.*

Démonstration. On a $(L_1 \otimes \mathbb{Q}) \cap L = L_1$ et $(L_2 \otimes \mathbb{Q}) \cap L = L_2$, donc:

$$\begin{aligned}(L_1 \cap L_2) \otimes \mathbb{Q} \cap L &= (L_1 \otimes \mathbb{Q}) \cap (L_2 \otimes \mathbb{Q}) \cap L \\ &= (L_1 \otimes \mathbb{Q} \cap L) \cap (L_2 \otimes \mathbb{Q} \cap L) \\ &= L_1 \cap L_2\end{aligned}$$

et donc $L_1 \cap L_2$ est primitif. □

On essaie maintenant d'étendre l'énoncé du Lemme 2.1.5 au corps des réels:

Proposition 2.1.12. *Soit $L \subset \mathbb{R}^n$ sous-ensemble discret tel que L soit un $\mathbb{Z}$-module libre de type fini. Alors* $\text{rang}(L) \leq n$.

Démonstration. Si $n = 1$: Soit $L \hookrightarrow \mathbb{R}$ discret avec $\text{rang}(L) \geq 2$, $v \in L$ de norme minimale, il existe alors $w \in L$ indépendant de v. On a donc que pour tout $\lambda \in \mathbb{Z}$, $\lambda v \neq w$, donc il existe $\lambda_0 \in \mathbb{Z}$ tel que $\lambda_0 v < w < (\lambda_0 + 1)v$,

donc $|w - \lambda_0 v| < v$ mais $w - \lambda_0 v \in L$, contradictoire avec l'hypothèse de minimalité de v.

Si $n \geq 2$: On suppose, sans perte de généralité, que les points de L engendrent $\mathbb{R}^n$ comme $\mathbb{R}$-espace vectoriel. Soit $\{v_i\}_{i\in I}$ une base de L comme $\mathbb{Z}$-module, on peut donc en extraire un sous-ensemble $v_1, \ldots, v_n$ base de $\mathbb{R}^n$ comme $\mathbb{R}$-espace vectoriel. Soit $R = \mathrm{span}_{\mathbb{Z}}(v_1, \ldots, v_n)$ et F le module engendré par les éléments de la base qui restent, alors $L = R \oplus F$.

On considère la projection $\pi : \mathbb{R}^n \to \frac{\mathbb{R}^n}{R}$ dans le tore de dimension n, comme $R \subset L$ on peut appliquer la projection sur L et on a $\pi(L) \simeq L/R \simeq F$. Soit $P \subset \mathbb{R}^n$ le polyèdre avec les arêtes données par $v_1, \ldots, v_n$, on a $\pi(L) = \pi(P \cap L)$ et donc $\pi(L)$ est de cardinalité finie. Comme $\pi(L) \simeq F$ on a que F est un ensemble fini aussi, mais F est un $\mathbb{Z}$-module libre, donc la seule possibilité est $F = 0$ et L est de rang n.

□

Exemple 2.1.13. Soit $n \in \mathbb{N}$, $L = \mathrm{span}_{\mathbb{Z}}(1, \pi, \pi^2, \ldots, \pi^{n-1}) \subset \mathbb{R}$ le sous-groupe abélien additif engendré par l'ensemble $B = (1, \pi, \pi^2, \ldots, \pi^{n-1})$. On a alors que L est un $\mathbb{Z}$-module libre de rang n, car les vecteurs de B forment une base. Autrement, il existerait $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$ tels que $\lambda_1 + \lambda_2\pi + \cdots + \lambda_n\pi^{n-1}$, donc π serait solution d'un polynôme, impossible car π est transcendant. On a alors $L \simeq \mathbb{Z}^n \hookrightarrow \mathbb{R}$, mais cela ne contredit pas la Proposition 2.1.12 car L n'est pas un sous-ensemble discret.

2.1.3 Matrice de Gram

Au cours de nos études,nous rencontrons souvent les formes bilinéaires définies sur un corps, mais rien ne nous empêche de les voir aussi dans un contexte plus ample:

Définition 2.1.14. Soient B, M deux modules sur un anneau commutatif A, $b : M \times M \to B$ linéaire en les deux termes:

$$\begin{aligned} b(ax + a'x', y) &= a\, b(x, y) + a'\, b(x', y) \\ b(y, ax + a'x') &= a\, b(y, x) + a'\, b(y, x') \end{aligned}$$

alors b est une *application bilinéaire*. De plus, on dira que $b(\cdot, \cdot)$ est:

- *symétrique* si pour tout $x, y \in M$ on a $b(x, y) = b(y, x)$;
- *anti-symétrique* si pour $x, y \in M$ on a $b(x, y) = -b(y, x)$;
- *dégénérée* s'il existe $x, y \in M\backslash\{0\}$ tels que $b(x, y) = 0$;
- *non-dégénérée* si pour tout $x \in M\backslash\{0\}$ il existe $y \in M$ tel que $b(x, y) \neq 0$;

On dira aussi que un sous-module $U \subseteq M$ est *totalement isotrope* si pour tout $x, y \in U$ on a $b(x, y) = 0$.

Remarque 2.1.15. Souvent on demande que le co-domaine de l'application bilinéaire coïncide avec l'anneau ($B = A$), dans ce cas on parle de *forme*

bilinéaire. Pourtant cela ne sera pas toujours le cas dans les applications de ce chapitre (même si on gardera le terme « forme » dans le cas des formes finies).

Remarque 2.1.16. Soit M un A-module libre de type fini, donc $M \simeq A^r$ pour un certain r. Soit $(x_1, \ldots, x_r)$ une base de M et $b : M \times M \to B$ une application bilinéaire. Si $x, y \in M$, on a une décomposition de la forme $x = \lambda_1 x_1 + \cdots + \lambda_r x_r$, $y = \mu_1 x_1 + \cdots + \mu_r x_r$, donc en appliquant la bilinéarité on obtient que:

$$\begin{aligned} b(x,y) &= b(\lambda_1 x_1 + \cdots + \lambda_r x_r, \mu_1 x_1 + \cdots + \mu_r x_r) \\ &= \lambda_1 b(x_1, \mu_1 x_1 + \cdots + \mu_r x_r) + \cdots + \lambda_r b(x_r, \mu_1 x_1 + \cdots + \mu_r x_r) \\ &= \lambda_1\mu_1 b(x_1, x_1) + \cdots + \lambda_1\mu_r b(x_1, x_r) + \cdots + \\ &+ \lambda_r\mu_1 b(x_r, x_1) + \cdots + \lambda_r\mu_r b(x_r, x_r) \\ &= \sum_{i,j=1}^{r} \lambda_i\mu_j b(x_i, x_j) \end{aligned}$$

On a alors que $b(\cdot,\cdot)$ est déterminée de façon unique par ses valeurs sur les éléments de la base $b(x_i, x_j)$. D'ailleurs, si on considère la matrice (dite *matrice d'intersection* ou *matrice de Gram* dans le cas d'un réseau):

$$B = \begin{pmatrix} b(x_1,x_1) & \cdots & b(x_1,x_r) \\ \vdots & \ddots & \vdots \\ b(x_r,x_1) & \cdots & b(x_r,x_r) \end{pmatrix}$$

on a $b(x,y) = (\lambda_1, \ldots, \lambda_r) B (\mu_1, \ldots, \mu_r)^t$. Réciproquement, si on choisit $B = (\alpha_{ij})$ une matrice $r \times r$ à valeurs dans B, on peut bien définir la forme bilinéaire $b(x,y) = \sum_{i,j=1}^{r} \lambda_i\mu_j\alpha_{ij}$ donnée par le produit par B.

Donc, pour un module libre et un choix de la base, on a une correspondance biunivoque entre les formes bilinéaires et les matrices $\mathcal{M}_r(B)$.

On remarque aussi que $b(\cdot,\cdot)$ est respectivement *bilinéaire/anti-symétrique/(non)dégénérée* si et seulement si la matrice d'intersection associée est aussi *bilinéaire/anti-symétrique/(non)dégénérée.*

On est maintenant plus que prêts à donner la définition de réseau:

Définition 2.1.17. Un *réseau* L est un $\mathbb{Z}$-module libre fini doté d'une forme bilinéaire symétrique non-dégénérée $b(\cdot,\cdot) : L \times L \to \mathbb{Z}$.

Dans la suite on notera la forme bilinéaire comme un produit scalaire, i.e. $\langle x, y\rangle := b(x,y)$ et pour $x \in L$ on appellera *carré* de x la valeur $x^2 = \langle x, x\rangle$ (et si elle est positive on appellera *norme* la valeur $\sqrt{\langle x, x\rangle}$).

On a vu qu'en général une forme bilinéaire est déterminée de façon unique par sa matrice d'intersection. Dans le cas des réseaux, comme on demande une forme symétrique non-dégénérée, on aura qu'un réseau L sera déterminé par une matrice symétrique de rang maximal à coefficients dans $\mathbb{Z}$.

Par simplicité de notation, dans la suite, quand on parlera de matrice de Gram associée à un réseau, on sous-entendra parfois le choix d'une base adaptée.

Exemple 2.1.18. On peut associer des réseaux aux matrices I_n et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, mais pas à $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$.

Exemple 2.1.19. Soit $L = v\mathbb{Z}$ un réseau de rang 1, alors L est complètement déterminé par le carré de leur générateur $a = \langle v, v \rangle$. On indiquera les réseaux de ce type par la forme $\langle a \rangle$.

Définition 2.1.20. Si L est le réseau donné par la matrice de Gram M, pour $d \in \mathbb{Z}$ on notera $L(a)$ le réseau donné par la matrice aM.

Remarque 2.1.21. Si M_1, M_2 sont respectivement les matrices de Gram du réseau L dans les bases $\mathcal{B}_1$ et $\mathcal{B}_2$, et A la matrice de changement de base, alors:

$$A^t M_2 A = M_1$$

en particulier $\det(M_1) = \det(M_2)$.

Définition 2.1.22. Soit M la matrice de Gram d'un réseau L. Alors on note $\det(L) := \det(M) \in \mathbb{Z}$ le *déterminant* du réseau, qui est un invariant du réseau par la Remarque 2.1.21.

2.2 Exemples de réseaux

Afin de se familiariser avec cet objet, on va montrer quelques exemples de réseaux et leurs propriétés de base.

2.2.1 Réseaux euclidiens

Définition 2.2.1. Soit L un réseau de rang r et M la matrice de Gram associée à L. Alors en tensorisant on peut étendre la forme bilinéaire donnée par M sur $L \otimes \mathbb{R}$, en obtenant une forme de rang maximal de signature (i^+, i^-), qu'on identifiera comme la *signature* du réseau L.

Si la signature de L est définie positive ou négative on dira que L est un *réseau défini*. Autrement on dira que L est *indéfini*. On appellera *euclidien* un réseau défini positif.

Remarque 2.2.2. On considère $\mathbb{R}^n$ avec le produit scalaire standard $\langle \cdot, \cdot \rangle$, alors si $L \subset \mathbb{R}^n$ est un sous-groupe additif on a que L hérite d'une forme bilinéaire donnée par $\langle \cdot, \cdot \rangle$. Si elle prend uniquement des valeurs entières alors L sera un réseau euclidien, car il est obtenu a partir d'une forme positive. On souligne que L doit forcément être un sous-ensemble discret,

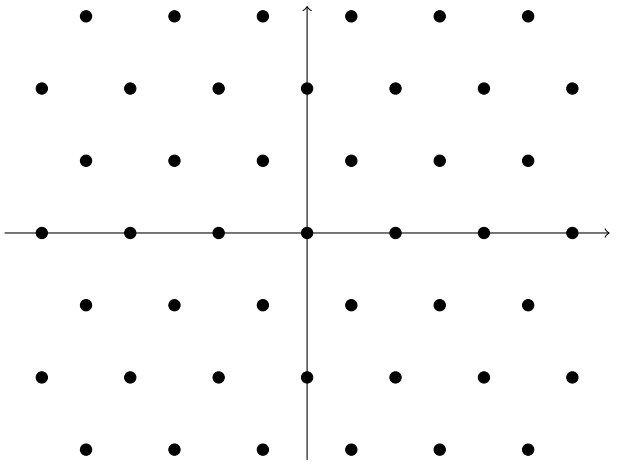


FIGURE 2.2.1 – Plongement de A_2 dans $\mathbb{R}^2$

sinon pour tout $\varepsilon > 0$ $\exists\, v_\varepsilon \in L$ tel que $\langle v_\varepsilon, v_\varepsilon \rangle < \varepsilon$, contradictoire avec l'hypothèse que la forme bilinéaire prend uniquement des valeurs entières positives et que la forme doit être non-dégénérée, sinon il existerait des éléments de carré nul.

Exemple 2.2.3. Soit $L \subset \mathbb{R}^n$ le sous-ensemble donné par tous les points à coordonnées entières, alors la restriction sur L du produit scalaire prendra uniquement des valeurs entières, donc L sera un réseau. Il s'agit du réseau avec matrice de Gram égale à la matrice identité.

Exemple 2.2.4. Soit $A_2 \subset \mathbb{R}^2$ le $\mathbb{Z}$-module engendré par $v_1 = (\sqrt{2}, 0)$, $v_2 = (-\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2})$ comme dans la Figure 2.2.1, alors $\langle v_1, v_1 \rangle = \langle v_2, v_2 \rangle = 2 \in \mathbb{Z}$ et $\langle v_1, v_2 \rangle = -1 \in \mathbb{Z}$ donc A_2 est un réseau. Il s'agit du réseau donné par la matrice $\mathrm{Gram}(A_2) = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$.

Exemple 2.2.5 (Construction de E_8)**.** Soit $E_8 \subset \mathbb{R}^8$ le sous-ensemble donné par les vecteurs $v = (x_1, \ldots, x_8)$ avec toutes les coordonnées entières ou toutes demi-entières (mais pas un mélange des deux !) donc $x_1, \ldots, x_8 \in \mathbb{Z}$ ou $x_1, \ldots, x_8 \in \mathbb{Z} + 1/2$, qui satisfont la condition selon laquelle la somme des coordonnées $x_1 + \cdots + x_8$ est un entier pair. On montre que E_8 est un réseau.

Soient $x, y \in E_8$, $x = (x_1, \ldots, x_8)$, $y = (y_1, \ldots, y_8)$, on montre que $\langle x, y \rangle \in \mathbb{Z}$. On a trois cas:

1 $x, y \in \mathbb{Z}^8$: dans ce cas il s'en suit immédiatement que $\langle x, y \rangle \in \mathbb{Z}$;

2 $x \in \mathbb{Z}^8$ et $y \in \left(\mathbb{Z} + \frac{1}{2}\right)^8$ (ou viceversa). On a $x_i \in \mathbb{Z}$, $y_i = \overline{y}_i + \frac{1}{2}$ avec

$\overline{y}_i \in \mathbb{Z}$, donc:

$$\begin{aligned}\langle x, y\rangle &= \sum_{i=1}^{8} x_i \left(\overline{y}_i + \frac{1}{2}\right) \\ &= \sum_{i=1}^{8} x_i \overline{y}_i + \frac{1}{2}\sum_{i=1}^{8} x_i\end{aligned}$$

mais par hypothèse $\sum_{i=1}^{8} x_i \in 2\mathbb{Z}$ et donc $\langle x, y\rangle \in \mathbb{Z}$;

3 $x, y \in \left(\mathbb{Z} + \frac{1}{2}\right)^8$: On a $x_i = \overline{x}_i + \frac{1}{2}$, $y_i = \overline{y}_i + \frac{1}{2}$ avec $\overline{x}_i, \overline{y}_i \in \mathbb{Z}$, donc:

$$\begin{aligned}\langle x, y\rangle &= \sum_{i=1}^{8} \left(\overline{x}_i + \frac{1}{2}\right)\left(\overline{y}_i + \frac{1}{2}\right) \\ &= \sum_{i=1}^{8} \overline{x}_i \overline{y}_i + \frac{1}{2}\sum_{i=1}^{8} \overline{x}_i + \frac{1}{2}\sum_{i=1}^{8} \overline{y}_i + 2\end{aligned}$$

et on conclut de manière similaire au point 2.

On peut se demander si le parcours inverse est possible: peut-on plonger tous les réseaux euclidiens dans $\mathbb{R}^n$ avec le produit scalaire standard ? La réponse est oui, comme on le voit dans la proposition suivante:

Proposition 2.2.6. *Soit L un réseau euclidien de rang r, alors il existe une inclusion $j : \mathbb{Z}^r \hookrightarrow \mathbb{R}^r$ qui réalise L.*

Démonstration. Comme un réseau est complètement déterminé par sa matrice de Gram, on doit montrer que pour tout $M = (\alpha_{ij}) \in \mathcal{M}_r(\mathbb{Z})$ matrice symétrique définie positive il existe $v_1, \ldots, v_r \in \mathbb{R}^r$ tels que $\langle v_i, v_j\rangle = \alpha_{ij}$. De façon équivalente, on cherche une matrice $F = \begin{pmatrix} v_1, & \cdots & , v_r \end{pmatrix} \in \mathcal{M}_r(\mathbb{R})$ telle que $FF^t = M$. Mais une décomposition dans une telle forme, pour les matrices symétriques définies positives est toujours assurée par la factorisation de Cholesky, ce qui conclut la preuve. □

Corollaire 2.2.7. *Soit L un réseau euclidien, $\mu \in \mathbb{N}$, alors l'ensemble $N_\mu = \{v \in L | \langle v, v\rangle \leq \mu\}$ est fini.*

Démonstration. Soit $r = \text{rang}(L)$, par la Proposition 2.2.6 on a l'existence d'un plongement $j : \mathbb{Z}^r \hookrightarrow \mathbb{R}^r$ qui réalise L. Si $B(\mu)$ est la boule fermée de rayon μ centrée en l'origine on a $N_\mu = B(\mu) \cap j(L)$ et donc $\#N_\mu < \infty$ car L est discret. □

Exemple 2.2.8. Si L est un réseau indéfini, pour $\mu \in \mathbb{Z}$ on peut avoir un nombre infini d'éléments de carré μ. Par exemple si L est le réseau donné par la matrice de Gram:

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

si on pose $v = (1, 0, 0)$, $w = (0, 1, 1)$ on a $(v + \lambda w)^2 = 1$ pour tous $\lambda \in \mathbb{Z}$.

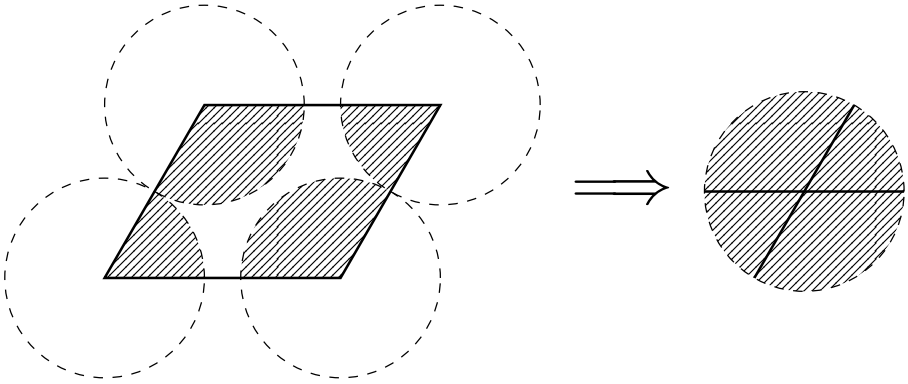


FIGURE 2.2.2 – « la somme de volumes de ces intersections pour toute sphère doit être égale au volume d'une seule sphère »

Définition 2.2.9. Pour L réseau euclidien on appelle:

$$\lambda = \min_{v \in L \setminus \{0\}} \sqrt{v^2} \neq 0$$

la *norme minimale de* L et λ^2 *le carré minimal de* L.

Théorème 2.2.10 (Minkowski)**.** *Soit* L *un réseau euclidien de rang* r*,* λ *la norme minimale de* L*, alors:*

$$\lambda^2 \leq \frac{4}{\pi} \Gamma\left(\frac{r}{2}+1\right)^{\frac{2}{r}} \det(L)^{\frac{1}{r}}$$

Démonstration. Soit $j : \mathbb{Z}^r \hookrightarrow \mathbb{R}^r$ tel que $\mathrm{Im}(j) \simeq L$, $v_1, \ldots, v_r$ une base de $\mathrm{Im}(j)$ et V le parallélépipède défini par $v_1, \ldots, v_r$, alors $\mathrm{vol}(V) = \det(F)$ avec $F = \begin{pmatrix} v_1, & \cdots & , v_r \end{pmatrix} \in \mathcal{M}_r(\mathbb{R})$, mais $FF^t = \mathrm{Gram}(L)$ donc $\mathrm{vol}(V) = \sqrt{\det(L)}$.

On place des boules r-dimensionelles de rayon $\lambda/2$ centrées sur les sommets du parallélépipède, avec λ la norme minimale. Chaque sphère intersecte une partie du parallélépipède et la somme de volumes de ces intersections pour toute sphère doit être égale au volume d'une seule sphère (Figure 2.2.2). Comme la distance entre deux sphères est équivalente à la longueur d'un vecteur de $\mathrm{Im}(j)$, celle-ci doit être inférieure ou égale à λ, donc deux sphères s'intersectent au plus en un point: cela implique que la somme des volumes des intersections est inférieure ou égale au volume du parallélépipède, donc:

$$\left(\frac{\lambda}{2}\right)^r V_1 \leq \mathrm{vol}(V)$$

avec V_r le volume d'une sphère de dimension r et rayon 1.

Il suffit de remplacer $V_1 = \frac{\pi^{\frac{r}{2}}}{\Gamma(\frac{r}{2}+1)}$ pour obtenir le résultat cherché. □

Exemple 2.2.11. Si L est de déterminant 1 on a les bornes suivantes pour le carré minimal de L:

rang(L)	1	2	3	4	5
$\lambda^2 \leq$	1	$1,27\ldots$	$1,54\ldots$	$1,80\ldots$	$2,06\ldots$

en particulier, si rang(L) ≤ 4 et det(L) $= 1$ alors L a un vecteur de norme 1 (car la norme prend uniquement des valeurs entières).

On peut se demander s'il existe un analogue du théorème de Minkowski pour le cas indéfini: plus précisément, si L est un réseau indéfini, est-ce qu'il existe une borne $B(r, D)$ dépendant uniquement de $r = \text{rang}(L)$ et $D = \det(L)$ telle qu'il existe $x \in L$ avec $0 < |x^2| \leq B(r, d)$?

Contrairement au cas euclidien, l'étude du cas indéfini est bien plus récente, et (à notre connaissance) le seul résultat de ce type (valable pour tout choix de r) est le suivant [BK]:

Théorème 2.2.12. *Soit L un réseau indéfini de rang r, alors il existe $x \in L$ tel que:*

$$0 < \left|x^2\right| \leq 2\sqrt[n]{\det(L)}$$

2.2.2 Morphismes entre réseaux

Soient L_1,L_2 deux réseaux, on veut définir ce qu'est un morphisme $f : L_1 \to L_2$. On rappelle que sur les réseaux on a deux structures, celle de $\mathbb{Z}$-module et la forme bilinéaire, donc il est naturel de demander que f préserve les deux. Par conséquent pour tous $x, y \in L_1$ on demande:

1 f doit être un morphisme de $\mathbb{Z}$ module, donc $f(x+y) = f(x)+f(y)$;

2 f doit préserver le produit bilinéaire, donc $\langle x, y\rangle_{L_1} = \langle f(x), f(y)\rangle_{L_2}$

Si on suppose que $f(x) = 0$, alors on aura $\langle x, y\rangle_{L_1} = \langle 0, f(y)\rangle_{L_2} = 0$ pour tout $y \in L_1$. Étant donné que la forme bilinéaire sur un réseau est toujours non-dégénérée, cela implique que le noyau de f doit être nul et donc f est forcément injective.

Dans le cas des réseaux on a donc uniquement des *plongement*s, ou dans le cas où f est une bijection, des *isométries* (ou *isomorphismes*). Si on a un plongement de réseaux $L' \subset L$ on dira que L' est un *sous-réseau* de L.

Remarque 2.2.13. En général, les sous-modules d'un réseau L ne sont pas toujours des réseaux. Par exemple soit U le *réseau hyperbolique* (i.e. le réseau donne par la matrice de Gram $M_U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ de signature $(1, 1)$). Si on pose $v = (1, 0) \in U$ on a que $L' = \text{span}_{\mathbb{Z}}(v)$ est un sous-module de U de rang 1, mais ce n'est pas un réseau, car la restriction de la forme bilinéaire est nulle sur L' vu que $\langle v, v\rangle = 0$.

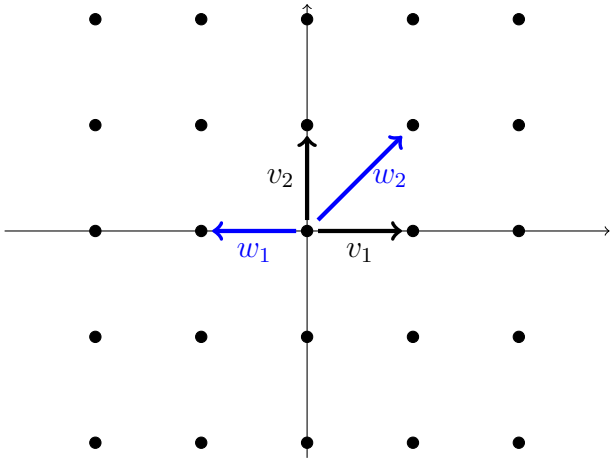


FIGURE 2.2.3 – Isométrie entre L_1 et L_2

Remarque 2.2.14. Si M_1, M_2 sont respectivement les matrices de Gram des réseaux L_1 et L_2 dans les bases $\mathcal{B}_1$ et $\mathcal{B}_2$, et $A = \mathrm{mat}_{\mathcal{B}_1,\mathcal{B}_2}(f)$, on aura:

$$A^t M_2 A = M_1$$

Donc deux réseaux de rang r sont isomorphes si et seulement s'il existe une matrice $A \in \mathcal{M}_r(\mathbb{Z})$ inversible tel que $A^t M_2 A = M_1$.

Exemple 2.2.15. Soient L_1,L_2 les réseaux donnés respectivement par les matrices de Gram $M_1 = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. La matrice $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ vérifie $A^t M_2 A = M_1$ et comme A est inversible on a montré que $L_1 \simeq L_2$. D'ailleurs on peut le voir aussi graphiquement sur la Figure 2.2.3 où on a représenté le réseau L_1 engendré par v_1 et v_2: on voit que (w_1, w_2) (c'est-à-dire les vecteurs qui forment la matrice A) donnent une base qui réalise le produit scalaire de L_2.

Étant donnés deux réseaux, il n'est pas toujours simple de déterminer s'il existe une isométrie entre les deux, mais la résolution du problème peut passer par l'utilisation des invariants. Des exemples d'invariants sont:

- Le rang ;
- La signature, car une isométrie de réseaux induit aussi un isomorphisme entre les espaces vectoriels sur $\mathbb{R}$ associés ;
- Le déterminant de la matrice de Gram, car si A est inversible dans $\mathcal{M}_r(\mathbb{Z})$ alors $\det(A) = \pm 1$ et donc si $A^t M_2 A = M_1$ alors $\det(M_1) = \det(M_2)$;
- La norme minimale pour les réseaux euclidiens.

On verra d'autres exemples d'invariants dans la suite, mais on anticipe dès maintenant en disant qu'il n'existe malheureusement pas de liste d'invariants pouvant classifier complètement les réseaux.

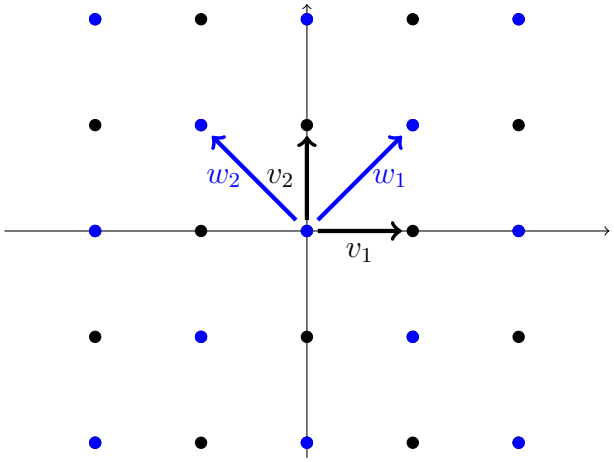


FIGURE 2.2.4 – L_1 est un sous-réseau de L_2

Exemple 2.2.16. Soient L_1,L_2 les réseaux donnés respectivement par les matrices de Gram $M_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, alors la matrice $A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ vérifie $A^t M_2 A = M_1$. Par contre, puisque A n'est pas inversible on n'a pas démontré l'isométrie ! (cf Figure 2.2.4). D'ailleurs il n'existe aucune isométrie possible, car $\det(M_1) = 4$ et $\det(M_2) = 1$ et le déterminant est un invariant par isométrie. On remarque d'ailleurs que plus en général, s'il existe un plongement $L_1 \hookrightarrow L_2$ non surjectif, alors $\det(L_1) > \det(L_2)$.

Exemple 2.2.17. Soient U le *réseau hyperbolique* (qu'on a vu dans la Remarque 2.2.13) et L_2 donné par $M_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On observe que les deux réseaux ont la même signature ($\text{sign}(U) = \text{sign}(L_2) = (1,1)$) et le même déterminant ($\det(U) = \det(L_2) = -1$). Si on veut montrer qu'ils ne sont pas isomorphes, il faut donc trouver un autre invariant. On a $v = (1,0) \in L_2$ a carré 1, on va donc prouver que pour tout $w \in U$ on a $\langle w, w \rangle \neq 1$. Soit $w = (a,b) \in U$, alors:

$$\langle w, w \rangle = (a,b) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = 2ab$$

Donc pour tout $w \in U$, $\langle w, w \rangle \in 2\mathbb{Z}$ (dans la suite on dira que U est un *réseau pair)* et en particulier est différent de 1.

2.2.3 Somme orthogonale

À partir de deux $\mathbb{Z}$-modules M_1 et M_2, on peut toujours construire un nouveau $\mathbb{Z}$-module en prenant la somme directe $M = M_1 \oplus M_2$. Et si les modules sont tous les deux dotés d'une forme bilinéaire b_1,b_2 dans ce cas

aussi on peut en prendre la somme, $b = b_1 \oplus b_2$, où si $x = x_1 + x_2, y = y_1 + y_2 \in M$ avec $x_i, y_i \in M_i$ alors $b(x, y) = b_1(x_1, y_1) + b_2(x_2, y_2)$.

On peut donc définir la *somme orthogonale* de deux réseaux $L = L_1 \oplus L_2$ et c'est évident que le résultat est toujours un réseau (car il s'agit d'un $\mathbb{Z}$-module libre fini doté d'une forme bilinéaire symétrique non-dégénérée).

On remarque aussi que si (α_{ij}) et (β_{st}) sont respectivement les matrices de Gram de L_1 et L_2 alors $L_1 \oplus L_2$ est donnée par la matrice par blocs $\begin{pmatrix} \alpha_{ij} & 0 \\ 0 & \beta_{st} \end{pmatrix}$, en particulier:

$$\det(L) = \det(L_1) \cdot \det(L_2)$$

On indiquera les sommes répétées d'un réseau avec $L^{\oplus a} := \underbrace{L \oplus \cdots \oplus L}_{a \text{ fois}}$; par exemple $\langle 1 \rangle^{\oplus n}$ indiquera le réseau donné par la matrice identité I_n. À pas confondre avec aL, qui indiquera le sous-réseau de L donné par le produit par a.

Définition 2.2.18. Soit L un réseau et $S \subset L$ un sous-ensemble. Alors on notera $S^\perp$ l'ensemble $S^\perp = \{x \in L | \langle x, s \rangle = 0 \, \forall s \in S)$, qu'on appellera *orthogonal* de S. Par convention, si $S = \{v\}$ on notera plus simplement $v^\perp := \{v\}^\perp$.

Lemme 2.2.19. *Soit L un réseau de rang r et $L' \subset L$ un sous-réseau avec $\operatorname{rang}(L') = r'$. Alors $L'^\perp$ est un sous-réseau primitif de L de rang $r - r'$ et $L' \cap L'^\perp = \{0\}$.*

Démonstration. Soient $V = L \otimes \mathbb{Q}$, $V' = L' \otimes \mathbb{Q} \subset V$ et $W = V'^\perp$ les $\mathbb{Q}$-espaces vectoriels de dimensions respectives r, r' et $r - r'$, alors on a $V \simeq V' \oplus W$ car V' est non-dégénérée. Comme la forme bilinéaire est de rang maximal sur V et V', elle est de rang maximal sur W aussi. Donc $L'^\perp = L \cap W$ de rang $r - r'$ est doté d'une forme bilinéaire non-dégénérée et donc c'est un réseau ; de plus il est primitif, car donné par l'intersection avec un sous-espace vectoriel et $L' \cap L \subseteq V' \cap W = 0$. □

Lemme 2.2.20. *Soit L un réseau, $n \in \mathbb{N} \backslash \{0\}$ $T_1, \ldots, T_n, K \subseteq L$ des sous-réseaux primitifs tels que $\operatorname{rang}(T_1 \oplus \cdots \oplus T_n) = \operatorname{rang}(L)$ et $\operatorname{rang}(K \cap T_1) + \cdots + \operatorname{rang}(K \cap T_n) = \operatorname{rang}(K)$. Alors:*

$$K \cap (T_1 \oplus \cdots \oplus T_n) = K \cap T_1 \oplus \cdots \oplus K \cap T_n$$

Démonstration. On a $K \cap T_1 \oplus \cdots \oplus K \cap T_n \subseteq K \cap (T_1 \oplus \cdots \oplus T_n)$ et par égalité des dimensions, $(K \cap (T_1 \oplus \cdots \oplus T_n)) \otimes \mathbb{Q} = (K \cap T_1 \oplus \cdots \oplus K \cap T_n) \otimes \mathbb{Q}$. Soit $x \in K \cap (T_1 \oplus \cdots \oplus T_n)$, alors $x = t_1 + \cdots + t_n$ avec $t_i \in T_i$, mais on a aussi $x = t'_1 + \cdots + t'_n$ avec $t'_i \in (K \cap T_i) \otimes \mathbb{Q}$. Comme la décomposition d'un élément de L sur $T_1 \otimes \mathbb{Q} \oplus \cdots \oplus T_n \otimes \mathbb{Q}$ est unique on a $t_i = t'_i \; \forall 1 \leq i \leq n$. Par le Lemme 2.1.11 $K \cap T_i$ est primitif, donc $t_i \in T_i \cap ((K \cap T_i) \otimes \mathbb{Q}) = T_i \cap (K \cap T_i) = T_i \cap K$, ce qui nous donne l'équivalence cherchée. □

Exemple 2.2.21. Soit U le réseau hyperbolique, alors il existe $v = (1, 1) \in U$ avec $v^2 = 0$. Donc $L' = \text{span}_{\mathbb{Z}}(v)$ n'est pas un réseau, car la forme bilinéaire est dégénérée et de plus $L' = L'^{\perp}$.

Définition 2.2.22. L est un réseau *décomposable* s'il existe deux sous-réseaux $L_1, L_2 \subset L$ orthogonaux entre eux tels que $L \simeq L_1 \oplus L_2$, sinon on dit que L est *indécomposable*.

Remarque 2.2.23. Si $\text{rang}(L) = 1$ alors L est indécomposable.

Exemple 2.2.24. On suppose que $U = L_1 \oplus L_2$, alors $\det(L_1)\det(L_2) = -1$ donc on peut choisir sans perte de généralité $\det(L_1) = 1$, $\det(L_2) = -1$. Mais L_1 de dimension 1 implique que $L_1 = \langle a \rangle$, avec $a = \det(L_1) = 1$ et de la même façon $L_2 = \langle -1 \rangle$, donc $L \simeq \langle 1 \rangle \oplus \langle -1 \rangle$, ce qui n'est pas le cas, comme on a déjà vu dans l'Exemple 2.2.17. Donc U est indécomposable.

Exemple 2.2.25. Soit L un réseau, $d \in \mathbb{Z}\backslash\{0\}$, alors $L(d)$ est indécomposable si et seulement si L est indécomposable. En effet, soit $B = (v_1, \ldots, v_n)$ la base de L associée à la matrice de Gram M, alors elle induit $C = (w_1, \ldots, w_n)$ base de $L(d)$ telle que la matrice de Gram associée soit dM, alors, $\varphi : L \to L(d)$, donné par $\varphi(v_i) = w_i$ est un isomorphisme de $\mathbb{Z}$-module. φ n'est pas un morphisme de réseau car il ne préserve pas le produit scalaire, par contre il préserve l'orthogonalité, c'est-à-dire que $v \perp v'$ dans L si et seulement si $\varphi(v) \perp \varphi(v')$ dans $L(d)$, donc une décomposition orthogonale sur un des deux réseaux induit une décomposition orthogonale sur l'autre.

Exemple 2.2.26. Décomposer un réseau en facteurs orthogonaux est plus compliqué que décomposer des espaces vectoriels, car si $L' \subset L$ est un sous-réseau (même primitif), en général $L \neq L' \oplus L'^{\perp}$. Par exemple si $L = \langle 1 \rangle^{\oplus 2}$, $L' = \text{span}_{\mathbb{Z}}((1, 1))$ alors $L' \oplus L'^{\perp} \simeq \langle 2 \rangle^{\oplus 2} \not\simeq L$: d'ailleurs il s'agit du cas décrit dans l'Exemple 2.2.16.

Exemple 2.2.27 (Décomposition non unique)**.** La décomposition d'un réseau en général n'est pas unique. On rappelle que $U \neq \langle 1 \rangle \oplus \langle -1 \rangle$, par contre soient $L_1 = U \oplus \langle 1 \rangle$ et $L_2 = \langle 1 \rangle^{\oplus 2} \oplus \langle -1 \rangle$, alors on a $M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Si on pose $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$ on voit que $A^t M_2 A = M_1$, donc $L_1 \simeq L_2$ représentent deux décompositions différentes.

Pour les réseaux euclidiens on a:

Théorème 2.2.28 (Eichler-Kneser)**.** *Soit L un réseau euclidien. Alors il existe une décomposition de $L = L_1 \oplus \cdots \oplus L_k$, somme orthogonale de réseaux indécomposables et elle est unique à l'ordre près.*

La preuve est assez simple, par contre elle nécessite l'introduction de quelque concepts, qu'on va donc introduire par étapes. On précise aussi que dans ces notes on a adapté la notion d'indécomposabilité, qu'on trouve normalement pour les seuls réseaux euclidiens, au cas général, en obtenant, pour les réseaux indéfinis qui satisfont certains critères, un résultat de décomposition similaire au cas des réseaux euclidiens. Cela a demandé donc de modifier la preuve originelle (qu'on trouve par exemple dans [Cop]), car dans le cas indéfini les réseaux ne sont pas tous décomposables de façon unique.

Définition 2.2.29. Un élément $x \in L$, avec L réseau, est dit *décomposable* si $x = 0$ ou s'il existe $v, w \in L\backslash\{0\}$ tels que $x = v + w$ et $\langle v, w\rangle = 0$. Dans le cas contraire on dit que x est *indécomposable.* On notera $\mathrm{Ind}(L)$ l'ensemble des éléments indécomposables de L.

Exemple 2.2.30. Si L est un réseau euclidien et v un vecteur de carré minimal, alors v est indécomposable.

Remarque 2.2.31. Si $L = L_1 \oplus L_2$ comme les éléments indécomposables ne sont pas somme d'éléments orthogonaux on a $\mathrm{Ind}(L) = (\mathrm{Ind}(L) \cap L_1) \cup (\mathrm{Ind}(L) \cap L_2)$. De plus, si $x \in L_1$ est indécomposable sur L, alors il l'est aussi sur L_1 , donc $\mathrm{Ind}(L) \subseteq \mathrm{Ind}(L_1) \cup \mathrm{Ind}(L_2)$.

Exemple 2.2.32. En général $\mathrm{Ind}(L) \neq \mathrm{Ind}(L_1) \cup \mathrm{Ind}(L_2)$, par exemple soit $L_1 \simeq L_2 \simeq \langle 1\rangle$, alors $(2, 0) \in \mathrm{Ind}(L_1)$ mais $(2, 0) \notin \mathrm{Ind}(L_1 \oplus L_2)$ car $(2, 0) = (1, 1) + (1, -1)$.

Définition 2.2.33. $x, y \in \mathrm{Ind}(L)$ sont dits *connexes* si $x = y$ ou s'il existe $x_1, \ldots, x_{n-1} \in \mathrm{Ind}(L)$ éléments indécomposables, tels que $\langle x_0 = x, x_1\rangle \neq 0$, $\langle x_1, x_2\rangle \neq 0$, $\ldots$, $\langle x_{n-2}, x_{n-1}\rangle \neq 0$, $\langle x_{n-1}, x_n = y\rangle \neq 0$.

Il est évident qu'il s'agit d'une relation d'équivalence, qui définit donc une partition des éléments indécomposables de la forme $\mathrm{Ind}(L) = \coprod_{i\in I} C_i$. On appellera *ensemble connexe* un ensemble contenu dans une des classes d'équivalence.

Lemme 2.2.34. *Soit L un réseau, $C \subset Ind(L)$ un ensemble connexe et $x, y \in \mathrm{span}_{\mathbb{Q}}(C) \cap L\backslash\{0\}$. Alors il n'existe aucune décomposition orthogonale $L = L_1 \oplus L_2$ telle que $x \in L_1$ et $y \in L_2$.*

Démonstration. Soit $L = L_1 \oplus L_2$ et $z, z' \in C \subset \mathrm{Ind}(L)$. Étant donné que $\mathrm{Ind}(L) \subseteq \mathrm{Ind}(L_1) \cup \mathrm{Ind}(L_2)$ alors soit $z \in L_1$, soit $z \in L_2$. On suppose, sans perte de généralité, que $z \in L_1$. Alors il existe $z_0 = z, z_1, \ldots, z_{n-1}, z_n = z' \in L$ tels que $\langle z_i, z_{i+1}\rangle \neq 0$. À nouveau, on a $z_1 \in L_1$ ou $z_1 \in L_2$, mais le deuxième cas est impossible car $\langle z, z_1\rangle \neq 0$, donc $z_1 \in L_1$ et de la même façon, tous les z_i, y compris z' appartiennent à L_1. Donc $C \subset L_1$ et par conséquent $\mathrm{span}_{\mathbb{Q}}(C) \cap L \subset \mathrm{span}_{\mathbb{Q}}(L_1) \cap L = L_1$ (car L_1 primitif par hypothèse) et donc $x, y \in L_1$. □

On obtient alors:

Corollaire 2.2.35. *Soit L un réseau et $C \subset Ind(L)$ un ensemble connexe tel que* $\mathrm{span}_{\mathbb{Q}}(C) \supseteq L$. *Alors L est un réseau indécomposable.*

Dans le cas où le réseau est engendré par ses éléments indécomposables, on a une décomposition unique du réseau:

Proposition 2.2.36. *Soit L un réseau tel que* $\mathrm{span}_{\mathbb{Z}}\, Ind(L) = L$, *$Ind(L) = \coprod_{i\in I} C_i$ la partition en sous-ensembles connexes, alors $L = \bigoplus_{i\in I} L_i$ avec $L_i = \mathrm{span}_{\mathbb{Z}}(C_i)$ est une somme orthogonale de réseaux indécomposables et elle est unique à l'ordre près.*

Démonstration. Il s'agit d'une décomposition en indécomposables car:

- Les L_i engendrent L, car $\sum_{i\in I} L_i = \mathrm{span}_{\mathbb{Z}}(\bigcup_{i\in I} C_i) = \mathrm{span}_{\mathbb{Z}} \mathrm{Ind}(L) = L$ par hypothèse ;
- Donc $L = L_j + \sum_{i\in I\setminus\{j\}} L_i$ et $L_j \perp \sum_{i\in I\setminus\{j\}} L_i$ car $C_i \perp C_j$ pour $i \neq j$, alors si $x \in L_j \cap \sum_{i\in I\setminus\{j\}} L_i$ on a $x \in L_j^{\perp} \cap \left(\sum_{i\in I\setminus\{j\}} L_i\right)^{\perp} \subseteq L^{\perp} = \{0\}$ car le produit scalaire sur L est non-dégénéré. Donc on a une somme directe $L = \bigoplus_{i\in I} L_i$ par conséquent le produit scalaire sur L_i est non-dégénéré, donc les L_i sont des réseaux et I est un ensemble fini.
- On a $C_i \subset \mathrm{Ind}(L_i)$ connexe, donc par le Corollaire 2.2.35 les L_i sont indécomposables ;

Il reste à démontrer qu'elle est unique. Soit donc $L = \overline{L}_1 \oplus \cdots \oplus \overline{L}_r$ une autre décomposition en facteurs indécomposables, alors pour tout $i \in I$, $C_i \subset \mathrm{Ind}(\overline{L}_1) \cup \cdots \cup \mathrm{Ind}(\overline{L}_r)$ et comme C_i est connexe, il existe $1 \leq j \leq r$ tel que $L_i \subseteq \overline{L}_j$. On montre maintenant que $\overline{L}_j = (L_i \oplus L_i^{\perp}) \cap \overline{L}_j$, ce qui implique $L_i = \overline{L}_j$ car $\overline{L}_j$ indécomposable: soit $z \in \overline{L}_j$, puisque $L = L_i \oplus L_i^{\perp}$ on a $z = x + y$ avec $x \in L_i$ et $y \in L_i^{\perp}$, mais $y = z - x \in \overline{L}_j$ car $x, z \in \overline{L}_j$ et donc $y \in L_i^{\perp} \cap \overline{L}_j$, ce qui complète la preuve.

□

On est donc maintenant prêt à conclure la preuve du Théorème 2.2.28, qui est une conséquence immédiate du résultat suivant et de la Proposition 2.2.36:

Proposition 2.2.37. *Soit L un réseau euclidien, alors* $\mathrm{span}_{\mathbb{Z}}\, Ind(L) = L$.

Démonstration. Soit $x \in L$, si $x \notin \mathrm{Ind}(L)$ alors $x = x_1 + x_2$ avec $\langle x_1, x_2\rangle = 0$ et $x_1, x_2 \neq 0$. Donc $\langle x, x\rangle = \langle x_1, x_1\rangle + \langle x_2, x_2\rangle$ et comme L est euclidien on a $x^2 > x_1^2$ et $x^2 > x_2^2$. Si $x_1, x_2 \in \mathrm{Ind}(L)$, on a terminé, sinon, on peut à nouveau déterminer une décomposition. Puisqu'on est dans un réseau euclidien le carré des éléments est toujours positif, mais toujours décroissant, donc la procédure doit forcément s'arrêter après un nombre fini de pas, nous donnant une décomposition de x comme somme d'éléments indécomposables. □

Remarque 2.2.38. Les résultats énoncés pour les réseaux euclidiens restent vrais pour les réseaux définis négatifs après un changement de signe. Le Théorème 2.2.28 s'applique donc à tous les réseaux définis.

Exemple 2.2.39 (Réseau sans élément indécomposable)**.** On a vu dans l'exemple 2.2.27 que la décomposition de $L = \langle 1\rangle^{\oplus 2} \oplus \langle -1\rangle$ n'est pas unique. Cela ne contredit pas le Théorème 2.2.28 car L est un réseau indéfini et donc il peut ne pas être engendré par ses éléments indécomposables. En fait, on peut même prouver que $\mathrm{Ind}(L) = \emptyset$. Pour montrer cela on considère une base u, v, w d'éléments orthogonaux entre eux tels que $u^2 = v^2 = 1$ et $w^2 = -1$: si $x \in L$, alors $x = au+bv+cw$, mais si au moins deux facteurs entre a, b, c sont différents de zéro, on a clairement que x est décomposable. Donc les seuls éléments susceptibles d'être décomposables sont u, v, w. Par contre on a bien les décompositions orthogonales données par $u = (u + v + w) + (-v - w)$, $v = (u + v + w) + (-u - w)$ et $w = (u + v + 2w) + (-u - v - w)$, donc aucun élément est indécomposable.

Exemple 2.2.40. Soit L un réseau euclidien, on veut montrer qu'on peut toujours écrire $L = L_1 \oplus \langle 1\rangle^k$ avec L_1 sans élément de carré 1. Soit $v \in L$ tel que $v^2 = 1$, alors v est indécomposable car il est de carré minimal, donc il suffit de montrer que v, ou éventuellement ses multiples, sont les seuls éléments de sa composante dans la partition de $\mathrm{Ind}(L)$, autrement dit, qu'il n'existe aucun $w \in \mathrm{Ind}(L)$, $w \neq \lambda v$ tel que $\langle v, w\rangle \neq 0$ (car w est orthogonal à v si et seulement s'il est orthogonal à tous ses multiples). Par conséquent on aura que dans la décomposition donnée par la Proposition 2.2.36 tous les éléments de carré 1 engendreront des réseaux de rang 1 et on aura conclu.

Soit donc $w \in L$ tel que $\langle w, v\rangle = b \neq 0$, on veut montrer que w n'est pas indécomposable, ce qu'on peut faire en exhibant une décomposition, comme par exemple $w = (w - bv) + (bv)$ qui vérifie $\langle w - bv, bv\rangle = b^2 - b^2 = 0$.

Remarque 2.2.41. Soit L un réseau de rang r et M la matrice de Gram associée, alors $\det(L(a)) = \det(aM) = a^r \det M = a^r \det L$. En particulier $a^r \mid \det(aL)$.

2.2.4 Réseaux pairs et impairs

Définition 2.2.42. Soit L un réseau, on dira que L est *pair* (ou de *type II*) si $\langle x, x\rangle \in 2\mathbb{Z}$ pour tout $x \in L$, sinon on dira que L est *impair* (ou de *type I*).

Remarque 2.2.43. Le réseau associé à une surface K3 est pair et il est clair que les sous-réseaux d'un réseau pair sont aussi pairs. C'est la raison pour laquelle dans cette thèse on se concentrera surtout sur ce type de réseaux.

Exemple 2.2.44. Si L est un réseau, $L(2)$ est toujours un réseau pair, car $\forall x \in L(2)$, $\langle x, x\rangle_{L(2)} = 2\langle x, x\rangle_L \in 2\mathbb{Z}$. Par contre tous les réseaux pairs ne sont pas de cette forme, par exemple on a vu que U est pair (Exemple

2.2.17), mais on vérifie facilement que U n'est pas de la forme $L(2)$ pour aucun réseau L.

Lemme 2.2.45. *Soit L un réseau avec matrice de Gram $M = (a_{ij})$. Alors L est pair si et seulement si les éléments de la diagonale de M sont pairs.*

Démonstration. Soit $x_1, \ldots, x_n$ la base de L associé à M, alors $a_{ii} = \langle x_i, x_i \rangle$ donc si L est pair on a a fortiori $a_{ii} \in 2\mathbb{Z}$. Réciproquement, on suppose que $a_{ii} \in 2\mathbb{Z}$ pour $1 \leq i \leq n$: soit $v \in L$, $v = \lambda_1 x_1 + \cdots + \lambda_n x_n$ avec $\lambda_i \in \mathbb{Z}$, alors:

$$\begin{aligned} \langle v, v \rangle &= \sum_{i,j=1}^{n} \lambda_i a_{ij} \lambda_j \\ &= 2\left(\sum_{1 \leq i < j \leq n} \lambda_i a_{ij} \lambda_j \right) + \sum_{1 \leq i \leq n} \lambda_i^2 \underbrace{a_{ii}}_{\in 2\mathbb{Z}} \end{aligned}$$

donc $\langle v, v \rangle \in 2\mathbb{Z}$ et L est pair. □

Exemple 2.2.46. Par analogie avec les réseaux pairs, pour $d \in \mathbb{N}$, $d \geq 3$, on peut se demander de quelle forme sont les réseaux «d-divisibles», c'est-à-dire, les réseaux L tels que pour tous $v \in L$, $d | v^2$. À nouveau, il est clair que si L est un réseau, alors $L(d)$ satisfait cette propriété, mais on peut montrer aussi que si d est impair, alors tous les réseaux d-divisibles sont de cette forme. Soit $M = (a_{ij})$ la matrice de Gram associée à la base $(v_1, \ldots, v_r)$ d'un réseau L d-divisible avec d impair, alors on veut montrer que $d | a_{ij}$ $\forall 1 \leq i, j \leq r$. On a que pour tous i, j, $d | \langle v_i + v_j, v_i + v_j \rangle$ et donc $d | (a_{ii} + a_{jj} + 2a_{ij})$: on a $a_{ii} = v_i^2$ et $a_{jj} = v_j^2$, donc $d | a_{ii}$ et $d | a_{jj}$ et par conséquent $d | 2a_{ij}$, mais d est impair et donc $d | a_{ij}$. Donc $M' = \frac{1}{d} M$ est une matrice à coefficients entiers et $L = L'(d)$ avec L' le réseau associé à M'.

Lemme 2.2.47. *Soit L un réseau pair avec* $\det(L)$ *impair, alors* $2 | \operatorname{rang}(L)$.

Démonstration. Soit M la matrice de Gram de L et $\overline{M} \in \mathcal{M}_r(\mathbb{F}_2)$ son quotient modulo 2. Alors $\overline{M}$ représente une forme bilinéaire sur $\mathbb{F}_2^r$, inversible car $\det(\overline{M}) \equiv \overline{1} \pmod 2$. Comme L est pair, pour tout $v \in \mathbb{F}^r$ on a $\langle v, v \rangle = \overline{0}$ dans $\mathbb{F}_2$, alors par la classification des formes quadratiques inversibles sur $\mathbb{F}_2$ on a que $\overline{M}$ peut être diagonalisée par blocs 2×2 de la forme:

$$\begin{pmatrix} \overline{0} & \overline{1} & & & \\ \overline{1} & \overline{0} & & & \\ & & \ddots & & \\ & & & \overline{0} & \overline{1} \\ & & & \overline{1} & \overline{0} \end{pmatrix}$$

En particulier $2 | \operatorname{rang}(L)$. □

2.2.5 Réseaux de racines

Les réseaux de racines méritent une attention particulière, car très souvent les réseaux qu'on rencontrera seront de ce type ou construits à partir de ce type.

Définition 2.2.48. Soit $x \in L$ avec L réseau, alors x est dit *racine* si $\langle x, x\rangle = 2$ (le terme est emprunté aux algèbres de Lie). Un réseau euclidien L est dit *réseau de racines* s'il est engendré par ses racines.

Comme tout élément d'un réseau de racines se décompose comme somme de vecteurs de carré égal à 2, on a en particulier que les réseaux de racines sont des réseaux pairs.

Lemme 2.2.49. *Soit L un réseau, S un sous-ensemble fini de $L\backslash\{0\}$, alors il existe $v \in L$ tel que $v^\perp \cap S = \emptyset$.*

Démonstration. La forme bilinéaire sur $L\otimes\mathbb{Q}$ est non-dégénérée, donc pour tout $s \in S$, $s^{\perp_{L\otimes\mathbb{Q}}}$ est un hyperplan de $L\otimes\mathbb{Q}$, mais puisque S est un ensemble fini alors $\bigcup_{s\in S} s^{\perp_{L\otimes\mathbb{Q}}} \neq L\otimes\mathbb{Q}$ et donc il existe $v \in L\backslash\bigcup_{s\in S} s^{\perp_{L\otimes\mathbb{Q}}}$. □

Définition 2.2.50. Un *système fondamental de racines* dans un réseau de racines L est un ensemble de racines Π qui engendre L et tel que $\langle s, t\rangle = -1$ ou $\langle s, t\rangle = 0$ pour tous $s, t \in \Pi$.

On dira que Π est un *système fondamental de racines réduit* si les éléments de Π sont linéairement indépendants.

Proposition 2.2.51. *Tout réseau de racines admet un système fondamental de racines réduit. En particulier il admet une base de racines.*

Démonstration. Soit L un réseau de racines, alors L a un nombre fini de racines et donc il existe $u \in L$ orthogonal à aucune racine. Soit $\Phi^+(u)$ l'ensemble des racines $r \in L$ tels que $\langle r, u\rangle > 0$, alors si r est une racine, soit $r \in \Phi^+(u)$ soit $-r \in \Phi^+(u)$. Maintenant on pose $\Pi(u) = \{r \in \Phi^+(u) | r \neq s + t \text{ avec } s, t \in \Phi^+(u)\}$. On montre que $\Pi(u)$ est un système fondamental de racines réduit:

- $\Pi(u)$ engendre $\Phi^+(u)$ (et donc L): Soit $r \in \Phi^+(u)$, alors soit $r \in \Pi(u)$, soit $r = r_1 + r_2$ avec $r_i \in \Phi^+(u)$; si $r_1, r_2 \in \Pi(u)$ on a conclu, sinon on décompose à nouveau, et dans le cas général après n passages on aura une décomposition récurrente de la forme $r = \sum_{I_n} r_i$. On montre qu'après un nombre fini de passages on obtient des éléments qui ne sont pas ultérieurement décomposables, ce qui nous donne la décomposition en éléments de $\Pi(u)$. D'abord on suppose qu'il existe $j \in I_n$ tel que $r = r_j$, alors $r = r + \sum_{I_n\backslash\{j\}} r_i$ et donc $\sum_{I_n\backslash\{j\}} r_i = 0$, mais cela est impossible car $0 = \left\langle u, \sum_{I_n\backslash\{j\}} r_i \right\rangle = \sum_{I_n\backslash\{j\}} \langle u, r_i\rangle > 0$ car $r_i \in \Phi^+(u)$ et $\#I_n \geq 2$. Par conséquent r n'apparaît jamais dans sa décomposition et de la même façon aucune des racines r_j n'est

jamais répétée à nouveau dans sa propre décomposition. Donc dans la décomposition des $r_j \in I_n$, il n'apparaîtra ni r_j ni aucun autre des éléments pour lequel r_j a participé dans la décomposition, y compris r lui même: comme le nombre de racines est un ensemble fini on a que la décomposition doit s'arrêter après un nombre des passages fini majoré par $\#(\Phi^+(u))$.

- Si $r, s \in \Pi(u)$ alors $\langle r, s\rangle = -1$ ou $\langle r, s\rangle = 0$: On considère le sous-réseau donné par $\mathrm{span}_{\mathbb{Z}}(r, s)$ avec matrice de Gram

$$M = \begin{pmatrix} 2 & \langle r, s\rangle \\ \langle r, s\rangle & 2 \end{pmatrix}$$

Comme L est un réseau euclidien on a que $\det(M) > 0$ et donc $\langle r, s\rangle \in \{-1, 0, +1\}$. On montre alors que $\langle r, s\rangle \neq 1$: soient $r, s \in \Pi(u)$ avec $\langle r, s\rangle = 1$, alors $r' = r - s$ est une racine aussi, car $\langle r - s, r - s\rangle = 2$, donc soit $r' \in \Phi^+(u)$, soit $-r' \in \Phi^+(u)$. Dans le premier cas on a $r = r' + s$, en contradiction avec $r \in \Pi(u)$ et dans le deuxième cas $s = r + (-r')$, ce qui nous donne une autre contradiction.

- Les éléments de $\Pi(u)$ sont indépendants: On suppose que $\lambda_1 r_1 + \cdots + \lambda_n r_n = 0$ avec $r_i \in \Pi(u)$, on sépare alors les coefficients λ_i en positifs et négatifs, et on obtient alors :

$$a_1 r_{i_1} + \cdots + a_k r_{i_k} = b_1 r_{j_1} + \cdots + b_{k'} r_{j_{k'}} = x$$

avec $a_i, b_j > 0$, $x \neq 0$ car $\langle x, u\rangle > 0$. Alors:

$$0 < \langle x, x\rangle = \left\langle a_1 r_{i_1} + \cdots + a_k r_{i_k}, b_1 r_{j_1} + \cdots + b_{k'} r_{j_{k'}} \right\rangle \leq 0$$

car $\langle r_i, r_j\rangle \leq 0$ par le point précédent et on a la contradiction.

□

Remarque 2.2.52. Donc être engendré par des racines est équivalent a avoir une base de racine. Cela ne pas vrai pour le choix de n'importe quel norme. Par exemple, soit $L = \langle 1\rangle \oplus \langle 5\rangle$, alors les éléments de carré 9 sont de la forme $\pm 3e_1$ et $\pm 2e_1 \pm e_2$. On vérifie facilement que $v_1 = 3e_1$, $v_2 = 2e_1 + e_2$, $v_3 = 2e_1 - e_2$ sont trois éléments de norme 9 qui engendrent L ($e_1 = v_2 + v_3 - v_1$, $e_2 = 2v_1 - v_2 - 2v_3$), par contre il n'existe aucune base de L composée uniquement par des éléments de norme 9.

Exemple 2.2.53. On appelle $A_n \subset \mathbb{Z}^{n+1}$ l'ensemble des vecteurs $(x_0, \ldots, x_n)$ tels que la somme des $n + 1$ coordonnées entières $x_0 + \cdots + x_n$ est nulle. Par exemple A_2 est le réseau de rang 2 engendré par $(1, -1, 0)$ et $(0, 1, -1)$. Plus généralement, on a que A_n est un réseaux de racines engendré par les n racines:

$$v_i = (0, \ldots, 0, \underbrace{1}_{i-1}, \underbrace{-1}_{i}, 0, \ldots, 0)$$

avec $\langle r_i, r_{i+1}\rangle = -1$ et $\langle r_i, r_j\rangle = 0$ pour $j \neq i, i + 1$.

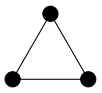
Exemple 2.2.54. Pour $n \geq 2$, soit $D_n \subset \mathbb{Z}^n$ l'ensemble des vecteurs $(x_1, \ldots, x_n)$ tels que la somme des n coordonnées entières $x_1 + \cdots + x_n$ est paire. On appelle D_n le *réseau à échiquier*, car les éléments de D_n correspondent aux cases noires d'un échiquier à n dimensions. Par exemple D_2 est le réseau de rang 2 engendré par $(1,1)$ et $(1,-1)$. Plus généralement, on a que D_n est engendré par les n racines $r_1 = (1,1,0,\ldots,0)$ et pour $i \geq 2$ $r_i = (0,\ldots,0,\underbrace{1}_{i-1},\underbrace{-1}_{i},0,\ldots,0)$ avec $\langle r_i, r_{i+1}\rangle = -1$ pour $i \geq 2$,$\langle r_1, r_3\rangle = -1$ et $\langle r_i, r_j\rangle = 0$ sinon.

Soit Π un système fondamental de racines réduit d'un réseau de racines L. On peut définir le *diagramme de Dynkin* comme le graphe dont l'ensemble des sommets est donné par Π avec $r, s \in \Pi$ reliés par un arc (non orienté) si $\langle r, s\rangle = -1$. Vu que tous les réseaux de racines admettent un système fondamental réduit, il est toujours possible d'exprimer un réseau de racines avec son diagramme de Dynkin. De plus, vu que les racines d'un réseau pair sont aussi des éléments indécomposables (car ils sont de norme minimale), on a que L est indécomposable si et seulement si le diagramme associé est connexe (cf. Proposition 2.2.36).

Exemple 2.2.55. On résume dans le Tableau 2.2.1 les diagrammes de Dynkin de A_n et D_n avec leurs matrices de Gram. On voit qu'il s'agit de réseaux indécomposables, car les diagrammes associés sont connexes (à l'exception de D_2 qui est donné par deux points non reliés). On peut calculer aussi le déterminant des matrices de Gram M_n, grâce à la relation de récurrence $\det(M_n) = 2\det(M_{n-1}) - \det(M_{n-2})$ (vérifiée par les deux types de réseaux) qui peut être prouvée en développant selon la dernier ligne. On remarque aussi que $A_3 \simeq D_3$.

Exemple 2.2.56. Il y a encore trois autres réseaux de racines, dont on va donner le diagramme de Dynkin dans le Tableau 2.2.2 (le réseau de racine E_8 ici décrit est le même qu'on a rencontré dans l'Exemple 2.2.5). On a que A_n, D_n avec $n \geq 4$, E_6, E_7 et E_8 sont indécomposables et différents entre eux (car soit les déterminants, soit les rangs, ne sont pas les mêmes). De plus, ils sont les seuls réseaux de racines indécomposables [Con].

Remarque 2.2.57. À chaque réseau de racines on peut associer son diagramme de Dynkin, mais le contraire est faux: on ne peut pas toujours associer un réseau à un diagramme quelconque. Par exemple, On considère le diagramme:



Alors la matrice associée est:

$$M = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$$

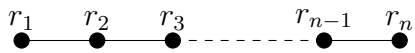
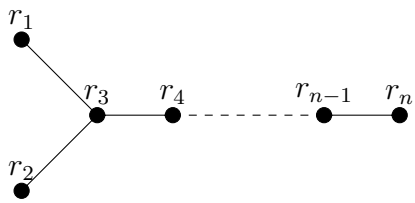
L	Diagramme de Dynkin	Gram(L)	det(L)
A_n		$\begin{pmatrix} 2 & -1 & & & \\ -1 & 2 & \ddots & & \\ & \ddots & \ddots & -1 & \\ & & -1 & 2 & \end{pmatrix}$	$n+1$
D_n		$\begin{pmatrix} 2 & 0 & & & & \\ 0 & 2 & -1 & & & \\ & -1 & 2 & \ddots & & \\ & & \ddots & 2 & -1 & \\ & & & -1 & 2 & \end{pmatrix}$	4

TABLE 2.2.1 – Diagrammes de A_n et D_n

qui n'est pas de rang maximal et donc ne donne aucun réseau.

2.3 Groupe discriminant

2.3.1 Réseau dual

Pour un réseau L, on note $L^* := \mathrm{Hom}(L, \mathbb{Z})$ son dual, alors L^* est un $\mathbb{Z}$-module libre de même rang que L. De plus on a un morphisme canonique donné par la forme bilinéaire sur L:

$$\begin{array}{rcl} \Phi : L & \hookrightarrow & L^* \\ v & \mapsto & \langle v, \bullet \rangle \end{array}$$

D'ailleurs Φ est injective car la forme bilinéaire est non-dégénérée. Donc, si on tensorise par $\mathbb{Q}$, on obtient un isomorphisme, car les deux espaces ont la même dimension:

$$\Phi \otimes \mathbb{Q} : L \otimes \mathbb{Q} \xrightarrow{\simeq} L^* \otimes \mathbb{Q}$$

Et donc si on prend l'inverse on obtient un plongement $L^* \hookrightarrow L \otimes \mathbb{Q}$, qu'on peut définir, en étendant le produit scalaire sur $L \otimes \mathbb{Q}$ comme:

$$L^* = \{w \in L \otimes \mathbb{Q} |\, \langle w, v \rangle \in \mathbb{Z} \text{ pour tout } v \in L\} \subset L \otimes \mathbb{Q} \tag{2.3.1}$$

On appellera L^*, avec la forme bilinéaire héritée, le *réseau dual de* L.

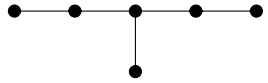
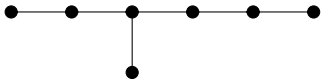
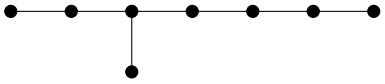
L	Diagramme de Dynkin	Gram(L)	det
E_6		$\begin{pmatrix} 2 & -1 & & & & \\ & 2 & -1 & & & \\ & -1 & 2 & -1 & & -1 \\ & & -1 & 2 & -1 & \\ & & & -1 & 2 & \\ & & -1 & & & 2 \end{pmatrix}$	3
E_7		$\begin{pmatrix} 2 & -1 & & & & & \\ -1 & 2 & -1 & & & & \\ & -1 & 2 & -1 & & & -1 \\ & & -1 & 2 & -1 & & \\ & & & -1 & 2 & -1 & \\ & & & & -1 & 2 & \\ & & -1 & & & & 2 \end{pmatrix}$	2
E_8		$\begin{pmatrix} 2 & -1 & & & & & & \\ -1 & 2 & -1 & & & & & \\ & -1 & 2 & -1 & & & & -1 \\ & & -1 & 2 & -1 & & & \\ & & & -1 & 2 & -1 & & \\ & & & & -1 & 2 & -1 & \\ & & & & & -1 & 2 & \\ & & -1 & & & & & 2 \end{pmatrix}$	1

TABLE 2.2.2 – Diagrammes de E_6, E_7, E_8

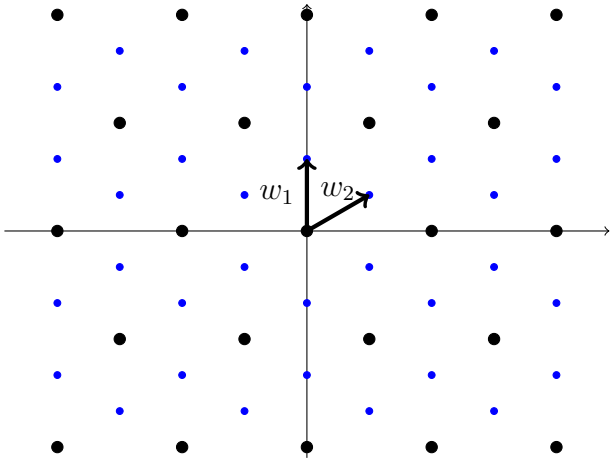


FIGURE 2.3.1 – Réseau dual de A_2

Exemple 2.3.1. Soit $L = A_2$, alors on rappelle que la matrice de Gram pour une base (v_1, v_2) est:

$$M = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

Donc $L^* = \{(a,b) \in L | \langle (a,b), v \rangle \in \mathbb{Z} \text{ pour tout } v \in L\}$, c'est-à-dire:

$$(a,b) \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \lambda(2a-b) + \mu(2b-a) \in \mathbb{Z} \text{ pour tout } \lambda, \mu \in \mathbb{Z}$$

Donc cela est équivalent à chercher les couples a, b qui satisfont

$$\begin{cases} 2a - b \in \mathbb{Z} \\ 2b - a \in \mathbb{Z} \end{cases} \tag{2.3.2}$$

En sommant on obtient que $3a \in \mathbb{Z}$ et $3b \in \mathbb{Z}$, donc $a = \frac{p}{3}$,$b = \frac{q}{3}$ avec $p, q \in \mathbb{Z}$. Le système 2.3.2 devient alors:

$$p + q \equiv 0 \pmod 3$$

Donc $L^* = \text{span}_{\mathbb{Z}}(w_1, w_2)$ avec $w_1 = \frac{2}{3}v_1 + \frac{1}{3}v_2$ et $w_2 = \frac{1}{3}v_1 + \frac{2}{3}v_2$ comme on a représente dans la Figure 2.3.1. En développant les calculs on obtient que la matrice d'intersection associée à L^* est:

$$M' = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

Remarque 2.3.2. Comme on vient de voir dans l'exemple précédent, la matrice d'intersection du réseau dual n'est pas toujours à valeurs entières. Donc en général, *le réseau dual n'est pas un réseau* selon la définition qu'on a donnée. On précise que certains auteurs appelle «réseau» un $\mathbb{Z}$-module libre de type fini avec une forme bilinéaire dans $\mathbb{Q}$, et «réseau entier» quand la forme bilinéaire prend ses valeurs dans $\mathbb{Z}$.

On a aussi une formulation «duale» de (2.3.1) qui décrit le plongement $L \hookrightarrow L^*$:

Lemme 2.3.3. *Soit L un réseau, L^* son dual, alors:*

$$L = \{w \in L^* \otimes \mathbb{Q} | \, \langle w, v\rangle \in \mathbb{Z} \text{ pour tout } v \in L^*\} \subseteq L^*$$

Démonstration. Soit $w \in L^* \otimes \mathbb{Q}$ tel que $\langle w, v\rangle \in \mathbb{Z}$ pour tout $v \in L^*$, en particulier par (2.3.1) on a $w \in L^*$. Soient donc $\lambda, \mu \in \mathbb{Z}$ tels que $\lambda w = \mu u$ avec $u \in L$ vecteur primitif, p.g.c.d.$(\lambda, \mu) = 1$, alors comme u est primitif et $L^* \simeq \mathrm{Hom}(L, \mathbb{Z})$, il existe $w' \in L^*$ tel que $\langle w', u\rangle = 1$ et donc $\langle w', w\rangle = \frac{\mu}{\lambda} \in \mathbb{Z}$, alors $|\lambda| = 1$ et $w = \mu u \in L$. □

Dans l'Exemple 2.3.1 on a déterminé, de façon indirecte, une base de L^* qui exprime le plongement $L \hookrightarrow L^*$. En réalité le calcul est bien plus simple. Soit donc L un réseau et $M = \mathrm{Gram}(L)$ pour une base $B = (v_1, \ldots, v_n)$. On rappelle que le produit scalaire définit l'application $\Phi : L \to L^*$, donc si on prend comme base de L^* la base duale $B^* = (v_1^*, \ldots, v_n^*)$ on aura $\mathrm{mat}_{B,B^*}(\Phi) = M$, qui naturellement est aussi la matrice de $\Phi \otimes \mathbb{Q}$. Par conséquent:

$$\mathrm{mat}_{B^*,B}((\Phi \otimes \mathbb{Q})^{-1}) = M^{-1}$$

et vu que $(\Phi \otimes \mathbb{Q})^{-1}$ définit le plongement $L^* \hookrightarrow L \otimes \mathbb{Q}$ on a que les colonnes de M^{-1} donnent une base de L^*.

Donc la matrice d'intersection de L^* est de la forme $(M^{-1})^t M M^{-1} = (M^{-1})^t = M^{-1}$ car M est symétrique, ce qui nous donne que L^* est un réseau si et seulement si $\det(M) = \pm 1$, et dans ce cas $L \simeq L^*$.

On remarque qu'en appliquant la forme normale de Smith au morphisme $\Phi : L \to L^*$ on obtient:

Lemme 2.3.4. *Soit L un réseau, alors il existe une base $(v_1, \ldots, v_n)$ de L et $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$ tels que $\left(\frac{v_1}{\lambda_1}, \ldots, \frac{v_n}{\lambda_n}\right)$ soit une base de $L^* \subset L \otimes \mathbb{Q}$.*

Définition 2.3.5. Pour un réseau L, on appelle *groupe discriminant* le groupe abélien $A_L := \frac{L^*}{L}$.

Exemple 2.3.6. Soit $L = \langle d\rangle$ avec $d \in \mathbb{Z}\backslash\{0\}$ et v un des deux générateurs de L. Alors $v^* = \frac{1}{d}v$ et donc:

$$A_L = \frac{\mathrm{span}(\frac{v}{d})}{\mathrm{span}(v)} = \frac{\mathbb{Z}}{|d|\mathbb{Z}}$$

Si on choisit une base $(u_1, \ldots, u_n)$ de L comme dans le Lemme 2.1.6, alors A_L est engendré par $\frac{u_1}{\lambda_1}, \ldots, \frac{u_n}{\lambda_n}$ et donc est de la forme:

$$A_L \simeq \frac{\mathbb{Z}}{\lambda_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{\lambda_n\mathbb{Z}}$$

De plus, comme $\mathrm{Gram}(M) = B_1 \mathrm{diag}(\lambda_1, \ldots, \lambda_n) B_2$ avec B_i inversible dans $\mathcal{M}_n(\mathbb{Z})$, on a $\det(M) = \pm \prod_{i=1}^n \lambda_i$ et en particulier:

Lemme 2.3.7. *A_L est un groupe fini de cardinalité $\#A_L = |\det(L)|$.*

Exemple 2.3.8. Soit L un réseau de signature (s^+, s^-), alors le signe de $\det(L)$ est donné par $(-1)^{s^-}$, donc $\det(L) = (-1)^{s^-}\#A_L$.

Remarque 2.3.9. On appelle *réseaux unimodulaires,* les réseaux avec déterminant unitaire. Ils sont isomorphes à leurs duaux et correspondent donc aux réseaux avec groupe discriminant trivial. On verra que cette classe de réseaux mérite une attention particulière.

Exemple 2.3.10. Soit L un réseau de rang n, $L(d)$ le réseau obtenu en multipliant par d la matrice de Gram de L. On choisit une base $(u_1, \dots, u_n)$ de L comme dans le Lemme 2.1.6, donc $A_L \simeq \frac{\mathbb{Z}}{\lambda_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{\lambda_n\mathbb{Z}}$ (avec éventuellement les $\lambda_i = 1$) et vu qu'on a $\mathrm{Gram}(L(d)) = d\mathrm{Gram}(L)$ on obtient:

$$A_{L(d)} \simeq \frac{\mathbb{Z}}{d\lambda_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d\lambda_n\mathbb{Z}}$$

Réciproquement, si pour un groupe abélien A on pose:

$$A_{,d} := \{x \in A | dx = 0\}$$

alors $\left(\frac{\mathbb{Z}}{d\lambda\mathbb{Z}}\right)_{,d} \simeq \frac{\lambda\mathbb{Z}}{d\lambda\mathbb{Z}}$ pour tout $\lambda \in \mathbb{Z}$, donc:

$$A_{L(d),d} \simeq \frac{\lambda_1\mathbb{Z}}{d\lambda_1\mathbb{Z}} \oplus \cdots \oplus \frac{\lambda_n\mathbb{Z}}{d\lambda_n\mathbb{Z}}$$

et enfin:

$$A_L \simeq \frac{\left(\frac{\mathbb{Z}}{d\lambda_1\mathbb{Z}}\right)}{\left(\frac{\lambda_1\mathbb{Z}}{d\lambda_1\mathbb{Z}}\right)} \oplus \cdots \oplus \frac{\left(\frac{\mathbb{Z}}{d\lambda_n\mathbb{Z}}\right)}{\left(\frac{\lambda_n\mathbb{Z}}{d\lambda_n\mathbb{Z}}\right)} \simeq \frac{A_{L(d)}}{A_{L(d),d}}$$

Définition 2.3.11. On note $l(A_L)$ la *longueur* de A_L, c'est-à-dire le nombre minimal de générateurs du groupe A_L.

Comme A_L est engendré par une base de L^* on a $l(A_L) \leq \mathrm{rang}(L)$.

Exemple 2.3.12. Soit A_n le réseau de racines qu'on a défini dans l'Exemple 2.2.53, comme $\det(A_n) = n+1$ on a que $\#A_{A_n} = n+1$. Par contre si $n+1$ est divisible par un carré, la cardinalité ne suffit pas à définir de façon unique le groupe. On rappelle donc que A_n est donné par les points de $\mathbb{Z}^{n+1}$ avec somme des coordonnées nulle, et on considère le vecteur $u = \frac{1}{n+1}(1, \dots, 1, -n)$. Comme la somme des coordonnées de u est nulle on a $u \in A_n \otimes \mathbb{Q}$, et pour tout $v \in A_n$ on a $v = (a_0, \dots, a_{n-1}, -a_0 - \cdots - a_{n-1})$, donc le produit scalaire nous donne:

$$\langle v, u\rangle = \frac{1}{n+1}\left(a_0 + \cdots + a_{n-1} + n(a_0 + \cdots + a_{n-1})\right) = a_0 + \cdots + a_{n-1} \in \mathbb{Z}$$

Donc $u \in A_n^*$, et son image dans le quotient $\overline{u} \in A_{A_n}$ a clairement ordre $n+1$, donc $\frac{\mathbb{Z}}{(n+1)\mathbb{Z}} \hookrightarrow A_{A_n}$, mais vu qu'ils ont la même cardinalité on a l'isomorphisme:

$$A_{A_n} \simeq \frac{\mathbb{Z}}{(n+1)\mathbb{Z}}$$

Exemple 2.3.13. Soit D_n le réseau échiquier de l'Exemple 2.2.54 et on pose $u_1 = (\frac{1}{2}, \ldots, \frac{1}{2})$ et $u_2 = (1, 0, \ldots, 0)$, $u_i \in D_n \otimes \mathbb{Q}$. Pour tout $v = (a_1, \ldots, a_n) \in D_n$, alors $\langle u_2, v\rangle = a_1 \in \mathbb{Z}$ et $\langle u_1, v\rangle = \frac{1}{2}\sum_{i=1}^n a_i \in \mathbb{Z}$ car $\sum_{i=1}^n a_i \in 2\mathbb{Z}$, donc $u_1, u_2 \in D_n^*$.

Si n est impair, on a que u_1 a ordre 4, mais $\det(D_n) = 4$ et donc $\overline{u}_1$ engendre $A_{D_n} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$.

Si n est pair, alors $\overline{u}_1$ et $\overline{u}_2$ ont ordre 2 dans A_{D_n} et $u_1 - u_2 \not\equiv 0 \pmod{D_n}$ donc sont deux générateurs de $A_{D_n} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Lemme 2.3.14. *Soit L un réseau de rang r, $d \in \mathbb{Z}\backslash\{0\}$ tel que $\left(\frac{\mathbb{Z}}{d\mathbb{Z}}\right)^r \hookrightarrow A_L$, alors il existe un réseau L' tel que $L = L'(d)$.*

Démonstration. On choisit une base de L et L' telle que la matrice de $\Phi : L \to L^*$ soit $\mathrm{mat}(\Phi) = \mathrm{diag}(\lambda_1, \ldots, \lambda_r)$, alors $\left(\frac{\mathbb{Z}}{d\mathbb{Z}}\right)^r \hookrightarrow A_L$ implique que $d|\lambda_i$ pour $1 \leq i \leq r$, donc $\mathrm{Im}(\Phi) \subseteq dL^*$. Mais $\Phi(x) = \langle x, \cdot\rangle$, donc pour tout $y \in L$ on a $\langle x, y\rangle \in d\mathbb{Z}$, donc la matrice de Gram de L est divisible par d, donc $L = L'(d)$ avec $\mathrm{Gram}(L') = \mathrm{Gram}(L)/d$. □

2.3.2 Forme discriminante

Soit L un réseau, on a déjà montré que sur L^* on a une forme bilinéaire à valeurs dans $\mathbb{Q}$: on cherche alors à la transporter sur le quotient $A_L = \frac{L^*}{L}$.

Si $x_1, x_2, y_1, y_2 \in L^*$ tels que $x_1 - x_2, y_1 - y_2 \in L$ alors $\overline{x}_1, \overline{x}_2$ (et respectivement $\overline{y}_1, \overline{y}_2$) représentent les mêmes éléments de A_L, mais en général $\langle x_1, y_1\rangle \neq \langle x_2, y_2\rangle$, ce qui nous empêche d'obtenir une forme à valeurs dans $\mathbb{Q}$.

Il faut donc changer le co-domaine de la forme bilinéaire, on remarque que:

$$\begin{aligned}\langle x_1, y_1\rangle - \langle x_2, y_2\rangle &= \langle x_1, y_1\rangle - \langle x_1, y_2\rangle + \langle x_1, y_2\rangle - \langle x_2, y_2\rangle \\ &= < \underbrace{x_1}_{\in L^*}, \underbrace{y_1 - y_2}_{\in L} > + < \underbrace{x_1 - x_2}_{\in L}, \underbrace{y_2}_{\in L^*} > \in \mathbb{Z}\end{aligned}$$

Donc le produit scalaire est bien défini sur A_L si on considère les valeurs modulo $\mathbb{Z}$, c'est-à-dire:

Lemme 2.3.15. *Soit L un réseau, alors A_L hérite d'une forme bilinéaire discriminante de la forme:*

$$\begin{aligned} b_L : A_L \times A_L &\to \frac{\mathbb{Q}}{\mathbb{Z}} \\ (\overline{x}, \overline{y}) &\mapsto \overline{\langle x, y\rangle}\end{aligned}$$

On considère maintenant la forme quadratique sur L^*, $L^* \to \mathbb{Q}$, $x \mapsto x^2$. Si L est un réseau impair, on a que sur A_L elle est toujours définie modulo

$\mathbb{Z}$, donc $q_L : A_L \to \mathbb{Q}/\mathbb{Z}, \overline{x} \mapsto \overline{x^2}$. Par contre, si L est un réseau pair, on peut en dire plus, car si $x_1, x_2 \in L^*$ sont tels que $x_1 - x_2 \in L$, alors:

$$\begin{aligned} q_L(x_1) - q(x_2) &= \langle x_1, x_1\rangle - \langle x_2, x_2\rangle \\ &= \langle x_1, x_1\rangle - \langle x_1, x_2\rangle + \langle x_1, x_2\rangle - \langle x_2, x_2\rangle \\ &= \langle x_1, x_1 - x_2\rangle + \langle x_1 - x_2, x_2\rangle \\ &= \langle x_1 + x_2, x_1 - x_2\rangle \\ &= \underbrace{\langle x_1 - x_2, x_1 - x_2\rangle}_{2\mathbb{Z}} + 2\underbrace{\langle x_2, x_1 - x_2\rangle}_{\mathbb{Z}} \in 2\mathbb{Z} \end{aligned}$$

On a donc gagné quelque chose, vu que q_L est défini modulo $2\mathbb{Z}$!

Lemme 2.3.16. *Soit L un réseau pair, alors A_L hérite d'une forme quadratique discriminante:*

$$\begin{aligned} q_L : A_L &\to \frac{\mathbb{Q}}{2\mathbb{Z}} \\ \overline{x} &\mapsto \overline{x^2} \end{aligned}$$

Exemple 2.3.17. Donc si L est un réseau pair, sur A_L on peut définir la forme bilinéaire b_L et la forme quadratique q_L. En particulier $q_L(x) \equiv b_L(x, x) \pmod{\mathbb{Z}}$. Si on part de la forme quadratique q_L, on peut toujours remonter à la forme bilinéaire, en considérant:

$$b_L(x, y) = \frac{q_L(x + y) - q_L(x) - q_L(y)}{2} \pmod{\mathbb{Z}}$$

par contre l'inverse n'est pas toujours possible car on peut avoir des formes quadratiques non équivalentes associées à la même forme bilinéaire. Par exemple si $L_1 = \langle 2\rangle$, $L_2 = \langle -2\rangle$ alors $b_{L_1} = b_{L_2} \pmod{\mathbb{Z}}$, par contre $q_{L_1} \neq q_{L_2}$: en effet, si $A_{L_1} = \{0, v_1\}$, $A_{L_2} = \{0, v_2\}$ alors $q_{L_1}(0) = q_{L_2}(0) = 0$ alors que $\frac{1}{2} = q_{L_1}(v_1) \not\equiv \frac{3}{2} = q_{L_2}(v_2) \pmod{2\mathbb{Z}}$.

Les deux formes discriminantes (quadratique et bilinéaire) constituent un invariant très important, qui mérite donc une étude approfondie et on s'y attardera un peu avant de revenir aux réseaux.

Il est clair qu'on peut exprimer la forme discriminante bilinéaire avec sa matrice d'intersection. Plus précisément, on prend $B = (x_i)$ un système de générateurs indépendants de A_L, c'est-à-dire un ensemble qui satisfait:

- $A_L = \mathrm{span}(x_1, \ldots, x_n)$
- $A_L \simeq \mathrm{span}(x_1) \oplus \cdots \oplus \mathrm{span}(x_n)$

On appellera B une *base* de A_L avec abus de notation, car on utilisera ce terme aussi dans le cas des modules non libres, où par exemple la cardinalité de B n'est pas invariante. Par exemple si $A_L \simeq \mathbb{Z}/6\mathbb{Z}$ alors $(\overline{1})$ est une base du module, mais aussi $(\overline{2}, \overline{3})$ est une base de A_L, car elle engendre A_L et $A_L \simeq \langle\overline{2}\rangle \oplus \langle\overline{3}\rangle \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Alors la matrice $M_{b_L} = (a_{ij})$ avec $a_{ij} = b_L(x_i, x_j) \in \mathbb{Q}/\mathbb{Z}$ décrit complètement b_L, car si $x, y \in A_L$ alors on peut le décomposer selon la base B, $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$ et $y = \mu_1 x_1 + \cdots + \mu_n x_n$ et donc:

$$b_L(x, y) = (\lambda_1, \ldots, \lambda_n) M \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$$

Par contre, si on veut décrire la forme discriminante quadratique d'un réseau pair on a besoin des valeurs modulo $2\mathbb{Z}$.

Pour résoudre cela, on va considérer la matrice $M_{q_L} = (a_{ij})$ avec $a_{ij} = b_L(x_i, x_j) \in \mathbb{Q}/\mathbb{Z}$ si $i \neq j$ et $a_{ii} = q_L(x_i) \in \mathbb{Q}/2\mathbb{Z}$. On aura alors que pour tout $x = \lambda_1 x_1 + \cdots + \lambda_n x_n \in A_L$:

$$\begin{aligned} (\lambda_1, \ldots, \lambda_n) M \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} &= 2 \left(\sum_{1 \leq i < j \leq n} \lambda_i \lambda_j a_{ij} \right) + \sum_{1 \leq i < j \leq n} \lambda_i^2 a_{ii} \\ &\equiv q_L(x) \pmod{2\mathbb{Z}} \end{aligned}$$

Et pour réobtenir la matrice de la forme bilinéaire il suffit de prendre les valeurs sur la diagonale modulo $\mathbb{Z}$.

Exemple 2.3.18. Pour le réseau A_n on a montré que $w = \frac{1}{n+1}(1, \ldots, 1, -n)$ est un générateur de A_{A_n}. On a:

$$q_{A_n}(\overline{w}) = \overline{w^2} \equiv \frac{n}{n+1} \pmod{2\mathbb{Z}}$$

Donc la matrice d'intersection associée à la forme discriminante est:

$$q_{A_n} = \left(\frac{n}{n+1} \right)$$

Exemple 2.3.19. Soit $d \in \mathbb{Z} \backslash \{0\}$, $L = \langle d \rangle$, v le générateur de L associé à la matrice:

$$\text{Gram}(\langle d \rangle) = \begin{pmatrix} d \end{pmatrix}$$

Alors $w = v/d$ est une base de L^* et la projection de w dans le quotient engendre A_L, donc la matrice d'intersection de q_L est:

$$q_{\langle d \rangle} = \left(\frac{1}{d} \right)$$

Exemple 2.3.20. Soit $d \in \mathbb{Z} \backslash \{0\}$, $L = U(d)$, soient v_1, v_2 les générateurs de L associés à la matrice:

$$\text{Gram}(U(d)) = \begin{pmatrix} 0 & d \\ d & 0 \end{pmatrix}$$

Alors $w_1 = \frac{v_1}{d}$,$w_2 = \frac{v_2}{d}$ forment une base de L^* et leur projections forment aussi une base de A_L. La matrice d'intersection de q_L est donc:

$$q_{U(d)} = \begin{pmatrix} 0 & \frac{1}{d} \\ \frac{1}{d} & 0 \end{pmatrix}$$

Exemple 2.3.21. On a vu que si n est pair alors D_n^* est engendré par $w_1 = (\frac{1}{2}, \ldots, \frac{1}{2})$ et $w_2 = (1, 0, \ldots, 0)$. Si on choisit alors la base de A_{D_n} donnée par $\overline{w}_1$ et $\overline{w}_2$ on a:

$$q_{D_n} = \begin{pmatrix} \frac{n}{4} & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

On rappelle que les valeurs sur la diagonale sont calculées modulo $2\mathbb{Z}$ (c'est pour cela qu'on a noté 1 à la place de 0) et les autres valeurs de la matrice sont modulo $\mathbb{Z}$.

Si n est impair, alors D_n^* est engendré par w_1, et donc:

$$q_{D_n} = \left(\frac{n}{4}\right)$$

Exemple 2.3.22. Soient $L_1 = U(2)$, $L_2 = D_4$, $L_3 = D_8$ alors:

$$q_{L_1} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}, \quad q_{L_2} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}, \quad q_{L_3} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

Si x_1, x_2 forment la base de A_{L_1} associée à la matrice de q_{L_1} donnée, il suffit de considérer le changement de base $x_1' = x_1$, $x_2' = x_1 + x_2$ pour obtenir que $q_{L_1} \simeq q_{L_3}$. Par contre sur A_{L_1} on a trois éléments de carré 0, lorsqu'il n'y en a qu'un sur A_{L_2}, donc $q_{L_1} \not\simeq q_{L_2}$. On remarque sinon que les formes bilinéaires sont isomorphes, $b_{L_1} \simeq b_{L_2} \simeq b_{L_3}$, car les trois matrices coïncident modulo $\mathbb{Z}$.

Soit L un réseau, b_L sa forme discriminante et $d \in \mathbb{N}\backslash\{0\}$. Dans l'Exemple 2.3.10 on a vu que:

$$A_L \simeq \frac{A_{L(d)}}{A_{L(d),d}}$$

où on rappelle que $A_{L(d),d} = \{x \in A_{L(d)} | dx = 0\}$. Mais que peut-on dire sur la relation entre les formes discriminantes b_L et $b_{L(d)}$?

Lemme 2.3.23. *Soit L un réseau, $d \in \mathbb{Z}\backslash\{0\}$, alors:*

$$d \cdot b_{L(d)} \simeq b_L$$

où $d \cdot b_{L(d)}$ désigne la forme discriminante $b_{L(d)}$ quotientée par $A_{L(d),d}$ avec matrice d'intersection multipliée par d, en symboles:

$$\begin{array}{rccl} d \cdot b_{L(d)} : \dfrac{A_{L(d)}}{A_{L(d),d}} \times \dfrac{A_{L(d)}}{A_{L(d),d}} & \to & \mathbb{Q}/\mathbb{Z} \\ (\overline{x}, \overline{y}) & \mapsto & d \cdot b_{L(d)}(\overline{x}, \overline{y}) \end{array}$$

Démonstration. Soit f l'isomorphisme (de $\mathbb{Z}$-modules) $f : L^* \xrightarrow{\simeq} L(d)^*$, on obtient le diagramme:

$$\begin{array}{ccc} L & \xrightarrow[f_{|L}]{\simeq} & \frac{1}{d}L \\ \downarrow & & \downarrow \\ L^* & \xrightarrow[f]{\simeq} & L(d)^* \\ \downarrow & & \downarrow \\ A_L & \xrightarrow{\simeq} & \frac{A_{L(d)}}{A_{L,d}} \end{array}$$

donc si on passe au quotient f réalise l'isomorphisme entre A_L et $\frac{L(d)^*}{\frac{1}{d}L} = \frac{A_{L(d)}}{A_{L,d}}$. Soient $x, y \in L^*$, alors:

$$\begin{aligned} b_L(\overline{x}, \overline{y}) &\equiv \langle x, y \rangle_{L^*} \pmod{\mathbb{Z}} \\ &\equiv d \langle f(x), f(y) \rangle_{L(d)^*} \pmod{\mathbb{Z}} \\ &\equiv d b_{L(d)}(\overline{x}, \overline{y}) \pmod{\mathbb{Z}} \end{aligned}$$

□

2.3.3 Formes finies

Définition 2.3.24. On appelle une *forme finie bilinéaire symétrique* (dans la suite on écrira plus simplement *« f.f. bilinéaire »* en sous-entendant la symétrie), une forme symétrique bilinéaire de la forme:

$$b : A \times A \to \mathbb{Q}/\mathbb{Z}$$

avec A un groupe fini abélien.

De façon similaire on appelle une *forme finie quadratique,* (*f.f. quadratique*) une application:

$$q : A \to \mathbb{Q}/2\mathbb{Z}$$

avec A un groupe fini abélien et q telle que:

1 $q(nx) = n^2 q(x)$ pour tout $n \in \mathbb{Z}$ et $x \in A$;

2 si on définit

$$b(x, y) := \frac{q(x+y) - q(x) - q(y)}{2} \tag{2.3.3}$$

alors b est une forme finie bilinéaire symétrique modulo $\mathbb{Z}$.

On dira qu'une f.f. bilinéaire sur A est *dégénérée* s'il existe $x \in A \backslash \{0\}$ tel que pour tout $y \in A$ $b_A(x, y) \equiv 0 \pmod{\mathbb{Z}}$.

Une f.f. quadratique est *dégénérée* si la forme bilinéaire associée l'est. Dans le cas contraire on parlera de forme *non-dégénérée.*

Remarque 2.3.25. Une f.f. quadratique est considérée dégénérée même si elle prend des valeurs non nulles modulo $2\mathbb{Z}$. Par exemple si on pose $A = \{0, x\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $q_A(x) = 1 \pmod{2\mathbb{Z}}$ alors q_A est dégénérée.

Lemme 2.3.26. *Soit L un réseau, alors b_L est une f.f. bilinéaire non-dégénérée sur A_L.*

Démonstration. Soit $x \in L^*$ tel que $b(\overline{x}, \bullet)$ soit identiquement nulle sur A_L, alors pour tout $y \in L^*$ on a $\langle x, y\rangle \in \mathbb{Z}$. Donc $x \in L$ par le Lemme 2.3.3 et $\overline{x} \equiv 0 \pmod{L}$. □

Lemme 2.3.27. *Soit b une f.f. bilinéaire sur A, $x \in A$ élément d'ordre n, alors $\mathrm{Im}(b(x, \bullet)) \subseteq \{\frac{a}{n} \pmod{\mathbb{Z}} | a \in \mathbb{Z}\} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$. De plus, si b est non-dégénérée, on a l'égalité.*

Démonstration. Si $x \in A$ a ordre n, alors pour tout $y \in A$, on a:

$$nb(x, y) = b(nx, y) = b(0, y) = 0$$

donc $b(x, \bullet) : A \to \{\frac{a}{n} \pmod{\mathbb{Z}} | a \in \mathbb{Z}\} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$. On veut montrer la surjectivité quand b est non-dégénérée. On a que $\mathrm{Im}(b(x, \bullet))$ est un groupe cyclique, donc il existe $m \in \mathbb{Z}$ diviseur de n tel que $\mathrm{Im}(b(x, \bullet)) = \mathrm{span}(\frac{1}{m})$. En particulier $\mathrm{Im}(b(mx, \bullet)) = m\,\mathrm{Im}(b(x, \bullet)) = 0$, donc $b(mx, y) \equiv 0 \pmod{\mathbb{Z}}$ pour tout $y \in \mathbb{Z}$ ce qui implique $mx = 0$ car b est non-dégénérée. Donc $m = n$ et $b(x, \bullet)$ est surjective. □

Remarque 2.3.28. Soit A un groupe abélien fini et $\mathrm{Hom}(A, \frac{\mathbb{Q}}{\mathbb{Z}})$ le groupe des applications $\mathbb{Z}$-linéaires $\varphi : A \to \frac{\mathbb{Q}}{\mathbb{Z}}$, alors une f.f. bilinéaire b sur A induit un morphisme:

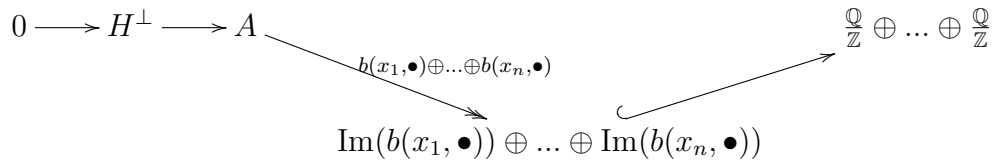
$$\begin{array}{rcl} b(\bullet, \bullet) : A & \to & \mathrm{Hom}(A, \dfrac{\mathbb{Q}}{\mathbb{Z}}) \\ x & \mapsto & b(x, \bullet) \end{array}$$

qui grâce au Lemme 2.3.27 est injectif dans le cas où b est non-dégénérée. Mais $\mathrm{Hom}(A, \frac{\mathbb{Q}}{\mathbb{Z}}) \simeq A$ comme groupes abéliens, donc si b est non-dégénérée on a un isomorphisme de groupes.

De la même façon que pour les réseaux, en utilisant une f.f. bilinéaire, on peut définir l'orthogonal d'un sous-groupe, qui est aussi un sous-groupe. De plus, contrairement au cas des réseaux, un sous-groupe avec une forme finie non-dégénérée détermine toujours une décomposition.

Lemme 2.3.29. *Soit b une f.f. bilinéaire sur A et soit $H \leq A$ un sous-groupe. Alors $\#H^\perp \geq \frac{\#A}{\#H}$ et on a l'égalité si b est non-dégénérée sur A.*

Démonstration. Soit $(x_1, \ldots, x_n)$ une base de H, on considère le diagramme suivant:



Mais par le Lemme 2.3.27 $\#\operatorname{Im}(b(x_i,\bullet)) \leq \operatorname{ord}(x_i)$ donc

$$\#H^\perp \geq \frac{\#A}{\operatorname{ord}(x_1)\cdot\ldots\cdot\operatorname{ord}(x_n)} = \frac{\#A}{\#H}$$

Si b est non-dégénérée, on a $\#\operatorname{Im}(b(x,\bullet)) = \operatorname{ord}(x)$ et donc on a l'égalité. □

En fait, on a même un isomorphisme de groupes:

Lemme 2.3.30. *Soit b une f.f. bilinéaire sur A non-dégénérée, $H \leq A$ un sous-groupe. Alors:*

$$H^\perp \simeq \frac{A}{H}$$

en tant que groupes abéliens.

Démonstration. Soit $\pi : A \to A/H$ le quotient par H, alors $\pi^* : \operatorname{Hom}(A/H, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})$ est injective avec:

$$\operatorname{Im}(\pi^*) = \left\{ \varphi \in \operatorname{Hom}(A, \frac{\mathbb{Q}}{\mathbb{Z}}) | \varphi_{|H} = 0 \right\}$$

On a aussi un morphisme de $H^\perp$ dans $\operatorname{Hom}(A, \frac{\mathbb{Q}}{\mathbb{Z}})$ donné par $b(\bullet,\bullet)$, dont l'image est contenue dans $\operatorname{Im}(\pi^*)$, donc la situation est la suivante:

$$\begin{array}{ccccc} \operatorname{Hom}(\frac{A}{H}, \frac{\mathbb{Q}}{\mathbb{Z}}) & \xrightarrow[\pi^*]{\simeq} & \operatorname{Im}(\pi^*) & \hookrightarrow & \operatorname{Hom}(A, \frac{\mathbb{Q}}{\mathbb{Z}}) \\ & & \uparrow{\scriptstyle b(\bullet,\bullet)} & & \\ & & H^\perp & & \end{array}$$

Par la Remarque 2.3.28, comme b est non-dégénérée alors $b(\bullet,\bullet)$ est injective, mais $\#H^\perp = \#(A/H) = \#\operatorname{Im}(\pi^*)$, donc $b(\bullet,\bullet)$ décrit un isomorphisme de groupes. □

Lemme 2.3.31. *Soit b une f.f. bilinéaire sur A non-dégénérée, $K, H \leq A$ deux sous-groupes tels que $K \leq H$. Alors:*

$$\frac{K^\perp}{H^\perp} \simeq \frac{H}{K}$$

en tant que groupes abéliens.

Démonstration. On considère la suite exacte:

$$0 \to \frac{H}{K} \to \frac{A}{K} \to \frac{A}{H} \to 0$$

et on applique $\operatorname{Hom}(\bullet, \mathbb{Q}/\mathbb{Z})$, on obtient alors:

$$0 \to \operatorname{Hom}(\frac{A}{H}, \frac{\mathbb{Q}}{\mathbb{Z}}) \to \operatorname{Hom}(\frac{A}{K}, \frac{\mathbb{Q}}{\mathbb{Z}}) \to \operatorname{Hom}(\frac{H}{K}, \frac{\mathbb{Q}}{\mathbb{Z}}) \to 0$$

Par le Lemme 2.3.30 on a les isomorphismes

$$\begin{aligned} b(\bullet,\bullet) : H^\perp &\xrightarrow{\simeq} \mathrm{Hom}(\frac{A}{H}, \frac{\mathbb{Q}}{\mathbb{Z}}) \\ b(\bullet,\bullet) : K^\perp &\xrightarrow{\simeq} \mathrm{Hom}(\frac{A}{K}, \frac{\mathbb{Q}}{\mathbb{Z}}) \end{aligned}$$

On obtient alors:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}(\frac{A}{H}, \frac{\mathbb{Q}}{\mathbb{Z}}) & \longrightarrow & \mathrm{Hom}(\frac{A}{K}, \frac{\mathbb{Q}}{\mathbb{Z}}) & \longrightarrow & \mathrm{Hom}(\frac{H}{K}, \frac{\mathbb{Q}}{\mathbb{Z}}) & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle b(\bullet,\bullet)} & & \uparrow{\scriptstyle b(\bullet,\bullet)} & & & & \\ 0 & \longrightarrow & H^\perp & \longrightarrow & K^\perp & \longrightarrow & \frac{K^\perp}{H^\perp} & \longrightarrow & 0 \end{array}$$

et donc il existe un isomorphisme de groupes abéliens $\frac{K^\perp}{H^\perp} \xrightarrow{\simeq} \mathrm{Hom}(\frac{H}{K}, \frac{\mathbb{Q}}{\mathbb{Z}})$, mais $\frac{H}{K} \simeq \mathrm{Hom}(\frac{H}{K}, \frac{\mathbb{Q}}{\mathbb{Z}})$ et on a conclu. □

Lemme 2.3.32. *Soit b une f.f. bilinéaire sur A non-dégénérée, $H \leq A$ un sous-groupe. Alors $\left(H^\perp\right)^\perp = H$.*

Démonstration. Par définition $H \subseteq \left(H^\perp\right)^\perp$ et comme b est non-dégénérée par le Lemme 2.3.29

$$\#\left(H^\perp\right)^\perp = \frac{\#A}{\#H^\perp} = \frac{\#A}{\#A/\#H} = \#H$$

□

Lemme 2.3.33. *Soit b une f.f. bilinéaire sur A non-dégénérée, $H_1, H_2 \leq A$ deux sous-groupes. Alors:*

$$(H_1 \cap H_2)^\perp = H_1^\perp + H_2^\perp$$

Démonstration. On a l'égalité triviale $(H_1 + H_2)^\perp = H_1^\perp \cap H_2^\perp$, on remplace alors H_i par $H_i^\perp$ et grâce au Lemme 2.3.32 on a:

$$\left(H_1^\perp + H_2^\perp\right)^\perp \;=\; H_1 \cap H_2$$

On prend à nouveau l'orthogonal pour obtenir l'équivalence cherchée. □

Lemme 2.3.34. *Soit b une f.f. bilinéaire sur A non-dégénérée, $H \leq A$ un sous-groupe.*

Alors H est primitif si et seulement si $H^\perp \leq A$ est primitif aussi.

Démonstration. On suppose que H est primitif, par la preuve du Lemme 2.3.30 on a que le plongement de $H^\perp \hookrightarrow A$ est donné par $\pi^* : \mathrm{Hom}(A/H, \mathbb{Q}/\mathbb{Z}) \hookrightarrow \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, il s'agit donc de démontrer que ce dernier est primitif.

Mais si $H \hookrightarrow A$ est primitif alors $A \simeq H \oplus \frac{A}{H}$ comme groupes abéliens, donc:

$$\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(A/H, \mathbb{Q}/\mathbb{Z}) \oplus \mathrm{Hom}(H, \mathbb{Q}/\mathbb{Z})$$

et $H^\perp$ et primitif aussi. L'implication contraire découle du fait que si $H^\perp$ est primitif, alors $H^{\perp\perp} = H$ est primitif. □

Proposition 2.3.35. *Soit b une f.f. bilinéaire sur un groupe abélien fini A et soit $H \leq A$ un sous-groupe. Si la restriction $b_{|H}$ est non-dégénérée alors:*

$$b = b_{|H} \oplus b_{|H^\perp}$$

Démonstration. Comme $b_{|H}$ est non-dégénérée, on a que $H \cap H^\perp = \{0\}$, donc $H \oplus H^\perp \hookrightarrow A$. Par le Lemme 2.3.29 les deux ensembles doivent avoir la même cardinalité, donc on a l'isomorphisme et $A = H \oplus H^\perp$. □

Corollaire 2.3.36. *Soit b une f.f. bilinéaire sur A et H un sous-groupe non primitif de A, alors $b_{|H}$ est dégénérée.*

Remarque 2.3.37. Soit q une f.f. quadratique sur A et b la f.f. bilinéaire associée à q, alors les conditions d'orthogonalité et dégénérescence coïncident totalement: donc les résultats précédents s'appliquent aussi au cas d'une forme quadratique.

Soit A un groupe abélien fini et p un nombre premier. On notera A_p la p-part de A, c'est-à-dire le plus grand sous-groupe d'ordre p^n contenu dans A. Comme il s'agit forcement d'un groupe primitif, on obtient une décomposition de la forme $A \simeq A_{p_1} \oplus \cdots \oplus A_{p_k}$ avec $p_1, \ldots, p_k$ premiers différents, et si b est une f.f. bilinéaire sur A, de plus il s'agit d'une décomposition orthogonale, car si $x_1, y_1 \in A$ avec $\mathrm{ord}(x_1) = k_1$, $\mathrm{ord}(x_2) = k_2$ alors:

$$k_1 b(x_1, x_2) \equiv k_2 b(x_1, x_2) \equiv 0 \pmod{\mathbb{Z}}$$

Si k_1, k_2 sont premiers entre eux, il existe $\lambda, \mu \in \mathbb{Z}$ tels que $\lambda k_1 + \mu k_2 = 1$, donc:

$$b(x_1, x_2) \equiv \lambda k_1 b(x_1, x_2) + \mu k_2 b(x_1, x_2) \equiv 0 \pmod{\mathbb{Z}}$$

Comme $k_i = p_i^{n_i}$ on a que les k_i sont premiers entre eux, donc pour $i \neq j$ on a $A_{p_i} \perp A_{p_j}$. On a montré:

Proposition 2.3.38. *Soit b [respectivement q] une f.f. bilinéaire [quadratique] finie sur A. Alors b [q] se décompose sous la forme:*

$$b = \bigoplus_{p \text{ premier}} b_p \qquad \left[q = \bigoplus_{p \text{ premier}} q_p \right]$$

où b_p [q_p] est la restriction de b [q] sur A_p. De plus si b [q] est non-dégénérée, alors elle se décompose comme somme de formes finies non-dégénérées.

Notre travail se réduit donc à étudier uniquement les formes finies sur les p-groupes. On a déjà remarqué que si $k = \mathrm{ord}(x)$, alors $b(x, y) = \frac{a}{k}$ avec $a \in \mathbb{Z}$, donc si A est un p-groupe, on a que b (et q) prennent leurs valeurs sur $\mathbb{Q}^{(p)}$, avec:

$$\mathbb{Q}^{(p)} := \left\{ \frac{a}{p^n},\ a \in \mathbb{Z},\ n \in \mathbb{N} \right\} \subset \mathbb{Q}$$

Remarque 2.3.39. Attention à ne pas confondre l'anneau $\mathbb{Q}^{(p)}$ avec les corps p-adiques $\mathbb{Q}_p$, les entiers p-adiques $\mathbb{Z}_p$ ou la localisation $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} | a \in \mathbb{Z},\ p \nmid b\}$.

Exemple 2.3.40. Soit $n = p_1^{\alpha_1} \cdot \cdots \cdot p_h^{\alpha_h}$, alors $A_{A_{n-1}} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$ est engendré par $\overline{w}$ avec $q(\overline{w}) = \frac{n-1}{n}$. Si on pose $\overline{w}_i = \frac{n}{p_i^{\alpha_i}}\overline{w}$, on a que $(w_1, \ldots, w_h)$ est une base de $A_{A_{n-1}}$, avec $\mathrm{span}(\overline{w}_i) \simeq \frac{\mathbb{Z}}{p^{\alpha_i}\mathbb{Z}}$ et $q(\overline{w}_i) = \frac{n(n-1)}{p_i^{2a_i}}$.

Il existe une réduction supplémentaire possible: soit $p \neq 2$, A_p un p-groupe et q une f.f. quadratique sur A_p, alors on peut montrer que q prend ses valeurs uniquement sur $2\mathbb{Q}^{(p)}/2\mathbb{Z}$ (q ne prend donc jamais des valeurs impair à dénominateur).

En effet soit $x \in A_p$, $\mathrm{ord}(x) = p^n$, $q(x) \equiv a \pmod{2\mathbb{Z}}$, alors:

$$q(p^n x) \equiv p^{2n} a \equiv 0 \pmod{2\mathbb{Z}}$$

car $p^n x = 0$. On a alors $p^{2n} a \in 2\mathbb{Z}$ et donc $a \in 2\mathbb{Q}^{(p)}$.

Donc, si q est une f.f. quadratique sur A_p et b sa forme bilinéaire associée, sachant que q prend ses valeurs sur $2\mathbb{Q}^{(p)}/2\mathbb{Z}$ on a une seule possibilité pour construire q à partir de b, c'est-à-dire:

$$q(x) = \begin{cases} b(x,x) & \text{si } b(x,x) \in 2\mathbb{Q}^{(p)} \\ b(x,x) + 1 & \text{sinon} \end{cases}$$

Donc pour p impair q est complètement déterminé par b.

On peut réécrire la relation ci-dessus de façon différente, soit 2^{-1} l'inverse de 2 dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, p^n la cardinalité de A_p, comme $2^{-1} \equiv \frac{p^n+1}{2} \pmod{p^n}$ alors:

$$q(x) = m_2\left(2^{-1} b(x,x)\right) \tag{2.3.4}$$

où m_2 est l'isomorphisme $m_2 : \frac{\mathbb{Q}^{(p)}}{\mathbb{Z}} \to \frac{2\mathbb{Q}^{(p)}}{2\mathbb{Z}}$ donné par la multiplication par 2.

D'ailleurs (2.3.4) implique aussi qu'à tout f.f. bilinéaire b on peut associer une f.f. quadratique q telle que b soit la forme bilinéaire associée à q par (2.3.3). On a donc une correspondance parfaite entre formes bilinéaires finies et formes quadratiques finies pour le cas impair.

Exemple 2.3.41. Soient $L_1 = A_2$, $L_2 = A_2(-1)$, alors les formes discriminantes sont données par les matrices d'intersections $b_{L_1} \simeq (\frac{2}{3})$ et $b_{L_2} \simeq (\frac{1}{3})$. À partir des b_{L_i}, on peut retrouver les q_{L_i}: soit $x \in A_{L_i}$ un générateur, alors grâce à (2.3.4) on trouve bien:

$$\begin{aligned} q_{L_1}(x) &= 2 \cdot (2 \cdot \frac{2}{3}) = \frac{8}{3} \equiv \frac{2}{3} \pmod{2\mathbb{Z}} \\ q_{L_2}(x) &= 2 \cdot (2 \cdot \frac{1}{3}) = \frac{4}{3} \pmod{2\mathbb{Z}} \end{aligned}$$

2.3.4 Discriminant

On rappelle d'abord les faits suivants (ils peuvent être montrés comme une conséquence du Lemme de Hensel [Ei]):

Lemme 2.3.42. *Soit p premier impair, $x, y \in \frac{\mathbb{Z}}{p\mathbb{Z}}\backslash\{0\}$, alors xy est un carré dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (i.e. $\exists\, r \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ tel que $r^2 = xy$) si et seulement si l'une des conditions suivante est vérifiée:*

- *x,y sont deux carrés ;*
- *ni x, ni y est un carré ;*

Lemme 2.3.43. *Soit p premier impair, $x \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ inversible, alors x est un carré dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ si et seulement si $\overline{x}$ est un carré dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$.*

À partir de ces deux résultats on prouve facilement:

Corollaire 2.3.44. *Soit p premier impair, $x, y \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ inversibles, alors:*

- *xy est un carré dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ si et seulement si x, y sont deux carrés ou aucun des deux ne l'est ;*
- *x^{-1} est un carré si et seulement si x est un carré ;*
- *$\exists\, r \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ inversible tel que $x = r^2 y$ si et seulement si x, y sont deux carrés ou aucun des deux ne l'est.*

Maintenant soit b une f.f. bilinéaire sur un p-groupe A_p, p impair, $B = (x_i)$ une base et $M = (a_{ij})$ la matrice d'intersection associée à B. Si $\mathrm{ord}(x_i) = p^n$, par le Lemme 2.3.27 on a $a_{ij} \in \frac{p^{-n}\mathbb{Z}}{\mathbb{Z}}$, $a_{ij} = c_{ij}/p^{n_{ij}}$ avec $c_{ij} \in \mathbb{Z}$ pour tout j, donc en développant:

$$\begin{aligned}
\det(M) &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \\
&= \sum_{\sigma \in S_n} \left(\mathrm{sgn}(\sigma) \prod_{i=1}^{n} \frac{c_{i\sigma(i)}}{p^{n_i}} + \mathbb{Z} \right) \\
&= \frac{c}{p^N} + \frac{1}{p^{N-m}}\mathbb{Z}
\end{aligned}$$

avec $p^N = \#A_p$, $c \in \mathbb{Z}$ et $p^m = \min_i(\mathrm{ord}(x_i))$. On a aussi que $p \nmid c$ si et seulement si b est non-dégénérée [MM]. . Par contre le déterminant n'est pas un invariant par changement de base: soient B, B' deux bases de A_p où b a pour matrice d'intersection respectivement M et M', si C est la matrice qui exprime le changement de base de B à B' alors:

$$M' = C^t M C$$

et en particulier $\det(M') = \det(M)\det(C)^2$ avec $\det(C)$ inversible (modulo p). Donc on a une relation d'équivalence sur les déterminants des formes non-dégénérées: soient $\frac{a}{p^N}, \frac{a'}{p^N} \in \frac{p^{-N}\mathbb{Z}}{p^{-N+m}\mathbb{Z}}$ avec $p \nmid a, p \nmid a'$ alors $\frac{a}{p^N} \sim \frac{a'}{p^N}$ s'il existe $m \in \mathbb{Z}$ tel que $a \equiv m^2 a' \pmod{p^N}$.

Le déterminant modulo cette relation d'équivalence constitue le discriminant de b:

Définition 2.3.45. Soit b une forme bilinéaire non-dégénérée sur un p-groupe A_p avec torsion maximale p^n et M la matrice d'intersection de b pour une certaine base, alors on appelle *discriminant de* b la classe de $\det(M)$ modulo la relation d'équivalence $\sim$ donnée par le produit par un carré de $\mathbb{Z}$ non divisible par p:

$$\mathrm{disc}(b) := {}^{\det(M)}/_{\sim}$$

Si p est impair, pour N donné, on a deux classes d'isomorphisme modulo les carrés inversibles qui sont données par le caractère quadratique modulo p, donc on peut choisir comme représentants p^{-N} et up^{-N} avec u le plus petit non carré modulo p.

Par contre, dans le cas pair, la situation est bien plus complexe, car il faut distinguer plusieurs cas, résumés dans le Tableau 2.3.1. Ces résultats sont partiellement montrés dans [MM], mais on donnera une preuve pour les résultats dont il n'a pas été possible de trouver une référence.

Une distinction sera faite par rapport à l'invariant δ_b de la forme finie:

Définition 2.3.46. Soit A_2 un 2-groupe, b une f.f. bilinéaire [q une f.f. quadratique] sur A_2, on notera alors:

$$\delta_b = \begin{cases} 0 & \text{si } b(x,x) \neq \frac{1}{2} \text{pour tout } x \in A_2 \text{ tel que } 2x = 0 \\ 1 & \text{sinon} \end{cases}$$

Aussi dans la suite pour une matrice M, on notera M_i^j la matrice privée de la ligne i et la colonne j, avec plusieurs indices si on veut enlever plusieurs lignes et colonnes. En outre on indiquera avec $E_{i,j}$ la matrice avec toutes les entrées égales à zéro, sauf un 1 à la place (i,j).

Lemme 2.3.47. *Soit A_2 un 2-groupe de cardinalité 2^N, b une f.f. non-dégénérée sur A_2 avec $\delta_b = 0$, $(x_1, \ldots, x_n)$ une base de A_2 et M la matrice d'intersection associée. Alors pour tout $1 \leq i \leq n$ on a $\det(M_i^i) \in 2^{-N+2}\mathbb{Z}$.*

Démonstration. Si $\mathrm{ord}(x_i) \geq 2^2$ alors M_i^i est la matrice d'une f.f. bilinéaire sur un groupe de cardinalité $\leq 2^{N-2}$ donc on a le résultat.

Sinon soit $A_2 \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^a \oplus A_2'$ avec $A_{2'}$ sans 2-torsion, alors si $\mathrm{ord}(x_i) = 2$, par la Proposition 2.3.61 on a que M_i^i est la matrice d'une forme bilinéaire $b \simeq b_{A_{2^1}} \oplus b_{A_{2^{\geq 2}}}$ avec $A_{2^1} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{a-1}$ et $A_{2^{\geq 2}}$ sans 2-torsion. Par la Proposition 2.3.69 comme b est non-dégénérée avec $\delta_b = 0$ alors a est pair, donc $a-1$ est impair est vu que $\delta_{b_{A_{2^1}}} = 0$ alors $b_{A_{2^1}}$ est dégénérée. Donc $\det(M_i^i)$ est le déterminant d'une forme dégénérée sur un groupe de cardinalité 2^{N-1}, cela implique que $\det(M_i^i) = a/2^{-N+1}$ avec $2|a$ et donc $\det(M_i^i) \in 2^{-N+2}\mathbb{Z}$. □

Lemme 2.3.48. *Soit A_2 un 2-groupe de cardinalité 2^N, b une f.f. non-dégénérée sur A_2 avec $\delta = 0$, $(x_1, \ldots, x_n)$ une base de A_2 et M la matrice d'intersection associée. Alors pour tout $1 \leq i < j \leq n$ on a:*

$$\det(M + E_i^j + E_j^i) - \det(M) \in 2^{-N+3}\mathbb{Z}$$

Démonstration. En utilisant la multilinéarité du déterminant on a:

$$\begin{aligned}\det(M+E_i^j+E_j^i) &= \det(M+E_i^j)+\det(M_j^i+E_i^j)\\ &= \det(M)+\det(M_i^j)+\det(M_j^i)+\det(M_{i,j}^{j,i})\\ &= \det(M)+2\det(M_i^j)+\det(M_{i,j}^{j,i})\end{aligned}$$

où $\det(M_i^j)=\det(M_j^i)$ car M est symétrique. □

Par la formule de condensation de Dodgson [Dod] on a:

$$\det(M)\det(M_{i,j}^{j,i})=\det(M_i^i)\det(M_j^j)-\det(M_i^j)^2$$

Par le Lemme précédent $\det(M_i^i)\det(M_j^j)\in 2^{-N+4}\mathbb{Z}$, et comme b est non-dégénérée on a $\det(M)=m2^{-N}$ avec m impair. On a donc deux cas:

1 $\det(M_{i,j}^{j,i})=m_1 2^{-N+2}$ avec m_1 impair, alors $\det(M_i^j)^2=m_2 2^{-N+1}$ avec m_2 impair et donc $2\det(M_i^j)+\det(M_{i,j}^{j,i})\in 2^{-N+3}\mathbb{Z}$;

2 $\det(M_{i,j}^{j,i})\in 2^{-N+3}\mathbb{Z}$, alors $\det(M_i^j)^2\in 2^{-2N+3}\mathbb{Z} \implies \det(M_i^j)\in 2^{-N+2}\mathbb{Z}$ et à nouveau $2\det(M_i^j)+\det(M_{i,j}^{j,i})\in 2^{-N+3}\mathbb{Z}$.

Lemme 2.3.49. *Soit A_2 un 2-groupe de cardinalité 2^N, b une f.f. bilinéaire [q une f.f. quadratique] non-dégénérée sur A_2 avec $\delta_b=0$, $(x_1,\dots,x_n)$ une base de A_2 et M matrice d'intersection associée. Alors pour tout $1\le i\le n$ on a:*

$$\det(M+E_i^i)-\det(M)\in 2^{-N+2}\mathbb{Z}\ \ [\det(M+2E_i^i)-\det(M)\in 2^{-N+3}\mathbb{Z}]$$

Démonstration. En développant le déterminant on trouve:

$$\det(M+E_i^i)=\det(M)+\det(M_i^i)\ \ [\det(M+2E_i^i)=\det(M)+2\det(M_i^i)]$$

Mais $\det(M_i^i)\in 2^{-N+2}\mathbb{Z}$ ce qui conclut la preuve. □

On obtient alors les corollaires suivants:

Corollaire 2.3.50. *Soit A_2 un 2-groupe de cardinalité 2^N, b une f.f. bilinéaire [q une f.f. quadratique] non-dégénérée sur A_2 avec $\delta_b=0$ [$\delta_q=0$]. Alors:*

$$\operatorname{disc}(b)\in\frac{2^{-N}\mathbb{Z}}{2^{-N+2}\mathbb{Z}}\quad\left[\operatorname{disc}(q)\in\frac{2^{-N}\mathbb{Z}}{2^{-N+3}\mathbb{Z}}\right]$$

Démonstration. Soient M, M' deux matrices d'intersections de b [q] associées à la même base, alors $M-M'$ est une matrice de la forme:

$$M-M'=\sum\lambda_i E_i^i+\sum\mu_{jk}\left(E_j^k+E_k^j\right)$$

$$\left[M-M'=\sum 2\lambda_i E_i^i+\sum\mu_{jk}\left(E_j^k+E_k^j\right)\right]$$

avec $\lambda_i,\mu_{jk}\in\mathbb{Z}$. Alors par les résultats précédents $\det(M)-\det(M')\in 2^{-N+2}\mathbb{Z}$ $\left[\det(M)-\det(M')\in 2^{-N+3}\mathbb{Z}\right]$. □

p	m	δ	représentants du discriminant dans $\frac{p^{-N}\mathbb{Z}}{p^{-N+m}\mathbb{Z}}$	
			forme bilinéaire	forme quadratique
impair	$m \geq 1$	/	$\{p^{-N}, up^{-N}\}$	$\{p^{-N}, up^{-N}\}$
2	$m \geq 3$	0/1	$\{2^{-N}, 3\cdot 2^{-N}, 5\cdot 2^{-N}, 7\cdot 2^{-N}\}$	$\{2^{-N}, 3\cdot 2^{-N}, 5\cdot 2^{-N}, 7\cdot 2^{-N}\}$
2	2	0/1	$\{2^{-N}, 3\cdot 2^{-N}\}$	$\{2^{-N}, 3\cdot 2^{-N}, 5\cdot 2^{-N}, 7\cdot 2^{-N}\}$
2	1	0	$\{2^{-N}, 3\cdot 2^{-N}\}$	$\{2^{-N}, 3\cdot 2^{-N}, 5\cdot 2^{-N}, 7\cdot 2^{-N}\}$
2	1	1	$\{2^{-N}\}$	$\{2^{-N}, 3\cdot 2^{-N}\}$

TABLE 2.3.1 – Représentants pour le discriminant

Pour terminer on a que dans $\mathbb{Z}/2^n\mathbb{Z}$ avec $n \geq 3$ tous les carrés inversibles sont exactement les valeurs $\equiv 1 \pmod 8$, donc $1, 3, 5, 7$ appartiennent à quatre classes différentes et les représentent toutes.

Exemple 2.3.51. On donne quelques exemples pour fixer les idées:

- Si b est donnée par la matrice d'intersection $\begin{pmatrix} up^{-n} & \\ & up^{-n-1} \end{pmatrix}$ alors $\mathrm{disc}(b) = u^2p^{-2n-1} = p^{-2n-1}$;
- Si b est une f.f. à valeurs sur $A \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^k$ avec $\delta_b = 1$ alors $\mathrm{disc}(b) = 2^{-k}$;
- Si b est une forme bilinéaire à valeurs dans $A \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^k$ alors $\mathrm{disc}(b) \in \{2^{-3k}, 3\cdot 2^{-3k}, 5\cdot 2^{-3k}, 7\cdot 2^{-3k}\}$;
- Si b est une forme bilinéaire sur $A \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^k \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$ avec $\delta_b = 1$ alors $\mathrm{disc}(b) = 2^{-3k-1}$;
- Si b est une forme bilinéaire sur $A \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^k \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$ avec $\delta_b = 0$ alors $\mathrm{disc}(b) = \{2^{-3k-1}, 3\cdot 2^{-3k-1}\}$;
- Si q est une forme quadratique sur $A \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^k \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$ avec $\delta_q = 1$ alors $\mathrm{disc}(q) \in \{2^{-3k-1}, 3\cdot 2^{-3k-1}\}$;
- Si q est une forme quadratique sur $A \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^k \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$ avec $\delta_q = 0$ alors $\mathrm{disc}(q) \in \{2^{-3k-1}, 3\cdot 2^{-3k-1}, 5\cdot 2^{-3k-1}, 7\cdot 2^{-3k-1}\}$.

2.3.5 Classification des formes finies

On rappelle qu'on s'est limité à étudier uniquement les cas suivants, dont on se donne comme objectif de donner une classification complète:

- Les f.f. bilinéaires sur les p-groupes, avec p premier, $b : A_p \times A_p \to \mathbb{Q}/\mathbb{Z}$;
- Les f.f. quadratiques sur les 2-groupes, $q : A_2 \to \mathbb{Q}/2\mathbb{Z}$;

Pour commencer on va montrer le résultat suivant, qui nous sera utile aussi dans le cas p-adique:

Proposition 2.3.52. *Soit $(R, \mathfrak{m})$ un anneau commutatif local tel que:*

1 $\mathfrak{m} = (m)$ *idéal maximal principal ;*

2 Pour tout $r \in R\backslash\{0\}$, $r = r'm^k$ *avec* r' *inversible ;*

3 $m \nmid 2$.

avec $2 = 1_R + 1_R$. *Soit* M *un* R*-module libre de type fini, si* $b : M \times M \to R$ *est une forme bilinéaire symétrique alors il existe une base de* M *qui diagonalise* b.

Démonstration. Si $r \in R$ on note $\nu_m(r) \in \mathbb{N}$ la valeur maximale de k telle que $m^k | r$ (et donc $m^{k+1} \nmid r$). Soit $k' = \min\{\nu_m(b(x,x)) \,|x \in M\}$ et x_1 un élément de M qui le réalise, alors $b(x_1, x_1) = a_1 m^{k'}$ avec a_1 inversible. On peut supposer que x_1 est un élément primitif de M (i.e. il peut être complété en une base, car M est libre), sinon soit $y_1, \ldots, y_n \in M$ une base, $\lambda_i \in R$ tels que $x_1 = \lambda_1 y_1 + \cdots + \lambda_n y_n$, alors:

$$b(x_1, x_1) = \sum \lambda_i \lambda_j b(y_i, y_j) = \sum \lambda_i \lambda_j r_{ij} m^{k_{ij}} = m^{k'} a_1$$

avec $k_{ij} \geq k'$, car comme 2 est inversible dans R, pour tout $x, y \in M$ on a:

$$b(x,y) = \frac{1}{2}\left(b(x+y, x+y) - b(x,x) - b(y,y)\right)$$

mais $m^{k'} \mid b(x,x)$ pour tout $x \in M$ donc $m^{k'} \mid b(x,y)$.

Comme $m^{k'+1} \nmid b(x_1, x_1)$ il existe y_i, y_j (éventuellement égaux) tels que $\nu_m(b(y_i, y_j)) = k'$, on a donc deux possibilités:

1 Soit $\nu_m(b(y_i, y_i)) = k'$ ou $\nu_m(b(y_j, y_j)) = k'$ et on peut poser $x_1 = y_i$ ou $x_1 = y_j$ primitif ;

2 Soit $\nu_m(b(y_i + y_j, y_i + y_j) = k'$ et on peut poser $x_1 = y_i + y_j$ qui est primitif, car somme de deux éléments d'une base.

il existe donc $x_2', \ldots, x_n' \in M$ tels que $B' = (x_1, x_2', \ldots, x_n')$ soit une base de M, $b(x_1, x_i') = a_i m^{k_i}$ avec $k_i \geq k'$. On pose $\lambda_i = -a_1^{-1} a_i m^{k_i - k'}$, alors on a:

$$\begin{aligned} b(x_1, x_i' + \lambda_i x_1) &= a_i m^{k_i} - a_1^{-1} a_i m^{k_i - k'} a_1 m^{k'} \\ &= a_i m^{k_i} - a_i m^{k_i} = 0 \end{aligned}$$

donc si on pose $x_i = x_i' + \lambda x_1$ pour $2 \leq i \leq n$, on a que $B = (x_1, \ldots, x_n)$ est une base avec matrice associée:

$$\begin{pmatrix} a_1 m^{k'} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Si on répète récursivement la procédure sur $\text{span}(x_2, \ldots, x_n)$, on arrive à une diagonalisation de la forme:

$$\begin{pmatrix} a_1 m^{k_1} & & & & & \\ & \ddots & & & & \\ & & a_n m^{k_n} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

avec les a_i inversibles et $k_1 \leq \cdots \leq k_n$. □

Remarque 2.3.53. Si 2 n'est pas inversible dans R (donc $2 = m^d a_2$ avec a_2 inversible) on peut montrer un résultat analogue à la Proposition 2.3.52 en obtenant une diagonalisation par blocs de dimension maximale 2 [MM].

Les hypothèses de la proposition sont satisfaites pour $R = \mathbb{Z}_p, \mathbb{Z}_{(p)}, \frac{\mathbb{Z}}{p^n\mathbb{Z}}, K$ avec $p \neq 2$ premier et K un corps de caractéristique différente de 2. En particulier, si b est une f.f. bilinéaire sur $A = \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^k$, alors b prend ses valeurs sur $\text{Im}(b) \subseteq \{\frac{a}{p^n} | a \in \mathbb{Z}\} \subset \frac{\mathbb{Q}^{(p)}}{\mathbb{Z}}$, mais on a l'isomorphisme de $\mathbb{Z}$-modules:

$$\frac{\{\frac{a}{p^n} | a \in \mathbb{Z}\}}{\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

On peut donc voir A comme un R-module libre avec $R = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$, et b' la forme bilinéaire à valeurs dans R donnée par:

$$\begin{array}{rcl} b' : A \times A & \to & R \\ (x, y) & \mapsto & b(x, y)p^n \end{array}$$

et grâce à la proposition on peut diagonaliser b' (et donc b aussi). Donc il existe une base $x_1, \ldots, x_k$ de A telle que:

$$b \simeq b_{|\,\text{span}(x_1)} \oplus \cdots \oplus b_{|\,\text{span}(x_k)}$$

En fait, on peut faire plus que cela: si b est un f.f. bilinéaire (non-dégénérée) sur $A = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$, x un générateur de A, alors b est complètement décrite par la valeur $b(x, x) = \frac{a}{p^n}$ avec a inversible dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ (car si $p|a$ on aurait que b ne serait pas dégénérée). Donc si a est un carré, comme 1 est aussi un carré dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, par le Corollaire 2.3.44 il existe r inversible tel que $r^2 a = 1$. Alors si on pose $y = rx$ on a que y est un générateur de A et:

$$b(y, y) = r^2 b(x, x) = 1$$

donc b est équivalent à la forme qu'associe 1 au générateur du groupe. Réciproquement, si a n'est pas un carré dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, alors on peut choisir

n'importe quel « non carré standard » $u \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ et il existera r tel que $r^2a = u$, donc si $y = rx$ on aura $b(y, y) = u$, donc b sera équivalent à la forme qu'associe u au générateur du groupe.

En utilisant la notation suivante:

Définition 2.3.54. Soit p premier impair, $n \in \mathbb{N}\backslash\{0\}$ et u le plus petit entier qui ne soit pas un carré modulo p (et donc $\overline{u}$ n'est pas un carré dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ pour aucun n). Alors on note $\overline{w}^{\epsilon}_{p,n}$ les f.f. bilinéaires non-dégénérées suivantes:

- $\begin{array}{rccc} \overline{w}^{1}_{p,n} : & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \times \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \\ & (x, y) & \mapsto & xy \end{array}$
- $\begin{array}{rccc} \overline{w}^{-1}_{p,n} : & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \times \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \\ & (x, y) & \mapsto & uxy \end{array}$

Remarque 2.3.55. On rappelle qu'il y a une correspondance parfaite entre f.f. bilinéaires à valeurs dans $\frac{\mathbb{Q}}{\mathbb{Z}}$ et formes bilinéaires à valeurs dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ et parfois on les identifiera par abus de notation. Par exemple en général avec $\overline{w}^{\epsilon}_{p,n}$ on sous-entendra les f.f. bilinéaires:

- $\begin{array}{rccc} \overline{w}^{1}_{p,n} : & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \times \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \to & \frac{\mathbb{Q}}{\mathbb{Z}} \\ & (x, y) & \mapsto & \frac{xy}{p^n} \end{array}$
- $\begin{array}{rccc} \overline{w}^{-1}_{p,n} : & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \times \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \to & \frac{\mathbb{Q}}{\mathbb{Z}} \\ & (x, y) & \mapsto & \frac{uxy}{p^n} \end{array}$

Remarque 2.3.56. Même si on utilise la notation $\overline{w}^{-1}$, on rappelle qu'en réalité -1 peut très bien être un carré modulo p, par exemple $2^2 = 4 \equiv -1 \pmod 5$. Plus généralement, pour p impair, -1 est un carré si et seulement si $p \equiv 1 \pmod 4$.

En résumant, on a montré que:

Lemme 2.3.57. *Soit b une f.f. bilinéaire non-dégénérée sur $A = \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^k$ avec p premier impair, alors b décompose comme:*

$$b \simeq \left(\overline{w}^{1}_{p,n}\right)^{\oplus i} \oplus \left(\overline{w}^{-1}_{p,n}\right)^{\oplus(k-i)}$$

On est pas encore arrivé à une décomposition unique, car on à le résultat suivant:

Lemme 2.3.58. $\overline{w}^{1}_{p,n} \oplus \overline{w}^{1}_{p,n} \simeq \overline{w}^{-1}_{p,n} \oplus \overline{w}^{-1}_{p,n}$

Démonstration. Soit x_1, x_2 une base telle que la matrice soit:

$$\begin{pmatrix} \frac{1}{p^n} & 0 \\ 0 & \frac{1}{p^n} \end{pmatrix}$$

on rappelle que u est le plus petit non-carré modulo p, en particulier $u \not\equiv 1 \pmod{p}$ et donc $\overline{u-1}$ est un carré inversible (car $1 < u < p$) dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$. il existe alors $r \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ tel que $r^2 = \overline{u-1}$. On pose alors $y_1 = x_1 + rx_2$ et $y_2 = rx_1 - x_2$, alors:

$$\begin{aligned} b(y_1, y_1) &= b(y_2, y_2) = \frac{1}{p^n} + \frac{r^2}{p^n} = \frac{u}{p^n} \\ b(y_1, y_2) &= \frac{r}{p^n} - \frac{r}{p^n} = 0 \end{aligned}$$

donc la matrice dans la base (y_1, y_2) est:

$$\begin{pmatrix} \frac{u}{p^n} & 0 \\ 0 & \frac{u}{p^n} \end{pmatrix}$$

ce qui montre l'équivalence. □

Cela permet de simplifier les termes $\overline{w}_{p,n}^{-1}$, si on en a plus d'un. Il reste à montrer qu'il n'est pas possible de simplifier plus que cela:

Lemme 2.3.59. *Soit b une f.f. bilinéaire non-dégénérée sur $A = \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^k$, alors b se décompose de façon unique comme:*

$$b \simeq \left(\overline{w}_{p,n}^1\right)^{\oplus k} \text{ ou } b \simeq \left(\overline{w}_{p,n}^1\right)^{\oplus k-1} \oplus \overline{w}_{p,n}^{-1}$$

i.e. b est complètement déterminée par son discriminant.

Démonstration. On a montré qu'on peut réduire b sous une de ces deux formes, il reste à montrer qu'elles sont distinctes. On a $\text{disc}\left(\overline{w}_{p,n}^1\right)^{\oplus k} = p^{-nk}$ et $\text{disc}\left(\left(\overline{w}_{p,n}^1\right)^{\oplus k-1} \oplus \overline{w}_{p,n}^{-1}\right) = up^{-nk}$, donc les deux formes bilinéaires ne sont pas isomorphes et on obtient l'unicité de la décomposition. □

Maintenant on a une classification complète des formes finies sur $\left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^k$. Il reste alors à montrer que toutes les f.f. bilinéaires sur un p-groupes A se décomposent comme somme de formes finies sur des $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$-modules libres.

On a d'abord besoin des résultats suivants:

Définition 2.3.60. Soit A un groupe abélien, p premier, on note

$$\begin{aligned} A_{p,j} &:= \{x \in A | p^j x = 0\} \\ \rho_{p,j}(A) &:= \frac{A_{p,j}}{A_{p,j-1} + pA_{p,j+1}} \end{aligned}$$

On remarque que $\rho_{p,j}(A) \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^k$ pour un certain k et que pour A,B groupes abéliens:

$$(A \oplus B)_{p,j} \simeq \{(x,y) \in A \oplus B | p^j x = p^j y = 0\} \simeq A_{p,j} \oplus B_{p,j}$$

donc on a aussi:

$$\begin{aligned}\rho_{p,j}(A\oplus B) &\simeq \frac{A_{p,j}\oplus B_{p,j}}{A_{p,j-1}+pA_{p,j+1}+B_{p,j-1}+pB_{p,j+1}}\\ &\simeq \rho_{p,j}(A)\oplus\rho_{p,j}(B)\end{aligned}$$

D'ailleurs $\rho_{p,j}$ est compatible avec les formes finies, car si b est une f.f. bilinéaire sur A alors $\mathrm{Im}\left(b_{|A_{p,j}}(\bullet,\bullet)\right)\subseteq\left\{\frac{a}{p^j}\pmod{\mathbb{Z}}|a\in\mathbb{Z}\right\}$ lorsque $\mathrm{Im}\left(b_{|A_{p,j-1}+pA_{p,j+1}}(\bullet,\bullet)\right)\subseteq\left\{\frac{a}{p^{j-1}}|a\pmod{\mathbb{Z}}\in\mathbb{Z}\right\}$, donc b descend sur $\rho_{p,j}(A)$ avec des valeurs dans:

$$\frac{\left\{\frac{a}{p^j}\pmod{\mathbb{Z}}|a\in\mathbb{Z}\right\}}{\left\{\frac{a}{p^{j-1}}\pmod{\mathbb{Z}}|a\in\mathbb{Z}\right\}}\simeq\left\{\frac{a}{p}\pmod{\mathbb{Z}}|a\in\mathbb{Z}\right\}$$

Donc on a une f.f. bilinéaire sur $\rho_{p,j}(A)$.

D'ailleurs on peut calculer facilement que $\rho_{p,j}(\overline{w}^1_{p,j})=\overline{w}^1_{p,1}$ et $\rho_{p,j}(\overline{w}^{-1}_{p,j})=\overline{w}^{-1}_{p,1}$.

Maintenant on est prêt pour prouver:

Proposition 2.3.61. *Soit b une f.f. bilinéaire non-dégénérée sur un p-groupe A_p avec p premier, alors b se décompose sous la forme:*

$$b\simeq b_{|A_{p^1}}\oplus\cdots\oplus b_{|A_{p^n}}$$

avec $A_{p^i}\simeq\left(\frac{\mathbb{Z}}{p^i\mathbb{Z}}\right)^{k_i}$. De plus, si $p\neq 2$, la décomposition est unique.

Démonstration. Soit p^n l'ordre maximal des éléments de A_p et k la valeur maximale telle que $A_{p^n}:=\left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{\oplus k}\hookrightarrow A_p$, ce qui nous donne une décomposition du type $A_p\simeq A_{p^n}\oplus B$ avec B qui contient des éléments d'ordre au plus p^{n-1}. On montre que $b_{|A_{p^n}}$ est non-dégénérée: soit $x\in A_{p^n}\backslash\{0\}$ d'ordre p^j, alors par le Lemme 2.3.27 il existe $x'\in A_{p^n}$ d'ordre p^n tel que $p^{n-j}x'=x$ et $y\in A_p$ tel que $b(x',y)=\frac{1}{p^n}$. Cela implique que y a ordre p^n, donc on peut le décomposer comme $y=y_1+y_2$ avec $y_1\in A_{p^n}$ et $y_2\in B$ d'ordre p^m, $m<n$. Soit a tel que $b(x',y_2)=a/p^m$, alors:

$$\begin{aligned}b(x',y_1) &= b(x',y)-b(x',y_2)\\ &= \frac{1}{p^n}-\frac{a}{p^m}\\ &= \frac{1-p^{n-m}a}{p^n}=\frac{a'}{p^n}\end{aligned}$$

avec $p\nmid a'$, et donc $b(x,y_1)=\frac{a'}{p^{n-j}}\not\equiv 0\pmod{\mathbb{Z}}$ ce qui implique $b_{|A_{p^n}}$ est non-dégénérée. Par la Proposition 2.3.35 on a une décomposition $b\simeq b_{|A_{p^n}}\oplus b_{|A^\perp_{p^n}}$ avec $A^\perp_{p^n}$ qui contient des éléments d'ordre au plus p^{n-1}, et en itérant

la procédure sur $A_{p^n}^{\perp}$ on obtient la décomposition désirée après un nombre fini d'étapes.

Il reste à démontrer l'unicité pour $p \neq 2$: soit donc $b \simeq b_{|\tilde{A}_{p^1}} \oplus \cdots \oplus b_{|\tilde{A}_{p^n}}$ une autre décomposition, on doit montrer que:

$$b_{|\tilde{A}_{p^j}} \simeq b_{|A_{p^j}} \text{ pour tout } 1 \leq j \leq n$$

Si on applique $\rho_{p,j}$, on a $\rho_{p,j}(b) = \rho_{p,j}(b_{|A_{p^j}}) = \rho_{p,j}(b_{|\tilde{A}_{p^j}})$.

Comme $p \neq 2$, d'après le Théorème 2.3.59 on peut diagonaliser $b_{A_{p^j}}$ de façon unique et en appliquant $\rho_{p,j}$:

$$\begin{aligned} b_{|A_{p^j}} \simeq \left(\overline{w}_{p,n}^1\right)^{\oplus k_j} &\implies \rho_{p,j}(b_{|A_{p^j}}) = \left(\overline{w}_{p,1}^1\right)^{\oplus k_j} \text{ ou} \\ b_{|A_{p^j}} \simeq \left(\overline{w}_{p,n}^1\right)^{\oplus (k_j-1)} \oplus \overline{w}_{p,n}^{-1} &\implies \rho_{p,j}(b_{|A_{p^j}}) = \left(\overline{w}_{p,1}^1\right)^{\oplus k_j} \oplus \overline{w}_{p,1}^{-1} \end{aligned}$$

Donc l'image $\rho_{p,j}$ dépend uniquement de la décomposition de $b_{|A_{p^j}}$ et comme $\rho_{p,j}(b_{|A_{p^j}}) = \rho_{p,j}(b_{|\tilde{A}_{p^j}})$ on obtient que $b_{|\tilde{A}_{p^j}} \simeq b_{|A_{p^j}}$. □

Exemple 2.3.62. Si $p = 2$ on n'a plus l'unicité de la décomposition. Par exemple soit $A \simeq \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{8\mathbb{Z}}$ avec base x_1, x_2 et b une forme avec matrice d'intersection:

$$\begin{pmatrix} \frac{1}{4} & 0 \\ 0 & \frac{1}{8} \end{pmatrix}$$

Si on prend $y_1 = x_1 + 2x_2$, $y_2 = x_1 - x_2$, alors la nouvelle matrice d'intersection est:

$$\begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{3}{8} \end{pmatrix}$$

donc $\operatorname{span}(x_1) \simeq \operatorname{span}(y_1) \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ donnent deux décompositions de b avec $b_{|\operatorname{span}(x_1)} \not\simeq b_{|\operatorname{span}(y_1)}$, car sur $\operatorname{span}(x_1)$ les éléments ont carré $\frac{1}{4}$ ou 0 lorsque sur $\operatorname{span}(y_1)$ les carrés valent $\frac{3}{4}$ ou 0.

Exemple 2.3.63. Si b est une forme dégénérée le résultat n'est plus vrai, par exemple soit $A = \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}}$, (x_1, x_2) une base de A avec $\operatorname{ord}(x_1) = 9$, $\operatorname{ord}(x_2) = 3$ et b donnée par la matrice:

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 \end{pmatrix}$$

alors il n'existe aucune décomposition orthogonale de b de la forme $b_{|\frac{\mathbb{Z}}{3\mathbb{Z}}} \oplus b_{|\frac{\mathbb{Z}}{9\mathbb{Z}}}$.

Finalement on a:

Corollaire 2.3.64. *Soit b une forme bilinéaire sur un p-groupe A_p, avec p impair. Alors b se décompose de façon unique sous la forme:*

$$b \simeq \bigoplus_i \left(\overline{w}_{p,i}^1\right)^{\oplus k_i} \oplus \bigoplus_j \left(\overline{w}_{p,j}^{-1}\right)^{\oplus k_j'}$$

avec $0 \leq k_j' \leq 1$ pour tout j.

On rappelle que pour le cas impair on a une équivalence parfaite entre f.f. bilinéaires et f.f. quadratiques et on peut donc conserver nos résultats dans ce cas:

Définition 2.3.65. Soit p premier impair, $n \in \mathbb{N}\backslash\{0\}$ et u le plus petit entier qui ne soit pas un carré modulo p. On pose alors $u' = u$ si u est pair, sinon $u' = u + p^n$ (ou de façon équivalente, $u' = m_2(2^{-1}u)$). On note $w^{\epsilon}_{p,n}$ (sans la barre pour les distinguer du cas bilinéaire) les f.f. quadratiques non-dégénérées suivantes:

- $w^1_{p,n} : \begin{array}{ccc} \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \to & \frac{\mathbb{Q}}{2\mathbb{Z}} \\ x & \mapsto & (p^n+1)x^2 \end{array}$
- $w^{-1}_{p,n} : \begin{array}{ccc} \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \to & \frac{\mathbb{Q}}{2\mathbb{Z}} \\ x & \mapsto & u'x^2 \end{array}$

En particulier la f.f. bilinéaire associée à $w^{\epsilon}_{p,n}$ est $\overline{w}^{\epsilon}_{p,n}$.

Corollaire 2.3.66. *Soit q une forme bilinéaire sur un p-groupe A_p, avec p impair. Alors q se décompose de façon unique sous la forme:*

$$q \simeq \bigoplus_i \left(w^1_{p,i}\right)^{\oplus k_i} \oplus \bigoplus_j \left(w^{-1}_{p,j}\right)^{\oplus k'_j}$$

avec $0 \leq k'_j \leq 1$ pour tout j.

On a donc terminé complètement le discours pour ce qui concerne la classification des formes bilinéaires finies sur un groupe abélien de cardinalité impaire. Par contre, on a seulement évoqué les passages les plus importants pour ce qui concerne le cas pair.

Pour le cas pair on procède de façon assez similaire, mais avec beaucoup plus de difficultés techniques. Vue la nature introductive de ces notes on se limitera à reporter les résultats, renvoyant au [MM] pour les preuves.

Proposition 2.3.67. *Pour les 2-groupes on a les f.f. bilinéaires indécomposables suivantes:*

A	*Notation*	*Définition*
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$\overline{w}^1_{2,1}$	$b(x,y) = xy/2$
$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	$\overline{u}_1$	$b((x_1,y_1),(x_2,y_2)) = (x_1y_2 + x_2y_1)/2$
$\frac{\mathbb{Z}}{4\mathbb{Z}}$	$\overline{w}^1_{2,2}$	$b(x,y) = xy/2$
$\frac{\mathbb{Z}}{4\mathbb{Z}}$	$\overline{w}^3_{2,2}$	$b(x,y) = 3xy/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 3$	$\overline{w}^1_{2,n}$	$b(x,y) = xy/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 3$	$\overline{w}^3_{2,n}$	$b(x,y) = 3xy/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 3$	$\overline{w}^5_{2,n}$	$b(x,y) = 5xy/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 3$	$\overline{w}^7_{2,n}$	$b(x,y) = 7xy/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$\overline{u}_n$	$b((x_1,y_1),(x_2,y_2)) = (x_1y_2 + x_2y_1)/2^n$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$\overline{v}_n$	$b((x_1,y_1),(x_2,y_2)) = (2x_1y_1 + 2x_2y_2 + x_1y_2 + x_2y_1)/2^n$

Et pour les formes quadratiques finies:

Proposition 2.3.68. *Pour les 2-groupes on a les f.f. quadratiques indécomposables suivantes:*

A	*Notation*	*Définition*
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$w_{2,1}^1$	$q(x) = x^2/2$
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$w_{2,1}^3$	$q(x) = 3x^2/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$w_{2,n}^1$	$q(x) = x^2/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$w_{2,n}^3$	$q(x) = 3x^2/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$w_{2,n}^5$	$q(x) = 5x^2/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$w_{2,n}^7$	$q(x) = 7x^2/2$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^n\mathbb{Z}}$	u_n	$q((x_1, x_2)) = x_1x_2/2^n$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^n\mathbb{Z}}$	v_n	$q((x_1, x_2)) = (x_1^2 + x_1x_2 + x_2^2)/2^n$

Malheureusement cela ne suffit pas à donner une classification complète, car comme on a vu dans l'Exemple 2.3.62 en général la décomposition dans le cas pair n'est pas unique. Il faut donc essayer de se ramener à une forme « normale », qui soit la même pour les formes équivalentes. On ne présentera pas la forme normale dans le cas général, renvoyant (encore une fois) le lecteur intéressé à [MM], mais on se limitera à donner l'énoncé pour une forme finie sur $(\mathbb{Z}/2\mathbb{Z})^n$, un résultat que l'on utilisera dans la suite:

Proposition 2.3.69. *Soit $A = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$, b une f.f. bilinéaire sur A. Alors b décompose sous une (et une seule) de ces formes:*

1 $b \simeq \overline{u}_1^{\oplus \frac{n}{2}}$ *(uniquement si n est pair);*

2 $b \simeq \overline{w}_{2,1}^{\oplus n}$.

On rappelle qu'on associe à b le symbole δ_b, qui vaut $\delta_b = 0$ dans le premier cas et $\delta_b = 1$ dans le deuxième. Donc $\delta_b = 0$ si et seulement si tous les éléments de A ont carré $0 \pmod{\mathbb{Z}}$.

Proposition 2.3.70. *Soit $A = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$, q une f.f. quadratique sur A. Alors q se décompose toujours sous une (et une seule) de ces formes:*

1 $q \simeq u_1^{\oplus \frac{n}{2}}$;

2 $q \simeq u_1^{\oplus \frac{n}{2}-1} \oplus v_1$;

3 $q \simeq \left(w_{2,1}^1\right)^{\oplus n-d} \oplus \left(w_{2,1}^3\right)^{\oplus d}$ *avec* $0 \leq d \leq 3$.

b	$\mathrm{disc}(b)$	q	$\mathrm{disc}(q)$
$\overline{w}^1_{p,n}$, p impair	p^{-n}	$w^1_{p,n}$, p impair	p^{-n}
$\overline{w}^{-1}_{p,n}$, p impair	up^{-n}	$w^{-1}_{p,n}$, p impair	up^{-n}
$\overline{w}^{\epsilon}_{2,n}$	$\epsilon 2^{-n}$	$w^{\epsilon}_{2,n}$	$\epsilon 2^{-n}$
$\overline{u}_n$	$7 \cdot 2^{-2n}$	u_n	$7 \cdot 2^{-2n}$
$\overline{v}_n$	$3 \cdot 2^{-2n}$	v_n	$3 \cdot 2^{-2n}$

TABLE 2.3.2 – Discriminants des f.f. bilinéaires/quadratiques indécomposables

2.3.6 Extensions de réseaux

Définition 2.3.71. Soient $L \subseteq R$ deux réseaux avec $\mathrm{rang}(L) = \mathrm{rang}(R)$, alors on dira que R est un *sur-réseau* de L.

Exemple 2.3.72 (Construction de D_{16}^+)**.** On rappelle que:

$$D_{16} = \{(a_1, \ldots, a_{16}) \in \mathbb{Z}^{16} | a_1 + \cdots + a_{16} \equiv 0 \pmod 2\}$$

et D_{16}, u_1, u_2 engendrent D_{16}^*, avec $u_1 = (\frac{1}{2}, \ldots, \frac{1}{2})$ et $u_2 = (1, 0, \ldots, 0)$. Comme $\langle u_1, u_1 \rangle = 4$ on a que

$$D_{16}^+ := D_{16} + \mathrm{span}_{\mathbb{Z}}(u_1)$$

est un réseau pair, et comme $u_1 \in D_{16}^+ \backslash D_{16}$, $u_2 \in D_{16}^* \backslash \left(D_{16}^+\right)^*$ alors:

$$D_{16} \subsetneq D_{16}^+ \subseteq \left(D_{16}^+\right)^* \subsetneq D_{16}^*$$

Mais $A_{D_{16}} = \frac{D_{16}^*}{D_{16}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}^2$, donc $A_{D_{16}^+} = \frac{\left(D_{16}^+\right)^*}{D_{16}^+} \simeq \{0\}$ et D_{16}^+ est unimodulaire et pair de signature $(16, 0)$.

Bien que cela puisse sembler moins naturel, la construction de sur-réseaux est pourtant une opération sous certains côtés plus importante que la construction des sous-réseaux, car:

- On verra qu'un réseau L admet au maximum un nombre fini de sur-réseaux, contre un nombre toujours infini de sous-réseaux (par exemple $nL \subset L$ pour $n \in \mathbb{N}^*$) ;
- On utilisera les sur-réseaux pour étudier les isomorphismes des réseaux.

Soit donc L un réseau, si R est un sur-réseau de L alors R est obtenu en ajoutant des vecteurs à L, donc:

$$R = L + \mathrm{span}(u_1, \ldots, u_k)$$

Comme R est aussi un réseau, en particulier $\langle u_i, x\rangle \in \mathbb{Z}\ \forall x \in L$, ce qui implique que $u_i \in L^*$, donc $L \subseteq R \subseteq L^*$. D'ailleurs le choix des u_i est fait modulo L, car si $x_1, \ldots, x_k \in L$, alors:

$$L + \mathrm{span}(u_1, \ldots, u_k) = L + \mathrm{span}(u_1 + x_1, \ldots, u_k + x_k)$$

en effet un choix des u_i nous ramène à choisir un sous-groupe de A_L, plus précisément un sous-groupe *totalement isotrope* car $\langle u_i, u_j\rangle \in \mathbb{Z} \implies b_L(\overline{u_i}, \overline{u_j}) \equiv 0 \pmod{\mathbb{Z}}$ (on rappelle qu'une forme bilinéaire b est *totalement isotrope* sur un sous-groupe si elle est identiquement nulle sur tous les couples d'éléments).

On a donc le résultat suivant:

Proposition 2.3.73. *Soit L un réseau avec groupe discriminant A_L, pour chaque sur-réseau $R \supseteq L$ on associe le groupe $H_R := R/L \subseteq A_L$.*

Alors l'application $R \to H_R$ décrit une bijection entre les sur-réseaux de L et les sous-groupes totalement isotropes de A_L.

Démonstration. Comme $\mathrm{rang}(R) = \mathrm{rang}(L)$ et $L \subseteq R$ on a que $\mathrm{span}_{\mathbb{Q}}(R) = \mathrm{span}_{\mathbb{Q}}(L)$ et donc $R \subseteq L \otimes \mathbb{Q}$, mais R est un réseau, donc $\langle x, y\rangle \in \mathbb{Z}$ pour tout $x, y \in R$, donc en particulier pour tout $x \in R$, $y \in L$ ce qui implique que $R \subseteq L^*$. Donc $H_R \subseteq A_L$ est un sous-groupe de A_L, totalement isotrope car pour tout $\overline{x}, \overline{y} \in H_R$ il existe $x, y \in R$ avec $\overline{x} = x + L$, $\overline{y} = y + L$ et

$$b_L(\overline{x}, \overline{y}) \equiv \langle x, y\rangle \equiv 0 \pmod{\mathbb{Z}}$$

On a donc une application:

$$\begin{array}{rcl} \varphi : \{\text{sur-réseaux de } L\} & \longrightarrow & \{\text{sous-groupes isotropes de } A_L\} \\ R & \mapsto & H_R \end{array}$$

et on veut montrer qu'elle est bijective. Grâce au troisième théorème d'isomorphisme on a une bijection entre:

$$\begin{array}{rcl} \psi : \left\{ \begin{array}{c} \text{sous-groupes abéliens} \\ \text{de } L^* \text{qui contiennent } L \end{array} \right\} & \longrightarrow & \{\text{sous-groupes de } A_L\} \\ L \subseteq K \subseteq L^* & \longmapsto & K/L \end{array}$$

Mais K/L est totalement isotrope si et seulement si la forme bilinéaire sur K prend ses valeurs dans $\mathbb{Z}$ (i.e. si K est un réseau), donc la bijectivité de ψ implique que φ est bijective aussi. □

Remarque 2.3.74. Si R est un sur-réseau de L, une condition nécessaire pour que R soit pair est que L soit pair aussi. Dans ce cas, soit q_L la forme quadratique discriminante de L, alors R est pair si et seulement si $q_{L|A_R} \equiv 0 \pmod{2\mathbb{Z}}$: dans ce cas on dira que la *f.f. quadratique* est totalement isotrope ou que A_R est totalement q-isotrope. Pour un réseau L pair on a donc une correspondance bijective:

$$\begin{array}{rcl} \{\text{sur-réseaux pairs de } L\} & \longleftrightarrow & \{\text{sous-groupes } q\text{-isotropes de } A_L\} \\ R & \mapsto & H_R \end{array}$$

Exemple 2.3.75. Soit $L = U(2)$, (x_1, x_2) une base de L tel que la matrice de Gram soit:

$$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

alors $q_L = u_2$, donc $(\frac{1}{2}\overline{x}_1, \frac{1}{2}\overline{x}_2)$ est une base de A_L telle que la matrice d'intersection soit:

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$$

On a donc trois choix pour un sous-espace totalement isotrope de A_L, $H_1 = \text{span}(\frac{1}{2}\overline{x}_1)$, $H_2 = \text{span}(\frac{1}{2}\overline{x}_2)$, $H_3 = \text{span}(\frac{1}{2}\overline{x}_1 + \frac{1}{2}\overline{x}_2)$; on remarque que sur H_1, H_2 la f.f. quadratique est totalement isotrope, alors que sur H_3 uniquement la f.f. bilinéaire est totalement isotrope mais pas la f.f. quadratique (car $q_L(\frac{1}{2}\overline{x}_1 + \frac{1}{2}\overline{x}_2) = 1 \not\equiv 0 \pmod{2\mathbb{Z}}$ mais $b_L(\frac{1}{2}\overline{x}_1 + \frac{1}{2}\overline{x}_2, \frac{1}{2}\overline{x}_1 + \frac{1}{2}\overline{x}_2) = 1 \equiv 0 \pmod{\mathbb{Z}}$).

En effet pour H_1 et H_2 on obtient le sur-réseau ;

$$\text{span}_{\mathbb{Z}}(\frac{1}{2}x_1, x_2) \simeq \text{span}_{\mathbb{Z}}(x_1, \frac{1}{2}x_2) \simeq U$$

qui est pair, lorsque pour H_3 on a $R_3 = \text{span}_{\mathbb{Z}}(\frac{1}{2}x_1 + \frac{1}{2}x_2, x_2)$ qui a pour matrice de Gram:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

et on vérifie facilement que $R_3 \simeq \langle 1 \rangle \oplus \langle -1 \rangle$ qui est impair.

On peut aussi obtenir le groupe discriminant de R en travaillant sur le groupe discriminant de L:

Proposition 2.3.76. *Soit L un réseau et $R \supseteq L$ un sur-réseau, alors:*

$$A_R \simeq \frac{H_R^\perp}{H_R}$$

et en particulier $b_R = \frac{b_L|_{H_R^\perp}}{H_R}$ [et $q_R = \frac{q_L|_{H_R^\perp}}{H_R}$ si L, R sont pairs], où b_R [q_R] est définie sur $\frac{H_R^\perp}{H_R} \simeq A_R$.

Démonstration. Comme $L \subseteq R$, on a:

$$\begin{aligned} R^* &= \{x \in R \otimes \mathbb{Q} | \, \langle x, y \rangle \in \mathbb{Z} \forall y \in R\} \\ &\subseteq \{x \in R \otimes \mathbb{Q} | \, \langle x, y \rangle \in \mathbb{Z} \forall y \in L\} \\ &= L^* \end{aligned}$$

et donc $L \subseteq R \subseteq R^* \subseteq L^*$. On a alors $A_R \simeq \frac{R^*/L}{H_R}$, donc si on prend le quotient $\pi : L^* \to A_L$:

$$\begin{aligned} R^*/L &= \pi(R^*) \\ &= \pi(\{x \in L^* | \, \langle x, y \rangle \in \mathbb{Z} \forall y \in R\}) \\ &= \{\overline{x} \in A_L | b_L(\overline{x}, \overline{y}) \equiv 0 \pmod{\mathbb{Z}}\} \\ &= H_R^\perp \end{aligned}$$

Donc $A_R \simeq \frac{H_R^\perp}{H_R}$. Maintenant, soient $x_1, x_2 \in R^*$, $y_1, y_2 \in R$, alors $\overline{x}_1, \overline{x}_2 \in H_R^\perp$ et $\overline{y}_1, \overline{y}_2 \in H_R$, donc $b_L(\overline{x}_i, \overline{y}_i) = b_L(\overline{y}_i, \overline{y}_j) = 0$ et on obtient:

$$\begin{aligned}\langle x_1+y_1, x_2+y_2\rangle &\equiv b_L(\overline{x}_1+\overline{y}_1, \overline{x}_2+\overline{y}_2) \pmod{\mathbb{Z}} \\ &\equiv b_L(\overline{x}_1,\overline{x}_2) + \underbrace{b_L(\overline{y}_1,\overline{x}_2)+b_L(\overline{x}_1,\overline{y}_2)+b_L(\overline{y}_1,\overline{y}_2)}_{=0} \pmod{\mathbb{Z}} \\ &\equiv b_L(\overline{x}_1,\overline{x}_2) \pmod{\mathbb{Z}}\end{aligned}$$

Donc $b_R = \left(b_L|_{H_R^\perp}\right)/H_R$. Dans le cas pair on obtient de la même façon que $q_R = \left(q_L|_{H_R^\perp}\right)/H_R$ □

Exemple 2.3.77. Soit L un réseau, alors il existe $x_1 \in L$ avec $x_1^2 \neq 0$ et L est un sur-réseau de $\mathrm{span}(x_1) \oplus x_1^\perp$. En procédant par récurrence on obtient qu'il existe $x_1, \ldots, x_r \in L$ vecteurs orthogonaux indépendants tels que L est un sur-réseau de $\mathrm{span}(x_1) \oplus \cdots \oplus \mathrm{span}(x_r)$ et $x_i^2 \neq 0$.

Lemme 2.3.78. *Soit R un sur-réseau de L, alors:*

$$\#A_L = \#A_R \cdot (\#H_R)^2$$

Démonstration. Comme $A_R \simeq H_R^\perp/H_R$ on a $\#A_R = \#H_R^\perp/\#H_R$, mais b_L est non-dégénérée, donc par le Lemme 2.3.29 $\#H_R^\perp = \#A_L/\#H_R$ et en remplaçant on trouve le résultat cherché. □

Corollaire 2.3.79. *Soit R un sur-réseau de L, alors $R = L$ si et seulement si $det(L) = det(R)$.*

En particulier si L est unimodulaire alors $L = R$.

Corollaire 2.3.80. *Soit L_1 un sous-réseau primitif d'un réseau R, alors:*

$$\left|\det(L_1)\cdot\det(L_1^\perp)\right| = |\det(R)| \cdot \left(R : (L_1 \oplus L_1^\perp)\right)^2$$

Exemple 2.3.81. Soit L un réseau pair avec comme base $v_1, \ldots, v_r$, on prend sur $L(-1)$ la base correspondante $w_1, \ldots, w_r$, donc $\langle v_i, v_j\rangle = -\langle w_i, w_j\rangle$ pour tout $1 \leq i, j \leq r$. Soit $\varphi : A_L \to A_{L(-1)}$ tel que $\varphi(\overline{v_i^*}) = \overline{w_i^*}$, alors φ est l'opposé d'une isométrie.

Soit $H_R = \{(x, \varphi(x)) | x \in A_L\} \leq A_L \oplus A_{L(-1)}$, alors H_R est un groupe totalement $q_{L\oplus L(-1)}$-isotrope, qui correspond au sur-réseau $R \supseteq L \oplus L(-1)$ engendré par $\mathrm{span}(v_i, w_i, v_i^* + w_i^*,\ 1 \leq i \leq r)$. Maintenant soient $u_i = v_i^* + w_i^*$, alors $\langle u_i, u_j\rangle = 0$ et $\langle u_i, v_j\rangle = \delta_i^j$, donc la matrice sur $\mathrm{span}(v_1, u_1, \ldots, v_r, u_r)$ est de la forme:

$$\begin{pmatrix}
\langle v_1,v_1\rangle & 1 & * & 0 & \cdots & * & 0 \\
1 & 0 & 0 & 0 & \cdots & 0 & 0 \\
* & 0 & \langle v_2,v_2\rangle & 1 & \cdots & * & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
* & 0 & * & 0 & \cdots & \langle v_r,v_r\rangle & 1 \\
0 & 0 & 0 & 0 & \cdots & 1 & 0
\end{pmatrix}$$

avec $\langle v_i, v_i \rangle \equiv 0 \pmod 2$. On remplace les v_i par des vecteurs de la forme $v_i' = v_i - \langle v_1, v_i \rangle u_1$ pour $i \geq 2$ et $v_1' = v_i - \frac{\langle v_1, v_1 \rangle}{2} u_1$, alors la matrice devient:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \langle v_2, v_2 \rangle & 1 & \cdots & * & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & * & 0 & \cdots & \langle v_r, v_r \rangle & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

et par récurrence on peut répéter la procédure avec tous les u_i de façon à obtenir une matrice par blocs de la forme:

$$\begin{pmatrix} U & & \\ & \ddots & \\ & & U \end{pmatrix}$$

Donc $|\det(\text{span}(v_1, u_1, \ldots, v_r, u_r))| = 1$, mais $\text{span}(v_1, u_1, \ldots, v_r, u_r) \subseteq R$ ce qui implique :

$$R \simeq \text{span}(v_1, u_1, \ldots, v_r, u_r) \simeq U^{\oplus r}$$

Bonus: Dessiner un réseau en Latex

On reporte ci-dessous le code utilisé pour la Figure 2.3.1 à titre d'exemple:

Algorithme 2.1

```
\begin{tikzpicture}
% On defini un cadre dont on ne peut pas sortir
\clip (0,0) rectangle (8cm,6cm);

% L'origine est fixée au centre du cadre
\pgftransformshift{\pgfpoint{4cm}{3cm}}

\draw[->] (-4,0)--(4,0); %On dessine
\draw[->] (0,-3)--(0,3); %les axes


\pgftransformcm{1}{0}{-0.5}{0.866}{\pgfpoint{0}{0}}
% On pose comme coordonnées la base du réseau

\pgftransformscale{1.65} % On defini le zoom

% On dessine d'abord le dual
\foreach \x in {-10,...,10}{     % Deux indices pour chaque
    \foreach \y in {-10,...,10}{ % vecteur qu'on va dessiner
        \node[draw,circle,inner sep=0.9pt,fill,blue]
        at (\x*2/3+\y/3,\x/3+\y*2/3) {};
        % On dessine des points fins
    }
}
% Après on dessine A2
\foreach \x in {-3,...,3}{
    \foreach \y in {-3,...,3}{
        \node[draw,circle,inner sep=1.5pt,fill] at (\x,\y) {};
        % On dessine des points épais
    }
}

% On dessine les vecteurs
\draw [->,ultra thick] (0,0) to node[above]{$w_2$}(2/3,1/3);
\draw [->,ultra thick] (0,0) to node[left]{$w_1$}(1/3,2/3);

\end{tikzpicture}
```

2.4 Critères d'existence

2.4.1 Genre d'un réseau

Le théorème de Hasse–Minkowski est un résultat très connu de théorie des nombres, qui nous permet de classifier complètement les formes qua-

dratiques sur $\mathbb{Q}$ en utilisant leur évaluation sur les corps p-adiques $\mathbb{Q}_p$ pour toutes les valeurs de p.

Malheureusement il n'existe pas de résultat aussi fort pour les réseaux, cependant, l'évaluation sur les anneaux p-adiques $\mathbb{Z}_p$ reste un outil très important, à la fois comme invariant et pour la détermination des critères d'existence.

On appellera $\mathbb{Z}_p$-réseau un $\mathbb{Z}_p$-module libre de type fini, équipé d'une forme bilinéaire symétrique non-dégénérée à valeurs dans $\mathbb{Z}_p$. Soit donc L un réseau et p un premier, en tensorisant par $\mathbb{Z}_p$ on obtient $L_p = L \otimes \mathbb{Z}_p$; si b est la forme bilinéaire sur L, alors $b_p = b \otimes \mathbb{Z}_p$ est aussi une forme bilinéaire sur L_p non-dégénérée à valeurs dans $\mathbb{Z}_p$, donc L_p est un $\mathbb{Z}_p$-réseau.

Par convention dans la suite on appellera $L_\infty = \mathbb{Z} \otimes \mathbb{R}$.

Définition 2.4.1. Soit L un réseau, le *genre* de L est la donnée de l'ensemble des L_p, pour toutes les valeurs de p, $p = \infty$ inclus.

Remarque 2.4.2. $L_\infty \simeq L \otimes \mathbb{R}$ consiste en la donnée de la signature (s^+, s^-) de L, car il s'agit du seul invariant des forme bilinéaires sur $\mathbb{R}$.

Comme dans la section précédente, on analysera uniquement le cas impair, en se limitant à énoncer les résultats pour le cas pair.

Soit donc p premier impair, alors par la Proposition 2.3.52 on peut diagonaliser L_p sous la forme:

$$\begin{pmatrix} a_1^0 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & a_{k_0}^0 & & & & & & & \\ & & & pa_1^1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & pa_{k_1}^1 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & p^n a_1^n & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & p^n a_{k_n}^n \end{pmatrix} \tag{2.4.1}$$

Comme dans le cas des formes finies, on veut simplifier ultérieurement en cherchant les carrés dans $\mathbb{Z}_p$. On trouve alors que la réponse est donnée par le résultat suivant [Ei]:

Théorème 2.4.3 (Lemme de Hensel)**.** *Soit f un polynôme à coefficients dans $\mathbb{Z}_p$, s'il existe $\alpha_0 \in \mathbb{Z}_p$ tel que:*

$$f(\alpha_0) \equiv 0 \pmod{p} \text{ et } f'(\alpha_0) \not\equiv 0 \pmod{p}$$

alors il existe $\alpha \in \mathbb{Z}_p$ tel que:

$$f(\alpha) = 0 \text{ et } \alpha \equiv \alpha_0 \pmod{p}$$

Soit $\pi_p : \mathbb{Z}_p \to \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ la projection modulo p, dans la suite, pour un élément $a \in \mathbb{Z}_p$ on notera $\overline{a}$ la projection de a, $\overline{a} = \pi_p(a)$.

Lemme 2.4.4. *Soit p premier impair, $a \in \mathbb{Z}_p$ inversible est un carré si et seulement si $\overline{a}$ est un carré dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$.*

Démonstration. Soit $f = X^2 - a$, alors a est un carré si et seulement si f admet une racine dans $\mathbb{Z}_p$. On suppose qu'il existe $r \in \mathbb{Z}_p$ tel que $r^2 = a$, alors $\overline{r}^2 \equiv \overline{a} \pmod{p}$ et donc $\overline{a}$ est un carré dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Réciproquement, si $\overline{a}$ est un carré (inversible) dans $\mathbb{Z}/p\mathbb{Z}$, alors il existe $r_0 \in \frac{\mathbb{Z}}{p\mathbb{Z}} \backslash \{0\}$ tel que $f(r_0) \equiv 0 \pmod{p}$, vu que 2 est inversible aussi dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ alors $f'(r_0) = 2r_0 \not\equiv 0 \pmod{p}$. On peut donc appliquer le Lemme de Hensel pour obtenir que f a une solution dans $\mathbb{Z}_p$ et a est un carré. □

En appliquant le Lemme 2.3.44 on obtient tout de suite:

Corollaire 2.4.5. *Soit p premier impair, $x, y \in \mathbb{Z}_p$ inversibles, alors xy est un carré dans $\mathbb{Z}_p$ si et seulement si:*

- *x,y sont deux carrés ;*
- *ni x, ni y est un carré.*

En poursuivant exactement comme dans le cas des formes finies, dans (2.4.1) on peut remplacer les éléments sur la diagonale par des carrés ou des non-carrés:

Définition 2.4.6. Soit p premier impair, $n \in \mathbb{N}$ et u le plus petit entier positif qui ne soit pas un carré modulo p. Alors on note $W_{p,n}^{\epsilon}$ les $\mathbb{Z}_p$-réseaux suivants:

- $$\begin{array}{rccc} W_{p,n}^{1} : & \mathbb{Z}_p \times \mathbb{Z}_p & \to & \mathbb{Z}_p \\ & (x, y) & \mapsto & p^n xy \end{array}$$
- $$\begin{array}{rccc} W_{p,n}^{-1} : & \mathbb{Z}_p \times \mathbb{Z}_p & \to & \mathbb{Z}_p \\ & (x, y) & \mapsto & p^n uxy \end{array}$$

On a aussi l'analogue du Lemme 2.3.58:

Lemme 2.4.7. $W_{p,n}^{1} \oplus W_{p,n}^{1} \simeq W_{p,n}^{-1} \oplus W_{p,n}^{-1}$

On arrive donc à:

Proposition 2.4.8. *Soit L_p un $\mathbb{Z}_p$-réseau, alors on a une décomposition unique:*

$$L_p \simeq \bigoplus_{n \in \mathbb{N}} \left(\left(W_{p,n}^{1} \right)^{\oplus k_n} \oplus \left(W_{p,n}^{-1} \right)^{\oplus \epsilon_n} \right)$$

avec $\epsilon_n \in \{0, 1\}$, $k_n = \epsilon_n = 0$ pour presque toutes les valeurs de n.

La seule chose qu'il nous reste à démontrer est l'unicité de la décomposition, mais pour cela on va procéder de façon un peu différente. On commence par:

Définition 2.4.9. Soit L_p un p-réseau, on appelle *discriminant* de L_p la classe de $\det(L_p)$ modulo les carrés inversibles de $\mathbb{Z}_p$:

$$\operatorname{disc}(L_p) \equiv \det(L_p) \pmod{\left(\mathbb{Z}_p^*\right)^2}$$

Remarque 2.4.10. On peut montrer que, comme dans le cas des formes finies, pour p impair on a que deux classes d'isomorphisme données par p^n et up^n, lorsque pour $p = 2$ on a les représentants 2^n,$3 \cdot 2^n$,$5 \cdot 2^n$,$7 \cdot 2^n$ [MM].

Maintenant, de manière similaire à ce qu'on a fait dans la sous-section 2.3.1, pour un $\mathbb{Z}_p$-réseau L_p, on définit le réseau dual L_p^* comme le $\mathbb{Z}_p$-module $\operatorname{Hom}_{\mathbb{Z}_p}(L_p, \mathbb{Z}_p)$ équipé de la forme bilinéaire à valeurs dans $\mathbb{Q}_p$, donnée par l'injection $L_p \to L_p^*$ $x \mapsto \langle x, \bullet \rangle$.

On peut donc prendre comme groupe discriminant le quotient $A_{L_p} = \frac{L_p^*}{L_p}$, doté d'une forme bilinéaire $b_{A_{L_p}}$ à valeurs dans:

$$\frac{\mathbb{Q}_p}{\mathbb{Z}_p}$$

Comme la forme bilinéaire est non-dégénérée, L_p et L_p^* ont le même rang et donc le quotient est un module de torsion. Comme il s'agit de plus d'un $\mathbb{Z}_p$-module et $\mathbb{Z}_p$ est principal on a que A_{L_p} est de la forme:

$$A_{L_p} \simeq \bigoplus_i \frac{\mathbb{Z}_p}{p^{k_i}\mathbb{Z}_p} \simeq \bigoplus_i \frac{\mathbb{Z}}{p^{k_i}\mathbb{Z}}$$

De plus, la forme bilinéaire b_{L_p} prend ses valeurs dans $\mathbb{Q}^{(p)}/\mathbb{Z}$ car:

Lemme 2.4.11.

$$\frac{\mathbb{Q}_p}{\mathbb{Z}_p} \simeq \frac{\mathbb{Q}^{(p)}}{\mathbb{Z}}$$

Démonstration. Soit $f : \mathbb{Q}^{(p)}/\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p$, on a que f est injective car $\mathbb{Z}_p \cap \mathbb{Q}^{(p)} = \mathbb{Z}$, il reste à montrer que f est surjective. Soit $x \in \mathbb{Q}_p$, alors $x = \frac{a}{p^n}$ avec $a \in \mathbb{Z}_p$. Soit $m \in \mathbb{Z}$ tel que $a \equiv m \pmod{p^n}$, donc $p^n | (a - m)$ et il existe $y \in \mathbb{Z}_p$ tel que $yp^n = a - m$. On obtient:

$$x = y + \frac{m}{p^n}$$

donc $f(\frac{m}{p^n}) \equiv x \pmod{\mathbb{Z}_p}$ et f est surjective. □

Donc, en dépit de l'apparente complexité, on a que b_{L_p} n'est rien d'autre qu'une f.f. bilinéaire.

Remarque 2.4.12. La preuve que b_{L_p} [q_{L_p}] est une f.f. bilinéaire [quadratique] s'applique aussi dans le cas $p = 2$, où par contre il est nécessaire de faire la distinction entre $\mathbb{Z}_2$-réseaux pairs et impairs.

Définition 2.4.13. Soit b une f.f. bilinéaire sur A, alors on note $l(b) := l(A)$, c'est-à-dire le nombre minimal de générateurs du groupe A sur lequel la forme est définie.

Comme A_L est engendré par une base de L^* on a $l(A_L) \leq \text{rang}(L)$.

Lemme 2.4.14. *Soit L_p un $\mathbb{Z}_p$-réseau avec* $\text{rang}(L_p) = l(b_{L_p})$ *. Alors:*

$$\text{disc}(b_{L_p}) = \frac{1}{\text{disc}(L_p)}$$

En particulier dans ce cas L_p est déterminé par sa forme discriminante.

Démonstration. On rappelle que par le Lemme 2.3.14 $\text{rang}(L_p) = l(b_{L_p})$ si et seulement si p divise la matrice d'intersection de L_p. On suppose p impair: on vérifie facilement que pour un réseau de la forme $W^{\epsilon}_{p,n}$ avec $n \geq 1$, on a $b_{W^{\epsilon}_{p,n}} \simeq \overline{w}^{\epsilon}_{p,n}$ alors:

$$L_p \simeq \bigoplus_{n\in\mathbb{N}\setminus\{0\}} \left(\left(W^1_{p,n}\right)^{\oplus k_n} \oplus \left(W^{-1}_{p,n}\right)^{\oplus \epsilon_n}\right)$$

avec $\text{disc}(L_p) = \prod_{n\in\mathbb{N}\setminus\{0\}} p^{nk_n}(up^n)^{\epsilon_n}$, donc:

$$b_{L_p} \simeq \bigoplus_{n\in\mathbb{N}\setminus\{0\}} \left(\left(\overline{w}^1_{p,n}\right)^{\oplus k_n} \oplus \left(\overline{w}^{-1}_{p,n}\right)^{\oplus \epsilon_n}\right)$$

et comme u^{-1} est aussi dans la classe des non carrés:

$$\text{disc}(b_{L_p}) = \prod_{n\in\mathbb{N}\setminus\{0\}} p^{-nk_n}(\overline{u}^{-1}p^{-n})^{\epsilon_n} = \frac{1}{\text{disc}(L_p)}$$

Pour $p = 2$ on peut raisonner de la même façon en prenant une décomposition (non unique) de b_{L_2}. □

Remarque 2.4.15. La preuve du résultat précédent s'applique aussi, pour $p = 2$, à la forme discriminante quadratique, donc si $p = 2$ et L_2 est pair on peut montrer que $\text{disc}(q_{L_2}) = \text{disc}(L_2)^{-1}$.

On est maintenant prêt pour:

Preuve de la Proposition 2.4.8 (unicité). On a donc:

$$L_p \simeq \left(\left(W^1_{p,0}\right)^{\oplus k_n} \oplus \left(W^{-1}_{p,0}\right)^{\oplus \epsilon_n}\right) \oplus \underbrace{\left(\bigoplus_{n\in\mathbb{N}\setminus\{0\}} \left(\left(W^1_{p,n}\right)^{\oplus k_n} \oplus \left(W^{-1}_{p,n}\right)^{\oplus \epsilon_n}\right)\right)}_{(*)}$$

et par le Lemme 2.4.14 $(*)$ est unique, car déterminé complètement par b_L qui se décompose de façon unique. Il reste donc à montrer l'unicité de k_0 et ϵ_0, mais la somme $k_0 + \epsilon_0$ est déterminée par le rang de L_p, alors que:

$$\operatorname{disc}(L_p) = u^{\epsilon_0} \operatorname{disc}((*)) = u^{\epsilon_0} / \operatorname{disc}(b_L)$$

permet d'obtenir ϵ_0. □

De plus, on a démontré (pour p impair) que:

Proposition 2.4.16. *Soit L_p un $\mathbb{Z}_p$-réseau avec p impair [un $\mathbb{Z}_2$-réseau pair], alors L_p est totalement déterminé par le discriminant, le rang, et la forme discriminante $b_{A_{L_p}}$ [forme discriminante quadratique $q_{A_{L_2}}$].*

Exemple 2.4.17. Soit L un réseau de signature $(2,2)$ avec forme discriminante $b_L = \overline{w}_{3,1}^{-1} \oplus \overline{w}_{5,1}^{1} \oplus \overline{w}_{5,2}^{-1}$, on veut déterminer L_5. Comme $b_{L_5} = b_L \otimes \mathbb{Z}_5 = \overline{w}_{5,1}^{1} \oplus \overline{w}_{5,2}^{-1}$ on a uniquement deux possibilités: $L_5 = \left(W_{5,0}^{1}\right)^{\oplus 2} \oplus W_{5,1}^{1} \oplus W_{5,2}^{-1}$ ou $L_5 = W_{5,0}^{1} \oplus W_{5,0}^{-1} \oplus W_{5,1}^{1} \oplus W_{5,2}^{-1}$, mais

$$\operatorname{disc}(L_5) = \det(L) = (-1)^{s^-} \#A_L = 3 \cdot 5^3$$

Comme 3 n'est pas un carré dans $\mathbb{Z}_5$ on a que la condition sur le discriminant est satisfaite uniquement par $L_5 = W_{5,0}^{1} \oplus W_{5,0}^{-1} \oplus W_{5,1}^{1} \oplus W_{5,2}^{-1}$.

Exemple 2.4.18. Le résultat n'est pas vrai en général pour un $\mathbb{Z}_2$-réseau impair: soient L_1, L_2 deux $\mathbb{Z}_2$-réseaux donnés par les matrices:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

alors $\operatorname{rang}(L_1) = \operatorname{rang}(L_2) = 2$, $\det(L_1) = \det(L_2) = 1$ et $b_{L_1} = b_{L_2} \equiv 0$, mais L_1 et L_2 ne sont pas isomorphes. Car sinon $L_1 \simeq L_2$ impliquerait $L_1(2) \simeq L_2(2)$, mais:

$$q_{L_1(2)} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \quad q_{L_2(2)} = \begin{pmatrix} \frac{3}{2} & 0 \\ 0 & \frac{3}{2} \end{pmatrix}$$

et $q_{L_1(2)} \neq q_{L_2(2)}$ par la Proposition 2.3.70, donc $L_1 \neq L_2$.

On donne aussi le résultat suivant sur la classification des $\mathbb{Z}_2$-réseaux indécomposables [MM]:

Proposition 2.4.19. *Tous les $\mathbb{Z}_2$-réseaux indécomposables sont dans une des formes suivantes:*

- *Pour $n \in \mathbb{N}$, $\epsilon \in \{1,3,5,7\}$:* $\begin{array}{rccc} W_{2,n}^{\epsilon}: & \mathbb{Z}_2 \times \mathbb{Z}_2 & \to & \mathbb{Z}_2 \\ & (x,y) & \mapsto & 2^n \epsilon x y \end{array}$

- *Pour $n \in \mathbb{N}$:*
$$\begin{array}{rccc} U_{p,n}^n : & \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\ & ((x_1,x_2),(y_1,y_2)) & \mapsto & x \begin{pmatrix} 0 & 2^n \\ 2^n & 0 \end{pmatrix} y \end{array}$$

- *Pour $n \in \mathbb{N}$:*
$$\begin{array}{rccc} V_{p,n}^n : & \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\ & ((x_1,x_2),(y_1,y_2)) & \mapsto & x \begin{pmatrix} 2^{n+1} & 2^n \\ 2^n & 2^{n+1} \end{pmatrix} y \end{array}$$

Remarque 2.4.20. La distinction entre réseau pair et impair prend tout son sens dans le cadre p-adique. Dans $\mathbb{Z}_p$ avec $p \neq 2$, comme 2 est inversible il n'existe aucune différence entre réseaux pairs ou impairs, donc la parité du réseau est une donnée visible uniquement quand on tensorise par $\mathbb{Z}_2$. Regardons cela plus dans le détail: soit L_2 un $\mathbb{Z}_2$-réseau, alors en raisonnant de façon similaire à la preuve de la 2.3.52, on montre qu'il est possible de diagonaliser L_2 par blocs sous une de ces deux formes:

$$(1) \begin{pmatrix} a_1 & & & \\ & \ddots & & \\ & & a_s & \\ & & & 2\cdot[M] \end{pmatrix} \qquad (2) \begin{pmatrix} [B_1] & & & \\ & \ddots & & \\ & & [B_t] & \\ & & & 2\cdot[M] \end{pmatrix}$$

où les a_i sont inversibles dans $\mathbb{Z}_2$, B_i des blocs 2×2 inversibles avec diagonale paire et $2\cdot[M]$ la partie non inversible qui reste. On a que L_2 est pair si et seulement s'il se diagonalise comme (2), sinon il est impair: donc la parité d'un réseau L est en réalité une donné relative à la classe d'isomorphisme de $L \otimes \mathbb{Z}_2$. On peut montrer que, une fois le rang fixé, on a quatre classes d'isomorphisme pour le cas (1), lorsqu'on en a seulement deux dans le cas (2), qui peuvent donc être classifiés simplement a partir du déterminant du réseau [MM].

On trouve que pour un réseau pair, la forme quadratique est suffisante à déterminer la classe d'isomorphisme sur $\mathbb{Z}_2$, lorsque pour un réseau impair on a besoin de données supplémentaires (qui se révèlent être la signature du réseau).
On peut sûrement dire que cela est la différence principale entre les deux cas, à laquelle on peut ramener toutes les autres asymétries entre réseaux pairs et impairs dans les différents résultats.

À un réseau L on peut donc associer trois objets différents: la forme discriminante b_L (où la forme quadratique q_L dans le cas d'un réseau pair), le $\mathbb{Z}_p$-réseau L_p et sa forme discriminante b_{L_p}. Comme b_{L_p} et b_L sont deux f.f. bilinéaires, il est raisonnable de se demander s'il existe un lien direct entre eux. Heureusement la réponse est oui:

Proposition 2.4.21. *Soit L un réseau impair [pair], alors $b_{L_p} \simeq b_L \otimes \mathbb{Z}_p \simeq b_{|A_p}$ [$q_{L_p} \simeq q_L \otimes \mathbb{Z}_p \simeq q_{|A_p}$] avec $A_{L_p} \simeq A_L \otimes \mathbb{Z}_p \simeq A_p$, où A_p est la p-part de A_L.*

Démonstration. On considère le diagramme suivant, qui est clairement commutatif:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L\otimes\mathbb{Z}_p & \longrightarrow & L^*\otimes\mathbb{Z}_p \simeq \mathrm{Hom}(L,\mathbb{Z})\otimes\mathbb{Z}_p & \longrightarrow & A_L\otimes\mathbb{Z}_p \simeq \frac{L^*}{L}\otimes\mathbb{Z}_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\varphi}\ \wr & & \downarrow{\scriptstyle\psi} & & \downarrow & & \\
0 & \longrightarrow & L_p & \longrightarrow & L_p^* \simeq \mathrm{Hom}_{\mathbb{Z}_p}(L_p,\mathbb{Z}_p) & \longrightarrow & A_{L_p}\simeq\frac{L_p^*}{L_p} & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccc}
x\otimes a & \longmapsto & \langle x,\bullet\rangle\otimes a \\
\downarrow & & \downarrow \\
ax & \longmapsto & \langle ax,\bullet\rangle
\end{array}$$

On a vu que L_p^* a une forme bilinéaire héritée par L_p, lorsque $L^*\otimes\mathbb{Z}_p$ prend sa forme bilinéaire par L^*. Comme φ est une isométrie (car le produit bilinéaire est transporté par φ), la commutativité du diagramme implique que ψ est compatible avec les formes bilinéaires: cela implique que ψ est injective, car les formes sont non-dégénérées.

Il reste à démontrer la surjectivité: cela peut etre prouvé fonctoriellement en remarquant que la restriction des scalaires et le changement d'anneau sont deux foncteurs adjoints entre $\mathbb{Z}$-Mod et $\mathbb{Z}_p$-Mod. Alternativement, on peut le vérifier manuellement en développant les calculs sur une base. Dans les deux cas, on montre que ψ est une bijection, qui induit une isométrie entre $A_L\otimes\mathbb{Z}_p$ et A_{L_p} qui préserve la forme discriminante, bilinéaire ou quadratique.

Comme dans $\mathbb{Z}_p$ tous les éléments sont inversibles si et seulement s'ils ne sont pas divisibles par p, on obtient que $A_L\otimes\mathbb{Z}_p$ contient uniquement la p-torsion de A_L, c'est-à-dire la p-part A_p. □

Remarque 2.4.22. Dans la preuve on utilise implicitement le fait que $\mathbb{Z}_p$ est un $\mathbb{Z}$-module sans torsion, ce qui nous garantit qu'une forme bilinéaire non-dégénérée sur $\mathbb{Z}$ est non-dégénérée aussi sur $\mathbb{Z}_p$.

Finalement on a:

Proposition 2.4.23. *Soit L un réseau pair, alors connaître le genre de L est équivalent à connaître sa signature (s^+,s^-) et sa forme discriminante q_L.*

Démonstration. On rappelle que $L_\infty\simeq L\otimes\mathbb{R}$ est équivalent à (s^+,s^-). On a démontré dans la Proposition 2.3.38 que q_L décompose comme:

$$q_L\simeq\bigoplus_p q_{|A_p}\simeq\bigoplus_p q_L\otimes\mathbb{Z}_p$$

donc le genre de L détermine q_L et la signature.

Réciproquement, comme L est pair, on a vu que pour tout p premier L_p est déterminé par q_{L_p} et $\det(L_p)$, mais $q_{L_p} \simeq q_L \otimes \mathbb{Z}_p$ et pour le déterminant on a:

$$\det(L_p) = \det(L) = (-1)^{s^-} \# A_L$$

□

Exemple 2.4.24. On montre un exemple pratique avec $L = A_2$: on a $\text{sign}(L) = (2,0)$, $\text{rang}(L) = 2$ et $q_L = w_{3,1}^{-1}$. Par le résultat précédent cela implique que pour $p \neq 3$, p impair, on a $L_p \simeq W_{p,0}^1 \oplus W_{p,0}^\epsilon$ avec $\epsilon = \left(\frac{\det(L)}{p}\right) = \left(\frac{3}{p}\right)$, $L_3 \simeq W_{3,0}^{-1} \oplus W_{3,1}^{-1}$ (car $\det(L)/\det(W_{3,1}^{-1})$ n'est pas un carré dans $\mathbb{Z}_3$) et pour terminer $L_2 \simeq V_0$ où $L_2 \simeq U_0$ car L est pair, mais $\det(L) \equiv 3 \pmod 8$ donc $L_2 \simeq V_0$.

Pour vérifier le résultat, on procède à un calcul direct: soit (x_1, x_2) la base de L_p associée à la matrice d'intersection:

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

On a que 2 est inversible dans $\mathbb{Z}_p$ pour p impair et $x_1' = x_1$, $x_2' = 2x_1 + x_2$ est aussi une base de L_p, avec matrice d'intersection:

$$\begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$$

Donc si $p \neq 3$ alors L_p est équivalent à $W_{p,0}^1 \oplus W_{p,0}^\epsilon$ avec $\epsilon = \left(\frac{\det(L_p)}{p}\right) = \left(\frac{2^2 3}{p}\right) = \left(\frac{3}{p}\right)$, alors que dans le cas $p = 3$ on a bien $L_3 \simeq W_{3,0}^{-1} \oplus W_{3,1}^{-1}$. Il reste à vérifier L_2: on prend la base $x_1' = x_1$, $x_2' = -x_2$ qui nous donne la matrice:

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

qui est exactement la matrice de V_0 .

On donne (sans preuve) une formulation plus générale du résultat précédent [Nik, Cor. 1.16.3]:

Théorème 2.4.25. *La donnée du genre d'un réseau L est équivalente à la donnée de la parité (L pair ou impair), de la signature et de la forme bilinéaire b_L.*

Corollaire 2.4.26. *Soient L, L' deux réseaux avec même parité, signature et forme discriminante, $d \in \mathbb{Z}\backslash\{0\}$, alors $L(d)$ et $L'(d)$ ont la même forme discriminante. En particulier la forme discriminante de $L(d)$ est déterminée uniquement par la signature et la forme discriminante de L.*

Comme la complétion (dans notre cas p-adique) consiste en une étude locale d'un anneau, on peut donc considérer le genre comme la donnée « locale » d'un réseau.

Et pourtant, malgré son importance, on ne dédiera pas beaucoup d'espace à la représentation p-adique dans la suite .

La raison est simple: le genre est complètement équivalent à la donnée de signature et forme bilinéaire. Mais ces dernières ont l'avantage de nous fournir une représentation plus compacte ainsi que plus pratique dans les calculs, surtout pour ce qui concerne les isométries.

Le point de vue du genre, très puissant du point de vu théorique et qui nous permet de démontrer plusieurs résultats importants, sera donc abandonné dans les calculs pratiques en faveur de l'utilisation de la forme discriminante, qui finalement contient la même information, mais d'un point de vue différent.

2.4.2 Signature et invariant de Gauss

On a vu que le groupe discriminant, avec la signature, résume le genre d'un réseau. Par contre il reste impossible de déduire la signature à partir du groupe discriminant, car elle n'a aucune signification pour une forme finie.

D'ailleurs si L est un réseau impair, pour n'importe quel choix de $i, j \in \mathbb{N}$ alors $L \oplus \langle 1\rangle^{\oplus i} \oplus \langle -1\rangle^{\oplus j}$ est aussi un réseau impair, avec le même groupe discriminant mais de signature complètement différente.

Par contre, si L est un réseau pair, on verra que grâce au théorème de Milgram, il est quand même possible d'obtenir quelques informations sur sa signature à partir de l'étude de la f.f. (formes finies) quadratique. L'invariant qui nous permettra d'établir le lien est le suivant:

Définition 2.4.27. Soit q une f.f. quadratique sur un groupe abélien A, l'*invariant de Gauss* de q est la valeur complexe:

$$\gamma(q) = \frac{1}{\sqrt{\#A}} \sum_{x \in A} e^{i\pi q(x)}$$

Pour un réseau pair L on notera $\gamma(L) = \gamma(q_L)$ l'invariant de Gauss associé a la forme quadratique discriminante de L.

Comme les valeurs de q sont définies modulo $2\mathbb{Z}$ on a que $\gamma(q)$ est bien défini.

Exemple 2.4.28. Soit $L = U(2)$ et q_L la forme quadratique associée, alors la matrice d'intersection est:

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$$

et l'invariant de Gauss est:

$$\gamma(L) = \frac{1}{\sqrt{4}}\left(e^0 + e^0 + e^0 + e^{i\pi}\right) = 1$$

On peut montrer facilement que l'invariant de Gauss a la propriété suivante:

Lemme 2.4.29. *Soit q une f.f. quadratique sur $A \simeq A_1 \oplus A_2$, $q \simeq q_{A_1} \oplus q_{|A_2}$ une décomposition orthogonale, alors*

$$\gamma(q) = \gamma(q_{A_1})\gamma(q_{A_2})$$

Démonstration. En développant les calculs:

$$\begin{aligned}
\gamma(q) &= \frac{1}{\sqrt{\#A}} \sum_{x\in A} e^{i\pi q(x)} \\
&= \frac{1}{\sqrt{\#A_1\#A_2}} \sum_{\substack{x_1\in A_1 \\ x_2\in A_2}} e^{i\pi q(x_1+x_2)} \\
&= \frac{1}{\sqrt{\#A_1\#A_2}} \sum_{\substack{x_1\in A_1 \\ x_2\in A_2}} e^{i\pi q(x_1)} e^{i\pi q(x_2)} \\
&= \frac{1}{\sqrt{\#A_1}} \sum_{x\in A_1} e^{i\pi q(x_1)} \frac{1}{\sqrt{\#A_2}} \sum_{x\in A_2} e^{i\pi q(x_2)} \\
&= \gamma(q_{A_1})\gamma(q_{A_2})
\end{aligned}$$

□

Soit L un réseau pair et $L' \subset L$ un sous-réseau du même rang, alors on a vu qu'il existe $H \subset A_{L'}$ totalement isotrope tel que $A_L \simeq A_{\frac{H^\perp}{H}}$. Vu que notre objectif est d'avoir un invariant lié à la signature du réseau, il est raisonnable de demander que $\gamma(L) \simeq \gamma(L')$ et donc $\gamma(q_{A_L}) \simeq \gamma(q_{\frac{H^\perp}{H}})$. Avant de démontrer cela, on donne le résultat suivant qui nous sera utile dans la preuve:

Lemme 2.4.30. *Soit b une f.f. bilinéaire sur A, $H \leq A$ et $x \notin H^\perp$. Alors:*

$$\sum_{y\in H} e^{2i\pi b(x,y)} = 0$$

Démonstration. Soient $h \in H$ élément primitif tel que $b(x,h) \neq 0$ et $K \leq H$ tel que $H \simeq \mathrm{span}(h) \oplus K$ (somme non nécessairement orthogonale) alors:

$$\begin{aligned}
\sum_{y\in H} e^{2i\pi b(x,y)} &= \sum_{\substack{y_1\in \mathrm{span}(h) \\ y_2\in K}} e^{2i\pi b(x,y_1)} e^{2i\pi b(x,y_2)} \\
&= \left(\sum_{y_1\in \mathrm{span}(h)} e^{2i\pi b(x,y_1)}\right)\left(\sum_{y_2\in K} e^{2i\pi b(x,y_2)}\right)
\end{aligned}$$

Si $\mathrm{ord}(h) = n$ alors $n \cdot b(x,h) \in \mathbb{Z}$, donc $b(x,h) = \frac{a}{m}$ avec $(a,m) = 1$ et $m|n$. On a alors:

$$\sum_{y_1 \in \mathrm{span}(h)} e^{2i\pi b(x,y_1)} = \sum_{j=0}^{n-1} e^{\frac{2j}{m} i\pi} = 0$$

car il s'agit de la somme (éventuellement répété) de racines m-èmes. Donc $\sum_{y \in H} e^{2i\pi b(x,y)} = 0 \cdot \sum_{y_2 \in K} e^{2i\pi b(x,y_2)} = 0$. □

Proposition 2.4.31. *Soit q une forme quadratique non-dégénérée sur A, $H \leq A$ tel que $q_{|H} \equiv 0$ (i.e. H soit totalement q-isotrope). Alors:*

$$\gamma(q) = \gamma(q_{\frac{H^\perp}{H}})$$

Démonstration. Soient $x_1, \ldots, x_m \in A$ (avec $m = \#A/\#H$) un système de représentants de A/H, alors tout élément de A s'écrit de façon unique comme une somme $x_i + h$ avec $h \in H$, donc on a:

$$\begin{aligned}
\gamma(q) &= \frac{1}{\sqrt{\#A}} \sum_{x \in A} e^{i\pi q(x)} \\
&= \frac{1}{\sqrt{\#A}} \sum_{\substack{1 \leq i \leq m \\ h \in H}} e^{i\pi q(x_i + h)} \\
&= \frac{1}{\sqrt{\#A}} \sum_{1 \leq i \leq m} \left(e^{i\pi q(x_i)} \sum_{h \in H} e^{2i\pi b(x_i,h)} \right)
\end{aligned}$$

Par le Lemme précédent on a que $\sum_{h \in H} e^{2i\pi b(x_i,h)} = 0$ si $x_i \notin H^\perp$, sinon si $x_i \in H^\perp$ alors $b(x_i,h) \equiv 0$ et $\sum_{h \in H} e^{2i\pi b(x_i,h)} = \#H$. Donc:

$$\begin{aligned}
\gamma(q) &= \frac{\#H}{\sqrt{\#A}} \sum_{x \in \{x_1,\ldots,x_m\} \cap H^\perp} e^{i\pi q(x)} \\
&= \sqrt{\frac{\#H}{\#\frac{A}{H}}} \sum_{x \in \frac{H^\perp}{H}} e^{i\pi q(x)} \\
&= \gamma(q_{|\frac{H^\perp}{H}})
\end{aligned}$$

car comme q est non-dégénérée alors $\#H^\perp = \#A/\#H$ (Lemme 2.3.29). □

On obtient donc tout de suite:

Corollaire 2.4.32. *Soit L un réseau pair, $L' \subset L$ un sous-réseau du même rang. Alors $\gamma(L) = \gamma(L')$.*

Exemple 2.4.33. Soit L un réseau pair, q_L la forme discriminante quadratique, si on considère $L(-1)$ on a

$$\begin{aligned}\gamma(L(-1)) &= \frac{1}{\sqrt{\#A_{L(-1)}}} \sum_{x\in A_{L(-1)}} e^{i\pi q_{L(-1)}(x)} \\ &= \frac{1}{\sqrt{\#A_L}} \sum_{x\in A_L} e^{-i\pi q_L(x)}\end{aligned}$$

Comme $\left|e^{i\pi q_L(x)}\right| = e^{i\pi q_L(x)}\overline{e^{i\pi q_L(x)}} = 1$ on a $e^{-i\pi q_L(x)} = \overline{e^{i\pi q_L(x)}}$ et donc:

$$\gamma(L(-1)) = \overline{\gamma(L)}$$

Comme on a toujours le plongement dans le sur-réseau $L\oplus L(-1) \hookrightarrow U^{\oplus n}$ (Exemple 2.3.81) par le Corollaire 2.4.32 on a

$$\gamma(L)\overline{\gamma(L)} = \gamma(U)^n = 1$$

et donc $|\gamma(L)| = 1$.

Pour calculer l'invariant de Gauss on utilisera le résultat classique suivant (dont on peut trouver une preuve sur [Da]) :

Théorème 2.4.34 (Somme quadratique de Gauss)**.** *Pour $n \in \mathbb{N}^*$ on définit la somme quadratique de Gauss comme:*

$$G(n) = \sum_{x=0}^{n-1} e^{2i\pi\frac{x^2}{n}}$$

alors on a:

$$G(n) = \begin{cases} (1+i)\sqrt{n} & si\ n \equiv 0 \mod 4 \\ \sqrt{n} & si\ n \equiv 1 \mod 4 \\ 0 & si\ n \equiv 2 \mod 4 \\ i\sqrt{n} & si\ n \equiv 3 \mod 4 \end{cases}$$

En appliquant le théorème on obtient:

Lemme 2.4.35. *Soit $L = \langle 2d\rangle$, $d \in \mathbb{Z}\backslash\{0\}$, alors $\gamma(L) = e^{\frac{1}{4}i\pi\,\mathrm{sgn}(d)}$ où* $\mathrm{sgn}(d)$ *dénote le signe de d.*

Démonstration. On suppose $d > 0$. On a $A_L \simeq \frac{\mathbb{Z}}{2d\mathbb{Z}}$ engendré par un élément x d'ordre $2d$, $q_L(x) = \frac{1}{2d}$, donc:

$$\begin{aligned}\sqrt{2d}\gamma(L) &= \sum_{0\le x\le 2d-1} e^{i\pi\frac{x^2}{2d}} \\ &= \sum_{0\le x\le 2d-1} e^{2i\pi\frac{x^2}{4d}}\end{aligned}$$

Pour $2d \leq x \leq 4d-1$ on a:

$$\begin{aligned}\sum_{2d\leq x\leq 4d-1} e^{2i\pi\frac{x^2}{4d}} &= \sum_{0\leq x\leq 2d-1} e^{2i\pi\frac{(x+2d)^2}{4d}} \\ &= \sum_{0\leq x\leq 2d-1} e^{2i\pi\frac{x^2+4d+4dx}{4d}} \\ &= \sum_{0\leq x\leq 2d-1} e^{2i\pi\frac{x^2}{4d}} \\ &= \sqrt{2d}\gamma(L)\end{aligned}$$

En composant les deux résultats on a:

$$\begin{aligned}G(4d) &= \sum_{0\leq x\leq 4d-1} e^{2i\pi\frac{x^2}{4d}} \\ &= \sum_{0\leq x\leq 2d-1} e^{2i\pi\frac{x^2}{4d}} + \sum_{0\leq x\leq 2d-1} e^{2i\pi\frac{x^2}{4d}} \\ &= 2\sqrt{2d}\gamma(L)\end{aligned}$$

On remplace $G(4d) = (1+i)\sqrt{4d}$ et on obtient:

$$\begin{aligned}\gamma(L) &= \frac{1}{2\sqrt{2d}}(1+i)\sqrt{4d} \\ &= \frac{1+i}{\sqrt{2}} \\ &= e^{\frac{1}{4}i\pi}\end{aligned}$$

Si $d<0$, alors $\langle 2d\rangle = \langle |2d|\rangle(-1)$ et par l'Exemple 2.4.33 on a:

$$\gamma(\langle 2d\rangle) = \overline{e^{\frac{1}{4}i\pi}} = e^{-\frac{1}{4}i\pi}$$

□

On est finalement prêts pour démontrer:

Théorème 2.4.36 (Milgram)**.** *Soit L un réseau pair de signature (s^+, s^-), $s = s^+ - s^-$ alors:*

$$\gamma(L) = e^{\frac{1}{4}i\pi s}$$

Démonstration. Par l'Exemple 2.3.77 il existe $L' \subseteq L$ un sous-réseau du même rang qui se décompose comme somme orthogonale de réseaux de rang 1, $L' \simeq \langle a_1\rangle \oplus \cdots \oplus \langle a_r\rangle$ avec $r = s^+ + s^-$, donc par le Corollaire 2.4.32 et la fonctorialité de γ on a:

$$\gamma(L) = \gamma(L') = \gamma(\langle a_1\rangle)\cdot\cdots\cdot\gamma(\langle a_r\rangle)$$

Donc par le résultat précédent:

$$\begin{aligned}\gamma(L) &= \prod_{k=1}^{r} e^{\frac{1}{4}i\pi\,\mathrm{sgn}(a_k)} \\ &= e^{\frac{1}{4}i\pi(\mathrm{sgn}(a_1)+\cdots+\mathrm{sgn}(a_r))} \\ &= e^{\frac{1}{4}i\pi\left(s^+-s^-\right)}\end{aligned}$$

□

On a montré que si L est un réseau pair, alors $\gamma(q_L) = \omega^n$ pour un certain n, avec $\omega = e^{\frac{1}{4}i\pi}$. Comme toutes les f.f. quadratiques sont réalisées par un certain réseau (on verra cela dans la section suivante), on a que toutes les f.f. quadratiques vérifient cette propriété.

On peut donc définir la *signature* d'une f.f. quadratique q comme le plus petit entier positif n tel que $\gamma(q) = \omega^n$. Sinon, de façon équivalente, si L est un réseau pair de signature (s^+, s^-) tel que $q_L = q$, on peut donner comme définition:

$$\mathrm{sign}(q) \equiv s^+ - s^- \pmod 8$$

Remarque 2.4.37. Par le théorème de Milgram, la signature exprime un critère d'existence pour les réseaux avec forme quadratique donnée et il peut donc être utile de reporter les valeurs de la signature pour les f.f. quadratiques indécomposables (Tableau 2.4.1).

Exemple 2.4.38 (Réseaux unimodulaire pairs)**.** Soit L un réseau pair unimodulaire de signature (s^+, s^-), alors q_L est triviale et donc $\gamma(L) = 1$. Par le théorème de Milgram cela implique que:

$$s^+ - s^- \equiv 0 \pmod 8$$

C'est la seule condition d'existence nécessaire, car on sait déjà que E_8 est unimodulaire pair de signature $(8, 0)$ (donc $E_8(-1)$ a signature $(0, 8)$) et U a signature $(1, 1)$. Donc pour n'importe quel choix de (s^+, s^-) tel que $8|(s^+ - s^-)$ on peut trouver i,j,k tels que $L = E_8^{\oplus i} \oplus E_8(-1)^{\oplus j} \oplus U^{\oplus k}$ soit unimodulaire de signature (s^+, s^-). Par contre, comme on verra dans l'Exemple 2.4.49, tous les réseaux unimodulaires ne sont pas de cette forme.

On rappelle que dans le cas impair on a une correspondance parfaite entre forme f.f. bilinéaire et f.f. quadratique (cf. Section 2.3.3). Dans le cas pair, pour passer de la f.f. bilinéaire à la f.f. quadratique on nécessite de la signature [Nik, 1.11.3]:

Proposition 2.4.39. *Deux f.f. quadratiques q_1 et q_2 sont isomorphes si et seulement si:*

- *Les f.f. bilinéaires associées sont isomorphes ;*
- $\mathrm{sign}(q_1) \equiv \mathrm{sign}(q_2) \pmod 8$

A	q	$\text{sign}(q) \pmod 8$
$\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, n impair	$w_{p,k}^1$	$3(p-1)$
$\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, n impair	$w_{p,k}^{-1}$	$3(p-1)+4$
$\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, n pair	$w_{p,n}^1$	0
$\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, n pair	$w_{p,n}^{-1}$	0
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$	$w_{2,n}^1$	1
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$	$w_{2,n}^3$	$3+4n$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$w_{2,n}^5$	$5+4n$
$\frac{\mathbb{Z}}{2^n\mathbb{Z}}$, $n \geq 2$	$w_{2,n}^7$	7
$\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^n\mathbb{Z}}$	u_n	0
$\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^n\mathbb{Z}}$	v_n	$4n$

TABLE 2.4.1 – Signature des f.f. quadratiques indécomposables

2.4.3 Théorème d'existence de Nikulin

En résumant les résultats de cette section on obtient les conditions nécessaires d'existence pour un réseau suivantes:

Proposition 2.4.40. *Soit L un réseau pair avec signature (s^+, s^-), rang $r = s^+ + s^-$ et forme discriminante q_L sur A_L. On pose A_p la p-part de A_L, alors:*

1. $r \geq l(A_L)$;
2. $s^+ - s^- \equiv \text{sign}(q_L) \pmod 8$;
3. *Pour tout p premier, si* $\text{rang}(L) = l(A_p)$ *alors* $\text{disc}(q_p) = \det(L)^{-1} = \frac{(-1)^{s^-}}{\#A_L}$.

Démonstration. 1) est clair car A_L est engendré par les r vecteurs de la base de L^*, 2) est donné par le Théorème de Milgram. Pour montrer 3) on a que $\text{disc}(L_p) = \det(L) = (-1)^{s^-}\#A_L$ donc pour p impair c'est une conséquence de 2.4.14 sinon de la Remarque 2.4.15. □

Remarque 2.4.41. Soit p premier, $\#A_L = p^a m$ avec $p \nmid m$, alors relativement au calcul du discriminant on a:

$$\begin{aligned}
\frac{(-1)^{s^-}}{\#A_L} &= \frac{(-1)^{s^-}}{p^a}\frac{1}{m} \\
&\equiv \frac{(-1)^{s^-}}{p^a}\frac{m^2}{m} \pmod{\left\{\text{carrés inversibles dans } \tfrac{\mathbb{Z}}{p^a\mathbb{Z}}\right\}} \\
&\equiv \frac{(-1)^{s^-}m}{p^a} \pmod{\left\{\text{carrés inversibles dans } \tfrac{\mathbb{Z}}{p^a\mathbb{Z}}\right\}}
\end{aligned}$$

ce qui est une écriture plus claire.

On va donner une application de ces critères, qui nous sera utile dans l'étude des involutions [Nik]:

Proposition 2.4.42 (Classification des réseaux 2-élémentaires)**.** *Soit* $A_2 \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^a$, q_2 *une f.f. quadratique sur* A_2 *et* $s^-, s^+ \in \mathbb{N}$. *On pose* $\delta_q = 0$ *si* q_2 *n'a pas d'éléments de carré* $\pm\frac{1}{2}$ *et* $\delta_q = 1$ *sinon,* $s = s^+ - s^-$ *et* $r = s^+ + s^-$. *Alors il existe un réseau* L *avec* $q_L = q_2$ *et signature* (s^+, s^-) *si et seulement si les conditions suivantes sont satisfaites:*

1 $a \leq r$ *;*

2 $r \equiv a \pmod 2$ *;*

3 $s \equiv 0 \pmod 4$ *si* $\delta_q = 0$ *;*

4 $\delta_q = 0$, $s \equiv 0 \pmod 8$ *si* $a = 0$ *;*

5 $s \equiv 0 \pmod 8$ *si* $\delta_q = 0$ *et* $a = r$ *;*

6 $s \equiv \pm 1 \pmod 8$ *si* $a = 1$ *;*

7 $\delta = 0$ *si* $a = 2$ *et* $s \equiv 4 \pmod 8$.

Démonstration. On peut montrer que les conditions 1-7 sont équivalentes aux conditions 1-3 de la Proposition 2.4.40. On rédige ici un seul sens de l'implication, laissant l'autre comme exercice pour le lecteur:

Conditions nécessaires:

1 C'est équivalent à demander $\text{rang}(L) \geq l(A_2) = a$;

2 On a $\text{sign}(w_{2,1}^{\epsilon}) \equiv 1 \pmod 2$ et $\text{sign}(u_1) \equiv \text{sign}(v_1) \equiv 0 \pmod 2$, ce qui implique que $\text{sign}(q_2) \equiv a \pmod 2$. Comme $\text{rang}(L) \equiv s \pmod 2$ on conclut grâce à Milgram ;

3 Si $\delta = 0$ alors $q_2 = u_1^{\oplus a-\epsilon} \oplus v_1^{\oplus \epsilon}$ avec $\epsilon \in \{0, 1\}$, donc $\text{sign}(q_2) \equiv 4\epsilon \equiv 0 \pmod 4$;

4 Si $a = 0$ alors L est unimodulaire et on applique l'Exemple 2.4.38 ;

5 Si $q_2 = u_1^{\oplus a-\epsilon} \oplus v_1^{\oplus \epsilon}$ alors $\text{disc}(q_2) = 3^{\epsilon}(-1)^{a-\epsilon}/2^a$, donc si $a = r$ comme $\text{disc}(q_L) = \frac{(-1)^{s^-}}{\#A_L}$ on a $\epsilon = 0$, ce qui implique $s \equiv \text{sign}(q_2) \equiv 0 \pmod 8$;

6 Si $a = 1$ alors $q_2 = w_{2,1}^{\epsilon}$ donc $s \equiv \text{sign}(w^{\epsilon}) \equiv \pm 1 \pmod 8$;

7 Si $a = 2$ alors les possibilités pour q_2 sont: $q_2 = \left(w_{2,1}^1\right)^{\oplus 2}$ et $s \equiv 2 \pmod 8$, $q_2 = w_{2,1}^1 \oplus w_{2,1}^3$ et $s \equiv 0 \pmod 8$, $q_2 = \left(w_{2,1}^3\right)^{\oplus 2}$ et $s \equiv 6 \pmod 8$ ou sinon $\delta_q = 0$.

Ensuite on a deux façons de procéder, dont on énonce les idées dans les grandes lignes: soit exhiber des exemples explicites de L qui satisfont les conditions données, en prenant des sommes de U, $U(2)$, $E_8(\pm 1)$, $E_8(\pm 2)$, $D_4(\pm 1)$, $D_6(\pm 1)$, $E_7(\pm 1)$,$D_8(\pm 1)$ (la seule exception est pour $\delta_q = 0$, $a = 6$, $r = s^+ = 8$ où la seule possibilité est donnée par le réseau $D_8^*(2)$ (appelé *réseau de Nikulin*) qui n'est peut pas être écrit sous cette forme)), sinon on peut montrer le résultat en utilisant le Théorème 2.4.44.

□

Remarque 2.4.43. Il est possible de remplacer le critère sur le déterminant par une version plus faible, pour $p = 2$. Si A_i est un groupe fini de cardinalité m impaire, q_i une forme quadratique sur A_i, alors en regardant les différents possibilités pour la signature dans le Tableau 2.4.1 on vérifie facilement que:

$$\mathrm{sign}(q_i) \equiv \begin{cases} 0 \pmod 4 & \text{si } \#A_i \equiv 1 \pmod 4 \\ 2 \pmod 4 & \text{si } \#A_i \equiv 3 \pmod 4 \end{cases}$$

Si A_2 est un 2-groupe de cardinalité 2^N et $l = l(A_2)$, q_2 une forme quadratique sur A_2, en regardant les différents possibilités dans les Tableaux 2.4.1 et 2.3.2 on trouve aussi que:

$$\mathrm{sign}(q_2) \equiv \begin{cases} l \pmod 4 & \text{si } \mathrm{disc}(q_2) \in \{2^{-N}, 5 \cdot 2^{-N}\} \\ l+2 \pmod 4 & \text{si } \mathrm{disc}(q_2) \in \{3 \cdot 2^{-N}, 7 \cdot 2^{-N}\} \end{cases}$$

Soit donc L un réseau pair de rang r, $q_L = q_i \oplus q_2$, signature (s^+, s^-) avec $s \equiv s^+ - s^- \pmod 4$. Dans le cas $r = l(A_2) = l$ on a $s^- \equiv (l-s)/2 \pmod 2$ donc en remplaçant on trouve une redondance entre le critère relatif à la signature ($s \equiv \mathrm{sign}(q_i) + \mathrm{sign}(q_2)$) et celui sur le discriminant pour $p = 2$ ($(-1)^{s^-} 2^{-N} \#A_i = \mathrm{disc}(q_2)$). Plus précisément, en vérifiant les différents cas possibles, on trouve que si la condition sur la signature est respectée modulo 4, alors la condition sur la signature est aussi respectée « modulo 4 ».

Dans le détail, si $\delta_q = 1$ la condition sur la signature implique complètement la condition sur le discriminant, sinon si $\delta_q = 0$ il est suffisant de vérifier que $\mathrm{disc}(q_2) = \frac{\pm 1}{\#A_L}$.

Ces conditions d'existence nécessaires se révèlent être aussi des conditions suffisantes. L'idée principale de la preuve (qu'on ne rédige pas, mais que l'on trouve dans [Nik, 1.10.1] ou [MM, VI.5.2]) est de montrer d'abord que pour tous p il existe des $\mathbb{Z}_p$-réseaux L_p avec $q_{L_p} = q_p$, et ensuite, utiliser le Théorème de Hasse-Minkowski pour montrer que si les conditions sur les discriminants et la signature sont respectées, alors on peut choisir les L_p de façon à ce qu'il existe un réseau L avec $L \otimes \mathbb{Z}_p = L_p$.

Si de plus, on tient compte de l'équivalence des critères sur le discriminant et la signature qu'on a vu dans la Remarque 2.4.43 on obtient:

Théorème 2.4.44 (Nikulin)**.** *Soit q une forme quadratique sur un groupe fini A, alors il existe un réseau pair L avec signature (s^+, s^-), rang $r = s^+ + s^-$ tel que $q_L = q$ si et seulement si:*

1. $r \geq l(A)$;
2. $s^+ - s^- \equiv \mathrm{sign}(q) \pmod 8$;
3. *Pour tout p impair, si* $\mathrm{rang}(L) = l(A_p)$ *alors* $\mathrm{disc}(q_p) = \frac{(-1)^{s^-} m}{p^a}$ *avec* $\#A_L = p^a m$, $p \nmid m$;
4. *Si* $\mathrm{rang}(L) = l(A_2)$ *et* $\delta_q = 0$ *alors* $\mathrm{disc}(q_2) = \frac{\pm 1}{2^a}$ *avec* $\#A_L = 2^a m$, $2 \nmid m$;.

Comme $l(A_p) \leq l(A)$ on a immédiatement:

Corollaire 2.4.45. *Soit q une forme quadratique sur un groupe fini A, $s^+, s^- \in \mathbb{N}$, alors si:*

1 $r = s^+ + s^- > l(A)$ *;*

2 $s^+ - s^- \equiv \text{sign}(q) \pmod 8$ *;*

il existe un réseau pair L avec signature (s^+, s^-) et $q_L = q$.

En particulier tout f.f. quadratique est réalisée par un certain réseau pair.

On voit dans la suite deux exemples d'applications du théorème de Nikulin, qu'on utilisera dans la section 2.5.1 pour donner une preuve originale de deux résultats classiques: les théorèmes des trois et des quatre carrés.

Exemple 2.4.46. Soit $A = \mathbb{Z}/m\mathbb{Z}$, $b = \left(-\frac{1}{m}\right)$, est-ce qu'il existe toujours un réseau L de signature $(2,0)$, pair ou impair, qui réalise b ?

- On suppose d'abord que m est impair et on pose $b/2$ la f.f. sur A définie comme $(b/2)(x,y) = b(x,y)/2$ et $q = b/2 \oplus q_2$ avec q_2 une forme quadratique sur $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$. Par le Lemme 2.3.23 $2 \cdot q = b$ et il existe un réseau L qui réalise b avec les conditions donnés si et seulement si il existe un réseau L' qui réalise q (donc L' est forcement pair) de signature $(2,0)$ tel que $L(2) \simeq L'$

On veut donc appliquer les hypothèses du Théorème 2.4.44 à q et on a donc besoin de la signature de $b/2$: pour la calculer on considère le réseau $\langle -2m \rangle$, on a $q_{\langle -2m \rangle} = b/2 \oplus w_{2,1}^{\epsilon}$ avec $\epsilon \equiv -m \pmod 4$ et vu que $\text{sign}(\langle -2m \rangle) = -1$ on a:

$$\text{sign}(b/2) = \begin{cases} 0 & \text{si } m \equiv 1 \pmod 4 \\ -2 & \text{si } m \equiv 3 \pmod 4 \end{cases}$$

Dans le premier cas, si $\text{sign}(b/2) = 0$ pour $q_2 = \left(w_{2,1}^1\right)^{\oplus 2}$ on a $\text{sign}(q) = 2$, $\delta_q = 1$ et L' existe (et donc L aussi). Sinon dans le deuxième cas la signature impose $q_2 = v_1$, donc $\delta_q = 0$ et il faut vérifier l'hypothèse sur le discriminant, selon laquelle L' existe si et seulement si $m \equiv 3 \pmod 8$.

- Si $m = 2m'$ avec m' impair, alors $A \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m'\mathbb{Z}}$, donc $b = \overline{w}_{2,1}^1 \oplus b_i$ avec $b_2 = b_{|\frac{\mathbb{Z}}{2\mathbb{Z}}}$ et $b_i = b_{|\frac{\mathbb{Z}}{m'\mathbb{Z}}}$. Maintenant soit $q = b_i/2 \oplus w_{2,1}^1 \oplus w_{2,2}^{\epsilon}$, alors comme $b_i/2$ est une forme quadratique sur un groupe de cardinalité impaire, on a que $\text{sign}(b_i/2) \equiv 0 \pmod 2$ (cf. Remarque 2.4.43), donc il existe $\epsilon \in \{1,3,5,7\}$ tel que $\text{sign}(q) = 2$ et comme $\delta_q = 0$ on a qu'il existe toujours L' de signature $(2,0)$ qui réalise q et donc b aussi est toujours réalisée par un réseau de signature $(2,0)$.

- Si $4 \mid m$ alors $A \simeq \frac{\mathbb{Z}}{2^n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m'\mathbb{Z}}$ avec $n \geq 2$ et on a à nouveau $b = b_2 \oplus b_i$. Maintenant, comme b_i est une forme sur un groupe de cardinalité impaire, on a que $b_i/2$ est bien définie de façon unique, par contre, si $n = 2$, on a deux possibilités pour $q_2 = b_2/2$, forme quadratique sur $\frac{\mathbb{Z}}{2^{n+1}\mathbb{Z}}$: en effet

$2w^1_{2,3} = 2w^5_{2,3} = \overline{w}^1_{2,2}$ et de la même façon $2w^3_{2,3} = 2w^7_{2,3} = \overline{w}^3_{2,2}$: par contre dans tous les cas, indépendemment de la façon dont on « relève » b_2, on aura que la signature de q_2 sera déterminée de façon unique, car $\mathrm{sign}(w^1_{2,3}) = \mathrm{sign}(w^5_{2,3}) = 1$ et $\mathrm{sign}(w^3_{2,3}) = \mathrm{sign}(w^7_{2,3}) = 7$. Si $n \geq 3$, alors $q_2 = b_2/2$ est déterminée de façon unique (et sa signature aussi). Soit $q' = b_i/2 \oplus w^\epsilon_{2,n}$ avec ϵ tel que $2q' = b$, comme la signature de q' est donnée par la relation $2q' = b$ on aura que $\mathrm{sign}(q') = \mathrm{sign}(q_{\langle -2m \rangle}) = -1$ (car $2q_{\langle -2m \rangle} = b$ aussi), donc $\mathrm{sign}(q' \oplus w^\epsilon_{2,1}) \in \{0, -2\}$, donc il n'existe pas de réseau L' de signature $(2,0)$ avec $q_{|L'} = q' \oplus w^\epsilon_{2,1}$ et donc pas de réseau L non plus.

En résumant on a prouvé que $b = \left(-\frac{1}{m}\right)$ est réalisée par un réseau L de signature $(2,0)$ uniquement dans les cas suivants:

1 m impair et $m \not\equiv 7 \pmod 8$;

2 $m = 2m'$ avec m' impair

Exemple 2.4.47. On pose à nouveau la question précédente pour la dimension 3, donc soit $A = \mathbb{Z}/m\mathbb{Z}$, $b = \left(-\frac{1}{m}\right)$, est-ce qu'il existe toujours un réseau L de signature $(3,0)$, pair ou impair, qui réalise b ?

- Si m impair, en suivant la notation de l'Exemple 2.4.46, on considère $q = b/2 \oplus q_2$ avec q_2 une forme quadratique sur $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$, mais toute f.f. quadratique définie sur un groupe de cardinalité impair a signature pair (on peut voir cela comme une conséquence du Lemme 2.2.47 ou sinon en regardant le Tableau 2.4.1) donc $\mathrm{sign}(b/2) \equiv 0 \pmod 2$ et on peut donc toujours choisir q_2 de façon à ce que $\delta_{q_2} = 1$ et $\mathrm{sign}(q_2) + \mathrm{sign}(b/2) \equiv \pmod 8$;

- Si $m = 2m'$ avec m' impair, par l'Exemple 2.4.46 il existe L' de dimension deux avec $b_{L'} = \left(-\frac{1}{m}\right)$, donc il suffit de prendre $L' \oplus \langle 1 \rangle$;

- Si $m = 2^n m'$ avec m' impair et $n \geq 2$ alors comme dans l'exemple précédent si $2q' = b$ alors $\mathrm{sign}(q') = \mathrm{sign}(\langle -2m \rangle) = -1$, donc la seule possibilité pour avoir $\mathrm{sign}(q) \equiv 3 \pmod 8$ est de choisir $q = q' \oplus v_1$. Par contre $\delta_q = 0$ et si $n \geq 3$ le critère sur le discriminant n'est pas vérifié, car:

$$\begin{aligned} \mathrm{disc}(q) &= 3\,\mathrm{disc}(q') \\ &= 3 \cdot (-m')2^{-n-3} \\ &= 5m'2^{-n-3} \neq m'2^{-n-3}\frac{1}{\#A} \end{aligned}$$

Par contre si $n = 2$, comme on a deux alternatives dans le « relèvement » de la forme bilinéaire, on peut montrer que l'on peut choisir q de façon à respecter le critère sur le discriminant.

Donc $b = \left(-\frac{1}{m}\right)$ est réalisée par un réseau L de signature $(3,0)$ si et seulement si $8 \nmid m$.

2.4.4 Critères d'unicité

On a beaucoup parlé du genre d'un réseau et on a répondu à la question sur l'existence des réseaux avec genre assigné. Par contre le même genre

pourrait être réalisé par plusieurs réseaux de même signature mais pas isomorphes.

On dira qu'un réseau L est *unique en son genre* si pour tout réseau L' de mêmes signature, parité et genre de L on a $L \simeq L'$.

Exemple 2.4.48. Soient $L_1 \simeq \langle 1 \rangle \oplus \langle 14 \rangle$, $L_2 \simeq \langle 2 \rangle \oplus \langle 7 \rangle$ alors on vérifie facilement que $b_{L_1} \simeq b_{L_2}$ et comme ce sont deux réseaux impairs de même signature alors L_1 et L_2 ont le même genre. Par contre, par l'unicité de la décomposition, on a $L_1 \not\simeq L_2$.

Cela implique d'ailleurs que $L_1(2)$ et $L_2(2)$ constituent un exemple de réseaux pairs non isomorphes avec le même genre.

Exemple 2.4.49. On a vu dans l'Exemple 2.3.72 que D_{16}^+ est un réseau unimodulaire pair, donc du même genre que $(E_8)^{\oplus 2}$, car ils partagent la même signature et la même forme discriminante quadratique : sont-ils isomorphes ?

La réponse est non, car il existe $\Pi \subset D_{16}$ système de racines connexes qui engendre D_{16}, mais D_{16}^+ est pair, donc les racines sont des éléments indécomposables de D_{16}^+: comme $\mathrm{span}_{\mathbb{Q}}(\Pi) = \mathrm{span}_{\mathbb{Q}}(D_{16}) \supseteq D_{16}^+$ alors par le Corollaire 2.2.35 D_{16}^+ est un réseau indécomposable, contrairement à $(E_8)^{\oplus 2}$.

Exemple 2.4.50. Soit L un réseau unimodulaire euclidien de rang $r \leq 4$, est-il unique en son genre ? La réponse est oui: par le Théorème de Minkowski il existe $v \in L$ avec $v^2 = 1$. En itérant, en appliquant l'Exemple 2.2.40, on obtient alors $L \simeq \langle 1 \rangle^{\oplus r}$, donc $\langle 1 \rangle^{\oplus r}$ est le seul réseau unimodulaire euclidien de rang $r \leq 4$.

Exemple 2.4.51 (Unicité de U)**.** Soit L un réseau unimodulaire pair de signature $(1,1)$ avec matrice de Gram:

$$\begin{pmatrix} a & c \\ c & b \end{pmatrix}$$

Comme $\det(M) = ab - c^2 = -1$ on a que $v = (b, -c+1)$ vérifie $\langle v, v \rangle = 0$. Soit donc $x_1 \in \mathrm{span}(v)$ un vecteur primitif et x_2 un complément à une base de L, alors la matrice de Gram dans la base (x_1, x_2) est:

$$M = \begin{pmatrix} 0 & \alpha \\ \alpha & \beta \end{pmatrix}$$

Comme $\det(M) = -1$ on a $\alpha = 1$ (quitte à remplacer x_2 par $-x_2$). Si on choisit $x_2' = x_2 - \frac{\beta}{2} x_1$ (β est pair car L est pair) on a que x_1, x_2' définissent une isométrie entre L et U.

Le résultat suivant nous donne un critère suffisant (pour les seuls réseaux pairs indéfinis) pour établir si un réseau est unique en son genre [Nik, 1.13.2]:

Proposition 2.4.52. *Soit L un réseau pair indéfini qui satisfait les conditions suivantes:*

1 $\mathrm{rang}(L) \geq 3$ *;*

2 Pour tous $p \neq 2$*, au moins l'une des conditions suivantes est satisfaite:*

(a) $\mathrm{rang}(L) \geq l(A_p) + 2$ *;*

(b) il existe k *tel que:*

$$A_p \simeq \left(\frac{\mathbb{Z}}{p^k\mathbb{Z}}\right)^2 \oplus A_p^{'}$$

3 Pour $p = 2$*, au moins l'une des conditions suivantes est satisfaite:*

(a) $\mathrm{rang}(L) \geq l(A_2) + 2$ *;*

(b) il existe k *tel que* $q_2 \simeq u_k \oplus q_2'$ *;*

(c) il existe k *tel que* $q_2 \simeq v_k \oplus q_2'$

(d) il existe k *tel que* $q_2 \simeq w_{2,k}^{\epsilon_1} \oplus w_{2,k+1}^{\epsilon_2} \oplus q_2'$

alors L *est unique en son genre.*

Corollaire 2.4.53. *Soit* L *un réseau pair indéfini avec* $\mathrm{rang}(L) \geq l(A_L)+2$*, alors* L *est unique en son genre.*

Corollaire 2.4.54. *Soient* $s^+, s^- \in \mathbb{N}$*,* $s^+, s^- \geq 1$*,* $s^+ - s^- \equiv 0 \pmod 8$*, alors il existe un et un seul réseau pair unimodulaire de signature* (s^+, s^-)*.*

Démonstration. L'Exemple 2.4.38 nous donne le critère d'existence, il reste donc à montrer l'unicité. Soit L unimodulaire pair de rang $r = s^+ + s^-$ comme dans l'énoncé du Corollaire, si $r \leq 3$ la seule possibilité est $s^+ = s^- = 1$ et dans ce cas $L = U$ par l'Exemple 2.4.51, sinon si $r \geq 3$ alors L satisfait les hypothèses de la Proposition 2.4.52 car $l(A_p) = 0$ pour tout p premier et donc on a l'unicité. □

On a aussi que E_8 est le seul réseau unimodulaire pair de signature $(8, 0)$ ([Mor] ou [Gr] pour une preuve plus élémentaire). On en donnera aussi une preuve dans l'Exemple 2.5.10.

Remarque 2.4.55. On peut appliquer le critère d'unicité au cas des réseaux 2-élémentaires vu dans la Proposition 2.4.42.

Soit L un réseau 2-élémentaire pair indéfini, $A_L \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^a$, alors L est unique en son genre. En effet par la Proposition 2.4.42 on a $a \equiv \mathrm{rang}(L) \pmod 2$, donc soit $l(A_L)+2 \leq \mathrm{rang}(L)$ et dans ce cas l'unicité de L découle de la Proposition 2.4.52, soit $\mathrm{rang}(L) = l(A_L)$. Mais dans ce dernier cas par l'Exemple 2.3.10 $L(1/2)$ est unimodulaire et donc unique.

Comme corollaire des critères d'existence et unicité on a:

Lemme 2.4.56 (Scission)**.** *Soit* L *un réseau pair indéfini de signature* (s^+, s^-)*:*

1 Si $\mathrm{rang}(L) \geq 3 + l(A_L)$ *alors* $L \simeq U \oplus L'$ *pour un certain réseau* L' *;*

2 Si $s^+ \geq 8$ *et* $\mathrm{rang}(L) \geq 9 + l(A_L)$ *alors* $L \simeq E_8 \oplus L'$ *pour un certain réseau* L' *;*

Démonstration. 1) Par le Corollaire 2.4.45 il existe un réseau L' de signature $(s^+ - 1, s^- - 1)$ avec $q_{L'} = q_L$ et par le Corollaire 2.4.53 $L' \oplus U$ est le seul en son genre, donc $L \simeq U \oplus L'$. De la même façon on montre 2). □

Par contre, dans le cas des réseaux définis on a un résultat opposé [Wa]:

Théorème 2.4.57. *Si* L *est un réseau défini avec* $\mathrm{rang}(L) \geq 11$*, alors il existe toujours au moins deux réseaux non isomorphes dans la classe du genre de* L*.*

Ce résultat nous aide à comprendre les différents comportements des réseaux définis et indéfinis: les premiers doivent être étudiés dans leur « globalité », par exemple ils admettent une décomposition unique et le genre (qui est un invariant local) n'est pas suffisant à en donner une classification. Au contraire les réseaux indéfinis doivent être étudiés « localement » en prenant le genre (ou le « genre spinorial » dont on n'a pas pu parler dans ces notes, mais que le lecteur intéressé peut trouver dans [MM]).

On conclut avec le résultat suivant, qu'on prouvera dans l'Exemple 2.5.6:

Lemme 2.4.58. *Pour tout* $d \in \mathbb{Z}\backslash\{0\}$*,* $r \in \mathbb{N}\backslash\{0\}$ *il existe au plus un nombre fini de réseaux (non isomorphes entre eux) avec déterminant égal à* d *et rang* r*.*

En particulier, pour un choix du genre, il existe au plus un nombre fini de réseaux qui le réalisent.

2.5 Isométries d'un réseau

2.5.1 Extensions primitives

Une méthode efficace pour construire des nouveaux réseaux à partir d'une liste $L_1, \ldots, L_n$ de réseaux donnée, est de chercher des sur-réseaux de $L = L_1 \oplus \cdots \oplus L_n$: en général on appelle cette opération *collage de réseaux.* Dans le cas où les L_i sont des sous-réseaux primitifs de L (i.e. L/L_i sans torsion) on parle d*'extension primitive.*

Soit donc $R \supseteq L_1 \oplus \cdots \oplus L_n$ un sur-réseau, alors $H_R = R/L \subseteq A_{L_1} \oplus \cdots \oplus A_{L_n}$, soit donc $\pi_i : H_R \to A_{L_i}$ la projection de H_R sur l'i-ème groupe discriminant, alors pour tout $x \in H_R$ on écrit:

$$x = \pi_1(x) + \cdots + \pi_n(x)$$

comme $L_i \subseteq R$ est un sous-réseau primitif, $L_i \otimes \mathbb{Q} \cap R = L_i^* \cap R = L_i$. On quotiente par L pour obtenir:

Lemme 2.5.1. *Soit $R \supseteq L_1 \oplus \cdots \oplus L_n$ une extension de réseaux, alors:*

$$L_i \subseteq R \text{ primitif si et seulement si } A_{L_i} \cap H_R = \{0\}$$

donc il n'existe pas $x \in H_R$ tel que $\pi_i(x) \neq 0$ et $\pi_j(x) = 0$ pour tout $j \neq i$.

En particulier, si $n = 2$, cela implique que $\pi_i(x) \neq 0$ pour tout $x \in H_R \backslash \{0\}$, donc si $H_{R,L_i} := \mathrm{Im}(\pi_i)$:

$$\begin{aligned} \pi_1 : H_R &\rightarrow H_{R,L_1} \subseteq A_{L_1} \\ \pi_2 : H_R &\rightarrow H_{R,L_2} \subseteq A_{L_2} \end{aligned}$$

décrivent une injection. On peut alors construire l'isomorphisme de groupes:

$$\gamma = \pi_2 \circ \pi_1^{-1} : H_{R,L_1} \xrightarrow{\simeq} H_{R,L_2}$$

pour $x, y \in H_{R,L_1}$, comme H_R est totalement isotrope on a $b(x + \gamma(x), y + \gamma(y)) = 0$. Vu que $A_{L_1} \perp A_{L_2}$ on a aussi:

$$\begin{aligned} 0 &= b(x + \gamma(x), y + \gamma(y)) \\ &= b(x, y) + b(x, \gamma(y)) + b(\gamma(x), y) + b(\gamma(x), \gamma(y)) \\ &= b_{L_1}(x, y) + b_{L_2}(\gamma(x), \gamma(y)) \end{aligned}$$

Donc $b_{L_1}(x, y) = -b_{L_2}(\gamma(x), \gamma(y))$ [dans le cas des réseaux pairs, $q_{L_1}(x) = -q_{L_2}(\gamma(x))$].

Donc γ est une *anti-isométrie*, dans le sens où elle décrit une isométrie entre $b_{L_1|H_{R,L_1}}$ et $-b_{L_2|H_{R,L_2}}$.

On a montré [Nik]:

Proposition 2.5.2. *Soit R une extension primitive de $L_1 \oplus L_2$, alors R est déterminée de façon unique par les couples (H_R, γ) avec $H_R \simeq H_{R,L_1} \subseteq A_{L_1}$ et $\gamma : H_{R,L_1} \hookrightarrow A_{L_2}$ anti-isométrie entre $b_{L_1|H_{R,L_1}}$ et $b_{L_2|\gamma(H_{R,L_1})}$ [ou entre $q_{L_1|H_{R,L_1}}$ et $q_{L_2|\gamma(H_{R,L_2})}$ dans le cas pair].*

Corollaire 2.5.3. *Soit R une extension primitive de $L_1 \oplus L_2$, alors:*

$$\#A_R = \frac{\#A_{L_1} \#A_{L_2}}{(\#H_R)^2}$$

Démonstration. Par le Lemme 2.3.78 on a $\#A_R = (\#A_{L_1} \#A_{L_2}) / (\#H_R)^2$ □

Corollaire 2.5.4. *Soit R une extension primitive de $L_1 \oplus L_2$, R unimodulaire. Alors R est déterminée de façon unique par les isométries $\gamma : b_{L_1} \rightarrow -b_{L_2}$ [ou entre q_{L_1} et q_{L_2} dans le cas pair].*

En particulier $A_{L_1} \simeq A_{L_2} \simeq H_R$ et $b_{L_1} \simeq -b_{L_2}$ [$q_{L_1} \simeq -q_{L_2}$].

Démonstration. Si R est unimodulaire en appliquant le Corollaire 2.5.3 on obtient:

$$\begin{aligned} 1 &= \#A_R \\ &= \#A_{L_1}\#A_{L_1}/\#(H_R)^2 \end{aligned}$$

mais $H_R \hookrightarrow A_{L_1}$ et $H_R \hookrightarrow A_{L_2}$ donc $\#H_R \leq \#A_{L_1}$, $\#H_R \leq \#A_{L_2}$ ce qui implique $\#H_R = \#A_{L_1} = \#A_{L_2}$ donc $H_R \simeq A_{L_1} \simeq A_{L_2}$ et l'anti-isométrie entre $b_{L_1|H_{R,L_1}}$ et $b_{L_2|H_{R,L_2}}$ est en réalité une anti-isométrie entre b_{L_1} et b_{L_2}. □

Exemple 2.5.5. Soit $L_1 = \langle 2 \rangle$, $R = E_8$, $j : L_1 \hookrightarrow E_8$ un plongement de L_1 dans E_8, alors $j(L_1)$ est forcément un sous-réseau primitif, donc si on pose $L_2 = j(L_1)^\perp$, $R \supseteq L_1 \oplus L_2$ est une extension primitive. Par le résultat précédent $q_{L_1} \simeq -q_{L_2}$, donc $q_{L_2} = w_{2,1}^{-1}$ et la seule possibilité est $L_2 \simeq E_7$ (cf. Tableau 2.5.2). Comme il existe une seule isométrie $\gamma : q_{L_1} \to -q_{L_2}$ on obtient que j est unique modulo une isométrie de E_8.

Exemple 2.5.6. On donne une preuve du Lemme 2.4.58:. Soit L un réseau avec $|\det(L)| = d$, $\mathrm{rang}(L) = r$, on veut montrer qu'on a au plus un nombre fini de choix pour L (modulo les isométries du réseau).

Par les Théorèmes 2.2.10 et 2.2.12, il existe une borne $B(r,d)$ telle qu'il existe $x_1 \in L$ primitif de norme minimale avec $0 < |x_1^2| \leq B(r,d)$, donc $L \supseteq \mathrm{span}(x_1) \oplus x_1^\perp$ est une extension primitive avec:

$$\left|x_1^2 \det(x_1^\perp)\right| = |\det(L)| \, \# \left(\frac{L}{x_1 \oplus x_1^\perp}\right)^2$$

par le Corollaire 2.3.80, mais $\frac{L}{x_1 \oplus x_1^\perp} \hookrightarrow \mathrm{span}(x_1)$, donc $\#\frac{L}{x_1 \oplus x_1^\perp} \leq |x_1^2|$ et en remplaçant on obtient:

$$\left|\det(x_1^\perp)\right| \leq \left|x_1^2 \det(L)\right| \leq B(r,d)d$$

On peut donc répéter l'opération pour $x_2 \in x_1^\perp$ de norme minimale avec $0 < |x_2^2| \leq B_2(r,d) := B(r-1, dB(r,d))$, $L \supseteq \mathrm{span}(x_1) \oplus \mathrm{span}(x_2) \oplus x_1^\perp \cap x_2^\perp$ extension primitive et en itérant on obtient $L \supseteq \mathrm{span}(x_1) \oplus \cdots \oplus \mathrm{span}(x_r)$ avec $x_i^2 \leq B_i(r,d)$ bornes dépendant uniquement de r, d.

Donc L est déterminé par un choix de $H_L \subseteq A_R$ avec $R \simeq \langle \lambda_1 \rangle \oplus \ldots \langle \lambda_r \rangle$, $|\lambda_i| \leq B_i(r,d)$. Comme on a un nombre fini de choix pour les λ_i et pour H_L on obtient un nombre fini de choix pour L.

On propose dans la suite trois résultats très classiques, redémontrés de façon originale en appliquant la théorie des réseaux, qui démontre être un contexte naturel dans lequel répondre aux questions relatives aux formes quadratiques entières.

Exemple 2.5.7 (Théorème des deux carrés)**.** Quelles sont les valeurs $n \in \mathbb{N}$ qu'on peut écrire $n = \alpha^2 + \beta^2$ avec $\alpha, \beta \in \mathbb{Z}$?

On a que $n = \alpha^2 + \beta^2 \neq 0$ si et seulement s'il existe $x = (\alpha, \beta) \in \langle 1 \rangle^{\oplus 2}$ avec $x^2 = n$, quitte à diviser n par des carrés, on peut supposer p.g.c.d.$(\alpha, \beta) = 1$ et donc x vecteur primitif. Dans ce cas $\langle 1 \rangle^{\oplus 2}$ est une extension primitive de $\mathrm{span}(x) \oplus x^\perp \simeq \langle n \rangle \oplus x^\perp$, comme $x^\perp$ a rang 1, signature positive et même groupe discriminant de $\langle n \rangle$ la seule possibilité et $x^\perp \simeq \langle n \rangle$, donc pour la forme discriminante on a:

$$b_{\langle n \rangle} = -b_{\langle n \rangle}$$

De plus, comme $\langle 1 \rangle^{\oplus 2}$ est le seul réseau unimodulaire positif de rang 2, il s'agit aussi d'une condition suffisante. Par la classification des formes bilinéaires finies, $b_{\langle n \rangle} = -b_{\langle n \rangle}$ si et seulement si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ pour tous les p premiers impairs tels que $p \mid n$ et si $4 \nmid n$. On rappelle que -1 est un carré modulo p si et seulement si $p \equiv 1 \pmod 4$, donc il existe une extension primitive $\langle n \rangle^{\oplus 2} \subseteq \langle 1 \rangle^{\oplus 2}$ si et seulement si $n = p_1 \cdot \cdots \cdot p_k$ avec $p_i \equiv 1 \pmod 4$ ou $p_i = 2$.

Il s'ensuit qu'on peut écrire $n = \alpha^2 + \beta^2$ si et seulement si:

$$n = e^2 p_1 \cdot \cdots \cdot p_k$$

avec $e \in \mathbb{Z}$ et $p_i \equiv 1 \pmod 4$ ou $p_i = 2$.

Exemple 2.5.8 (Théorème des trois carrés)**.** Quelles sont les valeurs $n \in \mathbb{N}$ qu'on peut écrire $n = \alpha^2 + \beta^2 + \gamma^2$ avec $\alpha, \beta, \gamma \in \mathbb{Z}$?

En raisonnant comme dans l'exemple précédent, on cherche $n = e^2 m$ avec $\langle m \rangle \oplus L \subseteq \langle 1 \rangle^{\oplus 3}$ extension primitive. Donc L est de signature $(2, 0)$ avec $b_L = -\frac{1}{m}$, et grâce à l'Exemple 2.4.46 on sait qu'un tel L existe si et seulement si:

1 m impair et $m \not\equiv 7 \pmod 8$;

2 $m = 2m'$ avec m' impair

On rappelle que $\langle 1 \rangle^{\oplus 3}$ est le seul réseau unimodulaire positif de rang 3, donc l'existence de L avec les conditions données assure l'existence de l'extension primitive. Donc si $n = 4^a 2m'$ avec m' impair ou $n = 4^a m'$ avec $m' \not\equiv 7 \pmod 8$ alors on peut écrire n comme somme de trois carrés.

Au contraire, on suppose $n = \alpha^2 + \beta^2 + \gamma^2$ de la forme $n = 4^a m'$ avec $m' \equiv 7 \pmod 8$ alors on peut extraire des carrés $q^2 | n$ de façon à ce que p.g.c.d.$(\alpha/q, \beta/q, \gamma/q) = 1$. Mais n/q^2 est aussi de la forme $n/q^2 = 4^{a'} m''$ (car les carrés impairs sont $\equiv 1 \pmod 8$) et il n'existe donc pas un réseau L de signature $(3, 0)$ avec $b_L = -\frac{q^2}{n}$, donc n n'est pas une somme de trois carrés.

Exemple 2.5.9 (Théorème des quatre carrés)**.** On se pose encore une fois la question avec quatre carrés, donc $n^2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$.

Cette fois on cherche $n = e^2 m$ avec $\langle m \rangle \oplus L \subseteq \langle 1 \rangle^{\oplus 4}$ extension primitive. Comme on a l'unicité aussi pour $\langle 1 \rangle^{\oplus 4}$, une condition nécessaire et suffisante est l'existence d'un réseau L de signature $(3,0)$ avec $b_L = -\frac{1}{m}$, qui par l'Exemple 2.4.47 existe si $8 \nmid m$. Donc soit $n = 2^a k$ avec k impair, alors soit $n = 4^{a/2}k$, soit $n = 4^{(a-1)/2}2k$, dans les deux cas on peut décomposer n comme produit d'un carré et d'un nombre non divisible par 8, donc tous les naturels peuvent être écrits comme somme de quatre carrés.

En utilisant les extensions primitives et le théorème de Minkowski on peut donner une nouvelle preuve (qui n'utilise que des résultats basiques) de l'unicité de E_8.

Exemple 2.5.10 (Unicité de E_8)**.** Soit L unimodulaire pair euclidien de rang 8, alors par le théorème de Minkowski il existe $v_1 \in L$ de carré 2 (cf. Tableau 2.5.1), donc L est un sur-réseau de $\langle 2 \rangle \oplus v_1^\perp$, avec $A_{v_1^\perp} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$. En appliquant le théorème de Minkowski à nouveau, il existe $v_2 \in v_1^\perp$ de carré 2, donc $v_1^\perp$ est un sur-réseau de $\langle 2 \rangle \oplus v_1^\perp \cap v_2^\perp$, avec $A_{v_1^\perp \cap v_2^\perp} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ (car $A_{v_1^\perp \cap v_2^\perp} \simeq A_{\langle 2 \rangle} \oplus A_{\langle 2 \rangle}$). On vérifie qu'on peut répéter la procédure jusqu'à avoir:

$$L \supseteq \langle 2 \rangle^{\oplus 4} \oplus K$$

avec $A_K \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}^4$, donc $K(\frac{1}{2})$ est unimodulaire, mais par l'Exemple 2.4.50 $K(\frac{1}{2}) \simeq \langle 1 \rangle^{\oplus 4}$ et donc $K \simeq \langle 2 \rangle^{\oplus 4}$. On a alors obtenu que $L \subseteq \langle 2 \rangle^{\oplus 8} = R$.

rang	8	7	6	5
det	1	2	4	8
borne Mink. $\lambda \leq$	$2,82\ldots$	$2,83\ldots$	$2,91\ldots$	$3,12\ldots$

TABLE 2.5.1 – Bornes de Minkowski pour certains sous-réseaux de E_8

Soit $v_1, \ldots, v_n$ un base de R telle que la matrice de Gram soit 2Id, alors $u_1 = v_1/2, \ldots, u_n = v_n/2$ est une base de R^* et $\overline{u}_1, \ldots, \overline{u}_n$ réalisent $q_R \simeq \left(w_{2,1}^1\right)^{\oplus 8}$.

Donc si $x \in H_L \subseteq A_R$, comme $q_R(x) \equiv 0 \pmod{2\mathbb{Z}}$, alors on a deux possibilités:

1 $x = \overline{u}_{i_1} + \cdots + \overline{u}_{i_4}$

2 $x = \overline{u}_1 + \cdots + \overline{u}_8 =: u$.

Comme $\det(R) = 2^8$, $\det(L) = 1$, alors $H_L \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}^4$ et il existe $x_1, \ldots, x_4 \in A_L$ tel que $H_L = \mathrm{span}(x_1, \ldots, x_4)$. Si x_i est de la forme (2) pour un certain i, comme les v_i sont une base de H_L pour $j \neq i$ on aura que x_j est de la forme (1). On fixe $i' \neq i$, si on remplace x_i par $x_i' = x_i + x_{i'}$, alors x_i' sera de la forme (1) et donc on peut toujours choisir une base de H_L composée par des vecteurs de la forme (1).

Si tous les x_i sont de la forme (1) alors, L est engendré par les vecteurs de R plus des vecteurs de la forme $u_{i_1} + \cdots + u_{i_4}$, qui ont carré 2 et sont

donc des racines: donc L est un réseau de racines (car R est aussi engendré par des racines). Mais le seul réseau de racines unimodulaire de rang 8

est E_8, donc $L \simeq E_8$ est le seul réseau unimodulaire pair de rang 8.

Remarque 2.5.11. On rappelle qu'on peut trouver la preuve « classique » de l'unicité de E_8 dans [Mor] et dans [Gr] pour une preuve plus élémentaire

On se pose maintenant un problème légèrement différent: soient L, R deux réseaux, on veut déterminer les plongements primitifs $L \hookrightarrow R$. Cela est équivalent à déterminer les extensions primitives $L \oplus K \subseteq R'$, avec K tel que:

1 $\operatorname{sign}(K) + \operatorname{sign}(L) = \operatorname{sign}(R)$;
2 R' a même genre que R ;
3 il existe $H_{R'} \subseteq A_L \oplus A_K$ avec $b_{R'} \simeq \left(b_{L\oplus K}|_{H_R^\perp}\right)/H_{R'}$ (cela assure une extension primitive avec un réseau du même genre que R) ;
4 L'extension donnée par H_R soit isométrique à R.

La Proposition 2.5.2 nous permet donc d'aborder la question, bien qu'il puisse être difficile d'établir un lien direct. On va alors la reformuler pour plus de confort dans les calculs relatifs aux plongements primitifs.

On a d'abord besoin de:

Lemme 2.5.12. *Soient b_1, b_2 des f.f. bilinéaires non-dégénères sur A_1 et A_2, $H \hookrightarrow A_1 \oplus A_2$ tel que $H \cap A_1 = 0$, alors si π_1 est la projection sur A_1, $\pi_1 : A_1 \oplus A_2 \to A_1$, on a $\pi_1(H^\perp) = A_1$*

Démonstration. Soit $f : A_1 \oplus A_2 \twoheadrightarrow \frac{A_1 \oplus A_2}{H}$ le quotient par H, alors en procédant comme dans le Lemme 2.3.30 on obtient que le diagramme suivant commute:

$$\begin{array}{ccc} \left(\frac{A_1\oplus A_2}{H}\right)^* & \xrightarrow{f^*} & A_1^* \oplus A_2^* \\ \simeq \uparrow & & \simeq \uparrow b(\bullet,\bullet) \\ H^\perp & \longrightarrow & A_1 \oplus A_2 \end{array}$$

Comme $H \cap A_1 = 0$ on a que $f_{|A_1} : A_1 \to \frac{A_1 \oplus A_2}{H}$ est injective, donc $\left(f_{|A_1}\right)^* = \pi_1 \circ f^*$ est surjective et en regardant le diagramme cela est équivalant à affirmer que $\pi_1(H^\perp) = A_1$.

□

Proposition 2.5.13. *Soient A_1, A_2, A_3 des groupes abéliens finis, pour $1 \leq i \leq 3$ soit b_i forme bilinéaire non-dégénérée sur A_i [q_i forme quadratique non-dégénérée sur A_i].*

Alors on a une équivalence entre:

1 $H_3 \hookrightarrow A_1 \oplus A_2$ totalement isotrope [totalement q-isotrope] avec $H_3 \cap A_i = 0$ pour $i = 1, 2$ et

$$\frac{b_{H_3^{\perp(A_1\oplus A_2)}}}{H_3} \simeq -\, b_{A_3} \quad \left[\frac{q_{H_3^{\perp(A_1\oplus A_2)}}}{H_3} \simeq -\, q_{A_3}\right]$$

2 $H \hookrightarrow A_1 \oplus A_2 \oplus A_3$ *totalement isotrope [totalement q-isotrope] avec* $H \cap A_i = 0$ *pour* $i = 1, \ldots, 3$ *et* $H = H^\perp$.

Démonstration. 1) $\Longrightarrow$ 2) Soit $\varphi : b_{A_3} \to b_{\frac{H_3^\perp}{H_3}}$ une anti-isométrie, et $\tilde{H}$ le graphe de φ, $\tilde{H} = \{(x, \varphi(x)) | x \in A_3\}$. Donc $\tilde{H}$ est un groupe totalement isotrope dans $\frac{H_3^\perp}{H_3} \oplus (A_3)$ et $H = \tilde{H} + H_3$ est un sous-groupe totalement isotrope de $A_1 \oplus A_2 \oplus A_3$. Soit $\pi : H_3^\perp \to \frac{H_3^\perp}{H_3}$, alors:

$$H = \{(x_1, x_2, x_3) \in H_3^\perp \oplus A_3 | \varphi(x_3) = \pi(x_1 + x_2)\}$$

Donc $H \cap A_3 = 0$, car sinon il existerait $x_3 \in H$, $\varphi(x_3) = 0$ absurde car φ est un isomorphisme et $H \cap A_1 = H \cap A_2 = 0$ car sinon on aurait $x_i \in H$, $\pi(x_i) = 0$, donc $x_i \in H_3$ mais $H_3 \cap A_1 = H_3 \cap A_2 = 0$ par hypothèse.

De plus, comme $\frac{\#H_3^\perp}{\#H_3} = \#A_3$ et $\#H_3^\perp \#H_3 = \#A_1 \#A_2$:

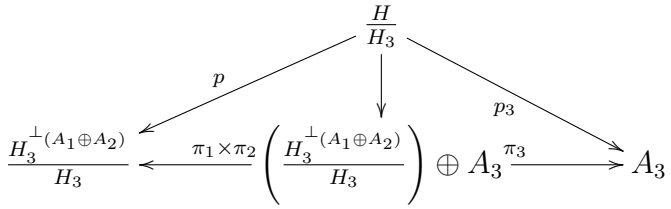
$$\begin{aligned}
(\#H)^2 &= \left(\#\tilde{H} \cdot \#H_3\right)^2 = (\#A_3 \cdot \#H_3)^2 \\
&= \#A_3 \cdot \#H_3 \cdot \left(\#H_3^\perp / \#H_3\right) \cdot \#H_3 \\
&= \#A_3 \cdot \#H_3^\perp \cdot \#H_3 = \#A_3 \cdot \#A_1 \cdot \#A_2
\end{aligned}$$

donc $\#H^\perp = \#H$, mais H totalement isotrope ce qui implique $H = H^\perp$.

2) $\Longrightarrow$ 1) Soit $\pi_i : A_1 \oplus A_2 \oplus A_3 \to A_i$ la projection sur l'i-ème facteur, on considère l'inclusion:

$$H_3 = \ker(\pi_3) \cap H = (A_1 \oplus A_2) \cap H_3 \hookrightarrow A_1 \oplus A_2$$

alors $H_3 \cap A_i = H \cap A_i = \{0\}$. Maintenant on a le diagramme:



p_3 est injectif car $\ker(p_3) \subseteq \ker(\pi_3) \cap H = H_3$, mais elle est aussi surjective par le Lemme 2.5.12 car $H = H^\perp$, donc p_3 est un isomorphisme de groupes.

Pour p on a la surjectivité car:

$$\begin{aligned}
H_3^{\perp(A_1 \oplus A_2)} &= H_3^\perp \cap (A_1 \oplus A_2) \\
&= ((A_1 \oplus A_2) \cap H)^\perp \cap (A_1 \oplus A_2) \\
&= \left((A_1 \oplus A_2)^\perp + H^\perp\right) \cap (A_1 \oplus A_2) \\
&= (A_3 + H) \cap (A_1 \oplus A_2) \\
&= (\pi_1 \times \pi_2)(H)
\end{aligned}$$

mais p_3 est aussi injective car $\ker(\pi_1 \times \pi_2)_{|H} = A_3 \cap H = 0$, donc p_3 est un isomorphisme de groupe aussi. Comme H est totalement isotrope $p_3 \circ p^{-1}$ définit une anti-isométrie:

$$p_3 \circ p^{-1} : \frac{b_{H_3^{\perp(A_1 \oplus A_2)}}}{H_3} \xrightarrow{\simeq} -b_{A_3}$$

□

Dans l'énoncé les A_i sont interchangeables, donc à partir de $H_3 \hookrightarrow A_1 \oplus A_2$ on peut obtenir $H \hookrightarrow A_1 \oplus A_2 \oplus A_3$ et à nouveau ré-appliquer la proposition mais en échangeant A_3 avec A_2, donc on obtient cette fois $H_2 \to A_1 \oplus (-A_2)$, qui reste toujours une façon équivalente de décrire le plongement de H_1. Donc on a:

Corollaire 2.5.14. *Soient A_1, A_2, A_3 des groupes abéliens finis, pour $i \in 1, \ldots, 3$ soit b_i forme bilinéaire non-dégénérée sur A_i [q_i forme quadratique non-dégénérée sur A_i].*

Alors on a une équivalence entre:

1. *$H_3 \to A_1 \oplus A_2$ totalement isotrope [totalement q-isotrope] avec $H_3 \cap A_i = 0$ pour $i = 1, 2$ et $b_{\frac{H_3^{\perp(A_1 \oplus A_2)}}{H_3}} \simeq b_{A_3}$ [$q_{\frac{H_3^{\perp(A_1 \oplus A_2)}}{H_3}} \simeq q_{A_3}$];*
2. *$H_2 \to A_1 \oplus -A_3$ totalement isotrope [totalement q-isotrope] avec $H_2 \cap A_i = 0$ pour $i = 1, 3$ et $b_{\frac{H_2^{\perp(A_1 \oplus -A_3)}}{H_2}} \simeq -b_{A_2}$ [$q_{\frac{H_2^{\perp(A_1 \oplus A_3)}}{H_2}} \simeq -q_{A_2}$].*

On revient alors au cas d'un plongement primitif $L \hookrightarrow R$, si $K = L^\perp$ alors on a un sous-groupe totalement isotrope $H_R \subseteq A_L \oplus A_K$ et grâce aux résultats ci-dessus cela est équivalent à choisir un sous-groupe totalement isotrope $H_K \subseteq A_L \oplus (-A_R)$.

On peut donc procéder ainsi:

- Déterminer les sous-groupes totalement isotrope $H_K \subseteq A_L \oplus (-A_R)$;
- Déterminer les réseaux K tels que:
  - $\operatorname{sign}(K) + \operatorname{sign}(L) = \operatorname{sign}(R)$;
  - $b_K \simeq -b_{\frac{H_K^\perp}{H_K}}$ [ou $q_K \simeq -q_{\frac{H_K^\perp}{H_K}}$ dans le cas pair] ;
- Choisir un isomorphisme $\gamma : q_K \to -q_{\frac{H_K^\perp}{H_K}}$;
- Réaliser l'extension primitive de $L \oplus K$ donnée par H_K.

On obtient de cette façon tous les plongements primitifs $L \hookrightarrow R$, mais pas seulement. En effet, comme on choisit un K arbitraire en général on obtiendra des extensions primitives $L \oplus K \hookrightarrow R'$ avec R' du même genre de R, mais en général $R \not\simeq R'$. Sinon, comme il existe au plus un nombre fini de réseaux qui réalisent un genre donné, on a que la procédure s'arrête après un nombre fini d'étapes.

Finalement on arrive à [Nik, 1.15.1]:

Proposition 2.5.15 (Nikulin)**.** *Soit L [pair] un réseau de signature (l^+, l^-). Alors les plongements primitifs de L dans un réseau R [pair] de signature (r^+, r^-), groupe discriminant A_R et forme discriminante q_R sont déterminés par les choix des:*

1 *Sous-groupes $H \hookrightarrow A_L \oplus -A_R$ totalement isotropes [totalement isotropes selon la forme quadratique] avec $H \cap A_L = H \cap A_R = 0$;*

2 *K réseau [pair] de signature (k^+, k^-) et forme discriminante q_K tel qu'il existe un isomorphisme γ:*

$$\gamma : q_K \xrightarrow{\simeq} -\frac{(q_L \oplus -q_R)_{|H^\perp}}{H} = \frac{(-q_L \oplus q_R)_{|H^\perp}}{H}$$

Remarque 2.5.16. Si R est unique en son genre (par exemple si R respecte les critères de la Proposition 2.4.52) alors la Proposition 2.5.15 est très efficace pour étudier les plongements primitifs $L \hookrightarrow R$, car chaque choix de K, H_K détermine un plongement dans R.

Remarque 2.5.17. La preuve originelle donnée par Nikulin dans [Nik] était un peu différente de celle présentée ici, essentiellement l'idée était la suivante: soit $L \hookrightarrow R$ alors si $K = L^\perp$ on a que $R \supseteq L \oplus K$ est une extension primitive. Soit $R \oplus R(-1) \hookrightarrow U^{\oplus r}$ comme dans l'Exemple 2.3.81, alors $L \oplus K \oplus R(-1) \hookrightarrow U^{\oplus r}$. Comme l'ordre n'est pas important on peut écrire $\mathrm{span}\,(L \oplus R(-1)) \oplus K \hookrightarrow U^{\oplus r}$ et comme U est unimodulaire on a une anti-isométrie entre A_K et $A_{\mathrm{span}(L \oplus R(-1))}$, ce qui revient à la Proposition 2.5.15 (car L et $R(-1)$ sont « collés » de façon à obtenir une forme finie anti-isométrique à K).

Dans ces notes on a choisi un approche différente, car on a voulu éviter d'utiliser des résultats sur les réseaux et leurs plongements dans un réseau unimodulaire, en préférant procéder avec une preuve directe utilisant uniquement les formes finies. On espère de cette façon rendre plus clair le mécanisme de la preuve.

Exemple 2.5.18 (Déterminer l'existence d'un plongement)**.** Donnons un exemple détaillé de comment appliquer ces résultats pour déterminer l'existence d'un plongement entre deux réseaux. Soit $R = U \oplus U(3)^{\oplus 2} \oplus A_2^{\oplus 2}$ et $L = A_5$, on veut déterminer s'il existe un plongement $L \hookrightarrow R$. On procède par étapes:

- On calcule les formes discriminantes, $A_L \simeq \mathbb{Z}/6\mathbb{Z}$, $q_L \simeq w_{3,1}^1 \oplus w_{2,1}^3$, $A_R \simeq (\mathbb{Z}/3\mathbb{Z})^6$, $q_R \simeq \left(w_{3,1}^{-1}\right)^{\oplus 7}$;
- A_L ne contient pas de sous-groupes isotropes, donc L n'a pas de sur-réseau. Dans ce cas, si un plongement $L \hookrightarrow R$ existe, il doit forcément être primitif. ;
- Supposons qu'il existe une extension $R \supseteq L \oplus K$ pour un certain réseau K de signature $(2, 3)$, alors les possibilités pour K sont données par la Proposition 2.5.15 ;

- Soit $q = q_R - q_L = \left(w_{3,1}^{-1}\right)^{\oplus 7} \oplus w_{2,1}^1$ et H un sous-groupe isotrope tel que $H \cap A_L = H \cap A_R = 0$, alors les seules possibilités sont $H = 0$ et $H = \mathbb{Z}/3\mathbb{Z}$.
- Si $H = 0$ alors K doit être un réseau de signature $(2, 3)$ avec $A_K = (\mathbb{Z}/3\mathbb{Z})^7 \oplus \mathbb{Z}/2\mathbb{Z}$ et $q_K = q = \left(w_{3,1}^{-1}\right)^{\oplus 7} \oplus w_{2,1}^1$. Pour savoir si un tel réseau existe, on utilise le Théorème 2.4.44:
  - Le deuxième critère, relatif à la signature, est sans doute vérifié, car $\operatorname{sgn}(q) \equiv \operatorname{sgn}(q_R) - \operatorname{sgn}(q_L) \equiv \operatorname{sgn}(q_K) \pmod 8$;
  - Le premier critère par contre n'est pas vérifié, car $l(A_K) = 7 > 5 = \operatorname{rang}(K)$;
  - Donc il ne correspond aucun plongement $L \hookrightarrow R$ à $H = 0$
- Si $H = \mathbb{Z}/3\mathbb{Z}$ alors on trouve que $H^\perp = (\mathbb{Z}/3\mathbb{Z})^5 \oplus \mathbb{Z}/2\mathbb{Z}$ et $q_K = q_{\frac{H^\perp}{H}} = \left(w_{3,1}^{-1}\right)^{\oplus 4} \oplus w_{3,1}^1 \oplus w_{2,1}^1$. On applique à nouveau le Théorème 2.4.44:
  - Comme toujours, le critère relatif à la signature est toujours satisfait, car $\operatorname{sgn}(q_{\frac{H^\perp}{H}}) \equiv \operatorname{sgn}(q) \equiv \operatorname{sgn}(q_R) - \operatorname{sgn}(q_L) \equiv \operatorname{sgn}(q_K) \pmod 8$;
  - Le premier critère est aussi vérifié, car $l(A_K) = 5 = \operatorname{rang}(K)$;
  - Comme $l(A_3) = \operatorname{rang}(K)$ il faut vérifier aussi le troisième critère: $q_3 = \left(w_{3,1}^{-1}\right)^{\oplus 4} \oplus w_{3,1}^1$ qui a discriminant $1/3^5$. Sinon on a $s^- = 3$ et $\#A_K = 2 \cdot 3^5$, donc:

    $$\frac{(-1)^{s^-} m}{p^a} = \frac{(-1)^3 2}{3^5} = \frac{-2}{3^5} = \frac{1}{3^5}$$

    donc le critère est respecté et il existe un réseau K avec les propriétés recherchées;
- On conclut alors par la Proposition 2.5.15 qu'il existe un réseau R', avec le même de R, tel que $R' \supseteq L \oplus K$ soit une extension de réseaux et en particulier $L \hookrightarrow R'$.
- Par la Proposition 2.4.52 R est unique dans son genre, donc $R = R'$ et il existe un plongement (primitif) $L \hookrightarrow R$.

Exemple 2.5.19. Si R n'est pas unique en son genre les choses sont plus compliquées. Par exemple soit $L = E_8$, $R = E_8^{\oplus 3}$, alors $A_L \oplus -A_R = 0$, donc $H_K = 0$ et les plongements primitifs $L \hookrightarrow R$ sont de la forme $L \hookrightarrow L \oplus K$ avec K unimodulaire pair de signature $(16, 0)$.

On peut alors choisir $K = E_8^{\oplus 2}$ ou $K = D_{16}^+$, dans le premier cas on obtient justement $E_8 \hookrightarrow E_8^{\oplus 3} \simeq R$ mais dans le deuxième cas on a $E_8 \hookrightarrow E_8 \oplus D_{16}^+$ et $E_8 \oplus D_{16}^+ \not\simeq E_8^3$ même s'ils partagent le même genre.

Corollaire 2.5.20. *Soit $R \supseteq L_1 \oplus L_2$ un sur-réseau, alors il existe $H_1 \subseteq A_R \oplus A_{L_2}$ tel que:*

$$b_{L_1} \hookrightarrow (b_R \oplus -b_{L_2})_{|H_1^\perp} / H_1 \quad \left[q_{L_1} \hookrightarrow (q_R \oplus -q_{L_2})_{|H} / H_1\right]$$

En particulier $A_{L_1} \subseteq (A_R \oplus A_{L_2})/H_1$.

Corollaire 2.5.21. *Soit* $L_1 \oplus L_2 \subseteq R$ *une extension primitive de réseaux pairs . Alors si l'invariant* δ_q *est égal à* 0 *pour deux réseaux parmi* L_1,L_2 *et* R, *il est égal à* 0 *pour le troisième aussi.*

2.5.2 Action d'un groupe sur un réseau

Soit L un réseau, $O(L)$ le groupe des isométries de L et $G \leq O(L)$ un sous-groupe: on veut étudier l'action de G sur L.

Une méthode est de choisir des sous-réseaux de L où l'action de G est plus simple, de façon à ce que L soit une extension primitive de la somme de ces réseaux. Ensuite on essaie d'étendre l'action sur L tout entier. On aura donc besoin de l'outil suivant:

Proposition 2.5.22. *Soit* G *un groupe qui agit sur un réseau* $L = L_1 \oplus \cdots \oplus L_n$ *(avec les* L_i *non nécessairement stables sous l'action de* G*) ,* $R \supseteq L$ *une extension primitive. Alors l'action de* G *s'étend sur* R *si et seulement si* $H_R = R/L \subseteq A_{L_1} \oplus \cdots \oplus A_{L_n}$ *est stable par l'action de* G.

Démonstration. L'action de G s'étend naturellement par linéarité de façon unique sur le réseau dual $L^* = L_1^* \oplus \cdots \oplus L_n^*$, donc G agit sur R si et seulement si $G \cdot R \subseteq R \subseteq L^*$. Comme L est un sous-espace stable par l'action de G c'est la même chose que demander que $G \cdot R/L \subseteq R/L$, i.e. $R/L = H_R$ est un sous-espace stable par l'action de G. □

Remarque 2.5.23. Si l'action de G sur H_R est triviale en particulier H_R est stable et on peut appliquer la proposition, donc on peut étendre l'action sur R.

Dans la suite, pour une action de G sur un réseau L, on notera $T_G := L^G = \{x \in L | \forall g \in G,\, g(x) = x\}$ le *réseau invariant* et $S_G := T_G^{\perp}$ le *réseau coinvariant.*

Lemme 2.5.24. *Soit* L *un réseau,* $G \subseteq O(L)$ *un groupe fini qui agit sur* L, *alors* T_G *et* S_G *sont des réseaux primitifs.*

Démonstration. Soit $x \in T_G$, alors il existe $y \in L$ tel que $\langle x, y\rangle \neq 0$. Maintenant soit $N = \sum_{g\in G} g(y)$, alors $N \in T_G$ mais $\langle x, N\rangle = \#G \cdot \langle x, y\rangle \neq 0$, donc T_G est un réseau car la forme bilinéaire est non-dégénérée et il est clairement primitif. Comme $S_G = T_G^{\perp}$, par le Lemme 2.2.19 S_G est aussi un réseau primitif. □

Dans la suite on considérera le cas suivant: soit p premier, $n \in \mathbb{N}$, $G \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ avec $G = \langle\varphi\rangle$, φ isométrie d'ordre p d'un réseau L. On trouve les résultats suivant dans [BNS]:

Lemme 2.5.25. *Soit* $\phi_p(x) = x^{p-1} + \cdots + x + 1$, *alors* $S_\varphi = \mathrm{Im}(\phi_p(\varphi))$

Démonstration. Soit $\tilde{\varphi}$ l'extension de φ sur $L \otimes \mathbb{Q}$, comme $\varphi^p - 1 = 0$ alors par le lemme des noyaux:

$$L \otimes \mathbb{Q} = \underbrace{\ker(\tilde{\varphi} - \mathrm{Id})}_{=T_\varphi \otimes \mathbb{Q}} \oplus \mathrm{Im}(\phi_p(\tilde{\varphi}))$$

mais φ est une isométrie et donc S_φ est stable par l'action de φ, donc on peut aussi écrire:

$$S_\varphi \otimes \mathbb{Q} \;=\; \ker(\tilde{\varphi} - \mathrm{Id}) \cap S_\varphi \oplus \mathrm{Im}(\phi_p(\tilde{\varphi})) \cap S_\varphi$$

Comme $T_\varphi = \ker(\varphi - \mathrm{Id})$ est non-dégénérée, alors $T_\varphi \cap S_\varphi = \{0\}$ et donc $S_\varphi \otimes \mathbb{Q} = \mathrm{Im}(\phi_p(\tilde{\varphi})) \cap S_\varphi$. Mais $\dim(\mathrm{Im}(\phi_p(\tilde{\varphi}))) = \dim(S_\varphi)$ et donc:

$$S_\varphi \otimes \mathbb{Q} = \mathrm{Im}(\phi_p(\tilde{\varphi}))$$

Mais S_φ et $\mathrm{Im}(\phi_p(\varphi))$ sont deux sous-réseaux primitifs et donc ils coïncident. □

Lemme 2.5.26. *$\frac{L}{S_\varphi \oplus T_\varphi}$ est un $\mathbb{Z}$-module de p-torsion (i.e. $pL \subseteq S_\varphi \oplus T_\varphi$).*

Démonstration. On a $p = \phi_p(x) - (x-1)(x^{p-2} + 2x^{p-1} + \cdots + p - 1)$, donc pour tout $l \in L$ on a:

$$pl = \underbrace{\phi_p(\varphi)(l)}_{t} - \underbrace{(\varphi^{p-2} + 2\varphi^{p-1} + \cdots + (p-1)\mathrm{Id}) \circ (\varphi - \mathrm{Id})(l)}_{s}$$

mais $(\varphi^p - \mathrm{Id})(l) = 0$, donc:

$$\begin{aligned} \mathrm{Im}\,\phi_p(\varphi) &\subseteq \ker(\varphi - \mathrm{Id}) = T_\varphi \\ \mathrm{Im}(\varphi - \mathrm{Id}) &\subseteq \ker(\Phi_p(\varphi)) = S_\varphi \end{aligned}$$

mais T_φ,S_φ sont des espaces stables donc $t \in T_\varphi$ et $s \in S_\varphi$. □

Corollaire 2.5.27. *Si L est unimodulaire alors T_φ et S_φ sont p-élémentaires (i.e. les groups discriminants sont de p-torsion).*

Démonstration. Par le Lemme 2.5.4 $A_{T_\varphi} \simeq A_{S_\varphi} \simeq H_R$ mais $H_R \simeq (\mathbb{Z}/p\mathbb{Z})^a$ par le Lemme 2.5.26. □

On considère maintenant le cas de plusieurs isométries commutant. Soit L un réseau, $\varphi_1, \ldots, \varphi_n$ des isométries d'ordre p premier de L commutant entre elles, i.e. on a une action de $G \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n$ sur L. On définit:

Définition 2.5.28. On définit par récurrence $U_{G,1} := S_{\varphi_1} \oplus T_{\varphi_1}$, pour $2 \leq i \leq n$ $U_{G,i} := (U_{G,i-1} \cap T_{\varphi_i}) \oplus (U_{G,i-1} \cap S_{\varphi_i})$. On pose aussi $U_G := U_{G,n}$

Remarque 2.5.29. Comme les φ_i commutent entre elles, on a que $S_{\varphi_i}, T_{\varphi_i}$ sont stables sous l'action de φ_j, pour tous $1 \leq i, j \leq n$. On peut donc appliquer le Lemme 2.2.20 et on obtient que:

$$U_{G,k} = \bigoplus_{(i_1,\ldots,i_k)\in\{0,1\}^k} V_{1,i_1} \cap \cdots \cap V_{k,i_k}$$

avec:

$$V_{j,i_j} = \begin{cases} T_{\varphi_j} & \text{si } i_j = 0 \\ S_{\varphi_j} & \text{si } i_j = 1 \end{cases}$$

Donc:

$$\begin{aligned} U_{G,1} &= T_{\varphi_1} \oplus S_{\varphi_i} \\ U_{G,2} &= (T_{\varphi_1} \cap T_{\varphi_2}) \oplus (S_{\varphi_1} \cap T_{\varphi_2}) \oplus (T_{\varphi_1} \cap S_{\varphi_2}) \oplus (S_{\varphi_1} \cap S_{\varphi_2}) \\ \ldots &= \ldots \\ U_{G,n} &= (T_{\varphi_1} \cap \cdots \cap T_{\varphi_n}) \oplus \cdots \oplus (S_{\varphi_1} \cap \cdots \cap S_{\varphi_n}) \end{aligned}$$

Lemme 2.5.30. *Soit $G \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n$ qui agit sur un réseau L, alors pour tout $k \in \{1,\ldots,n\}$, $L/U_{G,k}$ est un $\mathbb{Z}$-module de (au plus) p^k-torsion. En particulier L est un sur-réseau de U_G et L/U_G est un module de p^n-torsion.*

Démonstration. On procède par récurrence sur k: pour $k = 1$ c'est vrai par le Lemme 2.5.26.

($k \implies k+1$): Comme les φ_j commutent, on a que $U_{G,k}$ est stable sous l'action de φ_{k+1}, donc par le Lemme 2.5.26 on a que $U_{G,k}/U_{G,k+1}$ est un module de p-torsion. Mais $L/U_{G,k}$ a (au plus) p^k-torsion, donc $L/U_{G,k+1}$ est (au plus) de p^n-torsion □

Involutions d'un réseau

Proposition 2.5.31. *Soient L, S, T des réseaux, alors on a une équivalence entre:*

1. *il existe φ involution de L avec $T_\varphi \simeq T$ et $S_\varphi \simeq S$;*
2. *il existe $S, T \subseteq L$ primitifs et orthogonaux tels que $L/(S \oplus T) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus a}$;*
3. *il existe une extension primitive $L \supseteq S \oplus T$ telle que $H_L \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus a}$*

en plus si les conditions sont vérifiés alors l'involution est unique.

Démonstration. 1 $\implies$ 2 par le Lemme 2.5.26 et il est clair que 2 $\implies$ 3. Il reste à montrer 3 $\implies$ 1: On pose l'action de φ égale à $\varphi_{|T} = \mathrm{Id}$ et $\varphi_{|S} = -\mathrm{Id}$, donc φ est une involution de $S \oplus T$. Par conséquent, sur le groupe discriminant on a que $\overline{\varphi}_{|A_T} = \mathrm{Id}$ et $\overline{\varphi}_{|A_S} = -\mathrm{Id}$. Comme $H_L \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus a}$ on a $H_L \hookrightarrow H_{L,S} \oplus H_{L,T}$ avec $H_{L,S} \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus a} \subseteq A_S$ et $H_{L,T} \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus a} \subseteq A_T$ et donc $\overline{\varphi}$ agit comme l'identité sur $H_{L,S} \oplus H_{L,T}$ (car dans $\mathbb{Z}/2\mathbb{Z}$ on a que $-1 \equiv 1$) et en particulier sur H_L. Alors par la Proposition 2.5.22 on peut étendre φ à une involution de L. □

Exemple 2.5.32 (Réflection par rapport à une droite de carré 2)**.** Soit $v \in L$ tel que $v^2 = 2$, alors on peut définir une involution R_v de L de la façon suivante:

$$R_v(x) = \langle v, x\rangle\, v - x \;\; \forall x \in L$$

Alors $R_v(v) = v$ et $R_v(w) = -w$ pour tous $w \perp v$, donc R_v est une involution de L avec $T_{R_v} = \mathrm{span}(v)$ et $S_{R_v} = v^\perp$.

On donne une interprétation alternative dans l'esprit de la Proposition 2.5.31: on pose $T = \mathrm{span}(v)$ et $S = v^\perp$, alors $L \supseteq T \oplus S$ est une extension primitive avec $H_L \subseteq A_T \oplus A_S$. Comme $v = \langle 2\rangle$ on a $A_T \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$ donc soit $H_L = 0$ soit $H_L \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$, dans les deux cas on récupère l'involution de L.

La Proposition 2.5.31 nous donne un moyen pour classifier les involutions d'un réseau L: il s'agit de trouver toutes les extensions primitives $L \supseteq T \oplus S$ qui satisfont $L/(T \oplus S) \simeq (\mathbb{Z}/2\mathbb{Z})^a$. En particulier si L est unimodulaire on a $A_S \simeq A_T \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus a}$, on dit alors que S et T sont des réseaux 2-*élémentaires* et on pourra donc utiliser la classification contenue dans la Proposition 2.3.70 pour rechercher les différentes possibilités pour S et T. La tâche est simplifiée davantage quand les réseaux sont uniques en leur genre.

Exemple 2.5.33 (Involutions de E_8)**.** On veut classifier les involutions de E_8, donc les extensions primitives $E_8 \supseteq T \oplus S$ avec $A_T \simeq A_S \simeq (\mathbb{Z}/2\mathbb{Z})^a$. Sans perte de généralité on pose $r_T = \mathrm{rang}(T) \leq \mathrm{rang}(S) = r_S$ (car dans le cas contraire il suffit de remplacer l'involution φ par son opposée $-\varphi$, qu'on obtient en échangeant les réseaux invariants et coinvariants entre eux).

Comme E_8 est unimodulaire de rang 8 on aura donc $r_S = 8 - r_T$, $a_S = a_T = a$, $\delta_S = \delta_T =: \delta$

En utilisant la classification des réseaux définis 2-élémentaires de petit rang (Tableau 2.5.2) on vérifie facilement qu'on a uniquement les possibilités suivantes:

- Si $r_T = 1$ la seule possibilité est $T \simeq \langle 2\rangle$, par conséquent S doit avoir $r_S = 7$, $a = 1$ et $\delta_q = 1$, donc $S \simeq E_7$;
- De la même façon Si $r_T = 2$ on a $T \simeq \langle 2\rangle^{\oplus 2}$, $S \simeq D_6$;
- Si $r_T = 3$ on a $T \simeq \langle 2\rangle^{\oplus 3}$ et $S \simeq D_4 \oplus \langle 2\rangle$;
- Si $r_T = 4$ on a deux possibilités: $T \simeq D_4 \simeq S$ ou $T \simeq \langle 2\rangle^{\oplus 4} \simeq S$.

On peut vérifier que pour tous les cas cités ci-dessus on a $q_T = -q_S$, donc l'extension est réalisable et le sur-réseau obtenu est E_8 (car il est le seul réseau unimodulaire pair de rang 8). Le lecteur intéressé trouvera plus de détails sur les sous-réseaux primitifs de E_8 dans [Nis].

Remarque 2.5.34. Connaître les réseaux T,S ne suffit pas à identifier de manière unique l'isométrie, car il reste à établir les différentes possibilités pour la réalisation de l'extension $L \supseteq S \oplus T$, donc les différents plongements de $H_{E_8} \hookrightarrow A_S \oplus A_T$ (qui sont quand même en nombre fini).

Heureusement dans notre cas, comme on verra dans le Chapitre suivant, on n'aura pas besoin d'autant de détails pour déterminer les invariants associés aux isométries, donc on ne se penchera pas trop sur la question.

$a\backslash r$	1	2	3	4	5	6	7	8
0								(E_8)
1	$\langle 2\rangle$						E_7	
2		$\langle 2\rangle^{\oplus 2}$		(D_4)		D_6		$E_7\oplus\langle 2\rangle$ (D_8)
3			$\langle 2\rangle^{\oplus 3}$		$D_4\oplus\langle 2\rangle$		$D_6\oplus\langle 2\rangle$	
4				$\langle 2\rangle^{\oplus 4}$		$D_4\oplus\langle 2\rangle^{\oplus 2}$		$D_6\oplus\langle 2\rangle^2$ $(D_4\oplus D_4)$
5					$\langle 2\rangle^{\oplus 5}$		$D_4\oplus\langle 2\rangle^{\oplus 3}$	
6						$\langle 2\rangle^{\oplus 6}$		$D_4\oplus\langle 2\rangle^{\oplus 4}$ $(D_8^*(2))$
7							$\langle 2\rangle^{\oplus 7}$	
8								$\langle 2\rangle^{\oplus 8}$ $(E_8(2))$

$^{(*)}$source: http://www.lmfdb.org/Lattice/

TABLE 2.5.2 – $^{(*)}$Liste des réseaux 2-élémentaires définis de rang≤ 8. Entre parenthèses les réseaux avec $\delta_q = 0$.

Dans le cas de plusieurs involutions commutant la question est plus compliquée, on se limitera donc au résultat partiel suivant, qui nous sera très utile dans la suite:

Proposition 2.5.35. *Soit $n \in \mathbb{N}\backslash\{0\}$, $V_{(i_1,\dots,i_n)}$ des réseaux avec $(i_1,\dots,i_n) \in \{0,1\}^n$, on considère l'extension primitive:*

$$L \supseteq \bigoplus_{(i_1,\dots,i_n)\in\{0,1\}^n} V_{(i_1,\dots,i_n)}$$

telle que:

$$H_L = \frac{L}{\bigoplus\limits_{(i_1,\dots,i_n)\in\{0,1\}^n} V_{(i_1,\dots,i_n)}} \simeq (\mathbb{Z}/2\mathbb{Z})^a$$

Alors il existe une unique action de $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ sur L, $G = \langle\varphi_1,\dots,\varphi_n\rangle$ avec:

$$V_{(i_1,\dots,i_n)} = \bigcap_{1\leq j\leq n \ t.q. \ i_j=0} T_{\varphi_j} \cap \bigcap_{1\leq k\leq n \ t.q. \ i_k=0} S_{\varphi_k}$$

Démonstration. La preuve est une simple généralisation de celle de la Proposition 2.5.31. On a une action de G sur $\bigoplus_{(i_1,\dots,i_n)\in\{0,1\}^n} V_{(i_1,\dots,i_n)}$ et donc sur $\bigoplus_{(i_1,\dots,i_n)\in\{0,1\}^n} A_{V_{(i_1,\dots,i_n)}}$ aussi. Mais sur H_L on a $\mathrm{Id} = -\mathrm{Id}$ à cause de la 2-torsion, donc G agit trivialement sur H_L et donc par la Proposition 2.5.22 on peut étendre l'action sur L. □

Chapitre 3

Action d'un groupe sur une surface K3

3.1 Réseaux d'une surface K3

3.1.1 Qu'est-ce qu'une surface K3 ?

On donne dans la suite une courte introduction à la définition de surface K3 à partir de la classification birationnelle des surfaces algébriques d'Enriques–Kodaira.

Nous renvoyons à [BHPV] comme référence pour les résultats principaux.

Soit donc X une surface (i.e. une variété algébrique sur $\mathbb{C}$ lisse et compacte de dimension 2), on définit les invariants suivants:

Définition 3.1.1. Soit X une surface, pour $d \geq 1$ on appelle pluri-genre:

$$P_d(X) := \dim\left(H^0\left(X, \mathcal{O}(K_X^{\otimes d})\right)\right)$$

avec K_X le fibré canonique de X.

Définition 3.1.2. Soit X une surface, on appelle dimension de Kodaira :

$$\kappa(X) := \begin{cases} -\infty & \text{si } P_d(X) = 0 \ \forall d \geq 1 \\ \min\{n \text{ t.q. } \frac{P_d}{d^n} \text{ est borné}\} & \text{sinon} \end{cases}$$

Définition 3.1.3. Soit X une surface, on note:

$$\begin{aligned} p_g &:= \dim\left(H^{0,2}(X)\right) \text{ le genre géometrique} \\ q &:= \dim\left(H^{0,1}(X)\right) \text{ l'irrégularité} \end{aligned}$$

avec $H^{p,q}(X) := H^q(X, \Omega^p)$.

On peut donc classifier les surfaces de la façon suivante:

Théorème 3.1.4 (Enriques–Kodaira)**.** *Soit X une surface minimale (i.e. X ne peut pas être obtenue à partir d'une autre surface lisse par explosion d'un point), $\kappa(X)$, p_g et q définis comme précédemment, alors on a la classification suivante:*

$\kappa(X)$	p_g	q	Type de Surface
$-\infty$	0	≥ 1	Surface réglée
	0	0	Surface rationnelle
2			Surface de type général
1			Surface elliptique
0	1	2	Surface abélienne
	0	1	Surface hyperelliptique
	1	0	Surface K3
	0	0	Surface d'Enriques

On peut alors donner comme définition:

Définition 3.1.5. Une surface K3 est une surface avec $\kappa(X) = 0$, $p_g = 1$ et $q = 0$.

Remarque 3.1.6. Alternativement on peut définir une surface K3 comme une surface avec K_X trivial et $q = 0$ (voir [Beau2]).

Comme $p_g = 1$, il existe une seule 2-forme holomorphe ω_X au scalaire près:

$$H^{2,0}(X) \simeq H^0(X, \Omega^2) \simeq \mathbb{C}\omega_X$$

En tant que générateur, ω_X ne s'annule sur aucun point, c'est donc une forme symplectique.

On remarque que si σ est un automorphisme d'une surface K3 notée X, on a une action de σ^* sur $H^2(X, \mathbb{C})$ qui respecte la décomposition de Hodge, en particulier:

$$\sigma^*(H^{2,0}(X)) = H^{2,0}(X)$$

mais comme ω_X est le seul générateur, cela implique que $\sigma^*(\omega_X) = \lambda\omega_X$. On donne donc la distinction suivante:

Définition 3.1.7. Soit X une surface K3, $\sigma \in \mathrm{Aut}(X)$, alors σ est dit:
- symplectique si $\sigma^*(\omega_X) = \omega_X$;
- non-symplectique sinon.

On en vient donc à la partie qui nous concerne le plus, c'est-à-dire le réseau associé à une surface K3 (voir [BHPV, VIII]):

Théorème 3.1.8. *Soit X une surface K3, alors $H^1(X, \mathbb{Z}) = H^3(X, \mathbb{Z}) = 0$ et $H^2(X, \mathbb{Z}) \simeq \mathbb{Z}^{\oplus 22}$. En plus, le cup produit induit sur $H^2(X, \mathbb{Z})$ une structure de réseau unimodulaire pair de signature* $(3, 19)$.

Si on note:

$$\Lambda_{K3} := E_8^{\oplus 2}(-1) \oplus U^{\oplus 3}$$

par le Corollaire 2.4.54 on a une isométrie de réseaux $H^2(X,\mathbb{Z}) \simeq \Lambda_{K3}$.

On donne aussi les définitions suivantes:

Définition 3.1.9. Soit X une surface K3, on note le groupe de Neron-Severi:

$$\begin{aligned} NS(X) &:= \{x \in H^2(X,\mathbb{Z}) | x \cdot \omega_X = 0\} \\ &= H^2(X,\mathbb{Z}) \cap H^{1,1}(X) \end{aligned}$$

ou la deuxième équivalence est conséquence du théorème de Lefschetz sur les classes $(1,1)$.

On note le groupe transcendant:

$$T(X) := NS(X)^{\perp_{H^2(X,\mathbb{Z})}}$$

On remarque que $NS(X)$,$T(X)$ sont deux sous-réseaux primitifs de $H^2(X,\mathbb{Z})$, en particulier on a que:

$$H^2(X,\mathbb{Z}) \supseteq NS(X) \oplus T(X)$$

est une extension primitive.

De plus, comme $H^2(X,\mathbb{Z}) \simeq \Lambda_{K3}$, le choix d'une isométrie (ce qu'on appelle un *marquage*) donne un plongement $NS(X) \hookrightarrow \Lambda_{K3}$ et $T(X) \hookrightarrow \Lambda_{K3}$.

On rappelle qu'à partir de la suite exponentielle:

$$0 \to \mathbb{Z} \to \mathcal{O}_X \to \mathcal{O}_X^* \to 0$$

on obtient la suite exacte en cohomologie:

$$... \to H^1(X,\mathcal{O}_X) \to H^1(X,\mathcal{O}_X^*) \xrightarrow{\delta} H^2(X,\mathbb{Z}) \xrightarrow{\epsilon} H^2(X,\mathcal{O}_X) \to ...$$

Qu'on peut réécrire sous la forme:

$$0 \to \mathrm{Pic}(X) \xrightarrow{c_1} H^2(X,\mathbb{Z}) \xrightarrow{\epsilon} H^2(X,\mathcal{O}_X)$$

Car $q = 0$ et donc $H^1(X,\mathcal{O}_X) = 0$. On a $H^2(X,\mathcal{O}_X) \simeq H^{0,2}(X)$ et d'après le théorème de Lefschetz sur les classes (1,1) (voir [GH, p. 163]) ϵ coïncide avec la projection $\pi^{0,2}$ selon la décomposition de Hodge. Donc $\ker(\epsilon) = \ker(\pi^{0,2}) \cap H^2(X,\mathbb{Z})$, mais si $\theta \in H^2(X,\mathbb{Z})$ alors en particulier $\theta = \overline{\theta}$ et donc $\pi^{2,0}(\theta) = 0$ aussi. Cela implique que $\theta \in H^{1,1}(X)$ et donc:

$$\mathrm{Pic}(X) \simeq H^2(X,\mathbb{Z}) \cap H^{1,1}(X) \simeq NS(X)$$

3.1.2 Les théorèmes de Torelli

Dans la suite X sera toujours une surface K3.

On a vu qu'un automorphisme σ de X induit une isométrie de réseaux:

$$\sigma^* : \Lambda_{K3} \to \Lambda_{K3}$$

qui respecte la décomposition de Hodge, donc $\sigma^*(NS(X)) = NS(X)$ et $\sigma^*(T(X)) = T(X)$.

Cela permet de donner des conditions nécessaires, sur une isométrie de Λ_{K3}, pour qu'elle soit induite par un automorphisme de X.

Ce qui peut être est plus surprenant, c'est qu'il est aussi possible d'effectuer le parcours inverse, c'est-à-dire donner des conditions suffisantes pour une isométrie de Λ_{K3} afin qu'elle soit induite par un automorphisme d'une surface K3.

C'est le but des théorèmes dits « de Torelli ».

Il existe plusieurs formulations possibles, nous avons préféré donner la suivante, qu'on trouve dans [BR]:

Théorème 3.1.10 (Torelli fort pour les surfaces K3)**.** *Soient X et X' deux surfaces K3 et on suppose qu'il existe une isométrie $\phi^* : H^2(X', \mathbb{Z}) \xrightarrow{\sim} H^2(X, \mathbb{Z})$ qui:*

1. *envoie $H^{2,0}(X', \mathbb{C})$ sur $H^{2,0}(X, \mathbb{C})$*
2. *envoie la classe d'un certain diviseur ample de X' sur la classe d'un diviseur ample de X*

Alors ϕ^* est induite par un isomorphisme unique *$\phi : X \to X'$.*

On donne d'abord quelques définitions:

Définition 3.1.11. Soit X une surface K3, on note:

- $\Delta(X) := \{\delta \in NS(X) | \delta^2 = -2\}$, les δ sont appelés *diviseurs nodaux* ;
- $W(X) \subseteq \mathrm{Aut}(H^2(X, \mathbb{Z}))$ le sous-groupe engendré par $\{R_\delta | \delta \in \Delta(X)\}$ où R_δ est la réflection par rapport à la droite δ (cf. Exemple 2.5.32). $W(X)$ est le groupe de Weil de X.

Remarque 3.1.12. L'action du groupe de Weil préserve la décomposition de Hodge et en particulier le réseau de Neron-Severi.

On peut maintenant énoncer le résultat suivant [Na, 3.10]:

Théorème 3.1.13. *Soit X une surface K3 et $G \subseteq O(\Lambda_{K3})$. Soit ω_X la forme symplectique dans $H^2(X, \mathbb{C})$, T_G le réseau invariant et $S_{G,X} := T_G^\perp \cap NS(X)$. Alors il existe $w \in W(X)$ groupe de Weil tel que $wGw^{-1} \subseteq Aut(X)$ si et seulement si :*

1. *$\mathbb{C}\omega$ est stable sous l'action de G ;*
2. *S_G ne contient aucun élément de carré -2 ;*
3. *Si G contient uniquement des actions symplectiques alors $S_{G,X}$ est défini négatif et non nul ;*
4. *Si G contient au moins une action non-symplectique alors il existe $x \in T_G$ avec $\langle x, x \rangle > 0$.*

3.1.3 Action de $\mathbb{Z}/p\mathbb{Z}$ sur une surface K3

On rappelle que l'objectif principal de ce travail est d'étudier l'action de G sur une surface K3 quand $G \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$. Cela car l'action du groupe de Klein, tout en restant faisable, présente plusieurs difficultés supplémentaires par rapport au cas de $G \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ cyclique, dont on peut trouver le traitement dans [BNS].

Cependant nous avons quand même décidé de reproposer le cas cyclique dans cette section, et cela pas uniquement pour une exigence d'exhaustivité ou pour résumer les résultats dans le cas d'une surface K3, mais surtout pour présenter une preuve alternative basée sur une méthode différente.

L'idée principale est qu'il n'est pas nécessaire d'étudier dans le détail toutes les possibilités de décomposition, ni pour les $\mathbb{Z}[G]$-modules, ni pour les $\mathbb{F}_p[G]$-modules: en effet, les seuls modules qui nous intéressent, sont les $\mathbb{F}_p[G]$-modules obtenus en tensorisant des $\mathbb{Z}[G]$-modules, ce qui constitue un ensemble plutôt restreint. Mais comment arriver à obtenir cela ?

Les outils qu'on utilisera sont les *anneaux pullback* [Le], qui nous permettent de simplifier considérablement une des preuves principales.

Lemme 3.1.14. *Soient R_1,R_2,$\overline{R}$ des anneaux, on considère le diagramme:*

$$\begin{array}{ccc} & & R_1 \\ & & \downarrow{\scriptstyle \nu_1} \\ R_2 & \xrightarrow{\nu_2} & \overline{R} \end{array}$$

avec v_1 et v_2 morphismes d'anneaux , alors le pullback du diagramme:

$$R = \{(x_1, x_2) \in R_1 \times R_2 | \nu_1(x_1) = \overline{x} = \nu_2(x_2)\}$$

est un sous-anneau de $R_1 \times R_2$.

Démonstration. On a $1_{R_1 \times R_2} \in R$ car $\nu_1(1_{R_1}) = \nu_2(1_{R_2})$, et $(R, +)$ est un groupe car il est le pullback du diagramme par rapport à la structure de groupe additif.

$$\begin{array}{ccc} R & \dashrightarrow & R_1 \\ \downarrow & & \downarrow{\scriptstyle \nu_1} \\ R_2 & \xrightarrow{\nu_2} & \overline{R} \end{array}$$

Soient $x^1, x^2 \in R$, $x^i = (x_1^i, x_2^i)$ avec $\nu_1(x_1^i) = \nu_2(x_2^i)$, alors $\nu_1(x_1^1 x_1^2) = \nu_2(x_2^1 x_2^2)$ et $x^1 x^2 \in R$ aussi. Donc R est un anneau car fermé par rapport au produit. □

Une méthode simple pour construire des exemples d'anneaux pullback est la suivante: soient A un anneau commutatif, I, J des idéaux de A, alors si $I + J = A$ par le théorème des restes chinois on sait que $\frac{A}{I \cap J} \simeq \frac{A}{I} \times \frac{A}{J}$ en tant qu'anneaux. Mais que se passe-t-il si I et J ne sont pas premiers entre

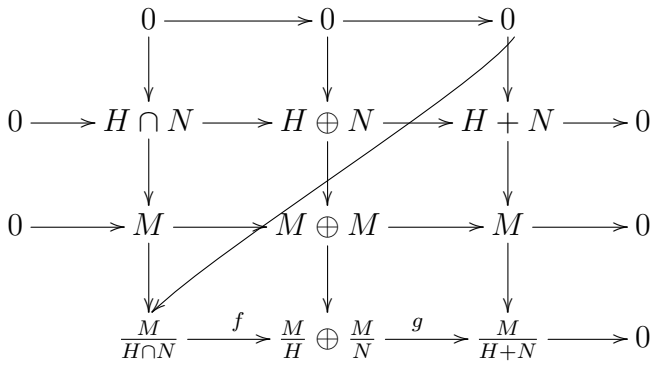
eux ? Dans ce cas on obtient en effet que $A/(I \cap J) \simeq A/I \times_{A/(I+J)} A/J$ est un anneau pullback.

On commence par présenter le résultat dans le cas des A-modules:

Proposition 3.1.15 (Théorème des restes chinois pour les modules)**.** *Soit A un anneau commutatif, M un A-module, $N, H \subseteq M$ des sous-modules. Alors:*

$$\frac{M}{N \cap H} \simeq \frac{M}{N} \times_{\frac{M}{N+H}} \frac{M}{H}$$

Démonstration. On considère le diagramme suivant avec ligne et colonnes exactes:



Par le Lemme du serpent la dernière ligne est exacte. Donc $M/(N \cap H) \simeq \ker(g)$, mais par définition $\ker(g)$ est égale au pullback $M/N \times_{M/(N+H)} M/H$ (avec signe opposé). □

Donc si I, J sont des idéaux de A, on a montré que $A/(I \cap J) \simeq A/I \times_{A/(I+J)} A/J$ en tant que A-modules, c'est-à-dire qu'il existe un isomorphisme de A-modules:

$$\begin{array}{rcl} \varphi : \dfrac{A}{I \cap J} & \xrightarrow{\simeq} & \dfrac{A}{I} \times_{\frac{A}{I+J}} \dfrac{A}{J} \\ x + I \cap J & \longmapsto & (x + I, x + J) \end{array}$$

mais comme φ est la co-restriction du produit des projections $\pi_I \times \pi_J : A/(I \cap J) \to A/I \times A/J$, on obtient que φ est aussi un morphisme d'anneaux. On a donc:

Proposition 3.1.16. *Soit A un anneau commutatif, $I, J \leq A$ des idéaux, alors on a un isomorphisme d'anneaux:*

$$\frac{A}{I \cap J} \simeq \frac{A}{I} \times_{\frac{A}{I+J}} \frac{A}{J}$$

Remarque 3.1.17. Dans le cas limite où $I + J = R$ le pullback coïncide avec le produit cartésien, et on obtient l'énoncé du théorème des restes chinois.

Soit $G = \mathbb{Z}/p\mathbb{Z}$, alors $\mathbb{Z}[G] \simeq \mathbb{Z}[x]/(x^p - 1)$, comme $(x^p - 1) = (x - 1)(x^{p-1} + \cdots + 1)$ on obtient que $\mathbb{Z}[G]$ est l'anneau pullback du diagramme:

$$\begin{array}{ccc} \mathbb{Z}[G] & \dashrightarrow & \frac{\mathbb{Z}[x]}{(x-1)} \simeq \mathbb{Z} \\ \downarrow & & \downarrow \\ \frac{\mathbb{Z}[x]}{(x^{p-1}+\cdots+1)} \simeq \mathbb{Z}[\xi] & \twoheadrightarrow & \frac{\mathbb{Z}[x]}{(x-1, x^{p-1}+\cdots+1)} \simeq \mathbb{F}_p \end{array}$$

Si M est un $\mathbb{Z}[G]$ module sans $\mathbb{Z}$-torsion (comme dans le cas où M est un réseau) alors par la Proposition 3.1.15 on a le diagramme:

$$\begin{array}{ccc} M & \dashrightarrow & \frac{M}{\ker(x^{p-1}+\cdots+1)} \\ \downarrow & & \downarrow \\ \frac{M}{\ker(x-1)} & \longrightarrow & \frac{M}{\ker(x-1) \oplus \ker(x^{p-1}+\cdots+1)} \end{array} \tag{3.1.1}$$

où:

- M est le pullback du diagramme ;
- Pour tout $m \in M$ on a $(x^p - 1) \cdot m = 0$, en particulier $(x - 1) \cdot m \in \ker(x^{p-1} + \cdots + 1)$ et donc sur $\frac{M}{\ker(x^{p-1}+\cdots+1)}$ l'action de x est triviale, i.e. $\frac{M}{\ker(x^{p-1}+\cdots+1)}$ est juste un $\mathbb{Z}$-module
- De la même façon $\frac{M}{\ker(x-1)}$ est un $\mathbb{Z}[\xi]$-module avec $\xi^p = 1$, $\xi \neq 1$
- $\frac{M}{\ker(x-1)\oplus\ker(x^{p-1}+\cdots+1)}$ est de p-torsion et donc est un $\mathbb{F}_p$-module. Il est alors de la forme $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^a$ pour un certain $a \in \mathbb{N}$.

On peut donc reconstruire M à partir des ces trois modules sur des anneaux où la classification est beaucoup plus simple.

De plus, on peut montrer que dans le cas où M est indécomposable, alors ces trois composantes sont aussi des modules indécomposables sur les anneaux respectifs:

Théorème 3.1.18 ([CR, Le])**.** *Soit $G \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premier et $M \neq 0$ un $\mathbb{Z}[G]$-module indécomposable de type fini tel que $(M, +)$ soit sans torsion. Soit ξ une racine primitive p-ième de l'unité.*

Alors on a les possibilités suivantes pour M:

1. *$M \simeq \mathbb{Z}$*
2. *$M \simeq I$ idéal non nul de $\mathbb{Z}[\xi]$;*
3. *$M \simeq \mathbb{Z} \times_{\mathbb{F}_p} I$ avec I idéal non nul de $\mathbb{Z}[\xi]$ tel que $I \simeq \ker(x^{p-1} + \cdots + \mathrm{Id})$ et $\ker(x - \mathrm{Id}) \simeq \mathbb{Z}$:*

$$\begin{array}{ccc} M & \dashrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ I & \twoheadrightarrow & \mathbb{F}_p \end{array}$$

On est prêt pour montrer:

Théorème 3.1.19. *Soit p premier et $G \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} \simeq \langle \eta \rangle$ qui agit sur un $\mathbb{Z}$-module L sans torsion. On pose $T_G := L^G = \ker(\eta)$, $S_G := \ker(\eta^{p-1} + \cdots + \eta + 1)$ et $a = \dim_{\mathbb{F}_p} \frac{L}{S_\varphi + T_\varphi}$. Alors $L \otimes \frac{\mathbb{Z}}{p\mathbb{Z}}$ comme $\mathbb{F}_p[G]$-module se décompose sous la forme:*

$$L \otimes \mathbb{F}_p \simeq \mathbb{F}_p^{\oplus \operatorname{rang}(T_G) - a} \oplus \left(\frac{\mathbb{F}_p[x]}{(x-1)^{p-1}}\right)^{\oplus \frac{\operatorname{rang}(S_G)}{p-1} - a} \oplus \left(\frac{\mathbb{F}_p[x]}{(x-1)^p}\right)^{\oplus a}$$

Démonstration. L'action de G sur L induit une structure de $\mathbb{Z}[G]$-module sur L, soit donc $L \simeq \bigoplus M_i$ une décomposition en composantes irréductibles. Soit M une composante irréductible, par le Théorème 3.1.18 on a trois possibilités:

1 L'action de G sur M est triviale et $M \simeq \mathbb{Z}$, dans ce cas $M \subseteq T_\varphi$ et $M \otimes \mathbb{F}_p \simeq \mathbb{F}_p$;

2 $M \simeq I$ idéal de $\mathbb{Z}[\xi]$ ($\mathbb{Z}[\xi] \simeq \mathbb{Z}[x]/(x^{p-1} + \cdots + 1)$ avec $\xi^p = 1$, $\xi \neq 1$), donc M est un module projectif et en particulier M est plat. Donc le produit tensoriel $M \otimes \mathbb{F}_p$ est un $\mathbb{Z}[\xi] \otimes \mathbb{F}_p$-module plat et donc libre car de type fini sur un anneau local, mais:

$$\dim_{\mathbb{F}_p}(M \otimes \mathbb{F}_p) = \operatorname{rang}(M) \leq \operatorname{rang}(\mathbb{Z}[\xi]) = p$$

donc:

$$M \otimes \mathbb{F}_p \simeq \mathbb{F}_p[\xi] \simeq \frac{\mathbb{F}_p[x]}{(x-1)^{p-1}}$$

En particulier $\operatorname{rang}(M) = p - 1$ et comme $M \simeq I$ on a aussi $M \subseteq \ker(\varphi - \mathrm{Id}) = T_\varphi$

3 M est le pullback du diagramme:

$$\begin{array}{ccc} M & \dashrightarrow & \mathbb{Z} \\ \vdots & & \downarrow \\ I & \longrightarrow & \mathbb{Z} \end{array}$$

donc M est un $\mathbb{Z}[G]$-module projectif car pullback de modules projectifs sur les anneaux respectifs ([Le, Wi]) et $M \otimes \mathbb{F}_p$ est plat sur $\mathbb{F}_p[G]$ et de dimension p sur $\mathbb{F}_p$, donc $M \otimes \mathbb{F}_p \simeq \mathbb{F}_p[G]$. En plus, M a rang p, $M \cap T_\varphi \simeq \mathbb{Z}$ a rang 1 et $M \cap S_\varphi \simeq I$ a rang $p - 1$.

Soit n_i pour $i = 1, 2, 3$ le nombre de modules indécomposables de type i dans la décomposition de L, alors on a montré que $\operatorname{rang}(T_\varphi) = n_1 + n_3$, $\operatorname{rang}(S_\varphi) = (n_2 + n_3)(p-1)$ et:

$$a = \dim_{\mathbb{F}_p}\left(\frac{L}{S_\varphi + T_\varphi}\right) = \dim_{\mathbb{F}_p}\left(\bigoplus \frac{M_i}{M_i \cap S_\varphi \oplus M_i \cap T_\varphi}\right) = n_3$$

ce qui conclut la preuve.

□

Remarque 3.1.20. Ce résultat est prouvé dans [BNS] pour p tel que $\mathbb{Z}[\xi]$ soit principal et dans [Tar] pour le cas général. Cependant, comme je l'ai mentionné avant, la preuve présente ici est différente, car elle ne fait pas une utilisation directe de la classification des $\mathbb{Z}[G]$-modules, ce qui la rend plus naturelle et donne aussi plus de possibilités (on espère !) pour étendre le résultat au cas général $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Si L est un réseau, comme $a = \dim_{\mathbb{F}_p} \frac{L}{S_\varphi + T_\varphi}$, on a $\#A_{S_\varphi} \#A_{T_\varphi} = p^{2a} \#A_L$. Donc si L est unimodulaire, comme dans le cas de Λ_{K3}, alors $\#A_{S_\varphi} = \#A_{T_\varphi} = p^a$ et donc les seuls invariants nécessaires pour déterminer la structure de $\mathbb{F}_p[G]$-module sont $\#A_{T_\varphi}$ et $\mathrm{rang}(T_\varphi)$.

En appliquant le Théorème 1.3.10 on obtient:

Théorème 3.1.21. *Soit X un surface K3, φ un automorphisme de X d'ordre p premier avec lieu fixe non vide. Soient $t = \mathrm{rang}(T_\varphi)$, $\#A_{T_\varphi} = p^a$ alors:*

$$\sum_i \dim_{\mathbb{F}_p} H^i(X^\varphi, \mathbb{F}_p) = t + \frac{(22-t)}{p-1} - 2a + 2$$

Démonstration. On rappelle que par le Théorème 3.1.19 on a que les $\mathbb{F}_p[G]$-modules indécomposables ont uniquement dimension 1 ($n_1 = t - a$), $p-1$ ($n_2 = (22-t)/(p-1) - a$) ou p ($n_3 = a$). Par le Théorème 1.3.10 on a $\sum_i \dim_{\mathbb{F}_p} H^i(X^\varphi, \mathbb{F}_p) = n_1 + n_2 + 2$ et en remplaçant on obtient le résultat cherché. □

3.2 Action de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ sur une surface K3

3.2.1 Un nouvel invariant pour les extensions de réseaux

On donne la définition suivante, présentée dans un cadre général, qui nous sera essentielle pour définir les invariants numériques qui vont apparaître dans le résultat principal de ce travail:

Définition 3.2.1. Soit $R \supseteq L_1 \oplus \cdots \oplus L_n$ une extension de réseaux, alors on note:

$$K_R := \frac{R}{L_1^\perp + \cdots + L_n^\perp}$$

Remarque 3.2.2. On rappelle que $H_R = R/(L_1 \oplus \cdots \oplus L_n)$, donc on a une projection:

$$H_R \twoheadrightarrow K_R$$

Plus en général, si on pose:

$$H_R^k := \frac{R}{\sum_{\{i_1,\ldots,i_k\} \subseteq \{1,\ldots,n\}} \left(R \cap \mathrm{span}_{\mathbb{Q}}(L_{i_1} + \cdots + L_{i_k})\right)}$$

alors $H_R^1 = H_R$, $H_R^{n-1} = K_R$, $H_R^n = 0$ et on a une filtration:

$$H_R^1 \twoheadrightarrow H_R^2 \twoheadrightarrow H_R^3 \twoheadrightarrow \cdots \twoheadrightarrow H_R^{n-1} \twoheadrightarrow H_R^n \tag{3.2.1}$$

Exemple 3.2.3. Si $n = 2$, $R \supseteq L_1 \oplus L_2$, on obtient:

$$K_R = \frac{R}{L_1^\perp + L_2^\perp}$$

Si l'extension est primitive alors $L_1^\perp = L_2$ et $L_2^\perp = L_1$, donc:

$$K_R = \frac{R}{L_1 \oplus L_2} = H_R$$

Exemple 3.2.4. On considère $L_1 = L_2 = L_3 = A_8$, $L_4 = A_2$. Alors $q_{L_i} = w_{3,2}^{-1}$ pour $i = 1, 2, 3$ et $q_{L_3} = w_{3,1}^{-1}$. Soient $v_i \in L_i^*$ tels que pour $1 \leq i \leq 4$ $A_{L_i} = \mathrm{span}(\overline{v}_i)$, alors on pose:

$$H_R = \mathrm{span}(\overline{w}_1, \overline{w}_2) \subseteq A_{L_1} \oplus \cdots \oplus A_{L_4}$$

avec $w_1 = v_1 + 2v_2 - v_3 + 2v_4$, $w_2 = 2v_1 + v_2 + v_3 + v_4$.

Comme $q(\overline{w}_1) \equiv q(\overline{w}_2) \equiv 4 \cdot \frac{8}{9} + \frac{8}{9} + \frac{8}{9} + \frac{2}{3} \equiv \frac{0}{9}$ et $b(\overline{w}_1, \overline{w}_2) \equiv -\frac{2}{9} - \frac{2}{9} + \frac{1}{9} + \frac{1}{3} \equiv \frac{0}{9}$, alors H_R est totalement isotrope et il définit donc une extension de réseaux $R \supseteq L_1 \oplus \cdots \oplus L_4$.

On a $\overline{w}_3 = 3\overline{v}_3 + 2\overline{v}_4 \in H_R^\perp$ et il suffit de vérifier les dimensions pour montrer que $H^\perp = \mathrm{span}(\overline{w}_1, \overline{w}_2, \overline{w}_3)$ et donc $A_R \simeq \frac{H_R^\perp}{H_R} \simeq (\mathbb{Z}/3\mathbb{Z})^3$ avec $q_{A_R} \simeq w_{3,1}^{-1}$.

On cherche à calculer K_R. On trouve:

$$\begin{aligned}
L_1^\perp &= \mathrm{span}(L_2, L_3, L_4) \\
L_2^\perp &= \mathrm{span}(L_1, L_3, L_4) \\
L_3^\perp &= \mathrm{span}(L_1, L_2, L_4, 3v_1 + 3v_2) \\
L_4^\perp &= \mathrm{span}(L_1, L_2, L_3, 3v_1 + 3v_2, 3w_2) \\
R &= \mathrm{span}(L_1, L_2, L_3, L_4, w_1, w_2)
\end{aligned}$$

donc:

$$\begin{aligned}
K_R &= \frac{R}{L_1^\perp + L_2^\perp + L_3^\perp + L_4^\perp} \\
&\simeq \frac{\mathrm{span}(L_1, L_2, L_3, L_4, w_1, w_2)}{\mathrm{span}(L_1, L_2, L_3, L_4, 3v_1 + 3v_3, 3w_2)} \\
&\simeq \frac{\mathrm{span}(w_1, w_2)}{\mathrm{span}(3v_1 + 3v_2, 3w_2)} \\
&\simeq \frac{\mathbb{Z}}{3\mathbb{Z}}
\end{aligned}$$

On complète le calcul pour tous les autres H_R^i. Pour H_R on a:

$$H_R \simeq \mathrm{span}(\overline{w}_1, \overline{w}_2) \simeq \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$$

Pour H_R^2 on a:

$$\begin{aligned} H_R^2 &= \frac{\text{span}(L_1, L_2, L_3, L_4, w_1, w_2)}{\text{span}(L_1, L_2, L_3, L_4, 3v_1 + 3v_2)} \\ &= \frac{\mathbb{Z}}{9\mathbb{Z}} \end{aligned}$$

Donc la filtration (3.2.1) devient:

$$\frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}} \twoheadrightarrow \frac{\mathbb{Z}}{9\mathbb{Z}} \twoheadrightarrow \frac{\mathbb{Z}}{3\mathbb{Z}} \twoheadrightarrow 0$$

Proposition 3.2.5. *Soit $R \supseteq L_1 \oplus \cdots \oplus L_n$ une extension primitive de réseaux. Alors:*

1

$$K_R \simeq \frac{H_R}{\sum_i \left(H_R \cap (A_{L_1} \oplus \cdots \oplus A_{L_{i-1}} \oplus A_{L_{i+1}} \oplus \cdots \oplus A_{L_n})\right)}$$

2

$$K_R \simeq \frac{\left(H_R^\perp + A_{L_1}\right) \cap \cdots \cap \left(H_R^\perp + A_{L_n}\right)}{H_R^\perp}$$

Démonstration. 1) On rappelle que:

$$\begin{aligned} K_R &= \frac{R}{L_1^\perp + \cdots + L_n^\perp} \\ &= \frac{R}{\sum_{i=1}^n \left(R \cap (L_1^* + \cdots + L_{i-1}^* + L_{i+1} + \cdots + L_n^*)\right)} \end{aligned}$$

On quotiente les deux termes par $L_1 \oplus \cdots \oplus L_n$:

$$\begin{aligned} K_R &\simeq \frac{R/L_1 \oplus \cdots \oplus L_n}{\sum_{i=1}^n \left(R \cap (L_1^* + \cdots + L_{i-1}^* + L_{i+1}^* + \cdots + L_n^*)\right)/(L_1 \oplus \cdots \oplus L_n)} \\ &\simeq \frac{H_R}{\sum_{i=1}^n \left(H_R \cap (A_{L_1} + \cdots + A_{L_{i-1}} + A_{L_{i+1}} + \cdots + A_{L_n}\right)} \\ &\simeq \frac{H_R}{\sum_{i=1}^n \left(H_R \cap A_{L_i}^\perp\right)} \end{aligned}$$

2) Par le Lemme 2.3.31 on a:

$$\begin{aligned} K_R &\simeq \frac{H_R}{\sum_{i=1}^n \left(H_R \cap A_{L_i}^\perp\right)} \\ &\simeq \frac{\left(\sum_{i=1}^n \left(H_R \cap A_{L_i}^\perp\right)\right)^\perp}{H_R^\perp} \\ &\simeq \frac{\bigcap_{i=1}^n \left(H_R \cap A_{L_i}^\perp\right)^\perp}{H_R^\perp} \\ &\simeq \frac{\bigcap_{i=1}^n \left(H_R^\perp + A_{L_i}\right)}{H_R^\perp} \end{aligned}$$

□

Remarque 3.2.6. Si $R \supseteq L_1 \oplus \cdots \oplus L_n$ est une extension avec R unimodulaire alors:

$$\frac{H_R^\perp}{H_R} \simeq A_R \simeq 0$$

donc $H_R^\perp = H_R$ et en particulier:

$$K_R \simeq \frac{(H_R + A_{L_1}) \cap \cdots \cap (H_R + A_{L_n})}{H_R}$$

Proposition 3.2.7. *Soit $R \supseteq L_1 \oplus \cdots \oplus L_n$ une extension primitive de réseaux avec R unimodulaire. Alors:*

1. $K_R \simeq \{(l_1^*, \ldots, l_n^*) \in A_{L_1} \times \cdots \times A_{L_n}$ *tel que* $l_j^* - l_i^* \in H_R$ *pour tout* $1 \leq i, j \leq n\}$;
2. $K_R \simeq \{(l_1^*, \ldots, l_n^*) \in A_{L_1} \times \cdots \times A_{L_n}$ *tel que* $l_1^* - l_i^* \in H_R$ *pour tout* $1 \leq i \leq n\}$;
3. *Il existe un plongement* $K_R \hookrightarrow A_{L_i}$.

Démonstration. 1) Soient:

$$\begin{aligned} N &:= \{(l_1^*, \ldots, l_n^*) \in A_{L_1} \times \cdots \times A_{L_n} \text{ tel que } l_j^* - l_i^* \in H_R\} \\ N_1 &:= \frac{\bigcap_{i=1}^n (H_R + A_{L_i})}{H_R} \end{aligned}$$

Par la Remarque 3.2.6 on a $K_R \simeq N_1$. Soit φ le morphisme:

$$\begin{aligned} \varphi : N &\to N_1 \\ (l_1^*, \ldots, l_n^*) &\mapsto l_1^* + H_R^\perp \end{aligned}$$

L'extension est primitive, donc par le Lemme 2.5.1 on a $A_{L_i} \cap H_R = 0$ et φ est injective.

De plus, φ est surjective, car par définition de N pour tout $l^* + H_R \in N_1$, il existe $h_1, \ldots, h_n \in H_R$ tels que:

$$l^* = l_1^* + h_1 = \cdots = l_n^* + h_n$$

donc $l_i^* - l_j^* = h_j - h_i \in H_R$ et $(l_1^*, \ldots, l_n^*) \in N$ avec $\varphi(l_1^*, \ldots, l_n^*) = l + H_R$.

2) Découle directement de 1).

3) On considère la restriction sur H de la projection sur A_{L_1}:

$$\begin{aligned} \pi_{A_{L_1}} : N &\to A_{L_1} \\ (l_1^*, \ldots, l_n^*) &\mapsto l_1^* \end{aligned}$$

alors si $(l_1^*, \ldots, l_n^*) \in \ker(\pi_{A_{L_1}})$ cela implique que $l_1^* = 0$ et donc $l_i^* \in H_R$ pour $1 \leq i \leq n$. Mais l'extension est primitive, donc $l_i^* = 0$ pour tout i et l'application est injective. □

Dans le cas particulier de notre intérêt, où $n = 3$ et $R \supseteq L_1 \oplus L_2 \oplus L_3$ est une extension primitive, on a l'expression suivante pour K_R:

Proposition 3.2.8. *Soit $R \supseteq L_1 \oplus L_2 \oplus L_3$ une extension primitive avec R unimodulaire. On note:*

$$\begin{aligned} H_{L_3^\perp} &:= H_R \cap (A_{L_1} \oplus A_{L_2}) \\ H_{L_3^\perp, L_1} &:= \pi_{A_{L_1}}(H_{L_3^\perp}) \end{aligned}$$

alors:

$$K_R \simeq \left(H_{L_3^\perp, L_1}\right)^\circ := \left(H_{L_3^\perp, L_1}\right)^{\perp_{H_{L_3^\perp, L_1}}}$$

Démonstration. Par la Proposition 3.2.7 on a:

$$K_R \simeq N = \{(l_1^*, l_2^*, l_3^*) \in A_{L_1} \times A_{L_2} \times A_{L_3} \text{ tel que } l_i^* - l_1^* \in H_R\}$$

Soit $\pi_{A_{L_1}}$ le morphisme:

$$\begin{aligned} \pi_{A_{L_1}} : N &\to A_{L_1} \\ (l_1^*, l_2^*, l_3^*) &\mapsto l_1^* \end{aligned}$$

on veut montrer que $\mathrm{Im}(\pi_{A_{L_1}}) = \left(H_{L_3^\perp, L_1}\right)^\circ$.

Soit $l = (l_1^*, l_2^*, l_3^*) \in N$, alors $l_1^* - l_2^* \in H_R$ et donc $l_1^* \in H_{L_3^\perp, L_1}$. On a aussi que $l_1^* - l_3^* \in H_R$ et comme H_R est totalement isotrope on a $l_1^* - l_3^* \perp H_R$, et en particulier $l_1^* - l_3^* \perp H_{L_3^\perp}$. Mais $l_3^* \perp H_{L_3^\perp}$ car $l_3^* \in A_{L_3}$ donc aussi $l_1^* \perp H_{L_3^\perp}$ et comme $l_i^* \perp A_{L_2}$ on a $l_1^* \perp H_{L_3^\perp, L_1}$. Donc $\mathrm{Im}(\pi_{A_{L_1}}) \subseteq \left(H_{L_3^\perp, L_1}\right)^\circ$.

Maintenant on montre l'inclusion inverse:

Soit $l_1^* + l_2^* \in H_{L_3^\perp}$ tel que $l_1^* \in \left(H_{L_3^\perp, L_1}\right)^\circ$, alors $l_1^* \in H_{L_3^\perp}^\perp$. Si on considère l'extension $R \supseteq L_3^\perp \oplus L_3$, comme $A_{L_3^\perp} \simeq \frac{H_{L_3^\perp}^\perp}{H_{L_3^\perp}}$ on obtient que $l_1^* \in A_{L_3^\perp}$ et comme R est unimodulaire, il existe $l_3^* \in A_{L_3}$ tel que $l_1^* + l_3^* \in H_R$. Donc $(l_1^*, -l_2^*, -l_3^*) \in N$, ce qui conclut la preuve. □

Exemple 3.2.9. Soient $L_1 = L_2 = L_3 = D_8$, alors $A_{L_i} \simeq u_1$ et soit (v_i, w_i) une base de A_{L_i} telle que la matrice soit:

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

On pose alors:

$$H_R = \mathrm{span}(v_1 + w_2 + w_3, w_1 + v_2 + w_3, w_1 + w_2 + v_3)$$

On vérifie facilement que H_R est totalement isotrope, donc il définit une extension de réseau $R \subseteq L_1 \oplus L_2 \oplus L_3$. Comme $H_R \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$, par le Lemme 2.3.78 on obtient que R est un réseau unimodulaire et on peut donc appliquer la Proposition 3.2.8 et $K_R \simeq \left(H_{L_3^\perp, L_1}\right)^\circ$.

Pour $H_{L_3^\perp}$ on trouve:

$$\begin{aligned} H_{L_3^\perp} &= H_R \cap (A_{L_1} \oplus A_{L_2}) \\ &= \text{span}(v_1 - w_1 + w_2 - v_2) \end{aligned}$$

et donc $H_{L_3^\perp, L_1} = \text{span}(v_1 - w_1)$. Comme $q(v_1 - w_1) \equiv 1 - 2 \cdot \frac{1}{2} + 0 \equiv 0$ on a

$$\left(H_{L_3^\perp, L_1}\right)^\circ = H_{L_3^\perp, L_1} = \text{span}(v_1 - w_1)$$

et donc $K_R \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$.

3.2.2 Définition du contexte

Soit X une surface K3 et $G \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ qui agit sur X.

- On s'intéresse d'abord au cas non-symplectique, donc on suppose que $\eta \in G$ est une involution non-symplectique, i.e $\eta^*(\omega) = -\omega$ avec ω forme symplectique de X.
  Dans ce cas il doit y avoir au moins une involution symplectique $\iota \in G$ (sinon on pourrait composer deux involutions non-symplectiques pour l'obtenir) et donc $G = \{Id, \iota, \eta, \iota \circ \eta = \eta \circ \iota = \nu\}$ avec η, ν involutions non-symplectiques et ι une involution symplectique.
- On sait que le lieu fixe de toute involution symplectique d'une surface K3 fixe est exactement 8 points [Nik2], donc le lieu fixe de G est un sous-ensemble du lieu fixe de l'action du morphisme symplectique $\iota \in G$. Donc soit X^G est vide (et dans ce cas on est hors des hypothèses d'application du Théorème 1.3.15), soit il doit être composé par n points, $1 \leq n \leq 8$, et toujours d'après le Théorème 1.3.15 dans ce cas on obtient:

Lemme 3.2.10. *Soit X une surface K3, $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ qui agit sur X avec lieu fixe non vide. Alors $X^G = \{n \text{ points}\}$ avec:*

$$n = \#\textit{modules impairs indécomposables de } H^2(X, \mathbb{F}_2) + 2$$

Démonstration. Par le Théorème 1.3.15 on a:

$$\sum_i \dim_{\mathbb{F}_2} H^i(X^G, \mathbb{F}_2) = \# \left\{ \begin{array}{c} \text{modules impairs indécomposables} \\ \text{dans la décomposition de } H^2(X, \mathbb{F}_2) \end{array} \right\} + 2$$

Comme le lieu fixe est un ensemble de points et $\sum_i \dim_{\mathbb{F}_2} H^i(\text{pt}, \mathbb{F}_2) = 1$ on obtient que $\sum_i \dim_{\mathbb{F}_2} H^i(X^G, \mathbb{F}_2) = \#X^G$. □

- Comme ι est une involution symplectique on a aussi $S_{\iota^*} = E_8(-2) \subseteq NS(X)$ ([Mo]).

- On passe maintenant à l'involution non-symplectique: on peut affirmer que X est une surface algébrique car elle admet un automorphisme non-symplectique d'ordre fini [Nik2]. On a alors que $NS(X)$ est un réseau hyperbolique, i.e. de signature $(1, r-1)$ [Nik2] avec r le nombre de Picard.
- On suppose aussi que l'action de η^* sur le groupe de Neron-Severi est triviale (ce qui représente le cas général), c'est à dire $NS(X) \subseteq T_{\eta^*}$ (on rappelle que $T_{\eta^*} := \Lambda_{K3}^{\eta^*}$ est le réseau invariant). En général on a aussi que $T_{\eta^*} \subseteq NS(X)$ [Nik2], donc dans notre cas on obtient $T_{\eta^*} = NS(X)$ et $S_{\eta^*} = T(X)$ (on rappelle que $S_{\eta^*} := T_{\eta^*}^{\perp}$ est le réseau coinvariant).
- Comme $S_{\iota^*} \subseteq NS(X) = T_{\eta^*}$ alors $S_{\iota^*} \cap T_{\eta^*} = S_{\iota^*}$ et $S_{\eta^*} = T_{\eta^*}^{\perp} \subseteq S_{\iota^*}^{\perp} = T_{\iota^*}$, qui implique $T_{\iota^*} \cap S_{\eta^*} = S_{\eta^*}$ et $S_{\iota^*} \cap S_{\eta^*} = 0$;
- Vu que $\nu^* = \iota^* \circ \eta^* = \eta^* \circ \iota^*$ alors $T_{\iota^*} \cap T_{\eta^*} = T_{\nu^*} \cap T_{\eta^*}$. Mais $T_{\nu^*} \cap S_{\eta^*} = S_{\iota^*} \cap S_{\eta^*} = 0$ donc $T_{\nu^*} \subseteq T_{\eta^*}$ et $T_{\iota^*} \cap T_{\eta^*} = T_{\nu^*} T_{\iota^*} \cap T_{\eta^*} = T_{\nu^*}$.

La situation est la suivante:

$$\left.\begin{array}{lrcll} (L_1) & T_{\nu^*} & = & T_{\iota^*} \cap T_{\eta^*} & \text{avec signature } (1, r-9) \\ (L_2) & S_{\iota^*} & = & S_{\iota^*} \cap T_{\eta^*} & \simeq E_8(-2) \end{array}\right\} \quad NS(X)$$

$$\left.\begin{array}{lrcll} (L_3) & S_{\eta^*} & = & T_{\iota^*} \cap S_{\eta^*} & \text{avec signature } (2, 20-r) \\ & & & S_{\iota^*} \cap S_{\eta^*} = 0 & \end{array}\right\} \quad T(X)$$

Dans la suite on notera L_1, L_2, L_3 les trois réseaux cités ci-dessus. Donc $L_3 = T(X)$ et par le Lemme 2.5.30 on a $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$, $NS(X) \supseteq L_1 \oplus L_2$ sont des extensions primitives. On a aussi $L_1 \simeq T_{\nu^*}$ est 2-élémentaire par le Corollaire 2.5.27 car c'est le réseau invariant d'une involution sur un réseau unimodulaire, et pour la même raison, $L_2 = S_{\iota^*}$ et $L_3 = S_{\eta^*}$ sont aussi 2-élémentaires.

On définit alors a_1, a_2, a_3 tels que:

$$\begin{array}{rcl} A_{L_1} & \simeq & (\mathbb{Z}/2\mathbb{Z})^{a_1} \\ A_{L_2} & \simeq & (\mathbb{Z}/2\mathbb{Z})^{a_2} \\ A_{L_3} & \simeq & (\mathbb{Z}/2\mathbb{Z})^{a_3} \end{array}$$

On rappelle que $H_{\Lambda_{K3}} = \Lambda_{K3}/(L_1 \oplus L_2 \oplus L_3)$ et $K_{\Lambda_{K3}} = \Lambda_{K3}/(L_1^{\perp} + L_2^{\perp} + L_3^{\perp})$ (cf Section 3.2.1). Comme $H_{\Lambda_{K3}} \subseteq A_{L_1} \oplus A_{L_2} \oplus A_{L_3}$ et $H_{\Lambda_{K3}} \twoheadrightarrow K_{\Lambda_{K3}}$ on a que $K_{\Lambda_{K3}}$ est sous la forme:

$$K_{\Lambda_{K3}} \simeq (\mathbb{Z}/2\mathbb{Z})^k$$

où k est un invariant numérique associé à l'extension.

On s'est donc ramené au langage des réseaux uniquement. Pour résumer, on a les inclusions suivantes:

$$\begin{array}{ccccc} \Lambda_{K3} & \supset & NS(X) & \oplus & T(X) \\ & & \cup & & || \\ & & L_1 \oplus L_2 & & L_3 \end{array}$$

On peut montrer que la procédure inverse est possible, c'est-à-dire à n'importe quelle extension de réseaux qui respecte les critères décrits ci-dessous on peut associer une couple d'involutions:

Théorème 3.2.11. *Soit $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ une extension primitive de réseaux telle que:*

1 $L_2 \simeq E_8(-2)$;

2 L_i est un réseau 2-élémentaire pour $i = 1, 2, 3$;

3 L_1 a signature $(1, r-9)$, avec $9 \leq r \leq 20$;

alors ils existent X surface K3 et une isométrie $\psi : \Lambda_{K3} \xrightarrow{\sim} H^2(X, \mathbb{Z})$ avec $NS(X) = \psi(L_3^{\perp})$, qui admet deux involutions commutant ι, η respectivement symplectique et non-symplectique, telles que $\psi(L_1) = T_{\iota^*} \cap T_{\eta^*}$, $\psi(L_2) = S_{\iota^*} \cap T_{\eta^*}$, et $\psi(L_3) = T_{\iota^*} \cap S_{\eta^*}$.

Démonstration. On remarque que la signature de $L_3^{\perp}$ est $(1, r-1)$, donc pour une conséquence de la surjectivité de l'application des périodes [Mo, 1.9] il existe X surface K3 et $\tilde{\psi} : \Lambda_{K3} \xrightarrow{\sim} H^2(X, \mathbb{Z})$ tels que $NS(X) = \tilde{\psi}(L_3^{\perp})$.

Comme les L_i sont des réseaux 2-élémentaires, en particulier on a $H_{\Lambda_{K3}} = \Lambda_{K3} / (L_1 \oplus L_2 \oplus L_3)$ est de 2-torsion et par la Proposition 2.5.35 ils existent $\tilde{\iota}, \tilde{\eta}$ involutions commutant de Λ_{K3} tels que $L_1 = T_{\tilde{\iota}} \cap T_{\tilde{\eta}}$, $L_2 = S_{\tilde{\iota}} \cap T_{\tilde{\eta}}$, et $L_3 = T_{\tilde{\iota}} \cap S_{\tilde{\eta}}$.

Soit $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ engendré par $\tilde{\iota}, \tilde{\eta}$, alors les hypothèses du Théorème 3.1.13 sont vérifiées car:

1 Soit $\tilde{\omega}_X = \tilde{\psi}^{-1}(\omega_X)$, alors $\mathbb{C}\omega_X \in T(X) \otimes \mathbb{C}$ donc $\mathbb{C}\tilde{\omega}_X \in L_3 \otimes \mathbb{C}$ est stable sous l'action de G, car $\tilde{\iota}(\tilde{\omega}_X) = \tilde{\psi}^{-1}(\tilde{\omega}_X)$ et $\tilde{\eta}(\tilde{\omega}_X) = -\tilde{\psi}^{-1}(\tilde{\omega}_X)$;

2 On a $T_G = T_{\tilde{\iota}} \cap T_{\tilde{\eta}} = L_1$, donc $S_G = T_G^{\perp} \cap \tilde{\psi}^{-1}(NS(X)) = L_2 \simeq E_8(-2)$ qui ne contient aucun élément de carré -2 ;

3 G n'a pas une action purement symplectique (car $\tilde{\eta}(\tilde{\omega}_X) = -\tilde{\psi}^{-1}(\tilde{\omega}_X)$) et L_1 contient au moins en élément de carré strictement positif car a signature $(1, r-9)$.

Il existe alors une isométrie w dans le groupe de Weil de X tel que $G' := wGw^{-1} \subseteq \mathrm{Aut}(X)$. Comme l'action de w préserve $NS(X)$, il suffit de choisir $\psi := \tilde{\psi} \circ w^{-1}$ pour conclure. □

On peut maintenant présenter le résultat principal de notre travail, dont la preuve est contenue dans la suite de ce chapitre. Soit $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ l'extension donnée par l'action de G et on rappelle que $A_{L_i} = (\mathbb{Z}/2\mathbb{Z})^{a_i}$ avec $a_2 = 8$ et $K_{\Lambda_{K3}} = (\mathbb{Z}/2\mathbb{Z})^k$, alors:

Théorème. 3.2.22 *Soit X une surface K3, ι et η deux involutions commutant de X tels que ι soit symplectique et η non-symplectique avec action triviale sur $NS(X)$. Avec les notations expliquées plus haut, si $X^G \neq \emptyset$ alors X^G est une réunion de points avec:*

$$\#X^G = 16 - a_1 - a_3 + 2k$$

3.2.3 Action modulo 2

Soit donc $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ un sur-réseau unimodulaire, avec $L_1 = T_{\iota^*} \cap T_{\eta^*}$, $L_2 = S_{\iota^*} \cap T_{\eta^*}$, et $L_3 = T_{\iota^*} \cap S_{\eta^*}$, ι^*, η^* involutions commutant de Λ_{K3}, $G = \langle \iota^*, \eta^* \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$, $A_{L_i} = (\mathbb{Z}/2\mathbb{Z})^{a_i}$ et $K_{\Lambda_{K3}} = (\mathbb{Z}/2\mathbb{Z})^k$.

On pose:

$$\overline{\Lambda} := \frac{\Lambda_{K3}}{2\Lambda_{K3}} = \Lambda_{K3} \otimes \mathbb{F}_2$$

et κ la projection sur le quotient, $\kappa : \Lambda_{K3} \twoheadrightarrow \overline{\Lambda}$.

Le but de cette section est de déterminer la structure de $\overline{\Lambda}$ en tant que $\mathbb{F}_2[G]$-module.

On note:

$$\begin{aligned} x &= \overline{\iota^*} - \mathrm{Id}_{\overline{\Lambda}} \\ y &= \overline{\eta^*} - \mathrm{Id}_{\overline{\Lambda}} \end{aligned}$$

en particulier on a:

$$x^2 = \overline{\iota^*}^2 - 2\overline{\iota^*} + \mathrm{Id}_{\overline{\Lambda}}^2 = 2 \cdot \mathrm{Id}_{\overline{\Lambda}} = 0 = y^2$$

On a donc explicité la structure de $\overline{\Lambda}$ en tant que $\mathbb{F}_2[x,y]/(x^2, y^2)$-module (on rappelle que $\mathbb{F}_2[x,y]/(x^2, y^2) \simeq \mathbb{F}_2[G]$ par le Lemme 1.2.2). Pour l'action de x, y sur l'ensemble on utilisera la notation d'une fonction sur l'ensemble.

Lemme 3.2.12. *Soit $l \in \Lambda_{K3}$ et $l = l_1^* + l_2^* + l_3^*$ avec $l_i^* \in L_i^*$ sa décomposition. Alors:*

$$\begin{aligned} x\,(\kappa(l)) &= \kappa(2l_2^*) \\ y\,(\kappa(l)) &= \kappa(2l_3^*) \end{aligned}$$

En particulier $x_{|\kappa(L_i)} = y_{|\kappa(L_i)} = 0$

Démonstration. On rappelle que $L_1, L_3 \subseteq T_{\iota^*}$ et $L_2 \subseteq S_{\iota^*}$, pour l'action de x on obtient alors:

$$\begin{aligned} x(\kappa(l)) &= \kappa(\iota^*(l)) - \kappa(l) \\ &= \kappa(\iota^*(l_1^* + l_2^* + l_3^*)) - \kappa(l_1^* + l_2^* + l_3^*) \\ &= \kappa(l_1^* - l_2^* + l_3^*) - \kappa(l_1^* + l_2^* + l_3^*) \\ &= \kappa(-2l_2^*) \\ &= \kappa(2l_2^*) \end{aligned}$$

Donc si $l_i \in L_i$ avec $1 \leq i \leq 3$ alors $x(\kappa(l_i)) = 0$ si $i = 1, 3$ et $x(\kappa(l_2)) = \kappa(2l_2) = 0$ si $i = 2$.

Pour y la preuve est identique. □

Lemme 3.2.13. *Avec les notations précédentes on a $x \circ y = 0$.*

Démonstration. Soit $\bar{l} \in \overline{\Lambda}$ et $l \in \Lambda_{K3}$ tels que $\kappa(l) = \bar{l}$ et $l = l_1^* + l_2^* + l_3^*$ une décomposition avec $l_i \in L_i^*$. Alors par le Lemme 3.2.12:

$$\begin{aligned} (x \circ y)(\bar{l}) &= x(\kappa(2l_3^*)) \\ &= x(0) \end{aligned}$$

□

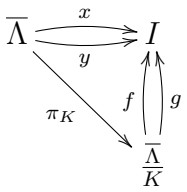
Dans le Chapitre 1 on a vu le résultat suivant qui nous donne une décomposition partielle pour un $\mathbb{F}_2[G]$-module qui respecte $x \circ y = 0$:

Corollaire. *1.2.25 Soit $\overline{\Lambda}$ un $\mathbb{F}_2[G]$-module avec $x \circ y = 0$. Si $I, K \subseteq \overline{\Lambda}$ sont deux sous-modules tels que:*

$$\mathrm{Im}(x) + \mathrm{Im}(y) \subseteq I \subseteq K \subseteq \ker(x) \cap \ker(y) \tag{3.2.2}$$

alors l'action de G se décompose partiellement comme:

- *Une somme de modules simples de la forme $\mathbb{F}_2^{\oplus(\dim(K)-\dim(I))}$, où l'action de G est triviale ;*
- *Un module (a priori non-indécomposable) décrit par les morphismes $\frac{\overline{\Lambda}}{K} \underset{g}{\overset{f}{\rightrightarrows}} I$ avec $f \circ \pi_K = x$ et $g \circ \pi_K = y$, $\pi_K : \overline{\Lambda} \twoheadrightarrow \frac{\overline{\Lambda}}{K}$ la projection sur le quotient par K, c'est-à-dire f et g tels que le diagramme suivant commute:*



Proposition 3.2.14. *Donc:*

$$\overline{\Lambda}\simeq\mathbb{F}_2^{\oplus(\dim(K)-\dim(I))}\oplus\left(\frac{\overline{\Lambda}}{K}\underset{g}{\overset{f}{\rightrightarrows}}I\right)$$

On rappelle que L_i est 2-élémentaire, donc $2L_i^*\subseteq L_i\subseteq\Lambda_{K3}$ et la définition suivante est cohérente:

Définition 3.2.15.

$$\begin{aligned}K &:= \kappa(L_1+L_2+L_3)\\ I &:= \kappa(2L_1^*+2L_2^*+2L_3^*)\end{aligned}$$

Lemme 3.2.16. *I et K vérifient:*

$$\mathrm{Im}(x)+\mathrm{Im}(y)\subseteq I\subseteq K\subseteq\ker(x)\cap\ker(y)$$

et on peut écrire:

$$\begin{aligned}K &\simeq \frac{L_1\oplus L_2\oplus L_3}{2\Lambda_{K3}}\\ I &\simeq \frac{L_1^*\oplus L_2^*\oplus L_3^*}{\Lambda_{K3}}\end{aligned}$$

Démonstration. Par le Lemme 3.2.12 $K\subseteq\ker(x)\cap\ker(y)$ et $\mathrm{Im}(x)+\mathrm{Im}(y)\subseteq I$ et aussi on a:

$$I=\kappa(2L_1^*+2L_2^*+2L_3^*)\subseteq\kappa(L_1+L_2+L_3)=K$$

L'extension primitive $\Lambda_{K3}\supseteq L_1\oplus L_2\oplus L_3$ implique que $\Lambda_{K3}=\Lambda_{K3}^*\subseteq L_1^*\oplus L_2^*\oplus L_3^*$. Comme $2L_i^*\subseteq L_i$ on obtient en composant que $2\Lambda_{K3}\subseteq L_1\oplus L_2\oplus L_3$, donc on peut développer les expressions suivantes:

$$K=\kappa(L_1+L_2+L_3)\simeq\frac{L_1\oplus L_2\oplus L_3}{2\Lambda_{K3}\cap(L_1\oplus L_2\oplus L_3)}\simeq\frac{L_1\oplus L_2\oplus L_3}{2\Lambda_{K3}}\subseteq\overline{\Lambda}$$

$$\begin{aligned}I &= \kappa(2L_1^*+2L_2^*+2L_3^*)\\ &\simeq \frac{2L_1^*\oplus 2L_2^*\oplus 2L_3^*}{2\Lambda_{K3}\cap(2L_1^*\oplus 2L_2^*\oplus 2L_3^*)}\\ &\simeq \frac{2L_1^*\oplus 2L_2^*\oplus 2L_3^*}{2\Lambda_{K3}}\simeq\frac{L_1^*\oplus L_2^*\oplus L_3^*}{\Lambda_{K3}}\end{aligned}$$

□

K et I satisfont (3.2.2) et donc $\overline{\Lambda}$ se décompose comme la somme de $\dim(K) - \dim(I)$ modules simples et un module décrit par le diagramme:

$$\frac{\Lambda_{K3}}{L_1 \oplus L_2 \oplus L_3} \underset{g}{\overset{f}{\rightrightarrows}} \frac{L_1^* \oplus L_2^* \oplus L_3^*}{\Lambda_{K3}} \tag{3.2.3}$$

Pour la valeur de $\dim(K) - \dim(I)$ on a le résultat suivant:

Lemme 3.2.17. $\dim(K) - \dim(I) = 22 - a_1 - a_2 - a_3$.

Démonstration. Comme $I \subseteq K$ on a que $\dim(K) - \dim(I) = \dim(K/I)$, donc:

$$\begin{aligned}
\dim(K/I) &= \dim\left(\frac{L_1 \oplus L_2 \oplus L_3}{2L_1^* \oplus 2L_2^* \oplus 2L_3^*}\right) \\
&= \sum_{i=1}^{3} \dim\left(\frac{L_i}{2L_i^*}\right) \\
&= \sum_{i=1}^{3} \dim\left(\frac{\frac{L_i}{2L_1}}{\frac{2L_i^*}{2L_i}}\right) \\
&= \sum_{i=1}^{3} \dim\left(\frac{L_i}{2L_1}\right) - \sum_{i=1}^{3} \dim\left(\frac{2L_i^*}{2L_i}\right) \\
&= \operatorname{rank}(\Lambda_{K3}) - \sum_{i=1}^{3} \dim\left(A_{L_i}\right) = 22 - a_1 - a_2 - a_3
\end{aligned}$$

□

On cherche maintenant à réécrire (3.2.3) différemment, de façon à faire le lien entre les plongements $L_i \hookrightarrow \Lambda_{K3}$ et l'action modulo 2.

Dans la suite on notera $\pi_i : A_{L_1} \oplus A_{L_2} \oplus A_{L_3} \to A_{L_1} \oplus A_{L_2} \oplus A_{L_3}$ la projection sur l'i-ième facteur:

$$\begin{aligned}
\pi_i : A_{L_1} \oplus A_{L_2} \oplus A_{L_3} &\to A_{L_1} \oplus A_{L_2} \oplus A_{L_3} \\
\pi_i(l_1^* + l_2^* + l_3^*) &= l_i^*
\end{aligned}$$

On rappelle que par la Proposition 2.3.73 une extension de réseau $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ correspond à un plongement $j : H_{\Lambda_{K3}} \hookrightarrow A_{L_1} \oplus A_{L_2} \oplus A_{L_3}$.

On notera aussi $p := \operatorname{coker}(j)$, i.e. la projection:

$$p : A_{L_1} \oplus A_{L_2} \oplus A_{L_3} \twoheadrightarrow \frac{A_{L_1} \oplus A_{L_2} \oplus A_{L_3}}{\operatorname{Im}(j)}$$

On a alors:

Proposition 3.2.18. *Avec les notations précédentes, la structure de $\mathbb{F}_2[G]$-module de $\overline{\Lambda} = \Lambda_{K3} \otimes \mathbb{F}_2$ est une somme directe de $\mathbb{F}_2^{\oplus(22-a_1-a_2-a_3)}$ avec action triviale et du $\mathbb{F}_2[G]$-module décrit par le couple de morphismes:*

$$H_{\Lambda_{K3}} \underset{g}{\overset{f}{\rightrightarrows}} \frac{A_{L_1} \oplus A_{L_2} \oplus A_{L_3}}{\mathrm{Im}(j)}$$

avec $f = p \circ \pi_2 \circ j$ et $g = p \circ \pi_3 \circ j$

Démonstration. Comme K et I satisfont (3.2.2) on peut appliquer le Corollaire 1.2.25. Par le Lemme 3.2.17 la partie triviale a pour dimension $22 - a_1 - a_2 - a_3$, il reste donc à décrire la partie donnée par le couple de morphismes.

Par définition on a:

$$H_{\Lambda_{K3}} \simeq \frac{\Lambda_{K3}}{L_1 \oplus L_2 \oplus L_3}$$

et par le troisième théorème d'isomorphisme:

$$\frac{A_{L_1} \oplus A_{L_2} \oplus A_{L_3}}{\mathrm{Im}(j)} \simeq \frac{\frac{L_1^* \oplus L_2^* \oplus L_3^*}{L_1 \oplus L_2 \oplus L_3}}{\frac{\Lambda_{K3}}{L_1 \oplus L_2 \oplus L_3}} \simeq \frac{L_1^* \oplus L_2^* \oplus L_3^*}{\Lambda_{K3}}$$

Comme $p = \mathrm{coker}(j)$ on obtient que:

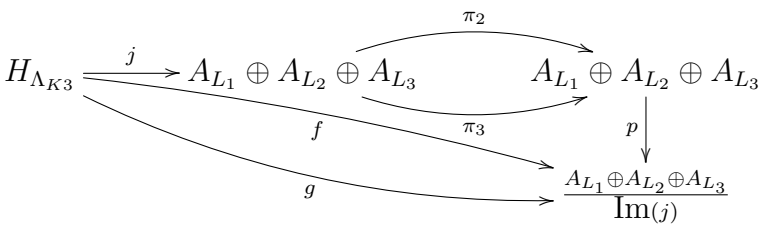
$$0 \to \frac{\Lambda_{K3}}{L_1 \oplus L_2 \oplus L_3} \overset{j}{\hookrightarrow} \frac{L_1^*}{L_1} \oplus \frac{L_2^*}{L_2} \oplus \frac{L_3^*}{L_3} \overset{p}{\longrightarrow} \frac{L_1^* \oplus L_2^* \oplus L_3^*}{\Lambda_{K3}} \to 0$$

est une suite exacte. Pour conclure on doit prouver que $f \circ \pi_{\kappa(L_1 \oplus L_2 \oplus L_3)} = x$ et $g \circ \pi_{\kappa(L_1 \oplus L_2 \oplus L_3)} = y$. Soit donc $\bar{l} \in \overline{\Lambda}$ et $l \in \Lambda_{K3}$ tels que $\kappa(l) = \bar{l}$ et $l = l_1^* + l_2^* + l_3^*$ est une décomposition avec $l_i \in L_i^*$. En utilisant le Lemme 3.2.12 on obtient:

$$\begin{aligned} f \circ \pi_{\kappa(L_1 \oplus L_2 \oplus L_3)}(\bar{l}) &= p \circ \pi_2 \circ j \circ \pi_{\kappa(L_1 \oplus L_2 \oplus L_3)}(\bar{l}) \\ &= \overline{l_2^*} \in \frac{L_1^* \oplus L_2^* \oplus L_3^*}{\Lambda_{K3}} \\ &= \kappa(2l_2^*) \in \frac{2L_1^* \oplus 2L_2^* \oplus 2L_3^*}{2\Lambda_{K3}} \\ &= x(\bar{l}) \end{aligned}$$

Pour g la preuve est identique. □

Le diagramme suivant résume les morphismes qu'on a défini jusqu'à ici:



Il reste donc à déterminer la décomposition du $\mathbb{F}_p[G]$-module défini par les morphismes f et g, qu'on retrouve dans la Proposition suivante, dont la preuve est l'objet de la prochaine section:

Proposition 3.2.19. *Avec les notations précédentes et celles des Théorèmes 1.2.27 et 1.2.28 sur la classifications des $\mathbb{F}[G]$-modules, la structure de $\mathbb{F}_2[G]$-module de $\overline{\Lambda} = \Lambda_{K3} \otimes \mathbb{F}_2$ décompose dans la forme:*

$$\begin{aligned}\overline{\Lambda} \simeq\ & \mathbb{F}_2^{\oplus(22-a_1-a_2-a_3)} \oplus E_{0,2}^{\oplus\frac{a_1+a_2-a_3}{2}-k} \oplus E_{\infty,2}^{\oplus\frac{a_1-a_2+a_3}{2}-k} \\ & \oplus E_{a+1,2}^{\oplus\frac{-a_1+a_2+a_3}{2}-k} \oplus W_3^{\oplus k} \oplus M_3^{\oplus k}\end{aligned}$$

3.2.4 Invariants numériques de l'action

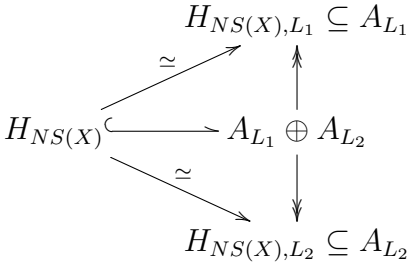
Il reste donc à déterminer le plongement j. Étant donnée j une application linéaire entre $\mathbb{F}_2$-espaces vectoriels on pourrait la décrire avec une matrice.

On cherche à l'obtenir en suivant le mécanisme de la preuve de la Proposition 2.5.13: on considère d'abord l'extension $NS(X) \supseteq L_1 \oplus L_2$ pour en suite regarder l'extension $\Lambda_{K3} \supseteq NS(X) \oplus T(X)$.

Donc $H_{NS(X)} = \frac{NS(X)}{L_1 \oplus L_2} \subseteq A_{L_1} \oplus A_{L_2}$ et on rappelle que puisque $H_{NS(X)}$ est un sous-groupe totalement isotrope, il décrit une anti-isométrie:

$$\psi : q_{H_{NS(X),L_1}} \subseteq A_{L_1} \to -q_{H_{NS(X),L_2}} \subseteq A_{L_2}$$

Donc on a:



Soit:

$$\begin{aligned}N_1 &= \left(H_{NS(X),L_1}\right)^\circ = H^\perp_{NS(X),L_1} \cap H_{NS(X),L_1} \\ N_2 &= \left(H_{NS(X),L_2}\right)^\circ = H^\perp_{NS(X),L_2} \cap H_{NS(X),L_2}\end{aligned}$$

comme ψ est une anti-isométrie on a $N_2 := \psi(N_1)$. On choisit $M_1 \subseteq A_{L_1}$ tel que:

$$H_{NS(X),L_1} = N_1 \oplus M_1$$

et on pose $M_2 = \psi(M_1)$. Alors:

$$H_{NS(X),L_2} = N_2 \oplus M_2$$

Lemme 3.2.20. *Soient:*

$$\begin{aligned}\mathrm{diag}(M_1, M_2) &:= \{(m, \psi(m))|m \in M_1\}\\ \mathrm{diag}(N_1, N_2) &:= \{(n, \psi(n))|n \in N_1\}\end{aligned}$$

alors:

$$H_{NS(X)} = \mathrm{diag}(M_1, M_2) \oplus \mathrm{diag}(N_1, N_2)$$

Démonstration. Par définition $H_{NS(X)} = \{(l + \psi(l))|l \in H_{NS(X),L_1}\}$, le résultat se déduit donc de la décomposition $H_{NS(X),L_1} = N_1 \oplus M_1$. □

On remarque que $N_i \oplus M_i$ est une somme orthogonale car $N_i \subseteq H^{\perp}_{NS(X),L_1}$ et donc M_i est non-dégénérée. Donc $N_1, N_2 \subseteq H^{\perp}_{NS(X)}$ et aussi $\mathrm{diag}(M_1, M_2) \subseteq H^{\perp}_{NS(X)}$, par contre $M_i \cap H^{\perp}_{NS(X)} = 0$.

On choisit $R_1 \subseteq A_{L_1}$, $S_2 \subseteq A_{L_2}$ tels que:

$$\begin{aligned}H^{\perp}_{NS(X)} \cap A_{L_1} &= N_1 \oplus R_1\\ H^{\perp}_{NS(X)} \cap A_{L_2} &= N_2 \oplus S_2\end{aligned}$$

et on choisit $P \subseteq A_{L_1} \oplus A_{L_2}$ tel que:

$$H^{\perp}_{NS(X)} = \left(H^{\perp}_{NS(X)} \cap A_{L_1}\right) \oplus \left(H^{\perp}_{NS(X)} \cap A_{L_2}\right) \oplus \mathrm{diag}(M_1, M_2) \oplus P \tag{3.2.4}$$

alors:

Lemme 3.2.21. *On a la décomposition (a priori non-orthogonale) suivante:*

$$A_{L_1} = \underbrace{N_1 \oplus M_1}_{H_{NS(X),1}} \oplus R_1 \oplus \pi_1(P)$$

$$A_{L_2} = \underbrace{N_2 \oplus M_2}_{H_{NS(X),2}} \oplus S_2 \oplus \pi_2(P)$$

pour $i = 1, 2$ où π_i est la projection sur A_{L_i}.

Démonstration. On remarque que:

- $P \cap A_{L_1} = P \cap A_{L_2} = 0$ grâce au choix de P, donc on a aussi $\dim(\pi_1(P)) = \dim(\pi_2(P))$;
- Par la Proposition 3.2.8 $N_1 \simeq K_{\Lambda_{K3}}$, donc $\dim(N_i) = \dim K_{\Lambda_{K3}} = k$;
- On rappelle que $a_i = \dim A_{L_i}$. Si on pose $c = \dim(H_{NS(X)})$ alors on vérifie facilement que:

$$\begin{aligned}\dim(N_1) &= k\\ \dim(M_1) &= c - k\\ \dim(R_1) &= a_1 - c - k\\ \dim(S_2) &= a_2 - c - k\\ \dim(H^{\perp}_{NS(X)}) &= a_1 + a_2 - c\\ \dim(\pi_i(P)) &= k\end{aligned} \tag{3.2.5}$$

Par le Lemme 2.5.12 on a $\pi_1(H^{\perp}_{NS(X)}) = A_{L_1}$, donc:

$$A_{L_1} = N_1 + M_1 + R_1 + \pi_1(P)$$

et en regardant les dimensions on obtient qu'il s'agit d'une somme directe. Pour A_{L_2} la preuve est la même. □

Par la Proposition 2.5.13 et en appliquant (3.2.4) on obtient pour A_{L_3} :

$$\begin{aligned} A_{NS(X)} = \frac{H^{\perp}_{NS(X)}}{H_{NS(X)}} &= \frac{N_1 \oplus N_2 \oplus \mathrm{diag}(M_1, M_2) \oplus R_1 \oplus S_2 \oplus P}{\mathrm{diag}(N_1, N_2) \oplus \mathrm{diag}(M_1, M_2)} \\ &\simeq \frac{N_1 \oplus N_2}{\mathrm{diag}(N_1, N_2)} \oplus R_1 \oplus S_2 \oplus P \\ &\simeq N_1 \oplus R_1 \oplus S_2 \oplus P \end{aligned}$$

Comme L est unimodulaire il existe alors une anti-isométrie

$$\varphi : q_{\frac{H^{\perp}_{NS(X)}}{H_{NS(X)}}} = q_{NS(X)} \to -q_{A_{L_3}}$$

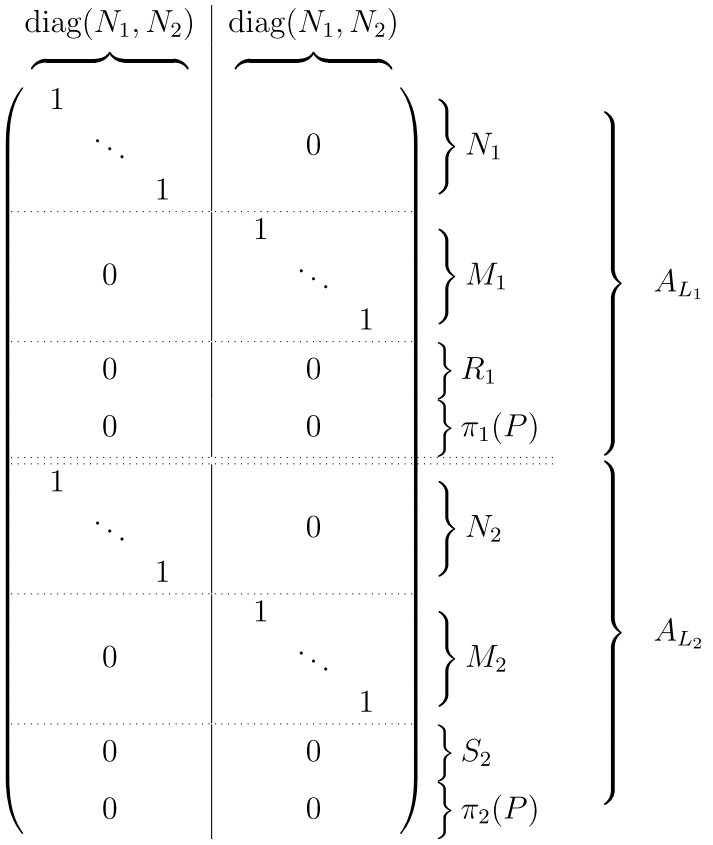
si on note $\tilde{H} = \{x, \varphi(x) | x \in \frac{H^{\perp}_{NS(X)}}{H_{NS(X)}}\}$ le graphe de φ, par la Proposition 2.5.13on a $H_{\Lambda_{K3}} = H_{NS(X)} + \tilde{H}$.

Maintenant on peut déterminer la matrice de:

$$j : H_{\Lambda_{K3}} \hookrightarrow A_{L_1} \oplus A_{L_2} \oplus A_{L_3}$$

On procède par étapes:

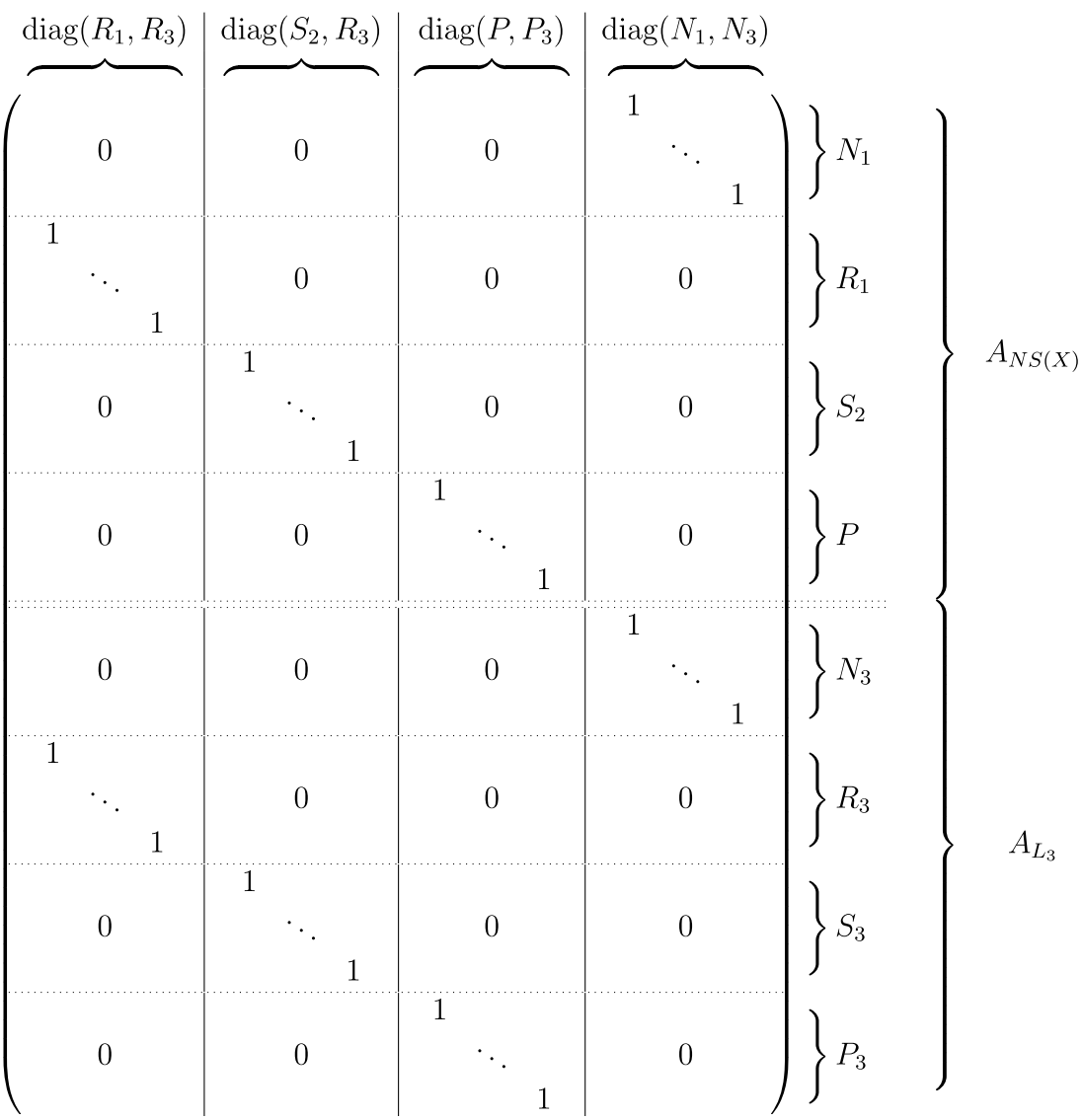
• On a des termes donnés par le plongement $j_1 : H_{NS(X)} \hookrightarrow A_{L_1} \oplus A_{L_2}$, c'est-à-dire les termes donnés par $\mathrm{diag}(N_1, N_2)$ et $\mathrm{diag}(M_1, M_2)$:



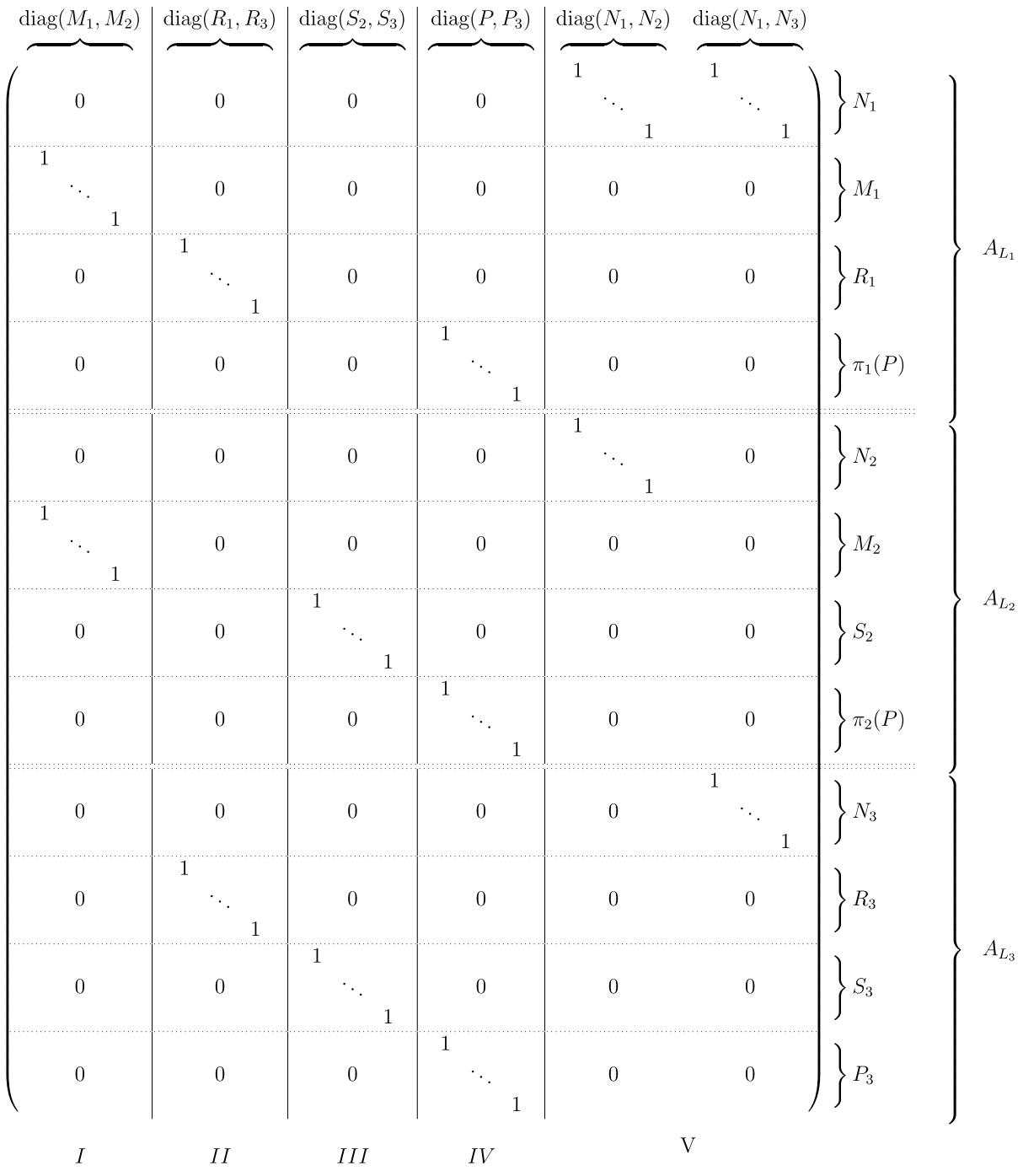
• Ensuite on a les termes donnés par le plongement $j_2 : H_{\Lambda_{K3}} \hookrightarrow A_{NS(X)} \oplus A_{L_3}$. On a vu que $A_{NS(X)} \simeq N_1 \oplus R_1 \oplus S_2 \oplus P$ (c'est-à-dire le plongement de $H^{\perp}_{NS(X)}$ dans $A_{L_1} \oplus A_{L_2}$ modulo $H_{NS(X)}$). L'image de j_2 est alors de la forme:

$$\mathrm{Im}(j_2) = \mathrm{diag}(A_{NS(X)}, A_{L_3}) := \{(l, \varphi(l)) | l \in A_{NS(X)}\}$$

Si on pose $N_3 := \varphi(N_1)$, $R_3 := \varphi(R_1)$, $S_3 := \varphi(S_2)$, $P_3 := \varphi(P)$ on obtient que j_2 est donné par la matrice suivante:



On peut composer les matrices de j_1 et de j_2 pour obtenir la matrice de j. On a aussi déplacé la composante donnée par diag(N_1, N_2) en avant-dernière position, ce qui nous sera utile dans la suite.



Matrice du plongement: $j : H_{\Lambda_{K3}} \hookrightarrow A_{L_1} \oplus A_{L_2} \oplus A_{L_3}$ (3.2.6)

On réécrit (3.2.5) en utilisant la relation $c = (a_1 + a_2 - a_3)/2$, alors:

- $\dim(M_1) = \dim(M_2) = \frac{a_1+a_2-a_3}{2} - k$
- $\dim(S_1) = \frac{a_1-a_2+a_3}{2} - k$
- $\dim(S_2) = \frac{-a_1+a_2+a_3}{2} - k$
- $\dim(P) = k$

Avec la matrice 3.2.6 on peut appliquer la Proposition 3.2.18 pour déterminer la structure de $\mathbb{F}_2[G]$-module de $\Lambda_{K3} \otimes \mathbb{F}_2$.

On a une décomposition de la matrice (et donc de l'application j) en 5 parties:

$$j = j_I \oplus j_{II} \oplus j_{III} \oplus j_{IV} \oplus j_V$$

qui induit aussi une décomposition de $\Lambda_{K3} \otimes \mathbb{F}_2$ en tant que $\mathbb{F}_2[G]$-module.

Ensuite on analyse chacune de ces parties séparément, en se restreignant à une seule colonne (ou deux dans la partie V).

On pose $\tilde{f} = \pi_2 \circ j$ et $\tilde{g} = \pi_3 \circ j$, et en prenant le quotient par l'image de j on obtient $f = p \circ \tilde{f}$ et $g = p \circ \tilde{g}$.

I) Pour chaque colonne i de $\mathrm{diag}(M_1, M_2)$, en prenant une restriction sur l'image, on obtient des plongements du type:

$$j_I^i = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{matrix} \} A_{L_1} \\ \} A_{L_2} \\ \} A_{L_3} \end{matrix}$$

$$j_I^i : \mathbb{F}_2 \longrightarrow \mathbb{F}_2^2$$

On calcule les compositions avec les projections π_2 et π_3 pour trouver:

$$\tilde{f} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \tilde{g} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\tilde{f}, \tilde{g} : \mathbb{F}_2 \longrightarrow \mathbb{F}_2^2$$

On a $\mathrm{Im}(j_I^i) = \mathrm{span}((1,1,0))$, p est le quotient par $\mathrm{Im}(j)$, alors si $v_1 = (1,0,0)$, $\mathcal{B} = (v_1)$ est une base du quotient par l'image de j_I^1.

On rappelle que $f = p \circ \tilde{f}$ et $g = p \circ \tilde{g}$, et si on exprime le morphisme dans la base $\mathcal{B}$ on a:

$$f = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad g = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

C'est-à-dire:

$$\begin{array}{rcl} f, g : \mathbb{F}_2 & \longrightarrow & \dfrac{\mathbb{F}_2^2}{\mathrm{Im}(j_I^i)} \simeq \mathbb{F}_2 \\ e_1 & \mapsto & f(e_1) = v_1 \\ e_1 & \mapsto & g(e_1) = 0 \end{array}$$

qui correspond au module $E_{0,2}$. La cardinalité des modules de ce type est égale au nombre de colonnes de $\mathrm{diag}(M_1, M_2)$, qui est égale à $\dim(M) = \frac{a_1+a_2-a_3}{2} - k$.

II) Cas très semblable à I). Pour chaque colonne i de $\mathrm{diag}(R_1, R_3)$ on a des plongements du type:

$$j^i_{II} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{matrix} \} A_{L_1} \\ \} A_{L_2} \\ \} A_{L_3} \end{matrix}$$

qui composé à π_2 et π_3 nous donne:

$$\tilde{f} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \ \tilde{g} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \implies f = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \ g = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

qui correspondent au module $E_{\infty,2}$. La cardinalité des modules de ce type est $\frac{a_1-a_2+a_3}{2} - k$.

III) Cas très semblable à I) et II). Pour chaque colonne i de $\mathrm{diag}(S_2, S_3)$ on a des plongements du type:

$$j^i_{III} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{matrix} \} A_{L_1} \\ \} A_{L_2} \\ \} A_{L_3} \end{matrix}$$

qui composé a π_2 et π_3 nous donne:

$$\tilde{f} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ \tilde{g} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \implies f = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ g = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

qui correspond au module $E_{a+1,2}$. La cardinalité des modules de ce type est $\frac{-a_1+a_2+a_3}{2} - k$.

IV) Pour chaque colonne i de $\mathrm{diag}(P, P_3)$ on a des plongements du type:

$$j^i_{IV} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{matrix} \} A_{L_1} \\ \} A_{L_2} \\ \} A_{L_3} \end{matrix}$$

$$j^i_{IV} : \mathbb{F}_2 \longrightarrow \mathbb{F}_2^3$$

On calcule les compositions avec les projections π_2 et π_3 pour trouver:

$$\tilde{f} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ \tilde{g} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\tilde{f}, \tilde{g} : \mathbb{F}_2 \longrightarrow \mathbb{F}_2^3$$

On a $\mathrm{Im}(j^i_{IV}) = \mathrm{span}((1,1,1))$, p est le quotient par $\mathrm{Im}(j)$, alors si $v_1 = (0,1,0)$, $v_2 = (0,0,1)$ on a alors que $\mathcal{B} = (v_1, v_2)$ est une base du

quotient par l'image de j^i_{IV}. On rappelle que $f = p \circ \tilde{f}$ et $g = p \circ \tilde{g}$, et si on exprime le morphisme dans la base $\mathcal{B}$ on a:

$$f = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad g = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

C'est-à-dire:

$$\begin{array}{rcl} f, g : \mathbb{F}_2 & \longrightarrow & \dfrac{\mathbb{F}_2^3}{\mathrm{Im}(j^i_{IV})} \simeq \mathbb{F}_2^2 \\ e_1 & \mapsto & f(e_1) = v_1 \\ e_1 & \mapsto & g(e_1) = v_2 \end{array}$$

qui correspond au module W_3. La cardinalité des modules de ce type est égale au nombre de colonnes de $\mathrm{diag}(P, P_3)$, qui est égal à $\dim(P) = k$.

V) Pour chaque colonne i de $\mathrm{diag}(N_1, N_2)$ réunie avec la colonne i de $\mathrm{diag}(N_1, N_3)$, on a des plongements du type:

$$j^i_V = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{array}{l} \} A_{L_1} \\ \} A_{L_2} \\ \} A_{L_3} \end{array}$$

$$j^i_V : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^3$$

qui composé a π_2 et π_3 nous donne:

$$\tilde{f} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \tilde{g} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

On a que $\mathrm{Im}(j^i_V) = \mathrm{span}((1,1,0),(1,0,1))$, p est le quotient par $\mathrm{Im}(j)$, alors si $v_1 = (1,0,0)$, on a alors que $\mathcal{B} = (v_1)$ est une base du quotient par l'image de j^i_{IV}. On compose par p pour obtenir:

$$f = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad g = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

C'est-à-dire:

$$\begin{array}{rcl} f, g : \mathbb{F}_2^2 & \longrightarrow & \dfrac{\mathbb{F}_2^3}{\mathrm{Im}(j^i_V)} \simeq \mathbb{F}_2 \\ e_1 & \mapsto & f(e_1) = v_1 \\ e_1 & \mapsto & g(e_1) = 0 \\ e_2 & \mapsto & f(e_2) = 0 \\ e_2 & \mapsto & g(e_2) = v_1 \end{array}$$

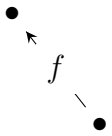
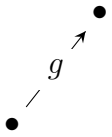
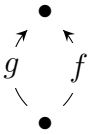
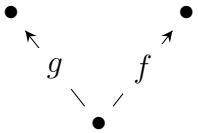
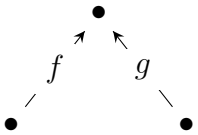
Partie	Type	$\dim_{\mathbb{F}_2}$	Diagramme	Nombre de modules
	$\mathbb{F}_2$	1		$22 - a_1 - a_2 - a_3$
I	$E_{0,2}$	2		$\frac{a_1 + a_2 - a_3}{2} - k$
II	$E_{\infty,2}$	2		$\frac{a_1 - a_2 + a_3}{2} - k$
III	$E_{a+1,2}$	2		$\frac{-a_1 + a_2 + a_3}{2} - k$
IV	W_3	3		k
V	M_3	3		k

TABLE 3.2.1 – Décomposition de $\Lambda_{K3} \otimes \mathbb{F}_2$

qui correspond au module M_3. La cardinalité des modules de ce type est k.

En résumant on obtient le Tableau 3.2.1.

Comme $a_2 = 8$ on obtient un total de $14 - a_1 - a_3 + 2k$ modules impairs dans la décomposition de $\Lambda_{K3} \otimes \mathbb{F}_2$. En appliquant le Lemme 3.2.10 on obtient le résultat principal ici présenté:

Théorème 3.2.22. *Soit X une surface K3, ι et η deux involutions commutant de X tels que ι soit symplectique et η non-symplectique avec action triviale sur $NS(X)$. Avec le notations expliquées plus haut, si $X^G \neq \emptyset$ alors X^G est une réunion de points (réduits) avec:*

$$\#X^G \quad = \quad 16 - a_1 - a_3 + 2k$$

3.2.5 Détermination des cas possibles

Le Théorème 3.2.11 montre qu'il existe une correspondance entre les extensions de la forme $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ et les actions de G sur X surface K3.

On se donne maintenant l'objectif de classifier les différentes possibilités pour le choix de L_1, L_2, L_3 et du nombre de points fixes de l'action associée.

On commence par les rappels suivants:

Lemme 3.2.23. *Soit $A \simeq (\mathbb{Z}/2\mathbb{Z})^a$, q une f.f. quadratique sur A non-dégénérée, alors q est uniquement déterminée par δ_q et* $\mathrm{sgn}(q)$

Démonstration. Soit b la forme bilinéaire associée à q, alors par la Proposition 2.4.39 q est déterminée par b et $\mathrm{sgn}(q)$, mais par la Proposition 2.3.69 b est déterminée par a et δ_q. □

Proposition 3.2.24. *Soit L un réseau pair 2-élémentaire hyperbolique, alors L est uniquement déterminé par* $\mathrm{sgn}(L)$, $\dim_{\mathbb{F}_2}(A_L)$, δ_L.

Démonstration. Si L est hyperbolique et 2-élémentaire alors par la Remarque 2.4.55 L est unique en son genre. Mais par la Proposition 2.4.23 le genre de L est déterminé par sa signature et par sa forme quadratique q_L et par le Lemme 3.2.23 q_L est déterminée par $\mathrm{sgn}(L)$, $\dim_{\mathbb{F}_2}(A_L)$ et δ_L. □

On répète rapidement la structure de l'extension de réseaux associée à l'action du couple d'involutions sur la surface K3 qu'on a vu dans la section précédente.

Comme $NS(X)$ a signature $(1, r)$, il est uniquement déterminé par $\delta_{NS(X)}$ et $\dim(A_{NS(X)})$, avec les différents choix possibles listées par la Proposition 2.4.42.

On considère l'extension:

$$\Lambda_{K3} \supseteq NS(X) \oplus T(X)$$

comme Λ_{K3} est unimodulaire, on a une isométrie $\varphi : q_{NS(X)} \to -q_{T(X)}$, en particulier $a_3 = \dim(A_{NS(X)})$ et $\delta_{T(X)} = \delta_{NS(X)}$.

Ensuite on a l'extension:

$$NS(X) \supseteq L_1 \oplus L_2$$

par le Corollaire 2.5.21, comme $\delta_{L_2} = 0$ on obtient que $\delta_{L_1} = \delta_{NS(X)}$. On rappelle que l'extension est déterminée par le plongement:

$$\begin{array}{ccc} & \overset{\pi_1}{\nearrow} & H_{NS(X),L_1} \subseteq A_{L_1} \\ H_{NS(X)} & & \downarrow \psi \\ & \underset{\pi_2}{\searrow} & H_{NS(X),L_2} \subseteq A_{L_2} \end{array}$$

Comme $\delta_{L_2} = 0$ on a que $q_{A_{L_2}} = -q_{A_{L_2}}$ et du même $\delta_{H_{NS(X),L_1}} = 0$ et $q_{|H_{NS(X),L_1}} = -q_{|H_{NS(X),L_1}} = q_{|H_{NS(X),L_2}}$. A priori la forme sur $H_{NS(X),L_1}$ n'est pas non-dégénérée, soit donc

$$N_1 = \left(H_{NS(X),L_1}\right)^\circ = H^\perp_{NS(X),L_1} \cap H_{NS(X),L_1}$$

de dimension k et M_1 tel que $H_{NS(X),L_1} = N_1 \oplus M_1$ avec $q_{|M_1}$ non dégénérée, comme on a vu dans la section précédente. On pose $N_2 = \psi(N_1)$ et $M_2 = \psi(M_1)$, alors $q_{|M_1} = q_{|M_2}$, $q_{|N_1} = q_{|N_2}$ et $\delta_{M_i} = 0$. Comme $M_i \hookrightarrow A_{L_i}$, si on pose $Q_i := M_i^{\perp_{A_{L_i}}}$ on a la décomposition:

$$A_{L_i} = M_i \oplus Q_i$$

et $N_i \hookrightarrow Q_i$ (qui ne nous donne pas une décomposition orthogonale car la forme sur N_i est totalement isotrope). Nous sommes prêts pour prouver:

Lemme 3.2.25. *Avec les notations expliquées plus haut, un choix de r,$a_{NS(X)}$, $\delta_{NS(X)}$,a_1,k est réalisé par une extension $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ si et seulement si il existe:*

1. *Un réseau $T(X)$ de signature $(2, 20 - r)$ avec $A_{T(X)} \simeq (\mathbb{Z}/2\mathbb{Z})^{a_{NS(X)}}$ et $\delta_{T(X)} = \delta_{NS(X)}$;*
2. *Un réseau L_1 de signature $(1, r - 9)$ avec $A_{L_1} \simeq (\mathbb{Z}/2\mathbb{Z})^{a_1}$ et $\delta_{L_1} = \delta_{NS(X)}$;*

et aussi:

1. *Une f.f. quadratique q_{N_1} sur $N_1 \simeq (\mathbb{Z}/2\mathbb{Z})^k$ totalement isotrope en tant que forme bilinéaire ;*
2. *Une f.f. quadratique q_{M_1} sur $M_1 \simeq (\mathbb{Z}/2\mathbb{Z})^{c-k}$ non-dégénérée avec $\delta_{M_1} = 0$;*
3. *Une f.f. quadratique q_{Q_i} sur $Q_i \simeq (\mathbb{Z}/2\mathbb{Z})^{a_i - c + k}$ non-dégénérée, pour $i = 1, 2$;*

tels que:

1 $c = \frac{a_1+8-a_{NS(X)}}{2}$;

2 $q_{L_i} \simeq q_{M_i} \oplus q_{Q_i}$;

3 *Il existe un plongement* $q_{N_1} \hookrightarrow q_{Q_i}$ *pour* $i = 1, 2$.

Démonstration. Soient L_1, $L_3 = T(X)$ les réseaux définis par les invariants donnés et $L_2 \simeq E_8(-2)$.

Soient $H_{NS(X),1} = H_{NS(X),2} = M_1 \oplus N_1$, par hypothèse il existe des plongements $H_{NS(X),i} \hookrightarrow A_{L_i}$ et donc $H_{NS(X)}$ est totalement isotrope avec $H_{NS(X)} \hookrightarrow A_{L_1} \oplus A_{L_2}$. $H_{NS(X)}$ détermine un sur-réseau $NS(X) \supseteq L_1 \oplus L_2$ de signature $(1, r-1)$ avec $A_{NS(X)} \simeq (\mathbb{Z}/2\mathbb{Z})^{a_{NS(X)}}$ par le Lemme 2.5.3 et $\delta_{NS(X)} = \delta_{L_1}$ par le Corollaire 2.5.21.

Comme $\dim(A_{NS(X)}) \simeq \dim(A_{TX})$, $\operatorname{sgn}(q_{NS(X)}) \equiv -\operatorname{sgn}(q_{L_3}) \equiv 6 - r \pmod 8$ et $\delta_{NS(X)} = \delta_{L_3}$ on a $q_{NS(X)} = -q_{L_3}$ et il existe donc $\psi : A_{NS(X)} \xrightarrow{\simeq} A_{L_3}$ anti-isométrie qui donne une extension $L \supseteq NS(X) \oplus L_3$ avec L unimodulaire de signature $(3, 19)$, donc $L \simeq \Lambda_{K3}$ par la Proposition 3.2.24. □

On cherche maintenant à donner des critères numériques qui soient équivalents aux hypothèses du Lemme 3.2.25:

Proposition 3.2.26. *Avec les notations expliquées plus haut, un choix de* $r, a_{NS(X)}, \delta_{NS(X)}, a_1, k$ *est réalisé par une extension* $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ *si et seulement si:*

1 *Il existe un réseau* L_1 *de signature* $(1, r-9)$ *avec* $A_{L_1} \simeq (\mathbb{Z}/2\mathbb{Z})^{a_1}$ *et* $\delta_{L_1} = \delta_{NS(X)}$;

2 $0 \leq a_{NS(X)} \leq \min(22 - r, r)$

3 $9 \leq r \leq 20$

4 $a_{NS(X)} \equiv a_1 \pmod 2$

5 $c - k \equiv 0 \pmod 2$

6 $c + k \leq \min(8, a_1)$

7 $r - 2 \equiv 0 \pmod 8$ *si* $a_{NS(X)} = 22 - r$ *et* $\delta_{NS(X)} = 0$.

8 $\delta_{NS(X)} = 0$ *si* $a_1 = c$

avec $c = \frac{a_1+8-a_{NS(X)}}{2}$.

Démonstration. On vérifie d'abord que les hypothèses du Lemme 3.2.25 impliquent les critères donnés précédemment:

- Les critères 1, 2 , 3, 7 découlent directement de l'existence des réseaux L_1, $NS(X)$ et $T(X)$.
- Les critères 4 et 5 découlent du fait qu'il existe une f.f. quadratique q_{M_1} sur $(\mathbb{Z}/2\mathbb{Z})^{c-k}$ avec $\delta_{q_{M_1}} = 0$ et donc $c - k$ est un entier pair.
- Le critère 6 vient du fait que $q_{M_1} \oplus q_{N_1} \hookrightarrow q_{L_1}$ et $q_{M_1} \oplus q_{N_1} \hookrightarrow q_{L_2}$ avec q_{N_1} f.f. quadratique sur $(\mathbb{Z}/2\mathbb{Z})^k$ complètement isotrope.

- L'hypothèse du critère 8 implique que $q_{L_1} \hookrightarrow q_{L_2}$ et donc:

$$\delta_{q_{L_1}} = \delta_{NS(X)} = \delta_{q_{L_2}} = 0$$

On montre maintenant que les critères donnés ci-dessus impliquent les hypothèses du Lemme 3.2.25, ce qui nous donne l'équivalence entre les deux énoncés et qui prouve donc la Proposition.

L'existence d'un réseau L_1 avec les invariants donnés et d'une extension $NS(X) \supseteq L_1 \oplus L_2$ assure l'existence de $NS(X)$. Comme $T(X)$ et $NS(X)$ ont signatures et formes quadratiques opposées, par la Proposition 2.4.42 la seule condition qui reste à vérifier pour assurer l'existence de $T(X)$ est le critère 7.

Il reste uniquement à prouver qu'une telle extension existe avec les invariants donnés.

Soit $c = \left(a_{NS(X)} - a_1 - 8\right)/2$, alors $c \in \mathbb{N}$ par le critère 4. On doit donc montrer qu'il existe q_H f.f. quadratique sur $(\mathbb{Z}/2\mathbb{Z})^c$ avec $\text{rang}(q_H) = c - k$ et $\delta_{q_H} = 0$ tel que $q_H \hookrightarrow q_{L_1}$ et $q_H \hookrightarrow q_{L_2}$. On rappelle que $q_{L_2} = u_1^{\oplus 4}$ et q_{L_1} est la forme non-dégénérée de rang a_1, $\delta_{q_{L_1}} = \delta_{NS(X)}$ et $\text{sgn}(q_{L_1}) \equiv 2 - r \pmod 8$.

Par le critère 4 on a $c - k \equiv 0 \pmod 2$ (ce qui constitue une condition nécessaire pour avoir $\delta_{q_H} = 0$), on considère maintenant les cas suivants:

- Si $k \geq 1$ il existe toujours q_H avec $\delta_{q_H} = 0$ et $\epsilon_{q_H} = 1$. Par la Proposition A.0.10 on a que:
  - Il existe toujours un plongement $q_H \hookrightarrow q_{L_2}$ car $c + k \leq 8$ par le critère 6.
  - Un plongement $q_H \hookrightarrow q_{L_1}$ existe toujours sauf si:

$$\text{sgn}(q_{L_1}) \in \{0, 4\} \text{ avec } \delta_{NS(X)} = 1,\ k = 1 \text{ et } c + k = a_1$$

    dans ce cas là on pose $\epsilon(q_h) = 0$, et $\text{sgn}(q_H) = \text{sgn}(q_{L_1}) \in \{0, 4\}$. Alors il existe toujours un plongement $q_H \hookrightarrow q_{L_1}$. Il existe aussi un plongement $q_H \hookrightarrow q_{L_2}$ sauf si $\text{sgn}(q_H) = 4$, $c = 7$, $k = 1$, $a_1 = 8$. Mais si $4 \equiv \text{sgn}(q_H) \equiv \text{sgn}(q_{L_1}) \equiv 2 - r \pmod 8$ alors la seule possibilité est $r = 14$ (car $r \geq 8$), en contradiction avec $a_1 = 8$ car $\text{rang}(L_1) = 14 - 8 = 6$.
- Si $k = 0$ on a $c \leq 8$ par le critère 6:
  - Si $c < 8$ et $c < a_1$ les deux plongements existent toujours, car par la Proposition A.0.10 on peut choisir la signature de q_H dans $\{0, 4\}$ de façon à avoir un plongement $q_H \hookrightarrow q_{L_1}$ et pour n'importe quel choix effectué le plongement $q_H \hookrightarrow q_{L_2}$ existe toujours.
  - Si $c = a_1 < 8$ alors on a $q_H = q_{L_1} \hookrightarrow q_{L_2}$ qui est possible si et seulement si $\delta_{L_1} = \delta_{NS(X)} = 0$, condition vérifiée par le critère 8.
  - Si $c = 8 = a_1$ les plongements existent si et seulement si $q_H = q_{L_2} = q_{L_1}$ et donc si $\text{sgn}(q_{L_1}) = 0$ et $\delta_{L_1} = 0$. Comme $a_1 \geq r - 8$ et $a_1 \equiv r \pmod 2$ les valeurs possible de r sont $16, 18, 20$. Par le critère 8 on a $\delta_{NS(X)} = 0$ et donc $\text{sgn}(q_{L_1}) \equiv 4 \pmod 4$ ce qui

implique $r \equiv 2 \pmod 4$. Donc la seule possibilité est $r = 18$ et par conséquent $\mathrm{sgn}(q_{L_1}) = 0$.

— Si $c = 8$ et $a_1 = 9$, le plongement $q_H \hookrightarrow q_{L_2}$ existe si $\mathrm{sgn}(q_H) = 0$. Par la Proposition A.0.10 on a aussi un plongement $q_H \hookrightarrow q_{L_1}$ si et seulement si $\mathrm{sgn}(q_{L_2}) = \mathrm{sgn}(q_H) \pm 1 = \pm 1$. Mais les seules valeurs de r qui peuvent réaliser $a_1 = 9$ sont $r = 17, 19$ qui correspondent à $\mathrm{sgn}(q_{L_1}) = 1$ et $\mathrm{sgn}(q_{L_1}) = -1$, donc il n'y a pas de conditions supplémentaires à vérifier pour ce cas là.

— Si $c = 8$ et $a_1 = 10$, en raisonnant comme dans le cas précédents on obtient que $\mathrm{sgn}(q_{L_1}) \neq 4$. Mais la seule valeur de r qui peut réaliser $a_1 = 10$ est $r = 18$ qui correspond à $\mathrm{sgn}(q_{L_1}) = 0$.

— Si $c = 8$ et $a_1 \geq 11$ il existe toujours les plongements $q_H \hookrightarrow q_{L_1}$ et $q_H \hookrightarrow q_{L_2}$ si $\mathrm{sgn}(q_H) = 0$.

□

Grâce à la Proposition 3.2.26 nous avons réalisé un simple algorithme (cf. 3.1) pour obtenir toutes les extensions possibles, ainsi que les invariants associés, que nous avons collecté s'ensuite dans les Tableaux 3.2.2 et 3.2.3.

On obtient aussi une preuve alternative du théorème suivant:

Théorème 3.2.27 (Théorème 3.1 [[GaSar]]). *La surface K3 $X_{r,a,1}$ admet une involution symplectique si et seulement si $a > 16 - r$.*

La surface K3 $X_{r,a,0}$ admet une involution symplectique si et seulement si soit $a > 16 - r$ soit $a = 6$, $r = 10$.

avec l'avantage que le résultat ici présenté donne les différentes possibilités d'action du groupe de Klein pour la même surface K3.

Remarque 3.2.28. Les Tableaux 3.2.2 et 3.2.3 ne résument pas toutes les possibilités pour une extension du type $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ (et donc pour toutes les couples d'involutions), mais il englobe toutes les possibilités pour un choix des L_i et de $k = \dim K_{\Lambda_{K3}}$. Donc chaque ligne des tableaux peut être réalisée par plusieurs couples d'involutions différentes.

Remarque 3.2.29. On rappelle que dans les hypothèses du Théorème 3.2.22 on demande que le lieu fixe de l'action soit non vide. Cela implique que les estimations de la cardinalité du lieu fixe contenues dans les Tableaux 3.2.2 et 3.2.3 s'appliquent uniquement si cette condition est vérifie.

Cela n'est pas toujours le cas, par exemple le résultat suivant donne le lieu fixe de η:

Théorème 3.2.30 (Théorème 4.2.2, [[Nik3]]). *Soit X une surface K3 et ρ une involution non-symplectique de X. Soient (r, a, δ) les invariants de ρ, alors le lieu fixe de ρ est:*

- *Vide si $r = 10$, $a = 10$ et $\delta = 0$;*
- *L'union disjointe de deux courbes elliptiques si $r = 10$, $a = 8$ et $\delta = 0$;*

- *L'union disjointe d'une courbe de genre g et k courbes rationnelles, avec $g = (22 - r - a)/2$, $k = (r - a)/2$ sinon.*

Donc dans le cas $r = 10$, $a_3 = 10$, $\delta_{NS(X)} = 0$, qui est présent dans le tableau avec lieu fixe estimé égal à 4 points, on obtient qu'en réalité $X^\eta = \emptyset$ et donc a fortiori le lieu fixe de l'action du groupe est vide aussi.

Remarque 3.2.31. La formule du Théorème 3.2.22 utilise (entre autres) la dimension du groupe $K_{\Lambda_{K3}}$ (décrit dans la Section 3.2.1) pour estimer le nombre de points fixes de l'action.

On pourrait donc se demander si le calcul de cet invariant est forcément nécessaire où s'il peut être déduit, peut être de façon indirecte, à partir de la connaissance des réseaux L_i.

Les Tableaux 3.2.2 et 3.2.3 répondent à cette question: il existe des couples d'exemples d'actions, où les réseaux L_i et $NS(X)$ sont exactement les mêmes et la seule différence est la valeur de k (cas 14 et 15 par exemple). Par conséquent le nombre de points fixes estimé est différent dans les deux cas.

Cela prouve que $k = \dim(K_{\Lambda_{K3}})$ donne une information importante sur l'action, qui ne peut pas être obtenue à partir de la seule connaissance des réseaux concernés.

Algorithme 3.1 Algorithme en SAGE pour la détermination de cas possibles pour une action de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ sur une K3

```
def exists_2el_lattice(s_p, s_m, a, delta):
    r = s_p + s_m
    s = (s_p - s_m) % 8
    flag = (a <= r)
    flag = flag & ((r - a) % 2==0)
    flag = flag & (not ((a==0) & (delta!=0)))
    flag = flag & (not ((a==0) & (s!=0)))
    flag = flag & (not ((delta==0) & (s % 4!=0))  )
    flag = flag & (not ((a==r) & (delta==0) & (s!=0)))
    flag = flag & (not ((a==1) & (s!=1) & (s!=7)))
    flag = flag & (not ((a==2) & (s==4) & (delta!=0)))
    return flag

for r in range(9, 21):
    for a_NS in range(0, min(r + 1, 23 - r)):
        for delta_NS in range(0,2):
            for a_1 in range(a_NS%2,r-8+1,2):
                if not exists_2el_lattice(1, r - 9, a_1, delta_NS):
                    continue
                if (a_NS==22-r)&(delta_NS==0)&((r-2)%8!=0):
                    continue
                if (a_1==8-a_NS)&(delta_NS==1):
                    continue
                c = (a_1 + 8 - a_NS)/2
                for k in range(c%2, min(8-c,a_1-c,c) +1,2):
                    print((r, delta_NS, a_NS, a_1, k))
```

	Invariants numeriques					(s^+, s^-, a, δ)		Nombre de modules par type						Pts
	r	δ	a_3	a_1	k	$NS(X)$	L_1	$\mathbb{F}_2$	$E_{2,0}$	$E_{2,\infty}$	$E_{2,1}$	M_3	W_3	fix
1	9	1	9	1	0	$(1,8,9,1)$	$(1,0,1,1)$	4	0	1	8	0	0	6
2	10	0	6	2	0	$(1,9,6,0)$	$(1,1,2,0)$	6	2	0	6	0	0	8
3	10	0	8	0	0	$(1,9,8,0)$	$(1,1,0,0)$	6	0	0	8	0	0	8
4	10	0	8	2	1	$(1,9,8,0)$	$(1,1,2,0)$	4	0	0	6	1	1	8
5	10	1	8	2	1	$(1,9,8,1)$	$(1,1,2,1)$	4	0	0	6	1	1	8
6	10	0	10	2	0	$(1,9,10,0)$	$(1,1,2,0)$	2	0	2	8	0	0	4
7	10	1	10	2	0	$(1,9,10,1)$	$(1,1,2,1)$	2	0	2	8	0	0	4
8	11	1	7	3	0	$(1,10,7,1)$	$(1,2,3,1)$	4	2	1	6	0	0	6
9	11	1	9	1	0	$(1,10,9,1)$	$(1,2,1,1)$	4	0	1	8	0	0	6
10	11	1	9	3	1	$(1,10,9,1)$	$(1,2,3,1)$	2	0	1	6	1	1	6
11	11	1	11	3	0	$(1,10,11,1)$	$(1,2,3,1)$	0	0	3	8	0	0	2
12	12	1	6	4	1	$(1,11,6,1)$	$(1,3,4,1)$	4	2	0	4	1	1	8
13	12	1	8	2	1	$(1,11,8,1)$	$(1,3,2,1)$	4	0	0	6	1	1	8
14	12	1	8	4	0	$(1,11,8,1)$	$(1,3,4,1)$	2	2	2	6	0	0	4
15	12	1	8	4	2	$(1,11,8,1)$	$(1,3,4,1)$	2	0	0	4	2	2	8
16	12	1	10	2	0	$(1,11,10,1)$	$(1,3,2,1)$	2	0	2	8	0	0	4
17	12	1	10	4	1	$(1,11,10,1)$	$(1,3,4,1)$	0	0	2	6	1	1	4
18	13	1	5	5	0	$(1,12,5,1)$	$(1,4,5,1)$	4	4	1	4	0	0	6
19	13	1	7	3	0	$(1,12,7,1)$	$(1,4,3,1)$	4	2	1	6	0	0	6
20	13	1	7	5	1	$(1,12,7,1)$	$(1,4,5,1)$	2	2	1	4	1	1	6
21	13	1	9	3	1	$(1,12,9,1)$	$(1,4,3,1)$	2	0	1	6	1	1	6
22	13	1	9	5	0	$(1,12,9,1)$	$(1,4,5,1)$	0	2	3	6	0	0	2
23	13	1	9	5	2	$(1,12,9,1)$	$(1,4,5,1)$	0	0	1	4	2	2	6
24	14	0	4	4	0	$(1,13,4,0)$	$(1,5,4,0)$	6	4	0	4	0	0	8
25	14	1	4	6	1	$(1,13,4,1)$	$(1,5,6,1)$	4	4	0	2	1	1	8
26	14	0	6	2	0	$(1,13,6,0)$	$(1,5,2,0)$	6	2	0	6	0	0	8
27	14	0	6	4	1	$(1,13,6,0)$	$(1,5,4,0)$	4	2	0	4	1	1	8
28	14	1	6	4	1	$(1,13,6,1)$	$(1,5,4,1)$	4	2	0	4	1	1	8
29	14	1	6	6	0	$(1,13,6,1)$	$(1,5,6,1)$	2	4	2	4	0	0	4
30	14	1	6	6	2	$(1,13,6,1)$	$(1,5,6,1)$	2	2	0	2	2	2	8
31	14	1	8	4	0	$(1,13,8,1)$	$(1,5,4,1)$	2	2	2	6	0	0	4
32	14	1	8	4	2	$(1,13,8,1)$	$(1,5,4,1)$	2	0	0	4	2	2	8
33	14	1	8	6	1	$(1,13,8,1)$	$(1,5,6,1)$	0	2	2	4	1	1	4
34	14	1	8	6	3	$(1,13,8,1)$	$(1,5,6,1)$	0	0	0	2	3	3	8
35	15	1	3	7	0	$(1,14,3,1)$	$(1,6,7,1)$	4	6	1	2	0	0	6
36	15	1	5	5	0	$(1,14,5,1)$	$(1,6,5,1)$	4	4	1	4	0	0	6
37	15	1	5	7	1	$(1,14,5,1)$	$(1,6,7,1)$	2	4	1	2	1	1	6
38	15	1	7	3	0	$(1,14,7,1)$	$(1,6,3,1)$	4	2	1	6	0	0	6
39	15	1	7	5	1	$(1,14,7,1)$	$(1,6,5,1)$	2	2	1	4	1	1	6
40	15	1	7	7	0	$(1,14,7,1)$	$(1,6,7,1)$	0	4	3	4	0	0	2
41	15	1	7	7	2	$(1,14,7,1)$	$(1,6,7,1)$	0	2	1	2	2	2	6

TABLE 3.2.2 – Cas possibles pour une action de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ sur une K3 avec $r \leq 15$. Pour chaque possibilité des réseaux $NS(X)$ et $L_1 = NS(X) \cap T_{\iota^*}$ on marque les invariants (s^+, s^-) qui correspondent à la signature, a tel que le groupe discriminant est dans la forme $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^a$ aussi que l'invariant δ. On rappelle que $a_3 = a_{NS(X)} = a_{T(X)}$.

	Invariants numeriques					(s^+, s^-, a, δ)		Nombre de modules par type						Pts
	r	δ	a_3	a_1	k	$NS(X)$	L_1	$\mathbb{F}_2$	$E_{2,0}$	$E_{2,\infty}$	$E_{2,1}$	M_3	W_3	fix
42	16	1	2	8	1	$(1,15,2,1)$	$(1,7,8,1)$	4	6	0	0	1	1	8
43	16	1	4	6	1	$(1,15,4,1)$	$(1,7,6,1)$	4	4	0	2	1	1	8
44	16	1	4	8	0	$(1,15,4,1)$	$(1,7,8,1)$	2	6	2	2	0	0	4
45	16	1	4	8	2	$(1,15,4,1)$	$(1,7,8,1)$	2	4	0	0	2	2	8
46	16	1	6	4	1	$(1,15,6,1)$	$(1,7,4,1)$	4	2	0	4	1	1	8
47	16	1	6	6	0	$(1,15,6,1)$	$(1,7,6,1)$	2	4	2	4	0	0	4
48	16	1	6	6	2	$(1,15,6,1)$	$(1,7,6,1)$	2	2	0	2	2	2	8
49	16	1	6	8	1	$(1,15,6,1)$	$(1,7,8,1)$	0	4	2	2	1	1	4
50	16	1	6	8	3	$(1,15,6,1)$	$(1,7,8,1)$	0	2	0	0	3	3	8
51	17	1	1	9	0	$(1,16,1,1)$	$(1,8,9,1)$	4	8	1	0	0	0	6
52	17	1	3	7	0	$(1,16,3,1)$	$(1,8,7,1)$	4	6	1	2	0	0	6
53	17	1	3	9	1	$(1,16,3,1)$	$(1,8,9,1)$	2	6	1	0	1	1	6
54	17	1	5	5	0	$(1,16,5,1)$	$(1,8,5,1)$	4	4	1	4	0	0	6
55	17	1	5	7	1	$(1,16,5,1)$	$(1,8,7,1)$	2	4	1	2	1	1	6
56	17	1	5	9	0	$(1,16,5,1)$	$(1,8,9,1)$	0	6	3	2	0	0	2
57	17	1	5	9	2	$(1,16,5,1)$	$(1,8,9,1)$	0	4	1	0	2	2	6
58	18	0	0	8	0	$(1,17,0,0)$	$(1,9,8,0)$	6	8	0	0	0	0	8
59	18	0	2	6	0	$(1,17,2,0)$	$(1,9,6,0)$	6	6	0	2	0	0	8
60	18	0	2	8	1	$(1,17,2,0)$	$(1,9,8,0)$	4	6	0	0	1	1	8
61	18	0	2	10	0	$(1,17,2,0)$	$(1,9,10,0)$	2	8	2	0	0	0	4
62	18	1	2	8	1	$(1,17,2,1)$	$(1,9,8,1)$	4	6	0	0	1	1	8
63	18	1	2	10	0	$(1,17,2,1)$	$(1,9,10,1)$	2	8	2	0	0	0	4
64	18	0	4	4	0	$(1,17,4,0)$	$(1,9,4,0)$	6	4	0	4	0	0	8
65	18	0	4	6	1	$(1,17,4,0)$	$(1,9,6,0)$	4	4	0	2	1	1	8
66	18	0	4	8	0	$(1,17,4,0)$	$(1,9,8,0)$	2	6	2	2	0	0	4
67	18	0	4	8	2	$(1,17,4,0)$	$(1,9,8,0)$	2	4	0	0	2	2	8
68	18	0	4	10	1	$(1,17,4,0)$	$(1,9,10,0)$	0	6	2	0	1	1	4
69	18	1	4	6	1	$(1,17,4,1)$	$(1,9,6,1)$	4	4	0	2	1	1	8
70	18	1	4	8	0	$(1,17,4,1)$	$(1,9,8,1)$	2	6	2	2	0	0	4
71	18	1	4	8	2	$(1,17,4,1)$	$(1,9,8,1)$	2	4	0	0	2	2	8
72	18	1	4	10	1	$(1,17,4,1)$	$(1,9,10,1)$	0	6	2	0	1	1	4
73	19	1	1	9	0	$(1,18,1,1)$	$(1,10,9,1)$	4	8	1	0	0	0	6
74	19	1	3	7	0	$(1,18,3,1)$	$(1,10,7,1)$	4	6	1	2	0	0	6
75	19	1	3	9	1	$(1,18,3,1)$	$(1,10,9,1)$	2	6	1	0	1	1	6
76	19	1	3	11	0	$(1,18,3,1)$	$(1,10,11,1)$	0	8	3	0	0	0	2
77	20	1	2	8	1	$(1,19,2,1)$	$(1,11,8,1)$	4	6	0	0	1	1	8
78	20	1	2	10	0	$(1,19,2,1)$	$(1,11,10,1)$	2	8	2	0	0	0	4

TABLE 3.2.3 – Cas possibles pour une action de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ sur une K3 avec $r \geq 16$. Pour chaque possibilité des réseaux $NS(X)$ et $L_1 = NS(X) \cap T_{\iota^*}$ on marque les invariants (s^+, s^-) qui correspondent à la signature, a tel que le groupe discriminant est dans la forme $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^a$ aussi que l'invariant δ. On rappelle que $a_3 = a_{NS(X)} = a_{T(X)}$.

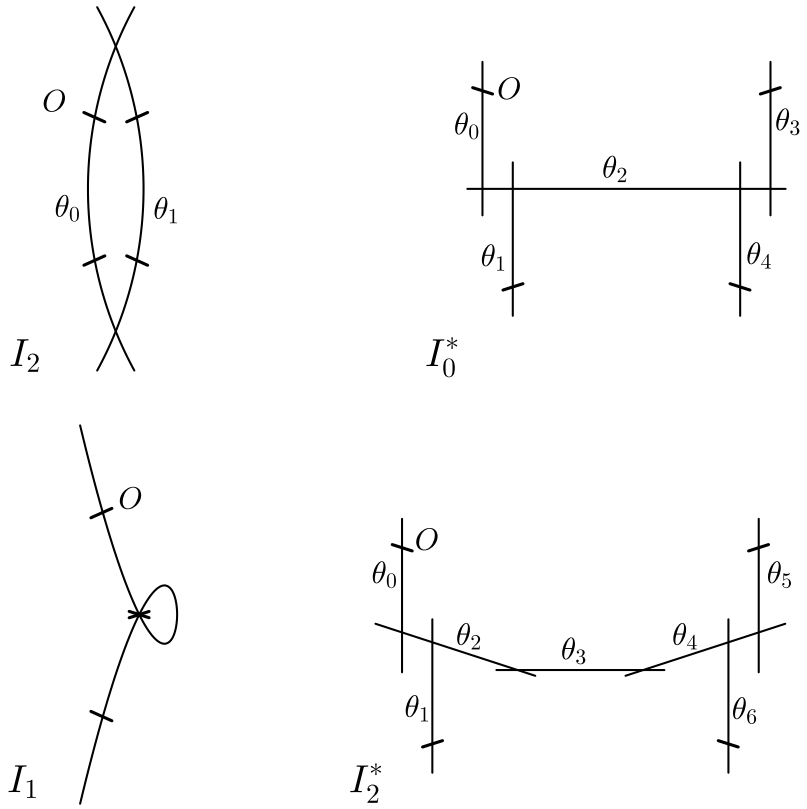


FIGURE 3.3.1 – Intersections et points de 2-torsion des composantes irréductibles des fibres singuliers

3.3 Exemples géométriques

Après une utilisation massive de la théorie des réseaux et de la cohomologie de groupes, nous revenons dans cette dernière section à la géométrie, en donnant des exemples destinés à illustrer géométriquement la formule des points fixes du Théorème 3.2.22.

Par ailleurs on trouve des exemples dans [AS], qui malheureusement ne sont pas les plus adaptés à notre cas, car on a la nécessité de pouvoir calculer l'action sur $NS(X)$ ainsi que le nombre de points fixes. À ces fins, les meilleurs candidats sont les fibrations elliptiques.

Nous renvoyons à [[SS, Mir]] comme référence pour les surfaces elliptiques et à [CG, GeSar] pour les détails sur les involutions dites de « van Geemen-Sarti », qui sont les involutions induites par les sections de 2-torsion de la fibration.

Pour les exemples présentés dans la suite on utilisera les mêmes techniques. Nous essayerons donc de ne pas trop nous répéter dans l'exposition d'argumentations similaires.

Je tiens surtout à remercier Alice Garbagnati pour ses explications très claires et pour son aide dans la recherche d'exemples d'involutions.

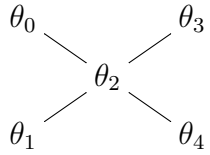
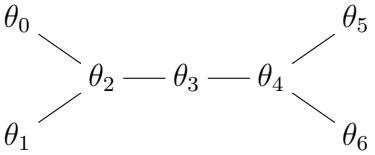
Type	Diagramme	Réseau	Décomposition de F
I_1	/	/	/
I_2	$\theta_0 = \theta_1$	$\langle -2 \rangle$	$\theta_0 + \theta_1$
I_0^*		$D_4(-1)$	$\theta_0 + \theta_1 + 2\theta_2 + \theta_3 + \theta_4$
I_2^*		$D_6(-1)$	$\theta_0 + \theta_1 + 2\theta_2 + 2\theta_3 + 2\theta_4 + \theta_5 + \theta_6$

TABLE 3.3.1 – Fibres singulières utilisées dans les exemples de cette section. Dans la dernière colonne on report la décomposition du diviseur associé à la fibre générale F (i.e. le diviseur donné par le produit d'intersection $\langle F, \bullet \rangle$) sur le réseau engendré par les diviseurs associés aux fibres singuliers.

3.3.1 $\rho = 10$, $a_{NS(X)} = 6$, $\delta_{NS(X)} = 0$, $k = 0$

Note: dans la suite on identifiera les courbes avec le diviseur associé, en écrivant par exemple, avec abus de notation, $F \cdot O$ au lieu de $\langle [F], [O] \rangle$.

L'exemple suivant est pris de [GeSar] et présenté aussi dans [AS].

Soit X une surface K3 qui admet une fibration elliptique avec les caractéristiques suivantes.

Les fibres sur X sont de la forme:

- La fibre générale F est une courbe elliptique lisse avec un point zéro et trois points de 2-torsion ;
- 8 fibres singulières réductibles de type I_2 (deux courbes rationnelles qui se rencontrent en deux points différents). On appelle $\theta_0^{(i)}$, $\theta_1^{(i)}$ les deux composantes de l'i-ème fibre de type I_2, qu'on note $I_2^{(i)}$.
  $I_2^{(i)}$ hérite une structure de groupe abélien avec point zéro sur la composante $\theta_0^{(i)}$ et trois points de 2-torsion, un sur $\theta_0^{(i)}$ et deux sur $\theta_1^{(i)}$. Les quatre points sont lisses ;
- 8 fibres singulière irréductibles de type I_1 (courbes avec un noeud). I_1 hérite aussi d'une structure de groupe abélien avec point zéro lisse et trois points de 2-torsion, dont un lisse et deux en correspondance du noeud.

Les sections de X sont de la forme:

- Une section zéro qu'on note O, qui par définition intersecte donc chaque fibre en un point:
  — L'intersection de O avec la fibre générale F est le neutre de la structure de groupe abélien sur F ;
  — L'intersection de O avec la fibre $I_2^{(i)}$ est un point lisse de $\theta_0^{(i)}$;
  — L'intersection de O avec la fibre I_1 est un point lisse.

- Une section de 2-torsion qu'on note P, qui intersecte chaque fibre en un point:
  — L'intersection de P avec la fibre générale F est un élément de 2-torsion de la structure de groupe abélien sur F ;
  — L'intersection de P avec la fibre $I_2^{(i)}$ est un point lisse de $\theta_1^{(i)}$;
  — L'intersection de P avec la fibre I_1 est un point lisse de I_1.
- Une bissection de 2-torsion qu'on note B, qui intersecte chaque fibre en deux points:
  — L'intersection de B avec la fibre générale F est constituée par les deux éléments de 2-torsion restants ;
  — L'intersection de B avec la fibre $I_2^{(i)}$ est donnée par un point lisse de $\theta_1^{(i)}$ et un point lisse de $\theta_0^{(i)}$;
  — L'intersection de B avec la fibre I_1 est ramifiée sur le noeud.

Remarque 3.3.1. En général l'intersection de la section de 2-torsion avec $I_2^{(i)}$ peut se trouver soit sur la composante θ_0, soit sur θ_1, et pour déterminer lequel de deux cas est vérifié on utilise le « height algorithm » (cf. [SS]).

Le réseau $NS(X)$ est engendré par les diviseurs suivants:

- La section O, qui est une courbe rationnelle, donc $O^2 = -2$.
- La classe F de la fibre générale, qui est une courbe de genre 1 avec $F^2 = 0$;
- Pour chaque fibre réductible $I_2^{(i)}$ on a les diviseurs donnés par $\theta_0^{(i)}$ et $\theta_1^{(i)}$ qui sont deux courbes rationnelles, donc $\theta_j^2 = -2$. L'intersection est composée par deux points singuliers, $\theta_0^{(i)} \cdot \theta_1^{(i)} = 2$
- La section P, qui est aussi une courbe rationnelle, donc $P^2 = -2$. On remarque que sur chaque fibre l'intersection avec P est différente de l'intersection avec O, on en conclut que $P \cdot O = 0$.

En résumant pour les produits scalaires on obtient:

$$\begin{array}{c} \\ O \\ P \\ F \\ \theta_0^{(1)} \\ \theta_1^{(1)} \\ \vdots \\ \theta_0^{(8)} \\ \theta_1^{(8)} \end{array} \begin{array}{c} \begin{array}{cccccccc} O & P & F & \theta_0^{(1)} & \theta_1^{(1)} & \cdots & \theta_0^{(8)} & \theta_1^{(8)} \end{array} \\ \begin{pmatrix} -2 & 0 & 1 & 1 & 0 & \cdots & 1 & 0 \\ 0 & -2 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -2 & 2 & & & \\ 0 & 1 & 0 & 2 & -2 & & & \\ \vdots & \vdots & \vdots & & & \ddots & & \\ 1 & 0 & 0 & & & & -2 & 2 \\ 0 & 1 & 0 & & & & 2 & -2 \end{pmatrix} \end{array}$$

Par contre ces diviseurs ne sont pas tous linéairement indépendants ! Plus précisément on a que:

- Les composantes $\theta_0^{(i)}$ et $\theta_1^{(i)}$ forment une fibre, donc $\theta_0^{(i)} + \theta_1^{(i)} = F$ pour $i = 1, \ldots, 8$;

- En regardant les produits d'intersection, on remarque que P est obtenue par combinaison rationnelle des fibres et de la section O. En calculant sa décomposition sur la base on obtient:

$$P = 2F + O - \frac{1}{2}\sum_{i=1}^{8} \theta_1^{(i)}$$

On remarque qu'un choix d'un ensemble minimal de générateurs de $NS(X)$ est donné par $(O, F, P, \theta_1^{(1)}, \theta_0^{(2)}, \ldots, \theta_0^{(8)}, \theta_1^{(8)})$. Pour la matrice d'intersection on obtient donc:

$$\begin{array}{c} \\ O \\ P \\ F \\ \theta_1^{(2)} \\ \vdots \\ \theta_1^{(8)} \end{array} \begin{array}{c} \begin{array}{cccccc} O & P & F & \theta_1^{(2)} & \cdots & \theta_1^{(8)} \end{array} \\ \begin{pmatrix} -2 & 0 & 1 & 0 & \cdots & 0 \\ 0 & -2 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & & \\ \vdots & \vdots & \vdots & & \ddots & \\ 0 & 1 & 0 & & & -2 \end{pmatrix} \end{array}$$

Il s'ensuit que $NS(X)$ est un réseau 2-élémentaire de rang 10 avec $A_{NS(X)} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^6$ et $\delta_{NS(X)} = 0$.

On passe maintenant aux involutions: grâce à la structure de fibration elliptique on peut définir deux involutions:

- L'involution hyperelliptique η qui agit sur chaque fibre en envoyant tout point sur son opposé (par rapport à la structure de groupe abélien). Il s'agit d'une involution non-symplectique avec action triviale sur $NS(X)$;
- La translation t_P qui agit aussi sur chaque fibre, en sommant à chaque point le point de 2-torsion donné par l'intersection avec P. τ_P Est une involution qui agit comme l'identité sur la forme symplectique, donc une involution symplectique, qui commute avec η. On appelle ces automorphismes des involutions de Van Geemen-Sarti.

On a donc une action de $G = \langle \eta, t_P \rangle \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ sur X. En regardant le Tableau 3.2.2 pour ce choix de X on une seule possibilité: $a_1 = 2$ et $k = 0$ (ligne 2) donc le lieu fixe (si non vide) doit être composé par 8 points. Essayons de vérifier cela.

- Le lieu fixe de η est lisse et composé par une courbe de genre $(22 - 10 - 6)/2 = 3$ et $(10 - 6)/2 = 2$ courbes rationnelles par le Théorème 3.2.30. Comme chaque point est envoyé sur son opposé il s'ensuit que les sections O et P sont fixées, ainsi que la bissection B. En appliquant le théorème de Riemann–Hurwitz on trouve que B a genre 3 car ramifiée sur les noeuds des 8 fibres I_1. On en conclut que $X^\eta = \{O, P, B\}$.

- Le lieu fixe de t_P doit être composé de 8 points, car t_P est une involution symplectique. Comme t_P agit comme une involution sur chaque fibre, en particulier les 8 fibres I_1 sont envoyées sur elles-mêmes, et donc les 8 noeuds sont les points fixes de l'involution.
- On en conclut que pour le lieu fixe de G on a:

$$X^G = X^\eta \cap X^{t_P} = \{8 \text{ noeuds des fibres } I_1\}$$

3.3.2 $\rho = 12$, $a_{NS(X)} = 6$, $\delta_{NS(X)} = 1$, $k = 1$

Le Théorème 3.2.22 porte à notre attention l'invariant numérique k, qui nous donne une information sur l'extension de réseaux $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ laquelle ne peut pas être extraite à partir uniquement des invariants des réseaux L_i pris séparément.

C'est donc naturel de vouloir chercher maintenant un exemple géométrique avec $k \neq 0$, ce qui fera l'objet de cette partie finale de notre travail.

D'après [GaSal] on peut choisir une fibration elliptique de X surface K3 avec:

- **Sections:** une section de 2-torsion P ainsi qu'une bissection de 2-torsion B (en plus de la section O qui est toujours présente dans toute fibration) ;
- **Fibres réductibles:** une fibre de type I_0^* et 6 fibres de type I_2 ;
- **Fibres singulières irréductibles:** 6 fibres de type I_1.

On a aussi les intersections suivantes:

- O intersecte $\theta_0^{(i)}$ pour $1 \leq i \leq 7$;
- P intersecte $\theta_1^{(i)}$ pour $1 \leq i \leq 7$;

On rappelle que les diviseurs associés à $\theta_0^{(i)}$ sont engendrés par la classe de la fibre générale et les autres composantes irréductibles de la fibre. D'après le Tableau 3.3.1 on a les décompositions:

$$\begin{aligned} \theta_0^{(1)} &= F - \theta_1^{(1)} - 2\theta_2^{(1)} - \theta_3^{(1)} - \theta_4^{(1)} \\ \theta_0^{(i)} &= F - \theta_1^{(i)} \text{ pour } i \geq 2 \end{aligned}$$

Le réseau $NS(X)$ est donc engendré par les diviseurs donnés par les sections O, P, la fibre générale F et les composantes irréductibles $\theta_1^{(1)}, \ldots, \theta_4^{(1)}, \theta_1^{(2)}, \ldots, \theta_1^{(7)}$.

Plus en détail, si on regarde les intersections, O, F engendrent un réseau U, les $\theta_i^{(1)}$ engendrent un réseau $D_4(-1)$ et les θ_1^i pour $2 \leq i \leq 7$ engendrent 6 réseaux $\langle -2 \rangle$. Par contre P est une combinaison rationnelle des autres diviseurs, ce qui ne change pas le rang du réseau mais qui donne une extension de réseaux. Donc $NS(X) \supseteq D_4(-1) \oplus \langle -2 \rangle^{\oplus 6} \oplus U$ est un sur-réseau avec $H_{NS(X)} \simeq \mathbb{Z}/2\mathbb{Z}$.

D'après calcules, la décomposition de P est de la forme:

$$P = 2F + O - \theta_1^{(1)} - \theta_2^{(1)} - \frac{1}{2}\theta_3^{(1)} - \frac{1}{2}\theta_4^{(1)} - \frac{1}{2}\sum_{i=2}^{7} \theta_1^{(i)}$$

On trouve ainsi que $NS(X)$ est le réseau 2-élémentaire de rang 12 avec invariants $a_{NS(X)} = 6$ et $\delta_{NS(X)} = 1$.

Comme dans l'exemple précédent, sur X on peut définir l'involution hyperelliptique η (non-symplectique et avec action triviale sur $NS(X)$) et la translation t_P (symplectique).

En regardant le Tableau 3.2.2 (ligne 12) pour ce choix de X on une seule possibilité: $a_1 = 4$ et $k = 1$, donc le lieu fixe (si non vide) doit être composé de 8 points.

À nouveau, essayons de vérifier cela géométriquement.

- Le lieu fixe de l'involution hyperelliptique η est lisse et composé par une courbe de genre $(22 - 12 - 6)/2 = 2$ et $(12 - 6)/2 = 3$ courbes rationnelles par le Théorème 3.2.30. Comme chaque point est envoyé sur son opposé il s'ensuit que les sections O et P sont fixées, ainsi que la bissection B. En appliquant le théorème de Riemann–Hurwitz on trouve que B a genre 2 car ramifiée sur les noeuds des 6 fibres I_1. Il reste donc une courbe fixe à trouver.
  La fibre I_0^* est envoyée sur elle-même, donc on a une action de η sur les composantes irréductibles $\theta_i^{(1)}$. Sur I_0^* il existe un point zéro, sur la composante $\theta_0^{(1)}$, donné par l'intersection avec O, et trois points de 2-torsion sur les composantes $\theta_1^{(1)}$,$\theta_3^{(1)}$,$\theta_4^{(1)}$, donnés respectivement par les intersections avec la section P et la bissection B. Comme O,P,B sont des courbes fixes, il s'ensuit que $\theta_1^{(1)}, \theta_3^{(1)}, \theta_4^{(1)}$ sont envoyées sur elles-mêmes.
  Donc $\theta_2^{(1)}$ est envoyée sur elle-même aussi, de plus $\theta_2^{(1)} \cap \theta_0^{(1)}$, $\theta_2^{(1)} \cap \theta_1^{(1)}$,$\theta_2^{(1)} \cap \theta_3^{(1)}$,$\theta_2^{(1)} \cap \theta_4^{(1)}$ sont quatre points fixes de $\theta_2^{(1)}$, mais une involution d'une courbe rationnelle qui fixe quatre points doit agir comme l'identité sur toute la courbe. On en conclut que $X^\eta = \{O, P, B, \theta_2^{(1)}\}$.
- Le lieu fixe de t_P doit être composé par 8 points, car t_P est une involution symplectique. Comme t_P agit séparément sur chaque fibre, en particulier les 6 fibres I_1 sont envoyées sur elles-mêmes, et donc les 6 noeuds sont des points fixes de l'involution. Il reste deux points à déterminer.
  À nouveau, la fibre I_0^* est envoyée sur elle-même, donc on a une action sur les composantes $\theta_i^{(1)}$. La seule composante qui a intersection non vide avec toutes les autres composantes de la fibre est $\theta_2^{(1)}$, qui est donc forcément envoyée sur elle-même. On a donc une involution de la courbe rationnelle $\theta_2^{(1)}$, qui doit donc fixer exactement deux points $M_2^1, N_2^1 \in \theta_2^{(1)}$.
- On en conclut que pour le lieu fixe de G on a:

$$X^G = X^\eta \cap X^{t_P} = \{\text{6 noeuds des fibres } I_1, M_2^1, N_2^1\}$$

3.3.3 $\rho = 18$, $a_{NS(X)} = 4$, $\delta_{NS(X)} = 1$, $k = 0, 2$

Pour terminer nous montrerons un exemple de surface K3 sur laquelle on peut définir deux actions différentes de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ où le seul invariant qui change est k.

Dans les deux cas on aura donc deux extensions de réseaux $\Lambda_{K3} \supseteq L_1 \oplus L_2 \oplus L_3$ avec exactement les mêmes réseaux L_i: ce qui changera sera uniquement la façon dont ces réseaux seront « collés ».

Par le Théorème 3.2.22, une valeur différente de k, quand les autres invariants sont les mêmes, implique forcément un nombre différent de points fixes, ce qui montre bien l'importance de l'invariant k que nous avons défini dans la Section 3.2.1. Par contre tout cela est subordonné à l'hypothèse que le lieu fixe soit non vide.

L'intérêt de ces exemples géométriques sera donc aussi de montrer qu'il existe des cas où cette dernière condition est vérifiée.

Dans les exemples précédents le calcul direct des invariants a_1 et k n'a pas été nécessaire, car il existait un seul choix possible des invariants de l'action pour les surface K3 considérées, mais malheureusement on ne pourra pas profiter de ce type de simplification dans ce cas et on sera donc obligé de calculer la matrice de l'involution et les invariants de l'extension associée. Le lecteur intéressé pourra retrouver les détails relatifs à ces calculs, ainsi que le code de l'algorithme utilisé dans l'annexe B.

Les exemples suivants sont pris de [CG].

3.3.3.1 Cas $a_1 = 8$, $k = 2$

On peut choisir une fibration elliptique de X surface K3 avec:

- **Sections:** trois sections de 2-torsion qu'on notera P,Q,R plus la section O ;
- **Fibres réductibles:** $I_2^* + 2I_0^* + 2I_2$;
- **Fibres singulières irréductibles:** non**.**

On a les intersections suivantes:

- O intersecte $\theta_0^{(1)}, \theta_0^{(2)}, \theta_0^{(3)}, \theta_0^{(4)}, \theta_0^{(5)}$;
- P intersecte $\theta_1^{(1)}, \theta_1^{(2)}, \theta_1^{(3)}, \theta_1^{(4)}, \theta_1^{(5)}$;
- Q intersecte $\theta_5^{(1)}, \theta_3^{(2)}, \theta_3^{(3)}, \theta_1^{(4)}, \theta_0^{(5)}$;
- R intersecte $\theta_6^{(1)}, \theta_4^{(2)}, \theta_4^{(3)}, \theta_0^{(4)}, \theta_1^{(5)}$;

D'après le Tableau 3.3.1 on a les décompositions:

$$\begin{aligned}
\theta_0^{(1)} &= F - \theta_1^{(1)} - 2\theta_2^{(1)} - 2\theta_3^{(1)} - 2\theta_4^{(1)} - \theta_5^{(1)} - \theta_6^{(1)} \\
\theta_0^{(i)} &= F - \theta_1^{(i)} - 2\theta_2^{(i)} - \theta_3^{(i)} - \theta_4^{(i)} \text{ pour } i = 2, 3 \\
\theta_0^{(i)} &= F - \theta_1^{(i)} \text{ pour } i = 4, 5
\end{aligned}$$

Les fibres I_2^*, I_0^*, I_2 correspondent respectivement aux réseaux $D_6(-1), D_4(-1), \langle -2 \rangle$, donc $NS(X) \supseteq D_6(-1) \oplus D_4(-1)^{\oplus 2} \oplus \langle -2 \rangle^{\oplus 2} \oplus U$ est une extension de réseau définie par les sections de 2-torsion P, Q, R.

D'après calcule, dans la base $(F, O, \theta_i^{(1)}, \theta_j^{(2)}, \theta_k^{(3)}, \theta_1^{(4)}, \theta_1^{(5)}\ i,j,k \geq 1)$ (qui n'engendre pas le réseau $NS(X)$ mais uniquement le sous-réseau dont $NS(X)$ est une extension) leur décomposition est de la forme:

$$\begin{aligned}
P &= \left(2,\ 1,\ -1,-1,-1,-1,-\frac{1}{2},-\frac{1}{2},\ -1,-1,-\frac{1}{2},-\frac{1}{2},\ -1,-1,-\frac{1}{2},-\frac{1}{2},\ -\frac{1}{2},\ -\frac{1}{2}\right)\\
Q &= \left(2,\ 1,\ -\frac{1}{2},-1,-\frac{3}{2},-2,-\frac{3}{2},-1,\ -\frac{1}{2},-1,-1,-\frac{1}{2},\ -\frac{1}{2},-1,-1,-\frac{1}{2},\ -\frac{1}{2},\ 0\right)\\
R &= \left(2,\ 1,\ -\frac{1}{2},-1,-\frac{3}{2},-2,-1,-\frac{3}{2},\ -\frac{1}{2},-1,-\frac{1}{2},-1,\ -\frac{1}{2},-1,-\frac{1}{2},-1,\ 0,\ -\frac{1}{2}\right)
\end{aligned}$$

On remarque que le diviseur associé à R est un combinaison linéaire de P,Q et des autres diviseurs car $R-P-Q$ est à coefficient entiers, donc $H_{NS(X)} = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ et on trouve que $NS(X)$ est le réseau 2-élémentaire de rang 18 avec invariants $a_{NS(X)} = 4$ et $\delta_{NS(X)} = 1$. On peut choisir comme base de $NS(X)$ les diviseurs $(F, O, \theta_i^{(1)}, \theta_j^{(2)}, \theta_k^{(3)}, P, Q\ i,j,k \geq 1)$ et avec ce choix la décomposition de R est:

$$R = (2,1,0,-1,-2,-3,-2,-2,0,-1,-1,-1,0,-1,-1,-1,1,-1)$$

Sur X on peut définir l'involution hyperelliptique η (non-symplectique et avec action triviale sur $NS(X)$) et les translations t_P, t_Q, t_R (symplectiques). On choisit dans la suite d'étudier uniquement t_P, car c'est le cas avec les invariants qui nous intéressent le plus.

En regardant le Tableau 3.2.2 pour ce choix de X on a quatre possibilités différentes et le lieu fixe peut être composé par 4 ou 8 points. On est donc obligé de calculer la matrice associée à t_P et pour faire cela on doit étudier l'action de deux involutions sur $NS(X)$.

- L'involution t_P préserve les fibres et en particulier la fibre générale, donc $t_P(F) = F$. Comme il s'agit de la translation par P on a $t_P(O) = P$, $t_P(P) = O$, $t_P(Q) = R$, $t_P(R) = Q$. En regardant I_2^*, $\theta_0^{(1)}$ est la composante qui intersecte O, elle doit donc être envoyée sur la composante qui intersecte P, c'est à dire $\theta_1^{(1)}$. De la même façon $\theta_4^{(1)}$ et $\theta_5^{(1)}$ doivent être échangées car elles intersectent respectivement Q et R. $\theta_2^{(1)}$ est stable car c'est la seule composante qui intersecte $\theta_0^{(1)}$ et $\theta_1^{(1)}$,$\theta_4^{(1)}$ aussi car elles intersectent respectivement $\theta_5^{(1)}$,$\theta_6^{(1)}$, donc par exclusion $\theta_3^{(1)}$ est envoyée sur elle-même aussi. En raisonnant de la même façon on détermine également l'action sur les autres fibres. On peut mieux visualiser l'action de t_P en regardant les diagrammes d'intersections de fibres: on remarque que t_P agit comme une symétrie verticale sur I_2^* et les deux composantes I_0^* , et en échangeant les deux composantes de I_2.
  En résumant l'action de t_P est la suivante:

$$\begin{array}{ccccc}
\theta_0^{(1)} \leftrightarrow \theta_1^{(1)} & \theta_5^{(1)} \leftrightarrow \theta_6^{(1)} & \theta_0^{(2)} \leftrightarrow \theta_1^{(2)} & \theta_3^{(2)} \leftrightarrow \theta_4^{(2)} & \theta_0^{(3)} \leftrightarrow \theta_1^{(3)}\\
\theta_3^{(3)} \leftrightarrow \theta_4^{(3)} & \theta_0^{(4)} \leftrightarrow \theta_1^{(4)} & \theta_0^{(5)} \leftrightarrow \theta_1^{(5)} & O \leftrightarrow P & Q \leftrightarrow R
\end{array}$$

et les courbes $\theta_2^{(1)}, \theta_3^{(1)}, \theta_4^{(1)}, \theta_2^{(2)}, \theta_2^{(3)}$ sont envoyées sur elles mêmes.

- L'involution hyperelliptique η est triviale sur $NS(X)$.

On a tous les éléments pour définir la matrice associée à t_P et calculer les invariants associés à l'extension. Sans répéter ici les détails du calcul (cf. Annexe B) on trouve finalement que $a_1 = 8$ et $k = 2$, donc le nombre de points fixes prévu est 8. Encore une fois, essayons de vérifier cela géométriquement.

- Le lieu fixe de l'involution hyperelliptique η est lisse et composé par 8 courbes rationnelles par le Théorème 3.2.30. Les sections O,P,Q,R sont des courbes fixes, il reste donc quatre courbes fixes à trouver.
  La fibre I_0^* est envoyée sur elle-même, donc on a une action de η sur les composantes irréductibles $\theta_i^{(1)}$. Comme les quatre sections sont fixes, on a que $\theta_0^{(1)}$,$\theta_1^{(1)}$,$\theta_5^{(1)}$, $\theta_6^{(1)}$ sont envoyées sur elles-mêmes et par conséquent $\theta_2^{(1)}$,$\theta_3^{(1)}$,$\theta_4^{(1)}$ sont préservées aussi. Donc $\theta_2^{(1)}$ a au moins trois points fixes: $\theta_0^{(1)} \cap \theta_2^{(1)}$, $\theta_1^{(1)} \cap \theta_2^{(1)}$, $\theta_3^{(1)} \cap \theta_2^{(1)}$ mais $\theta_2^{(1)}$ est une courbe rationnelle donc soit η fixe exactement deux points, soit η agit comme l'identité et fixe toute la courbe, donc $\theta_2^{(1)}$ est une courbe fixe. Symétriquement on trouve que $\theta_4^{(1)}$ est aussi une courbe fixe.
  L'action sur les fibres I_0^* est la même que dans l'exemple précédent, en raisonnant de la même manière on trouve les deux courbes fixes restantes: $\theta_2^{(2)}$ et $\theta_2^{(3)}$. On conclut que $X^\eta = \{O, P, Q, R, \theta_2^{(1)}, \theta_4^{(1)}, \theta_2^{(2)}, \theta_2^{(3)}\}$.
- On rappelle que le lieu fixe de t_P doit être composé par 8 points, comme on a déjà étudié l'action de t_P dans le détail on sait qu'en particulier t_P préserve les composantes irréductibles $\theta_2^{(1)}, \theta_4^{(1)}, \theta_2^{(2)}, \theta_2^{(3)}$. Comme il s'agit d'une involution sur des courbes rationnelles disjointes, elle doit fixer deux points par courbe, ce qui donne un total de 8 points fixes.
- Les points fixes de t_P appartiennent aux courbes préservées par η, donc:
$$X^G = X^\eta \cap X^{t_P} = \{8 \text{ points}\}$$

3.3.3.2 Cas $a_1 = 8$, $k = 0$

On peut choisir une fibration elliptique de X surface K3 avec:

- **Sections:** section O, trois sections de 2-torsion P, Q, R;
- **Fibres réductibles:** $2I_2^* + 4I_2$;
- **Fibres singulières irréductibles:** non

On a les intersections suivantes:

- P intersecte $\theta_5^{(1)}, \theta_5^{(2)}, \theta_1^{(3)}, \theta_1^{(4)}, \theta_0^{(5)}, \theta_0^{(6)}$;
- Q intersecte $\theta_1^{(1)}, \theta_6^{(2)}, \theta_0^{(3)}, \theta_1^{(4)}, \theta_1^{(5)}, \theta_1^{(6)}$;
- R intersecte $\theta_6^{(1)}, \theta_1^{(2)}, \theta_1^{(3)}, \theta_0^{(4)}, \theta_1^{(5)}, \theta_1^{(6)}$;

On rappelle les décompositions:

$$\begin{aligned} \theta_0^{(i)} &= F - \theta_1^{(i)} - 2\theta_2^{(i)} - 2\theta_3^{(i)} - 2\theta_4^{(i)} - \theta_5^{(i)} - \theta_6^{(i)} \text{ pour } i = 1, 2 \\ \theta_0^{(i)} &= F - \theta_1^{(i)} \text{ pour } i \geq 3 \end{aligned}$$

En raisonnant comme dans les exemples précédents $NS(X) \supseteq D_6(-1)^{\oplus 2} \oplus \langle -2 \rangle^{\oplus 4} \oplus U$ est une extension de réseaux définie par les sections de 2-torsion P, Q, R.

D'après calculs, dans la base $(F, O, \theta_i^{(1)}, \theta_j^{(2)}, \theta_1^{(3)}, \theta_1^{(4)}, \theta_1^{(5)}, \theta_1^{(6)}\ i, j \geq 1)$ (qui n'est pas une base du réseau $NS(X)$) leur décomposition est de la forme:

$$\begin{aligned} P &= \left(2, 1, -\frac{1}{2}, -1, -\frac{3}{2}, -2, -\frac{3}{2}, -1, -\frac{1}{2}, -1, -\frac{3}{2}, -2, -\frac{3}{2}, -1, -\frac{1}{2}, -\frac{1}{2}, 0, 0\right) \\ Q &= \left(2, 1, -1, -1, -1, -1, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -1, -\frac{3}{2}, -2, -1, -\frac{3}{2}, 0, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) \\ R &= \left(2, 1, -\frac{1}{2}, -1, -\frac{3}{2}, -2, -1, -\frac{3}{2}, -1, -1, -1, -1, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, 0, -\frac{1}{2}, -\frac{1}{2}\right) \end{aligned}$$

Pour $NS(X)$ on obtient les mêmes invariants de l'exemple précédent: $r = 18$, $a_{NS(X)} = 4$ et $\delta_{NS(X)} = 1$. On prend comme base de $NS(X)$ les diviseurs $(F, O, \theta_i^{(1)}, \theta_j^{(2)}, \theta_1^{(3)}, P, Q, \theta_1^{(6)}\ i, j \geq 1)$ et avec ce choix la décomposition de R est:

$$R = (2, 1, 0, -1, -2, -3, -2, -2, -1, -1, -1, -1, -1, 0, -1, -1, 1, 0)$$

On considère l'action sur X de l'involution hyperelliptique η et de la translation t_Q. On détermine la matrice associée à t_Q en regardant l'action sur les composantes irréductibles des fibres:

- Pour t_Q, comme dans l'exemple précédent on a $t_Q(F) = F$, $t_Q(O) = Q$, $t_Q(P) = R$, $t_Q(Q) = O$, $t_Q(R) = P$.
  Sur les deux fibres I_2^* l'action est différente: sur la première on a la même action de t_P vue dans l'exemple précédent, c'est-à-dire une symétrie verticale sur le diagramme qui échange les composantes $\theta_0^{(1)}, \theta_1^{(1)}$ et $\theta_5^{(1)}, \theta_6^{(1)}$ en préservant les autres.
  Sur la deuxième fibre I_2^* l'involution t_Q renverse le diagramme horizontalement. Pour détailler, $\theta_0^{(2)}$ qui intersecte O) est envoyée par t_Q sur $\theta_6^{(2)}$ (qui intersecte Q) et de la même façon $\theta_5^{(2)}$ et $\theta_1^{(2)}$ doivent être échangées car elles intersectent respectivement P et R. $\theta_2^{(2)}$ est donc envoyée sur $\theta_4^{(2)}$ car c'est la seule composante qui intersecte $\theta_0^{(1)}$ et $\theta_1^{(1)}$ et par exclusion $\theta_3^{(1)}$ est la seule composante qui est préservée. De la même façon on détermine l'action de t_Q sur les quatre fibres I_2. .
  En résumant l'action de t_Q est la suivante.

  $$\begin{array}{ccccc} \theta_0^{(1)} \leftrightarrow \theta_1^{(1)} & \theta_5^{(1)} \leftrightarrow \theta_6^{(1)} & \theta_0^{(2)} \leftrightarrow \theta_6^{(2)} & \theta_1^{(2)} \leftrightarrow \theta_5^{(2)} & \theta_2^{(2)} \leftrightarrow \theta_4^{(2)} \\ \theta_0^{(4)} \leftrightarrow \theta_1^{(4)} & \theta_0^{(5)} \leftrightarrow \theta_1^{(5)} & \theta_0^{(6)} \leftrightarrow \theta_1^{(6)} & O \leftrightarrow Q & P \leftrightarrow R \end{array}$$

  et les courbes $\theta_2^{(1)}, \theta_3^{(1)}, \theta_4^{(1)}, \theta_3^{(2)}, \theta_0^{(3)}, \theta_1^{(3)}$ sont envoyées sur elles mêmes.
- L'involution hyperelliptique η est triviale sur $NS(X)$.

En calculant la matrice associée à t_Q on trouve que $a_1 = 8$ et $k = 0$, donc le nombre de points fixes prévu est 4. On vérifie géometriquement:

- Comme dans l'exemple précèdent le lieu fixe de l'involution hyperelliptique η est lisse et composé par 8 courbes rationnelles: comme dans l'exemple précèdent on a les sections O,P,Q,R plus quatre autres courbes fixes données par les composantes θ_2 et θ_4 des deux fibres I_2^*. Donc $X^\eta = \{O, P, Q, R, \theta_2^{(1)}, \theta_4^{(1)}, \theta_2^{(2)}, \theta_4^{(2)}\}$.
- On cherche les 8 points qui composent le lieu fixe de t_Q. Dans la première fibre I_2^* les composantes $\theta_2^{(1)}, \theta_3^{(1)}, \theta_4^{(1)}$ sont préservées et nous donnent donc deux points fixes pour chaque composante. Comme deux points fixes correspondent à des intersections, on a un total de quatre points fixes: $\theta_2^{(1)} \cap \theta_3^{(1)}$, $\theta_4^{(1)} \cap \theta_3^{(1)}$, un point $M_2^1 \in \theta_2^{(1)}$ et un autre point $M_4^1 \in \theta_4^{(1)}$.
  Pour la deuxième fibre I_2^* la composante $\theta_3^{(2)}$ est préservée et a donc deux points fixes M_3^2 et N_3^2 .
  Pour terminer, sur la première fibre de type I_2 les deux courbes $\theta_0^{(3)}, \theta_1^{(3)}$ sont préservées, donc il y a deux points fixes sur chaque composante, mais comme il ne reste que deux points fixes à déterminer la seule possibilité est donnée par les deux points d'intersections $\theta_0^{(3)} \cap \theta_1^{(3)}$.
  En résumant:

  $$X^{t_Q} = \{\theta_2^{(1)} \cap \theta_3^{(1)}, \theta_4^{(1)} \cap \theta_3^{(1)}, M_2^1, M_4^1, M_3^2, N_3^2, \theta_0^{(3)} \cap \theta_1^{(3)} \text{ (deux points)}\}$$

- Les quatre points fixes de t_Q appartenant à la première fibre I_2^* sont fixés par η aussi. Par contre les seuls points de $\theta_3^{(2)}$ fixés par η sont donc M_3^2, N_3^2 n'appartient pas au lieu fixe de η (on rappelle que si on avait plus de deux points fixes alors toute la courbe devrait appartenir au lieu fixe, ce qui n'est pas le cas). De la même façon η sur $\theta_0^{(3)}$ fixe déjà les points d'intersections avec les sections O et Q et donc les deux points de l'intersection $\theta_0^{(3)} \cap \theta_1^{(3)}$ ne sont pas fixés non plus par η (ils sont en effet échangés). On a donc un total de quatre points fixes:

  $$X^G = \left\{\theta_2^{(1)} \cap \theta_3^{(1)}, \theta_4^{(1)} \cap \theta_3^{(1)}, M_2^1, M_4^1\right\}$$

Annexe A

Forme quadratiques dégénérées sur $(\mathbb{Z}/2\mathbb{Z})^n$

La plupart des résultats qu'on a prouvés dans le Chapitre 2 concernent les f.f. non-dégénérées. Cela n'est pas suffisant si on veut étudier les possibilités pour une extension de réseau $H_R \hookrightarrow A_{L_1} \oplus A_{L_2}$ où la restriction de la f.f. quadratique sur $H_{R,L_1} \subseteq A_{L_1}$ peut être dégénérée.

On ne rentrera pas dans les détails du sujet, mais comme les réseaux de notre intérêt sont 2-élémentaires, on se limitera à donner dans la suite les résultats principaux pour ce qui concerne les formes dégénérées sur $A = (\mathbb{Z}/2\mathbb{Z})^n$.

Définition A.0.2. Soit q une f.f. quadratique sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$, on appelle rang de q le rang de la forme bilinéaire associée, $b : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, c'est-à-dire le rang de la matrice qui décrit b.

On note les deux f.f. dégénérées sur $A = \mathbb{Z}/2\mathbb{Z}$ comme:

$$z_2^0 := \begin{pmatrix} 0 \end{pmatrix}$$

$$z_2^1 = \begin{pmatrix} 1 \end{pmatrix}$$

Lemme A.0.3. *Soit q une f.f. quadratique sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$ de rang 0, alors on a une des deux possibilités suivantes:*

1

$$q = \begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{pmatrix} = \left(z_2^0\right)^{\oplus n}$$

2

$$q = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} = \left(z_2^1\right)^{\oplus n}$$

Démonstration. Si q est totalement isotrope en tant que forme quadratique alors $q(x) = 0$ pour tout $x \in A$ et q est de la forme (1).

Sinon, il existe $x_1 \in A$ tel que $q(x_1) = 1$ et $x_2, \ldots, x_n \in A$ tels que $(x_1, \ldots x_n)$ soit une base de A. Comme q_A a rang 0, alors $b(x_i, x_j) = 0$ et $q(x_i) \in \{0, 1\}$ pour tout $1 \leq i, j \leq n$. Soient donc y_i ainsi définis:

$$y_i = \begin{cases} x_i & \text{si } q(x_i) = 1 \\ x_1 + x_i & \text{si } q(x_i) = 0 \end{cases}$$

alors la matrice de q_A dans la base (y_i) est de la forme (2). □

Définition A.0.4. Soit q une f.f. quadratique sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$, si $N = A^\circ := A^\perp \cap A$ (l'orthogonal de A), il existe $A_1 \subseteq A$ (en général non unique) tel que $A = A_1 \oplus N$.

On obtient une décomposition de la forme $q = q_1 \oplus q_N$ avec q_1 non-dégénérée et q_N de rang 0. Alors on associe à q le symbole ϵ_q avec la valeur:

$$\epsilon_q = \begin{cases} 0 & \text{si } q_N = (z_2^0)^{\oplus n-r} \text{ou } \dim(N) = 0 \\ 1 & \text{si } q_N = (z_2^1)^{\oplus n-r} \end{cases}$$

Lemme A.0.5. *Soient $A_1 = A_2 = (\mathbb{Z}/2\mathbb{Z})^r$, $N = (\mathbb{Z}/2\mathbb{Z})^k$, q_1, q_2 f.f. quadratiques non-dégénérées définies respectivement sur A_1 et A_2, q_N de rang 0 sur N tels que:*

$$q_1 \oplus q_N = q_2 \oplus q_N$$

Alors:

1 $\delta_{q_1} = \delta_{q_2}$;

2 *Si* $\epsilon_q = 0$ *alors* $q_1 = q_2$;

Démonstration. 1) On rappelle que $\delta_{q_1} = 0$ si et seulement si $q_1(x) \in \mathbb{Z}$ pour tout $x \in A_1$. Comme $q_N(x) \in \{0, 1\}$ pour tout $x \in N$ on a que $\delta_{q_1} = 0 \iff q(x) \in \mathbb{Z}$ pour tout $x \in A_1 \oplus N \iff \delta_{q_2} = 0$.

2) Si $\epsilon_q = 0$ alors l'invariant de Gauss vaut:

$$\begin{aligned} \gamma(q_N) &= \frac{1}{\sqrt{\#N}} \sum_{x \in N} e^{i\pi q_N(x)} \\ &= \frac{\#N}{\sqrt{\#N}} \\ &= = 2^{\frac{k}{2}} \end{aligned}$$

Donc si $q_1 \oplus q_N = q_2 \oplus q_N$ alors $\gamma(q_1)\gamma(q_N) = \gamma(q_2)\gamma(q_N)$ ce qui implique $\gamma(q_1) = \gamma(q_2)$ car $\gamma(q_N) \neq 0$ et donc $\text{sgn}(q_1) = \text{sgn}(q_2)$. Comme $\delta_{q_1} = \delta_{q_2}$ on a par le Lemme 3.2.23 $q_1 = q_2$. □

Cela justifie la définition suivante, qui étend les invariants déjà rencontrés au cas non-dégénéré:

Définition A.0.6. Soit q une f.f. quadratique sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$, $q = q_1 \oplus q_N$ avec q_1 non-dégénérée et q_N de rang 0. Alors on note:

1 $\delta_q := \delta_{q_1}$;

2 $\mathrm{sgn}(q) := \mathrm{sgn}(q_1)$ si $\epsilon_q = 0$.

Proposition A.0.7. *Soit q une f.f. quadratique sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$, alors q est uniquement déterminée par:*

1 $\mathrm{rang}(q)$, δ_q *et* $\mathrm{sgn}(q)$ *si* $\epsilon_q = 0$;

2 $\mathrm{rang}(q)$ *et* δ_q *si* $\epsilon_q = 1$.

Démonstration. 1) Soit $q = q_1 \oplus q_N$ avec q_1 non-dégénérée de rang $r = \mathrm{rang}(q)$ et q_N de rang 0. Alors q_N est totalement isotrope car $\epsilon_q = 0$ et par le Lemme 3.2.23q_1 est déterminée par δ_q et $\mathrm{sgn}(q_1) = \mathrm{sgn}(q)$.

2) Soient $A_1 = A_2 = (\mathbb{Z}/2\mathbb{Z})^r$, $N = (\mathbb{Z}/2\mathbb{Z})^{n-r}$, q_1, q_2 f.f. quadratiques non dégénérées définies respectivement sur A_1 et A_2, q_N de rang 0 sur N avec $\epsilon_{q_N} = 1$: on doit prouver que $q_1 \oplus q_N \simeq q_2 \oplus q_N$ si et seulement si $\delta_{q_1} = \delta_{q_2}$.

Si $\delta_{q_1} \neq \delta_{q_2}$ alors $\delta_{q_1 \oplus q_N} \neq \delta_{q_2 \oplus q_N}$ ce qui implique que les deux formes sont différentes.

Sinon soit b_i est la forme bilinéaire associée à q_i, alors $b_1 = b_2$. Il existe donc une base (x_i) de q_1 et (y_i) de q_2 tels que $b_1(x_i, x_j) = b_2(y_i, y_j)$ et $q_1(x_i) - q_2(y_i) \in \{0, 1\}$. Soit donc (z_i) une base de N telle que $q_N(z_i) = 1$, si on pose:

$$y_i' = \begin{cases} y_i & \text{si } q_1(x_i) = q_2(y_i) \\ y_i + z_1 & \text{si } q_1(x_i) \neq q_2(y_i) \end{cases}$$

alors les matrices de $q_1 \oplus q_N$ dans la base (x_i, z_i) et de $q_2 \oplus q_N$ dans la base (y_i', z_i) coïncident et donc les deux formes aussi. □

Lemme A.0.8. *Une f.f. quadratique q sur $A = (\mathbb{Z}/2\mathbb{Z})^n$ de rang r avec invariants δ_q,ϵ_q et* $\mathrm{sgn}(q)$ *existe si et seulement si les conditions suivantes sont vérifiées:*

1 $r \equiv 0 \pmod 2$ *si* $\delta_q = 0$;

2 $\mathrm{sgn}(q) \equiv 0 \pmod 4$ *si* $\epsilon_q = 0$ *et* $\delta_q = 0$;

3 $\mathrm{sgn}(q) \equiv r \pmod 2$ *si* $\epsilon_q = 0$ *et* $\delta_q = 1$;

4 $\mathrm{sgn}(q) \equiv \pm 1 \pmod 8$ *si* $\epsilon_q = 0$, $\delta_q = 1$ *et* $r = 1$;

5 $\mathrm{sgn}(q) \not\equiv 4 \pmod 8$ *si* $\epsilon_q = 0$, $\delta_q = 1$ *et* $r = 2$.

Démonstration. Si $\epsilon_q = 1$ on peut choisir $q = \left(w_{2,1}^1\right)^{\oplus r} \oplus \left(z_2^1\right)^{\oplus(n-r)}$ si $\delta = 1$ ou $q = u_1^{\oplus \frac{r}{2}} \oplus \left(z_2^1\right)^{\oplus(n-r)}$ si $\delta = 0$, donc la seule condition à respecter est la 1.

Si $\epsilon_q = 0$ on pose $q = q_1 \oplus \left(z_2^0\right)^{\oplus(n-r)}$ et on cherche q_1 non-dégénérée de rang r avec $\delta_{q_1} = \delta_q$ et $\mathrm{sgn}(q_1) = \mathrm{sgn}(q)$. Ensuite il s'agit juste de vérifier les différentes combinaisons possibles pour q_1 en utilisant la Proposition 2.3.70 et le Tableau 2.4.1 afin d'obtenir les conditions $2 - 5$. □

Lemme A.0.9. *Soit q_N une forme quadratique sur $N \simeq (\mathbb{Z}/2\mathbb{Z})^k$ de rang 0 avec $k > 0$ et q une forme quadratique sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$ non-dégénérée. Alors il existe un plongement $q_N \hookrightarrow q$ si et seulement si les conditions suivantes sont vérifiées:*

1 $k \leq n/2$;

2 $\mathrm{sgn}(q) = \pm 2$ *si* $k = 1$, $n = 2$, $\epsilon_{q_N} = 1$ *et* $\delta_q = 1$;

3 $\mathrm{sgn}(q) = 0$ *si* $2k = n$ *et* $\epsilon_{q_N} = 0$;

4 $\mathrm{sgn}(q) = \pm 1$ *si* $2k = n - 1$, $\epsilon_{q_N} = 0$ *et* $\delta_q = 1$;

5 $\mathrm{sgn}(q) \neq 4$ *si* $2k = n - 2$, $\epsilon_{q_N} = 0$ *et* $\delta_q = 1$;

Démonstration. 1) On suppose $q_N \hookrightarrow q$ avec $k > n/2$, alors par le Lemme 2.3.29 $\#N^\perp = \frac{n}{k} < \frac{2k}{k} = 2$ mais $N \subseteq N^\perp$ donc $n/2 < k \leq \#N^\perp < 2$ et on obtient une contradiction.

2) On montre que si $\epsilon_{q_N} = 1$, $k \leq n/2$ il existe un plongement $q_N \hookrightarrow q$ si et seulement si la condition 2 est respectée. En particulier il suffit de le prouver le cas $k = n/2$.

Si $\delta_q = 0$ on peut choisir une base $(x_1, \ldots, x_n)$ de A telle que la matrice de q soit:

$$q = \begin{pmatrix} 1 & \frac{1}{2} & & & & & \\ \frac{1}{2} & 0 & & & & & \\ & & \ddots & & & & \\ & & & 1 & \frac{1}{2} & & \\ & & & \frac{1}{2} & 0 & & \\ & & & & & 1 & \frac{1}{2} \\ & & & & & \frac{1}{2} & \alpha \end{pmatrix}$$

avec $\alpha = 0$ si $\mathrm{sgn}(q) \equiv 0 \pmod 8$ et $\alpha = 1$ si $\mathrm{sgn}(q) \equiv 4 \pmod 8$, donc la restriction de q sur $\mathrm{span}(x_1, x_3, \ldots, x_{n-1})$ correspond à q_N.

Si $\delta_q = 1$ et $n \geq 4$ on peut choisir une base $(x_1, \ldots, x_n)$ de A telle que la matrice de q soit:

$$q = \begin{pmatrix} 1 & \frac{1}{2} & & & & & & \\ \frac{1}{2} & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & \frac{1}{2} & & & \\ & & & \frac{1}{2} & 0 & & & \\ & & & & & 1 & \frac{1}{2} & \\ & & & & & \frac{1}{2} & \alpha & \\ & & & & & & & \frac{1}{2} \quad 0 \\ & & & & & & & 0 \quad \beta \end{pmatrix}$$

avec les valeurs de $\alpha \in \{0, 1\}$, $\beta \in \{\pm\frac{1}{2}\}$ qui dépendent de la signature de q et la restriction sur $\mathrm{span}(x_1, x_3, \ldots, x_{n-3}, x_{n-1} + x_n)$ correspond à q_N.

Pour conclure, si $\delta_q = 1$, $k = 1$ et $n \in \{2, 3\}$ une vérification directe de cas possibles nous permet de conclure.

3) On montre que si $\epsilon_{q_N} = 0$, $k = n/2$ il existe un plongement $q_N \hookrightarrow q$ si et seulement si la condition $\mathrm{sgn}(q) = 0$.

Condition nécessaire: soit $q_N \hookrightarrow q$ et $y_1, \ldots, y_k$ une base de $N \hookrightarrow A$. Comme q est non-dégénérée il existe $x_1 \in \mathrm{span}(y_2, \ldots, y_k)^{\perp} \backslash y_1^{\perp}$, donc $b(y_1, x_1) = \frac{1}{2}$, $b(y_i, x_1) = 0$ pour $2 \leq i \leq k$. Si on pose $A_1 = \mathrm{span}(y_1, x_1)$ alors:

$$q_{|A_1} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \alpha \end{pmatrix}$$

avec $\alpha \in \{0, 1, \pm\frac{1}{2}\}$. On vérifie facilement que pour n'importe quelle valeur de α, on obtient $\mathrm{sgn}(q_{|A_1}) = 0$. Soit $N_1 = \mathrm{span}(y_2, \ldots, y_k)$, comme $N_1 \perp A_1$ on a un plongement $N_1 \hookrightarrow A_1^{\perp}$. Il suffit donc de procéder par récurrence en choisissant $x_i \in \mathrm{span}(y_{i+1}, \ldots, y_k)^{\perp_{A_{i-1}^{\perp}}} \backslash y_i^{\perp}$, $A_i = \mathrm{span}(y_1, x_1, \ldots, y_i, x_i)$ et $N_i = \mathrm{span}(y_{i+1}, y_k)$ pour obtenir que $\mathrm{sgn}(A_k) = \mathrm{sgn}(A) = 0$.

Condition suffisante: si $\mathrm{sgn}(q) = 0$ on peut choisir une base $(x_1, \ldots, x_n)$ de A telle que la matrice de q soit:

$$q = \begin{pmatrix} 0 & \frac{1}{2} & & & \\ \frac{1}{2} & 0 & & & \\ & & \ddots & & \\ & & & 0 & \frac{1}{2} \\ & & & \frac{1}{2} & 0 \end{pmatrix} \text{ si } \delta_q = 0$$

$$q = \begin{pmatrix} 0 & \frac{1}{2} & & & \\ \frac{1}{2} & \frac{1}{2} & & & \\ & & \ddots & & \\ & & & 0 & \frac{1}{2} \\ & & & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \text{ si } \delta_q = 1$$

dans les deux cas on obtient que la restriction de q sur $\mathrm{span}(x_1, x_3, \ldots, x_{n-1})$ correspond à q_N.

4 et 5) Si $\epsilon_q = 0$ et $n > 2k$ il existe un plongement $q_N \hookrightarrow q$ si et seulement s'il existe q_1, q_2 f.f. quadratiques telles que $q = q_1 \oplus q_2$ avec q_1 définie sur $(\mathbb{Z}/2\mathbb{Z})^{2k}$ et $\mathrm{sgn}(q_1) = 0$. Cela est toujours vérifié si et seulement s'il existe q_2 définie sur $(\mathbb{Z}/2\mathbb{Z})^{n-2k}$ avec $\mathrm{sgn}(q_2) = \mathrm{sgn}(q)$ et en appliquant le Lemme A.0.8 on obtient le résultat cherché. □

Proposition A.0.10. *Soient q,q_H f.f. quadratiques non-dégénérées définies respectivement sur $A \simeq (\mathbb{Z}/2\mathbb{Z})^n$, $H \simeq (\mathbb{Z}/2\mathbb{Z})^c$ avec $c \leq n$, $\delta_{q_H} = 0$. On note $r := \mathrm{rang}(q_H)$ et $k := c - r$. Alors il existe un plongement $q_H \hookrightarrow q$ si et seulement si les conditions suivantes sont vérifiées:*

1 $q = q_H$ si $c = n$;

2 $r + 2k \leq n$;

3 $\mathrm{sgn}(q) = \pm 2$ si $r + 2k = n$, $k = 1$, $\epsilon_{q_H} = 1$ et $\delta_q = 1$;

4 $\mathrm{sgn}(q) = \mathrm{sgn}(q_H)$ si $r + 2k = n$, $k \geq 1$ et $\epsilon_{q_H} = 0$;

5 $\mathrm{sgn}(q) = \mathrm{sgn}(q_H) \pm 1$ si $r + 2k = n - 1$, $\epsilon_{q_H} = 0$ et $\delta_q = 1$;

6 $\mathrm{sgn}(q) \neq \mathrm{sgn}(q_H) + 4$ si $r + 2k = n - 2$, $\epsilon_{q_H} = 0$ et $\delta_q = 1$.

Démonstration. Soit $q_H = q_N \oplus q_1$ avec q_1 de rang r, alors $q_H \hookrightarrow q$ si et seulement si $q_1 \hookrightarrow q$ et $q_N \hookrightarrow q_1^{\perp}$, une condition nécessaire est donc $r \leq n$ et $2k \leq n - r$ ce qui revient au critère 2.

On considère le cas $\epsilon_{q_H} = 0$, donc $\mathrm{sgn}(q_1) = \mathrm{sgn}(q_H)$. Si $r = n$ alors $c = n$ donc le plongement est réalisable uniquement si $q_H = q$ (critère 1). Sinon il existe un plongement $q_1 \hookrightarrow q$ si et seulement s'il existe q_2 non-dégénérée de rang $n - r \geq 1$ avec $\mathrm{sgn}(q_2) = \mathrm{sgn}(q) - \mathrm{sgn}(q_H)$ et $\delta_{q_2} = \delta_{q_H}$ (par le Lemme 2.5.21).

On remarque que $\delta_{q_H} = 0 \implies \mathrm{sgn}(q_H) \equiv 0 \pmod 4$, $r \equiv 0 \pmod 2$. En particulier, par le Lemme A.0.8 on a $n \equiv \mathrm{sgn}(q_1) \pmod 2$ et donc $n - r \equiv \mathrm{sgn}(q) \pmod 2$.

On regarde donc dans quel cas l'existence de q_2 avec les invariants donnés est assurée par le Lemme A.0.8:

- Si $\delta_q = 0$ les possibilités sont uniquement $\mathrm{sgn}(q_2) = 0$ et $\mathrm{sgn}(q_2) = 4$ avec $n - r \equiv 0 \pmod 2$ donc l'existence est toujours assurée. Ensuite il existe toujours un plongement $q_N \hookrightarrow q_2$ sauf si $2k = n - r$ et $\mathrm{sgn}(q_2) \neq 0$.
- Si $\delta_q = 1$ alors q_2 existe dans les cas suivants:

  1 $n \geq r + 3$;

  2 $n = r + 2$ et $\mathrm{sgn}(q) - \mathrm{sgn}(q_H) \not\equiv 4 \pmod 8$;

  3 $n = r + 1$ et $\mathrm{sgn}(q) - \mathrm{sgn}(q_H) \equiv \pm 1 \pmod 8$;

  Ensuite on rappelle que par le Lemme A.0.9 il existe un plongement $q_N \hookrightarrow q_2$ si et seulement si:

  i $\mathrm{sgn}(q) - \mathrm{sgn}(q_H) = 0$ si $2k = n - r$;

  ii $\mathrm{sgn}(q) - \mathrm{sgn}(q_H) = \pm 1$ si $2k = n - r - 1$;

  iii $\mathrm{sgn}(q) - \mathrm{sgn}(q_H) \neq 4$ si $2k = n - r - 2$;

  On montre que $i) - iii) \implies 1) - 3)$.
  Si $k \geq 2$ alors par le critère 2 on a $n - r \geq 4$ donc 1) est vérifié.
  Si $k = 1$ alors $n - r \geq 2$, donc:
  — soit $n - r \geq 3$ et 1) est vérifié ;
  — soit $n - r = 2$ donc $i)$ est vérifié, mais $i) \implies 2)$.
  Si $k = 0$ alors on a aucun plongement $q_N \hookrightarrow q_2$, on doit donc prouver que dans ce cas on a $i) - iii) \iff 1) - 3)$. Le cas (i) ne se vérifie pas car $n - r \geq 1$, donc:
  — soit $n - r \geq 3$ et 1) est vérifié ;
  — soit $n - r = 2$ donc $iii)$ est vérifié, mais $iii) \iff 2)$;
  — soit $n - r = 1$ donc $ii)$ est vérifié, mais $ii) \iff 3)$.

Les conditions $i)-iii)$ correspondent aux critères $4-6$, donc cela termine la preuve dans le cas $\epsilon_{q_N} = 0$.

On considère le cas $\epsilon_{q_H} = 1$ (en particulier on a $k \geq 1$) et on pose $\mathrm{sgn}(q_1) = 0$ (comme $\epsilon_{q_H} = 1$ la signature de q_1 dépende de la décomposition choisie et si $\delta_{q_H} = 0$ on peut prendre $q_1 = u_1^{\oplus \frac{r}{2}}$). Si le critère 2 est réalisé on a $r < n$ et $2 \leq n - r$ donc:

- Si $\delta_q = 0$ on a toujours un plongement $q_1 \hookrightarrow q$. Comme $\delta_{q_1^\perp} = 0$ par le Lemme A.0.9 il existe aussi un plongement de $q_N \hookrightarrow q_1^\perp$, donc le plongement $q_H \hookrightarrow q$ est toujours réalisable.
- Si $\delta_q = 1$, dans la première partie de la preuve on a vu qu'il existe un plongement $q_1 \hookrightarrow q$ uniquement dans les cas suivants:

  1 $n \geq r + 3$;

  2 $n = r + 2$ et $\mathrm{sgn}(q) \neq 4$;

  3 $n = r + 1$ et $\mathrm{sgn}(q) = \pm 1$

  On rappelle que $2 \leq n - r$ donc le cas 3) n'est pas réalisable.
  Dans le cas 1) la condition $2k \leq n-r$ implique que soit $k = 1$,$n-r \geq 3$, soit $k \geq 2$ et $n - r \geq 2k$, dans les deux cas par le Lemme A.0.9 il existe toujours un plongement $q_N \hookrightarrow q_1^\perp$.
  Dans le cas 2) on a $k = 1$ et le plongement $q_N \hookrightarrow q_1^\perp$ existe si et seulement si $\mathrm{sgn}(q_1^\perp) = \pm 2$. Comme $\mathrm{sgn}(q) = \mathrm{sgn}(q_1) + \mathrm{sgn}(q_1^\perp)$ cela est équivalent à demander que $\mathrm{sgn}(q) = \mathrm{sgn}(q_1^\perp) = \pm 2$, ce qui revient au critère 3.

□

Annexe B

Calcul de l'invariant k

Il y a une question, un peu long et technique, qui n'a pas été traitée dans la Section 3.3 car nous avons décidé de la traiter plus calmement dans cette appendice : soit A la matrice associée à l'action de ι sur le réseau $NS(X)$ avec matrice d'intersection M, comment déterminer dans la pratique les invariants a_1 et k ?

Rappelons que dans la Section 3.2.2 nous avons défini $L_1 := T_{\iota^*} \cap T_{\eta^*} = T_{\iota^*} \cap NS(X)$, $L_2 \simeq E_8(-2)$ et $A_{L_1} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{a_1}$, il s'ensuit donc que:

$$L_1 = \ker(A - \mathrm{Id}) \cap NS(X)$$

Si l'action de A est définie sur une base de $NS(X)$ cela correspond à déterminer les points à coordonnées entières de $\ker(A - \mathrm{Id})$, c'est-à-dire les solutions entières du système:

$$(A - \mathrm{Id}) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{B.0.1}$$

où $r = \mathrm{rang}(NS(X))$. Pour effectuer ce calcul on utilise la décomposition en forme normale de Smith:

$$A - \mathrm{Id} = USV$$

avec U, V matrices inversibles sur $\mathbb{Z}$ et $S = (s_{ij})$ matrice diagonale.

Il suffit donc de résoudre le système:

$$S \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Comme S est une matrice diagonale, cela peut être fait simplement en prenant les éléments de la base qui correspondent à un zéro sur la diagonale de S et ensuite on applique V^{-1} pour obtenir les solutions de (B.0.1).

On obtient ainsi une base $(e_1, \ldots, e_{r-8})$ de L_1. De la même façon on peut calculer une base $(f_1, \ldots, f_8)$ de L_2 en répétant la procédure sur la matrice $A + \mathrm{Id}$.

Pour la matrice d'intersection de L_1 on a:

$$M_1 := B_1^t M B_1$$

où B_1 est la matrice de la base de L_1. Comme la signature de L_1 est $(1, r-9)$ pour a_1 on obtient:

$$\det(M_1) = (-1)^{r-9} 2^{a_1}$$

Le calcul de k demande quelques passages de plus. On utilisera la formulation donnée dans la Proposition 3.2.8, que nous rappelons ici. Si on note $\pi_{A_{L_1}} : A_{L_1} \oplus A_{L_2} \to A_{L_1}$ la projection sur le premier facteur, alors:

$$\begin{aligned} H_{NS(X)} &= \frac{NS(X)}{L_1 \oplus L_2} \\ H_{NS(X),1} &= \pi_1(H_{NS(X)}) \\ k &= \dim_{\mathbb{F}_2}(H_{NS(X),1}) - \mathrm{rang}(q_{H_{NS(X),1}}) \end{aligned}$$

où $\mathrm{rang}(q_{H_{NS(X),1}})$ indique le rang de la f.f. quadratique obtenue par restriction. On rappelle que:

$$\begin{aligned} \dim_{\mathbb{F}_2}(H_{NS(X),1}) &= \dim_{\mathbb{F}_2}(H_{NS(X)}) \\ &= \frac{a_1 + a_2 - a_{NS(X)}}{2} \end{aligned}$$

où $a_2 = 8$ dans notre cas. Il reste à déterminer $\mathrm{rang}(H_{NS(X),1})$.

On procède ainsi:

- Soient $B_1 = (e_1, \ldots, e_{r-8})$ et $B_2 = (f_1, \ldots, f_8)$ les matrices de la base respectivement de L_1 et L_2. On pose $B_{NS(X)} := (B_1 \mid B_2) = (e_1, \ldots, e_{r-8}, f_1, \ldots, f_8)$ la matrice obtenue par l'union des deux et $B_{NS(X)}^{-1}$ la matrice inversée calculée sur $\mathbb{Q}$;
- $B_{NS(X)}^{-1}$ est donc une base de $NS(X)$ dans les coordonnées $(e_1, \ldots, f_8)$, il suffit donc d'extraire les premières $r-8$ lignes pour obtenir une base de la projection de $NS(X)$ sur L_1^*. On appelle la matrice obtenue $B_{NS(X),1}$;
- La forme quadratique est donnée par la matrice:

$$M_{NS(X),1} := B_{NS(X),1}^t M \, B_{NS(X),1}$$

- Il reste à quotienter par L_1 pour obtenir la f.f. quadratique de $H_{NS(X),1}$. Comme on est s'intéresse uniquement au rang de la f.f. quadratique, on peut procéder autrement. Étant donné que L_1 est un réseau 2-élémentaires alors $2 \cdot M_{NS(X),1}$ est une matrice à coefficients entiers. La projection sur $\mathbb{F}_2$ est une matrice du même rang que $q_{H_{NS(X),1}}$. Donc:

$$\mathrm{rang}(q_{H_{NS(X),1}}) = \mathrm{rang}\left(\left(2M_{NS(X),1}\right) \otimes \mathbb{F}_2\right)$$

On reporte enfin l'Algorithme B.1 (codé en SAGE) utilisé pour les calculs dans l'exemple de la sous-section 3.3.3.1 avec invariants $r = 18$, $\delta = 1$, $a_{NS(X)} = 4$, $a_1 = 8$, $k = 2$. La méthode implémentée est celle que nous venons de décrire, avec deux précisions nécessaires:

- La résolution des systèmes linéaires sur $\mathbb{Z}$ peut être effectuée automatiquement en SAGE par exemple grâce à la commande `kernel` contenu dans la librairie `sage.matrix.matrix2`. Cette commande utilise à son tour la décomposition en forme normale de Smith.
- On a traité ici les vecteurs comme des matrices colonnes, mais malheureusement le standard en SAGE considère les vecteurs comme des lignes. Cela entraîne une fastidieuse dissymétrie en obligeant à inverser le sens dans tous les calculs.

Algorithme B.1 Algorithme en SAGE pour la détermination des invariants numériques dans l'exemple de la sous-section 3.3.3.1

```
def get_invariants(A,M):
    #Return the numerical invariants associated to an involution of NS(X)
    r_NS = M.nrows()
    a_NS = log_b(abs(det(M)), 2)
    I = identity_matrix(r_NS)
    B1 = (A - I).kernel().matrix()
    M1 = B1 * M * B1.transpose()
    a1 = log_b(abs(det(M1)), 2)
    B2 = (A + I).kernel().matrix()
    M2 = B2 * M * B2.transpose()
    B12 = B1.stack(B2)
    B_NS = B12.inverse()
    B_NS1 = B_NS[range(r_NS), range(r_NS - 8)]
    M_NS1 = B_NS1 * M1 * B_NS1.transpose()
    r1 = rank(matrix(Integers(2), 2 * M_NS1))
    dim = (8 + a1 - a_NS) / 2
    k = dim - r1
    return([a1, k])
#Construct the sublattice of NS(X) generated by fibers and zero section
U = Matrix([[0, -1], [-1, 2]])
M = - block_diagonal_matrix([U, CartanMatrix(['D', 6]), CartanMatrix(['D', 4]),
    CartanMatrix(['D', 4]), CartanMatrix(['A', 1]), CartanMatrix(['A', 1])])
r_NS = M.nrows()
#Define the overlattice NS(X) adding 2-torsion sections
P = Matrix([[ 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1 ]])
Q = Matrix([[ 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0 ]])
M[[16], range(r_NS)] = P
M[range(r_NS), [16]] = P.transpose()
M[[16], [16]] = -2
M[[17], range(r_NS)] = Q
M[range(r_NS), [17]] = Q.transpose()
M[[17], [17]] = -2
M[[16], [17]] = 0
M[[17], [16]] = 0
#Calculate invariants of NS(X)
a_NS = log_b(abs(det(M)), 2)
delta = 1 - int(matrix(Integers(2), M.inverse() * 2).diagonal() == 0)
#Define involution matrix
R = Matrix([[ 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0 ]])
R_dec = R * M.inverse()
t_P = Matrix([
      #General fiber and zero section
      [ 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(F) = F
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0 ], #t_P(O) = P
      #Fiber I2*
      [ 1, 0,-1,-2,-2,-2,-1,-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta1) = theta0
      [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta2) = theta2
      [ 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta3) = theta3
      [ 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta4) = theta4
      [ 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta5) = theta6
      [ 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta6) = theta5
      #Fiber I0*
      [ 1, 0, 0, 0, 0, 0, 0, 0,-1,-2,-1,-1, 0, 0, 0, 0, 0, 0 ], #t_P(theta1) = theta0
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta2) = theta2
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta3) = theta4
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0 ], #t_P(theta4) = theta3
      #Fiber I0*
      [ 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,-1,-2,-1,-1, 0, 0 ], #t_P(theta1) = theta0
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0 ], #t_P(theta2) = theta2
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0 ], #t_P(theta3) = theta4
      [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0 ], #t_P(theta4) = theta3
      #2-torsion sections
      [ 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ], #t_P(P) = O
      R_dec[0]                                                   #t_P(Q) = R
      ])
#Calculate invariants of involution
[ a1, k ] = get_invariants(t_P, M)
fix = 16 - a1 - a_NS + 2 * k
print("r_NS = %d, delta = %d, a_NS = %d, a_1 = %d, k = %d" %(r_NS, delta, a_NS, a1, k))
print("Fixed points : %d" %fix)
```

Bibliographie

[AP] C. Allday, V. Puppe: « *Cohomological methods in transformation groups* », Cambridge University Press (1993).

[AM] M. Atiyah, I. Macdonald: « *Introduction to Commutative Algebra* » Addison-Wesley Pub. Comp. (1969).

[AS] M. Artebani, A. Sarti, S. Taki: «*K3 surfaces with non-symplectic automorphisms of prime order*», Mathematische Zeitschrift **268** (2011), 507-533 .

[Av] L. Avramov, *« Modules of finite virtual projective dimension »*. Invent. Math. **96** (1989), n.1, 71–101.

[BHPV] W. Barth, K. Hulek, C.A.M. Peters, A. Van de Ven: *« Complex Compact Surfaces»*, Second edition.Springer-Verlag (2004).

[Beau] A. Beauville: « *Variétés kähleriennes dont la première classe de Chern est nulle* », J. Differential geometry **18** (1983), 755-782.

[Beau2] A. Beauville: « *Surfaces K3* », Séminaire Bourbaki volume 1982/83, exposés 597-614, Astérisque, n.105-106 , Exposé n.609 (1983), 217-229 .

[Ben] D. Benson, « *Representations and cohomology, I: Basic representation theory of finite groups and associative algebras* », Cambridge Studies in Advanced Mathematics **30**, Cambridge University Press (1991).

[BK] J. Bochnak, W. Kucharz: *« On successive minima of indefinite quadratic forms* » Enseign.Math. (2) **51** (2005), n.3-4, 319–330.

[BNS] S. Boissière, M. Nieper-Wisskirchen, A. Sarti: « *Smith theory and irreducible holomorphic symplectic manifolds* », J. Topo. **6(2)** (2013), 361-390.

[BCS] S. Boissière, C. Camere and A. Sarti: «*Classification of automorphisms on a deformation family of hyperkähler fourfolds by p-elementary lattices*», Kyoto J. Math. **56** (2016), n.3, 465-499.

[Br] K. S. Brown: « *Cohomology of groups* », Springer-Verlag (1982).

[BH] W. Bruns, J. Herzog: *« Cohen-Macaulay rings* », Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press (1993).

[BR] D. Burns, M. Rapoport: «*On the Torelli problem for kählerian K3 surfaces*». Ann.Sci. École Norm. Sup. (4) **8** (1975), n.2, 235–273.

[CTVZ] J. Carlson, L. Townsley, L. Valero-Elizondo, M. Zhang: *« Cohomology rings of finite groups »*, Kluwer Academic Publishers (2003).

[CFS] J. Carlson, E. Friedlander, A. Suslin: *« Modules for $\mathbb{Z}/p \times \mathbb{Z}/p$ »,* Comment. Math. Helv. **86** (2011), n.3, 609–657.

[CB] S. Chebolu, J. Mináe: *« Representations of the miraculous Klein group.* » Math. Newsl. **21/22** (2012), n.4-1, 135–145.

[CG] P. Comparin, A. Garbagnati: « *Van Geemen-Sarti involutions and elliptic fibrations on K3 surfaces double cover of P2* » J. Math. Soc. Japan.**66** (2014), n.4-1, 479–522.

[Con] J. Conway: «*The sensual (quadratic) form*», The Mathematical Association of America (1997).

[Cop] W. Coppel: « *Number theory. An introduction to mathematics* » Second edition, Springer (2009).

[CS] J. Conway, N. Sloane: *« Sphere packings, lattices and groups. Third edition.With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov* ». Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **290**, Springer-Verlag (1999).

[Cr] A. Croll: « *Periodic modules over Gorenstein local rings* ». J. Algebra **395** (2013), 47–62.

[CR] C. Curtis, I. Reiner « *Representation theory of finite groups and associative algebras* ». Wiley (1962).

[Da] H. Davenport: *« Multiplicative number theory* ». Third edition.Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics **74**, Springer-Verlag, (2000).

[De] P. Deligne: « *La conjecture de Weil pour les surfaces K3* », Invent. Math., **15** (1972) 206–226

[Dol] I. Dolgachev: «*Integral quadratic forms : applications to algebraic geometry*», Séminaire n.Bourbaki, exp. **611** (1982-83), 251-278.

[Dod] C. Dodgson: « *Condensation of Determinants, Being a New and Brief Method for Computing their Arithmetical Values* », Proceedings of the Royal Society of London, **15** (1867), 150-155.

[Ei] D. Eisenbud: « *Commutative algebra. With a view toward algebraic geometry* », Graduate Texts in Mathematics, **150**. Springer-Verlag, (1995).

[GaSal] A. Garbagnati, C. Salgado: « *Elliptic fibrations on K3 surfaces with a non-symplectic involution fixing rational curves and a curve of positive genus »,* arXiv:1806.03097v1

[GaSar] A. Garbagnati, A. Sarti: « *On symplectic and non-symplectic automorphisms of K3 surfaces »,* Rev. Mat. Iberoam. **29** (2013), n.1, 135–162.

[GeSar] B. van Geemen, A. Sarti: « *Nikulin involutions on K3 surfaces* », Math. Z. **255** (2007), 731–753.

[Gr] R. Griess: « *Positive definite lattices of rank at most 8* », J. Number Theory **103** (2003), n.1 77–84.

[GH] P. Griffiths, J. Harris: « *Principles of algebraic geometry* », Bull. Amer. Math. Soc. (N.S.) **2** (1980), n.1, 197-200

[Iy] S. Iyengar: « *Modules and Cohomology over group algebras: one commutative algebraist's perspective* », Trends in Comm. Alg. **51** (2004), 51-85.

[Kh] V. Kharlamov: *« The topological type of nonsingular surfaces in* $\mathbb{P}^3\mathbb{R}$ *of degree four* », Funct. Anal. Appl. **10** (1976), n.4, 295-304.

[Ko] S. Kondo: *« Automorphisms of algebraic K3 surfaces which act trivially on Picard groups »*, J. Math. Soc. Japan. **44** (1992), n.1, 75–98.

[Ko2] S. Kondo: *« Niemeier lattices, Mathieu groups, and finite groups of symplectic automorphisms of K3 surfaces With an appendix by Shigeru Mukai* », Duke Math. J. **92** (1998), n.3, 593–603

[La] T. Y. Lam, « *Lectures on modules and rings* », Graduate Texts in Mathematics, **189**. Springer-Verlag (1999)

[Le] L. Levy, « *Mixed modules over* $\mathbb{Z}G$*, G cyclic of prime order, and over related Dedekind pullbacks* » J. Algebra **71** (1981), n.1, 62–114.

[Mi] J. Milnor: *« Introduction to algebraic K-theory* » Annals of Mathematics Studies, **72**. Princeton University Press (1971).

[MM] R. Miranda, D.R. Morrison: «*Embeddings of Integral Quadratic Forms*», (2009). Disponible sur `web.math.ucsb.edu/~drm/manuscripts/eiqf.pdf`.

[Mir] R. Miranda: *« The basic theory of elliptic surfaces* », Università di Pisa, Dottorato di ricerca in matematica, ETS Editrice Pisa, (1989). Disponible sur `http://www.math.colostate.edu/~miranda/`.

[Mon] G. Mongardi: «*Automorphisms of Hyperkähler manifolds*», Thèse de Doctorat en mathématiques, sous la direction de K. O'Grady, Università degli Studi di RomaTRE (2013).

[Mor] L. Mordell: « *The definite quadratic forms in eight variables with determinant unity* », J. Math. Pures Appl. **17** (1938), 41–46.

[Mo] D. Morrison: «*On K3 surfaces with large Picard number*», Invent. Math. **75** (1984), 105-122.

[Mu] S. Mukai: *« Finite groups of automorphisms of K3 surfaces and the Mathieu group »*, Invent. Math. **94** (1988), 183-221.

[Na] Y. Namikawa: « *Periods of Enriques surfaces* », Math. Ann. **270** (1985), no. 2, 201–222

[Nik] V. Nikulin: « *Integral symmetric bilinear forms and some of their applications »,* Math. USSSR Izv. **14** (1980), 103-167 .

[Nik2] V. Nikulin: «*Finite groups of automorphisms of Kählerian K3 surfaces*», Trudy Moskov. Mat. Obshch. **38** (1979), 75–137.

[Nik3] V. Nikulin: «*Factor groups of groups of the automorphisms of hyperbolic forms with respect to subgroups generated by 2-reflections* », Soviet Math. Dokl. **20** (1979), 1156–1158.

[Nis] K. Nishiyama *« The Jacobian fibrations on some K3 surfaces and their Mordell-Weil groups* », Japan. J. Math. (N.S.) **22** (1996), n.2, 293–347

[OZ] K. Oguiso, D. Zhang: *« K3 surfaces with order 11 automorphisms* », Pure Appl. Math. Q. **7** (2011), n.4, 1657–1673.

[SS] M. Schütt, T. Shioda: « *Elliptic surfaces* », Algebraic geometry in East Asia–Seoul 2008, Adv. Stud. Pure Math. **60**, Math. Soc. Japan (2010), 51–160.

[Tak] S. Taki: « *Classification of non-symplectic automorphisms of order 3 on K3 surfaces* » Math. Nachr. **284** (2011), n.1, 124–135.

[Tar] K. Tari: «*Automorphismes des variétés de Kummer généralisées*», Thèse de Doctorat en mathématiques, sous la direction de S. Boissière, Université de Poitiers (2015).

[Wa] G. Watson: *« The class-number of a positive quadratic form,* » Proc. London Math. Soc. (3) **13** (1963), 549–576.

[Wi] A. Wiseman: « *Projective modules over pullback rings* », Math. Proc. Cambridge Philos. Soc. (97) **3** (1985), 399–406.

[Xi] G. Xiao: « *Galois covers between K3 surfaces »,* Annales de l'institut Fourier **46** (1996), n.1, 73-88.