Exposé de première année FIMFA

# Rationalité et intégralité des représentations de groupes finis

Jérémie Clerc Abel Lacabanne
Sous la direction d'Olivier Benoist

30 novembre 2012

# Introduction

Soit $G$ un groupe fini et $(V, \rho)$ une représentation linéaire de $G$ sur le corps des complexes. Se donner la représentation revient à se donner une matrice de $\mathcal{M}_n(\mathbb{C})$ pour chaque élément de $G$, de manière compatible avec la loi de $G$. Dans le cas d'un groupe abélien fini, on remarque que ces matrices sont codiagonalisables. Ainsi, à un changement de base près, on obtient des matrices diagonales à coefficients dans une extension finie de $\mathbb{Q}$.

On essaie alors d'écrire, en toute généralité, ces matrices avec des coefficients dans une extension finie de $\mathbb{Q}$, aussi appelée corps de nombres. Il est aisé de le faire pour une représentation donnée de $G$ car il suffit de considérer l'extension engendrée par les coefficients de toutes les matrices définissant la représentation. On dira alors qu'une représentation est réalisable ou rationnelle sur un corps $K$ si les matrices définissant la représentation sont à coefficients dans $K$.

Ensuite, on peut essayer d'espérer plus sur les coefficients des matrices. Si l'on dispose d'un corps $K$ sur laquelle la représentation est réalisable, on se demande si l'on pourrait écrire les matrices avec des coefficients dans $\mathcal{O}_K$, l'anneau des entiers algébriques de $K$. On dira alors que la représentation est intégrale sur le corps $K$.

En fait, pour la question de rationalité, on arrive à trouver un corps dépendant du groupe $G$ sur lequel toute représentation est réalisable. On montrera le théorème suivant :

**Théorème 0.1.** *Soit $G$ un groupe fini d'exposant $m$ et $\zeta$ une racine primitive $m$-ième de l'unité. Alors toute représentation de $G$ est réalisable sur $\mathbb{Q}[\zeta]$.*

L'étude de l'exemple du groupe quaternionique et de sa représentation irréductible d'ordre 2 permet de voir que cette question de rationalité est assez compliquée. En effet, il n'existe pas de plus petit sous-corps de $\mathbb{C}$ sur lequel la représentation est réalisable. On montrera le théorème suivant sur cette représentation et les corps quadratiques :

**Théorème 0.2.** *La représentation irréductible de dimension 2 du groupe quaternionique est réalisable sur $\mathbb{Q}[\sqrt{d}]$ si et seulement si $d$ est un entier négatif sans facteurs carrés et non congru à 7 modulo 8.*

Enfin, on continuera l'étude de cet exemple pour discuter de la question d'intégralité. On se rendra compte que cette question est nettement plus compliquée, mettant en jeu les propriétés arithmétiques des corps et de leurs entiers algébriques. Il est donc faux de croire naïvement qu'on arrive, quitte à changer de base pour exprimer les matrices de la représentation, à passer de coefficients dans $K$ à des coefficients dans $\mathcal{O}_K$. On démontrera le résultat suivant :

**Théorème 0.3.** *La représentation irréductible de dimension 2 du groupe quaternionique n'est pas intégrale sur $\mathbb{Q}[i\sqrt{35}]$.*

Ces problèmes de rationalité et d'intégralité sont encore étudiés de nos jours. Le théorème 0.1 est dû à Brauer, qui l'a démontré en 1945 dans [Bra45]. L'exemple des quaternions et le résultat 0.2 est historique, étudié par Schur. Enfin, le théorème 0.3 apparaît

dans [CRW92] et est étudié en détail pour les autres corps quadratiques par Serre dans [Ser06].

Il reste encore une conjecture à propos des questions d'intégralité. Le théorème 0.1 assure la rationalité des représentations d'un groupe fini sur certains corps cyclotomiques. L'intégralité de ces représentations sur ces corps est encore une question ouverte. La réponse est affirmative quand le groupe est résoluble, comme cela est montré dans [CRW92].

Les deux premières parties de cet exposé sont consacrées à des résultats préliminaires, nécessaires pour montrer le théorème 0.1. La troisième partie s'attelle à sa démonstration, en suivant la seconde partie de [Ser98], l'exemple des quaternions sur les corps quadratiques y est également traité. Dans la cinquième partie, on montre le théorème 0.3. La quatrième partie est quant à elle consacrée à une étude des anneaux de Dedekind et aux modules de type finis sur ces anneaux, nécessaire à la preuve du théorème 0.3.

***Remerciements :***
Nous tenons à remercier chaleureusement Olivier Benoist pour nous avoir proposé ce sujet d'étude, pour sa disponibilité, pour son aide précieuse et pour l'enthousiasme qu'il a su partager.

# Table des matières

# 1 Groupes $p$-élémentaires

Cette partie présentant les principales définitions et propriétés des groupes $p$-élémentaires est préliminaire à la démonstration du théorème de Brauer.

## 1.1 Définition

**Définition 1.1.** *Soient $G$ un groupe fini, $p$ un nombre premier et $x \in G$. On dit que $x$ est un $p$-élément si son ordre est une puissance de $p$, et que c'est un $p'$-élément si son ordre est premier avec $p$.*

**Proposition 1.2.** *Tout $x \in G$ peut être décomposé sous la forme $x = x_u \cdot x_r$, où $x_u$ est un $p$-élément, $x_r$ est un $p'$-élément, et $x_u \cdot x_r = x_r \cdot x_u$.*

*Démonstration.* On s'intéresse au sous-groupe cyclique engendré par $x$, c'est-à-dire $\mathbb{Z}/k\mathbb{Z}$, où $k$ est l'ordre de $x$. Déterminer les composantes $p$-élémentaire et $p'$-élémentaire de $x$ revient à décomposer ce sous-groupe cyclique en produit direct, sous la forme $\mathbb{Z}/k\mathbb{Z} = \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, où $k = p^\alpha m$, avec $p$ et $m$ premiers entre eux. Les deux composantes seront alors des puissances de $x$, que l'on peut déterminer par une relation de Bézout.

Comme $p^\alpha$ et $m$ sont premiers entre eux, il existe $a$ et $b$ entiers tels que $ap^\alpha + bm = 1$. Alors $x^{ap^\alpha}x^{bm} = x$. On a $(x^{bm})^{p^\alpha} = 1$, donc $x_u = x^{bm}$ est un $p$-élément car son ordre divise $p^\alpha$, puis $(x^{ap^\alpha})^m = 1$. L'ordre de $x_r = x^{ap^\alpha}$ divise $m$, donc est premier à $p$. L'élément $x_r$ est donc $p'$-élémentaire. □

**Définition 1.3.** *Un groupe $H$ est dit $p$-élémentaire s'il est produit direct d'un groupe cyclique $C$ d'ordre premier à $p$, et d'un $p$-groupe $P$.*

**Proposition 1.4.** *Si $H$ est un groupe $p$-élémentaire, alors la décomposition $H = C \times P$, où $C$ est un groupe cyclique d'ordre premier à $p$ et $P$ un $p$-groupe, est unique.*

*Démonstration.* Si $x \in C$, alors $x$ est un $p'$-élément de $H$, car son ordre divise celui de $C$, donc est premier avec $p$. Si $x = (x_C, x_P) \in H$ est un $p'$-élément, il existe $m$ premier avec $p$ tel que $x^m = (1, 1)$. Dans ce cas, $x_P^m = 1$, ce qui n'est possible que si $x_P = 1$, c'est-à-dire si $x \in C$. $C$ est donc exactement l'ensemble des $p'$-éléments de $H$, et cet ensemble est bien défini de manière unique.

De la même manière, on peut démontrer que $P$ est exactement l'ensemble des $p$-éléments de $H$. □

À un $p'$-élément de $G$, on souhaite associer un groupe $p$-élémentaire qui soit le plus gros possible et qui soit essentiellement unique. Pour cela, on s'aide des théorèmes de Sylow.

**Définition 1.5.** *Soit $x$ un $p'$-élément d'un groupe fini $G$. Soient $C$ le sous-groupe cyclique engendré par $x$, $Z(x)$ le centralisateur de $x$ et $P$ un $p$-Sylow de $Z(x)$.*

*Le groupe $H = C \times P$ est un sous-groupe $p$-élémentaire de $G$ qui est dit associé à $x$. D'après les thèorèmes de Sylow, ce groupe est unique à conjugaison près dans $Z(x)$.*

## 1.2 Groupes hyper-résolubles

On va maintenant détailler quelques caractéristiques des groupes $p$-élémentaires, qui seront utilisées pour démontrer le théorème de Brauer. On étudie alors une classe plus générale de groupes, dits hyper-résolubles, dont les groupes $p$-élémentaires ne sont qu'un cas particulier.

**Définition 1.6.** *Un groupe fini $G$ est dit hyper-résoluble s'il existe une suite finie*

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

*de sous-groupes de $G$, telle que pour tout $i \in \{0 \ldots n\}$, $G_i$ est distingué dans $G$, et pour tout $i \in \{1 \ldots n\}$, $G_i/G_{i-1}$ est cyclique.*

On va maintenant voir des cas particuliers de groupes hyper-résolubles : les $p$-groupes et les groupes $p$-élémentaires.

**Théorème 1.7.** *Soit $p$ un nombre premier. Un $p$-groupe est hyper-résoluble.*

Commençons par un lemme facile sur le centre d'un $p$-groupe.

**Lemme 1.8.** *Soit $G$ un $p$-groupe. Alors le centre de $G$ n'est pas réduit à l'élément neutre.*

*Démonstration.* En effet, si $G$ agit sur un ensemble $X$, et si $X^G$ désigne l'ensemble des éléments de $X$ fixes par $G$, alors $X \backslash X^G$ est réunion disjointe d'orbites non triviales de $G$, et chacune de ces orbites a pour cardinal une puissance non nulle de $p$. Donc $\mathrm{card}(X \backslash X^G) \equiv 0\ [p]$. En appliquant ce résultat à l'action de $G$ sur lui-même par conjugaison, on obtient $X^G = Z(G)$. On en déduit

$$\mathrm{card}(Z(G)) \equiv \mathrm{card}(G) \equiv 0\ [p]$$

donc $Z(G) \neq \{1\}$. □

*Démonstration de 1.7.* Démontrons par récurrence que tout $p$-groupe est hyper-résoluble. Si $\mathrm{card}(G) = p$, alors $G$ est cyclique, donc hyper-résoluble.

Soit $n \in \mathbb{N}$. Supposons que pour tout $m < n$, tout groupe d'ordre $p^m$ soit hyper-résoluble. Soit $G$ un groupe d'ordre $p^n$. Alors $Z(G) \neq \{1\}$ par 1.8 donc $Z(G)$ et $G/Z(G)$ sont deux $p$-groupes d'ordre des puissances de $p$ inférieures strictement à $n$, si $G$ est non commutatif, et on pose $Z = Z(G)$. Si $G$ est commutatif, on choisit un élément $x$ d'ordre $p$ de $G$ (existe par le lemme de Cauchy) et on pose $Z = \langle x \rangle$. G étant commutatif, $\langle x \rangle$ est distingué dans $G$.

Par hypothèse de récurrence, $G/Z$ et $Z$ sont hyper-résolubles, et en concaténant les deux suites de composition, on montre que $G$ est hyper-résoluble :

$$G/Z = J_r \supset J_{r-1} \supset \ldots \supset J_0 = \{1\}$$

$$Z = I_s \supset I_{s-1} \supset \ldots \supset I_0 = \{1\}$$

$$\Rightarrow G = \widetilde{J_r} \supset \widetilde{J_{r-1}} \supset \ldots \widetilde{J_0} = Z = I_s \supset I_{s-1} \supset \ldots \supset I_0 = \{1\}$$

où $\widetilde{J_i} = \pi^{-1}(J_i)$, $\pi$ étant la surjection canonique de $G$ dans $G/Z$.

Par récurrence, tout $p$-groupe est donc hyper-résoluble. □

**Théorème 1.9.** *Tout groupe p-élémentaire est hyper-résoluble.*

*Démonstration.* Soit $H = C \times P$ un groupe $p$-élémentaire. $C$ est un groupe cyclique, donc hyper-résoluble. D'après le théoréme précédent, $H/C = P$ est hyper-résoluble aussi, en tant que $p$-groupe. En concaténant comme précédemment les deux suites de composition, on montre que $H$ est un groupe hyper-résoluble. □

## 1.3 Représentations irréductibles de groupes hyper-résolubles

On cherche à étudier les représentations irréductibles des groupes $p$-élémentaires, et à se ramener à des cas plus simples, en s'autorisant l'opération d'induction de représentation. On définit alors les représentations monomiales, et on montre qu'on peut toujours se ramener à ce cas pour un groupe hyper-résoluble.

**Définition 1.10.** *Soit $G$ un groupe et $\rho$ une représentation de $G$. La représentation $\rho$ est dite monomiale s'il existe $H$ sous-groupe de $G$, $\sigma$ représentation de $H$ de dimension 1 tels que $\rho = \mathrm{Ind}_H^G(\sigma)$.*

**Théorème 1.11.** *Soit $G$ un groupe hyper-résoluble. Toute représentation irréductible de $G$ est monomiale.*

On a besoin de deux lemmes, qui sont des propriétés sur les groupes hyper-résolubles. L'un énonce une forme de stabilité par passage au quotient, et l'autre montre qu'il existe un sous-groupe commutatif distinct du centre le contenant.

**Lemme 1.12.** *Soit $G$ un groupe hyper-résoluble, et $H$ un sous-groupe distingué de $G$. Alors $G/H$ est hyper-résoluble.*

*Démonstration.* Soit $1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$ une suite de composition hyper-résoluble de $G$. Pour tout $i \in \{0 \ldots n\}$, on pose $G'_i = G_i/(G_i \cap H)$. Alors les $G'_i$ sont des sous-groupes distingués de $G' = G/H$ (l'invariance par conjugaison est maintenue), qui satisfont les mêmes relations d'inclusion que les $G_i$. Pour $i \in 1 \ldots n$, le groupe $G_i/G_{i-1}$ est cyclique, engendré par un élément $a$, c'est-à-dire que tout élément de $G_i$ s'écrit $x = a^m y$, avec $y \in G_{i-1}$.

Or, cette relation est conservée dans les groupes quotients $G'_i$ et $G'_{i-1}$ : on a toujours $x' = a^m y'$, où $x'$ et $y'$ sont les images de $x$ et $y$ par les projections canoniques. Donc $G'_i/G'_{i-1}$ est un sous-groupe de $G_i/G_{i-1}$. C'est donc aussi un groupe cyclique. Et la suite de composition obtenue ainsi montre bien que $G'$ est un groupe hyper-résoluble. □

**Lemme 1.13.** *Soit $G$ un groupe hyper-résoluble non commutatif. Il existe un sous-groupe commutatif distingué de $G$ qui n'est pas contenu dans le centre de $G$.*

*Démonstration.* Soit $Z$ le centre de $G$. Le quotient $H = G/Z$ est hyper-résoluble, d'aprés le lemme 1.12. Ce groupe admet donc une suite de composition dont le premier terme non trivial, $H_1$, est un sous-groupe distingué et cyclique (car $H_1/H_0 = H_1$). L'image réciproque de $H_1$ dans $G$ par la projection canonique associée au quotient $H$ est un sous-groupe commutatif distingué, non contenu dans le centre de $G$. □

*Démonstration de 1.11.* On raisonne par récurrence sur l'ordre de $G$. Soit $\rho$ une représentation de $G$. Si $\rho$ n'est pas fidèle ($\ker(\rho) \neq \{1\}$), on applique l'hypothèse de récurrence à $G/\ker(\rho)$. Cela permet de se borner à une représentation irréductible $\rho$ qui est fidèle.

Si $G$ est commutatif, alors $\rho$ est de dimension 1 et il n'y a rien à démontrer.

Supposons alors $G$ non commutatif, et soit $A$ un sous-groupe distingué et commutatif de $G$, non contenu dans le centre de $G$, donné par le lemme 1.13. La représentation $\rho$ étant fidèle, $\rho(A)$ n'est pas contenu dans le centre de $\rho(G)$. Il existe donc $a \in A$ tel que $\rho(a)$ ne soit pas une homothétie.

On note $V$ l'espace vectoriel associé à la représentation $\rho$, et donc aussi à $\mathrm{Res}^G_A(\rho)$. On décompose $V$ dans sa décomposition canonique, en tant que représentation linéaire de $A$ :

$$V = \bigoplus_{i=1}^{r} V_i$$

oùu pour tout $i \in \{1 \dots r\}$, $V_i = W_i \oplus W_i \oplus \dots \oplus W_i$, la droite $W_i$ étant une représentation irréductible de $A$. (Comme $A$ est abélien, toutes ses représetations irréductibles sont de dimension 1).

Si $s \in G$, $\rho(s) \in GL(V)$, donc $\bigoplus_{i=1}^{r} \rho(s)(V_i) = V = \bigoplus_{i=1}^{r} V_i$. Par unicité de la décomposition canonique d'une représentation, on en déduit que $\rho(s)$ permute les $V_i$. Comme $V$ est une représentation irréductible de $G$, l'action de $G$ sur les $V_i$ non nuls est transitive : si $V_{i_0}$ et $V_{i_1}$ ne peuvent pas être échangés, on va pouvoir construire un sous-espace strict de $V$ stable sous l'action de $G$, ce qui est absurde.

Soit $V_{i_0}$ un de ces $V_i$ non nuls. On a nécessairement $V_{i_0} \neq V$. Dans le cas contraire, $V = W_{i_0} \oplus W_{i_0} \oplus \dots \oplus W_{i_0}$ et alors $A$ n'agit sur $V$ que par homothéties, ce qu'on a déjà exclu. Donc $V_{i_0} \neq V$. Soit $H$ le sous-groupe de $G$ formé des $s \in G$ tels que $\rho(s)(V_{i_0}) = V_{i_0}$. On a $A \subset H$, $H \neq G$, et $\rho$ est induite par la représentation naturelle et irréductible $\sigma$ de $H$ dans $V_{i_0}$. On applique alors l'hypothèse de récurrence à $H$. Il existe $K$ un sous-groupe de $H$ et $\nu$ représentation de $K$ tels que $\sigma = \mathrm{Ind}^H_K(\nu)$. De là, $\rho = \mathrm{Ind}^G_H(\sigma) = \mathrm{Ind}^G_H\left(\mathrm{Ind}^H_K(\nu)\right) = \mathrm{Ind}^G_K(\nu)$. □

## 2 Un théorème de Brauer

Le but de cette partie est de démontrer le théorème suivant, dû à Brauer, qui permettra en particulier d'établir le théorème de représentabilité des groupes finis sur les corps cyclotomiques :

**Théorème 2.1.** *Soit $G$ un groupe fini. Tout caractère de $G$ est combinaison linéaire à coefficients entiers de caractères monomiaux.*

On définit dans un premier temps l'anneau $R(G)$ des caractères virtuels de $G$ et un anneau $A$ dans lequel on travaillera. Par la suite, on construit un caractère dans $A \otimes R(G)$ à valeurs entières ne s'annulant pas modulo un nombre premier. Enfin, on pourra démontrer le théorème de Brauer.

## 2.1 L'anneau $R(G)$

On se donne $G$ un groupe fini d'ordre $g$ et $\chi_1, \ldots, \chi_h$ ses caractères irréductibles de représentations complexes. Ces caractères irréductibles forment une base orthonormale de $\mathcal{C}(G)$, l'ensemble des fonctions centrales sur $G$, pour le produit scalaire $\langle \varphi, \psi \rangle_G = \sum_{x \in G} \varphi(x)\psi(x^{-1})$. Une fonction centrale est un caractère si et seulement si elle est combinaison à coefficients entiers positifs des caractères irréductibles.

**Définition 2.2.** *On définit l'anneau $R(G)$ des caractères virtuels par :*

$$R(G) = \bigoplus_{i=1}^{h} \mathbb{Z}\chi_i$$

*C'est alors un sous-anneau de $\mathcal{C}(G)$.*

On peut alors remarquer que $\mathbb{C} \otimes R(G)$ s'identifie à $\mathcal{C}(G)$.

Si $H$ est un sous-groupe de $G$, on définit les morphismes d'induction et de restriction de caractères :

$$\mathrm{Res}_H^G : \left\{ \begin{array}{ccc} R(G) & \longrightarrow & R(H) \\ \varphi & \longmapsto & \varphi_{|H} \end{array} \right.$$

$$\mathrm{Ind}_H^G : \left\{ \begin{array}{ccc} R(H) & \longrightarrow & R(G) \\ \varphi & \longmapsto & \left( g \mapsto \frac{1}{|H|} \sum\limits_{\substack{x \in G \\ xgx^{-1} \in H}} \varphi(xgx^{-1}) \right) \end{array} \right.$$

D'après le théorème de réciprocité de Frobenius, ces morphismes sont adjoints pour les produits scalaires $\langle \cdot, \cdot \rangle_H$ et $\langle \cdot, \cdot \rangle_G$.

Au lieu de travailler dans l'anneau $\mathbb{Z}$, on va travailler dans l'anneau $A$ engendré par $\mathbb{Z}$ et une racine primitive $g$-ième de l'unité. L'intérêt de cet anneau est que tout caractère de $G$ prend ses valeurs dans cet anneau. On prolonge alors les morphismes $\mathrm{Res}_H^G$ et $\mathrm{Ind}_H^G$ en applications $A$-linéaires :

$$\mathrm{Res}_H^G : A \otimes R(G) \to A \otimes R(H) \text{ et } \mathrm{Ind}_H^G : A \otimes R(H) \to A \otimes R(G)$$

Soit $p$ un nombre premier. On note $X(p)$ l'ensemble des sous-groupes $p$-élémentaires de $G$. On définit alors

$$\mathrm{Ind} : \bigoplus_{H \in X(p)} R(H) \to R(G)$$

et on note $V_p$ son image. On prolonge encore Ind à $\bigoplus\limits_{H \in X(p)} A \otimes R(H)$ et son image est alors $A \otimes V_p$.

## 2.2 Construction de caractères

On veut démontrer la proposition suivante :

**Proposition 2.3.** *Il existe $\psi$ dans $A \otimes V_p$ à valeurs entières tel que, pour tout $x$ dans $G$, $\psi(x) \not\equiv 0$ $[p]$.*

Tout d'abord, on se ramène à ne regarder que la valeur de la $p'$-composante de $x$ modulo $p$.

**Lemme 2.4.** *Soit $x \in G$ et $\chi \in A \otimes R(G)$ à valeurs entières. On note $x_r$ la $p'$-composante de $x$. Alors*

$$\chi(x) \equiv \chi(x_r) \ [p]$$

*Démonstration.* Quitte à considérer $\langle x \rangle$, on se ramène au cas où $G$ est cyclique et engendré par $x$. Le groups $G$ est ainsi abélien et tous ses caractères irréductibles sont de dimension 1. Ce sont alors des morphismes de $G$ dans $\mathbb{U}$.

On écrit alors $\chi = \sum_{i=1}^{h} a_i \chi_i$, avec $a_i \in A$ et $(\chi_i)_{1 \leq i \leq h}$ les caractères irréductibles de $G$. On choisit alors $q$ une puissance assez grande de $p$ telle que $x^q = x_r^q$ et ainsi, pour tout i, $\chi_i(x)^q = \chi_i(x_r)^q$. De là,

$$\begin{aligned}
\chi(x)^q &= \left( \sum_{i=1}^{h} a_i \chi_i(x) \right)^q \\
&\equiv \sum_{i=1}^{h} a_i^q \chi_i(x)^q \pmod{pA} \\
&\equiv \sum_{i=1}^{h} a_i^q \chi_i(x_r)^q \pmod{pA} \\
&\equiv \left( \sum_{i=1}^{h} a_i \chi_i(x_r) \right)^q \pmod{pA} \\
&\equiv \chi(x_r)^q
\end{aligned}$$

De plus, $\chi$ est à valeurs entières et $pA \cap \mathbb{Z} = p\mathbb{Z}$, l'égalité est donc modulo $p$. On a donc $\chi(x)^q \equiv \chi(x_r)^q$ $[p]$. De plus, $q$ étant une puissance de $p$, $\chi(x)^q \equiv \chi(x)$ $[p]$ et $\chi(x_r)^q \equiv \chi(x_r)$ $[p]$. □

On construit maintenant des caractères particuliers pour chaque $p'$-élément de $G$. Le lemme 2.4 permet en effet de se restreindre à ces derniers.

**Lemme 2.5.** *Soit $x$ un $p'$-élément de $G$ et $H$ un sous-groupe $p$-élémentaire de $G$ associé à $x$. Il existe alors $\psi \in A \otimes R(H)$ à valeurs entières tel que $\psi' = \mathrm{Ind}_H^G \psi$ ait les propriétés suivantes :*

1. *$\psi'(x) \not\equiv 0$ $[p]$*
2. *pour tout $y \in G$ $p'$-élément non conjugué à $x$, $\psi'(y) = 0$*

*Démonstration.* Soit $C$ le groupe cyclique engendré par $x$ et $P$ un $p$-Sylow de $Z(x)$, le centralisateur de $x$. Le produit direct $H = C \times P$ est alors un sous-groupe $p$-élémentaire associé à $x$. On note $c$ l'ordre de $C$ et $p^a$ l'ordre de $P$.

On définit sur C la fonction $\psi_C$ valant $c$ en $x$ et 0 ailleurs. On a ainsi $\psi_C = \sum \chi(x^{-1})\chi$, la somme étant faite sur tous les caractères irréductibles de $C$. Ainsi $\psi_C$ appartient à $A \otimes R(C)$.

On définit alors $\psi$ sur $H$ : si $a \in C$ et $b \in P$, $\psi(ab) = \psi_C(a)$. Le caractère $\psi$ est alors l'image réciproque de $\psi_C$ par la projection $H \to C$ et est donc dans $A \otimes R(H)$. Vérifions que $\psi$ convient.

Soit $y$ un $p'$-élément de $G$. Si $g \in G$ et $gyg^{-1} \in H$, $gyg^{-1}$ est un $p'$-élément de $H$ et donc appartient à $C$. Ainsi $\psi(gyg^{-1}) = 0$ sauf si $gyg^{-1} = x$. Ainsi, si $y$ n'est pas conjugué à $x$, pour tout $g \in G$ tel que $gyg^{-1} \in H$, $\psi(gyg^{-1}) = 0$ et alors $\psi'(y) = 0$.

Calculons maintenant $\psi'(x)$ :

$$\psi'(x) = \frac{1}{cp^a} \sum_{\substack{g \in G \\ gxg^{-1} \in H}} \psi(gxg^{-1}) = \frac{1}{cp^a} \sum_{\substack{g \in G \\ gxg^{-1} = x}} \psi(x) = \frac{\mathrm{card}(Z(x))}{p^a}$$

Comme $p^a$ est la plus grande puissance de $p$ divisant $Z(x)$, $\psi'(x) \not\equiv 0\ [p]$. □

*Démonstration de la proposition 2.3.* On choisit $(x_i)_{i \in I}$ un système de représentants des classes $p$-régulières des éléments de $G$. Pour chaque $i \in I$, le lemme 2.5 donne $\psi_i \in A \otimes V_p$ à valeurs entières tel que $\psi_i(x_i) \not\equiv 0\ [p]$ et pour $j \neq i$, $\psi_i(x_j) = 0$.

On pose alors $\psi = \sum_{i \in I} \psi_i$. Le caractère $\psi$ est alors à valeurs entières et dans $A \otimes V_p$. De plus, si $x \in G$, $x$ est conjugué à un unique $x_i$ et :

$$\psi(x) \equiv \psi(x_i) \equiv \psi_i(x_i) \not\equiv 0\ [p]$$

□

## 2.3 Preuve du théorème de Brauer

On va montrer le théorème suivant, qui permet alors de montrer aisément le théorème 2.1.

**Théorème 2.6.** *L'indice de $V_p$ dans $R(G)$ est fini et premier à $p$.*

*Démonstration du théorème de Brauer.* Montrons que tout caractère de $G$ est combinaison linéaire à coefficients entiers de caractères induits par des caractères de sous-groupes $p$-élémentaires. Pour cela, il faut montrer que $V = \bigoplus_{p \text{ premier}} V_p = R(G)$. L'espace $V$ contenant $V_p$, l'indice de $V$ dans $R(G)$ divise celui de $V_p$ et donc est premier à $p$ par le théorème 2.6. Ceci étant vrai pour tout $p$, $[R(G) : V] = 1$ et $V = R(G)$.

Comme tout caractère d'un groupe $p$-élémentaire est monomial par le théorème 1.11, tout caractère de $G$ est combinaison linéaire à coefficients entiers de caractères monomiaux. □

On note $|G| = p^a l$ avec $l$ et $p$ premiers entre eux. Pour montrer le théorème 2.6, il suffit de voir que $l \in V_p$. En effet, on remarque que $V_p$ est un idéal de $R(G)$, grâce à la formule

$$\mathrm{Ind}_H^G(\varphi)\psi = \mathrm{Ind}_H^G(\varphi \,\mathrm{Res}_H^G(\psi)) \text{ pour } \varphi \in R(H) \text{ et } \psi \in R(G)$$

Ainsi, si $l \in V_p$, on a $lR(G) \subset V_p$ et donc $[R(G)\colon V_p] | [R(G)\colon lR(G)]$. Mais ce dernier indice est une puissance de $l$ (si $h$ est le nombre de caractères irréductibles de $G$, $[R(G)\colon lR(G)] = l^h$) et ainsi $[R(G)\colon V_p]$ est premier avec $p$.

De plus, $(A \otimes V_p) \cap R(G) = V_p$. Donc il suffit de montrer que $l \in A \otimes V_p$.

**Lemme 2.7.** *Soit $\varphi$ une fonction centrale sur $G$ à valeurs entières divisibles par l'ordre de $G$. Alors $\varphi$ appartient à $A \otimes V_p$.*

*Démonstration.* On écrit $\varphi = g\chi$, $\chi$ étant une fonction centrale sur $G$ à valeurs entières.

Si $C$ est un sous-groupe cyclique de $G$ de cardinal $c$, on pose pour tout $x \in C$, $\theta_C(x) = \begin{cases} c & \text{si } x \text{ engendre } C \\ 0 & \text{sinon} \end{cases}$. On a alors $g = \sum_{C \subset G} \mathrm{Ind}_C^G(\theta_C)$, la somme étant faite sur tous les sous-groupes cycliques de $G$.

En effet, si $x \in G$, on a :

$$\begin{aligned} \mathrm{Ind}_C^G(\theta_C)(x) &= \frac{1}{c} \sum_{\substack{y \in G \\ \langle yxy^{-1} \rangle = C}} c \\ &= \sum_{\substack{y \in G \\ \langle yxy^{-1} \rangle = C}} 1 \end{aligned}$$

Or, pour tout $y \in G$, $yxy^{-1}$ engendre un unique sous-groupe cyclique de G. Ainsi, $\sum_{C \subset G} \mathrm{Ind}_C^G \theta_C(x) = \sum_{y \in G} 1 = g$.

On a ainsi $\varphi = \sum_{C \subset G} \mathrm{Ind}_C^G(\theta_C)\chi = \sum_{C \subset G} \mathrm{Ind}_C^G(\theta_C \,\mathrm{Res}_C^G(\chi))$, la somme étant toujours faite sur tous les sous-groupes cycliques de $G$. Tout groupe cyclique étant $p$-élémentaire, il suffit alors de voir que pour tout $C$ sous-groupe cyclique de $G$, $\theta_C \,\mathrm{Res}_C^G(\chi) \in A \otimes R(C)$. Les valeurs de $\theta_C \,\mathrm{Res}_C^G(\chi)$ sont divisibles par l'ordre de $C$, et ainsi, si $\psi$ est un caractère de $C$, $\langle \theta_C \,\mathrm{Res}_C^G(\chi), \psi \rangle_C$ est dans $A$ (l'anneau $A$ est choisi de telle sorte que $\psi$ prenne ses valeurs dans cet anneau). En prenant pour $\psi$ les caractères irréductibles de $C$, on obtient que $\theta_C \,\mathrm{Res}_C^G(\chi) \in A \otimes R(C)$ et donc $\varphi \in A \otimes V_p$. □

On peut désormais finir la preuve du théorème 2.6 en montrant que $l \in A \otimes V_p$.

*Démonstration de 2.6.* Soit $\psi \in A \otimes V_p$ à valeurs entières donné par 2.3. Soit $N = \varphi(p^a)$ l'ordre de $(\mathbb{Z}/p^a\mathbb{Z})^*$. Comme $\psi \not\equiv 0\ [p]$, on a nécessairement $\psi \not\equiv 0\ [p^a]$ et ainsi $\psi^N \equiv 1[p^a]$. La fonction centrale $l(\psi^N - 1)$ est alors à valeurs entières divisibles par l'ordre de $G$. Par le lemme 2.7, $l(\psi^N - 1)$ appartient à $A \otimes V_p$. Mais $A \otimes V_p$ est un idéal de $A \otimes R(G)$ et ainsi $l\psi^N$ appartient à $A \otimes V_p$. Par soustraction, on en déduit que $l \in A \otimes V_p$, comme voulu. □

# 3 Questions de rationalité

Toutes les représentations considérées jusqu'à maintenant étaient complexes. En fait, tous les résultats restent vrais si on se place sur un corps algébriquement clos de caractéristique nulle (par exemple $\overline{\mathbb{Q}}$, clôture algébrique de $\mathbb{Q}$). On se pose alors la question naturelle suivante : que se passe-t-il si le corps n'est plus algébriquement clos ?

De plus, $\overline{\mathbb{Q}}$ est une extension de degré infini de $\mathbb{Q}$. Les groupes étudiés étant finis, on peut espérer que toute représentation d'un tel groupe soit en fait définie sur un corps plus petit, sur une extension de degré fini de $\mathbb{Q}$. On exhibera pour tout groupe fini $G$ un corps sur lequel toute représentation est définie (dans un sens que nous préciserons).

## 3.1 Représentations sur des corps non algébriquement clos

On se donne $K$ un corps de caractéristique nulle et $C$ une clôture algébrique de $K$. Si $V$ est un $K$-espace vectoriel, on note $V_C = C \otimes_K V$ l'espace vectoriel obtenu par extension des scalaires de $K$ à $C$ à partir de $V$. C'est un $C$-espace vectoriel et $\dim_K V = \dim_C V_C$.

Soit $\rho\colon G \longrightarrow GL(V)$ une représentation de $G$ sur $V$. On dispose alors naturellement de $\rho_C\colon G \longrightarrow GL(V_C)$ et c'est une représentation de $G$ sur $V_C$. On remarque que ces deux représentations ont même caractère $\chi_\rho$ et c'est une fonction centrale sur $G$ à valeurs dans $K$.

**Définition 3.1.** *On définit l'anneau $R_K(G)$ comme le sous-anneau de $R(G)$ engendré par les caractères de représentations de $G$ sur $K$.*

On dispose toujours de la même forme bilinéaire sur $R_K(G)$ : $\langle \varphi, \psi \rangle = \frac{1}{g} \sum\limits_{x \in G} \varphi(x)\psi(x^{-1})$.

L'anneau $R_K(G)$ ne jouit pas exactement de mêmes propriétés que $R(G)$. En effet, le lemme de Schur assurant que $\mathrm{Hom}^G(V,V) = K$ si $V$ est une représentation irréductible ne s'applique plus quand $K$ n'est plus algébriquement clos. On n'a plus l'équivalence « $\chi$ caractère irréductible si et seulement si $\langle \chi, \chi \rangle = 1$ ».

**Proposition 3.2.** *Soient $\chi_i \in R_K(G)$ les caractères des représentations irréductibles de $G$ sur des $K$-espaces vectoriels. Les $\chi_i$ forment une base orthogonale de $R_K(G)$ (mais pas orthonormale* a priori).

*Démonstration.* Le fait que les $\chi_i$ engendrent $R_K(G)$ découle du théorème de Maschke. En effet, si $\chi$ est un caractère d'une représentation $V$ de $G$ sur $K$, on peut écrire $V = \bigoplus\limits_{i \in I} n_i V_i$ où les $(V_i)_{i \in I}$ sont les représentations irréductibles de $G$ sur $K$ de caractère $(\chi_i)_{i \in I}$. On a alors $\chi = \sum\limits_{i \in I} n_i \chi_i$.

Pour l'orthogonalité, on remarque que si $V$ est associée au caractère $\varphi$ et $W$ à $\psi$, on a :

$$\dim_K \mathrm{Hom}^G(V,W) = \dim_C \mathrm{Hom}^G(V_C, W_C) = \langle \varphi, \psi \rangle$$

Ainsi, si $i \neq j$, $\langle \chi_i, \chi_j \rangle = 0$. Par contre, $\dim_C \mathrm{Hom}^G((V_i)_C, (V_i)_C) > 0$ et $\langle \chi_i, \chi_i \rangle > 0$. Les $\chi_i$ sont alors orthogonaux et linéairement indépendants. □

Le fait que la représentation $V$ soit irréductible n'assure pas que $V_C$ l'est. C'est pour cela que, si $\chi$ est le caractère associé à $V$ (et donc aussi à $V_C$), $\langle \chi, \chi \rangle \geq 1$, avec égalité si et seulement si $V_C$ *est irréductible.*

## 3.2 Réalisabilité et corps cyclotomiques

**Définition 3.3.** *Une représentation linéaire de $G$ sur $C$ est dite* réalisable *sur $K$ si elle est isomorphe à $\rho_C$, $\rho$ étant une représentation linéaire de $G$ sur $K$.*

Ceci revient alors à dire que, dans une base adaptée, les matrices de la représentation sont dans $\mathcal{M}_n(K)$. On arrive alors à réduire la représentation à un corps plus petit, mais qui n'est plus algébriquement clos. Si $K$ est un sous-corps de $C$, toute représentation de $G$ est réalisable sur une extension finie de $K$. Il suffit de prendre le corps engendré par les coefficients des matrices de la représentation.

Peut-on alors trouver des corps sur lesquels toute représentation d'un groupe $G$ est réalisable ?

**Proposition 3.4.** *Une représentation linéaire est réalisable sur $K$ si et seulement si son caractère appartient à $R_K(G)$.*

*Démonstration.* Soit $(\rho, V)$ une représentation linéaire de $G$ sur $C$ et $\chi$ son caractère.

Supposons que $\rho$ est réalisable sur $K$. On écrit alors $V = W \otimes_K C$, $W$ étant un $K$-espace vectoriel. Le théorème de Maschke s'applique alors (on travaille en caractéristique nulle) et $W = \bigoplus_{i \in I} n_i V_i$, les représentations $V_i$ étant les représentations irréductibles de $G$ sur $K$ et $n_i \in \mathbb{N}$. De là, $\chi = \sum_{i \in I} n_i \chi_i$ est dans $R_K(G)$.

Réciproquement, si $\chi$ appartient à $R_K(G)$, on écrit $\chi = \sum_{i \in I} n_i \chi_i$, avec $n_i \in \mathbb{Z}$. Il suffit alors de voir que pour tout $i \in I$, $n_i \geq 0$ : on pourra réaliser la représentation $V$ sur $K$ par $\bigoplus_{i \in I} n_i V_i$. Or $\langle \chi, \chi_i \rangle = n_i \langle \chi_i, \chi_i \rangle$ et $\chi$ étant le caractère d'une représentation sur $C$, on a $\langle \chi, \chi_i \rangle \geq 0$ : on a bien $n_i \geq 0$. □

On va donc chercher des corps particuliers, pour lesquels $R(G) = R_K(G)$. Ainsi toute représentation de $G$ sur $C$ aura son caractère dans $R_K(G)$ et sera donc réalisable sur $K$. On note $m$ l'exposant du groupe $G$ (c'est le PPCM des ordres des éléments de $G$).

**Théorème 3.5.** *Si le corps $K$ contient les racines $m$-ièmes de l'unité alors $R(G) = R_K(G)$ et ainsi toute représentation linéaire de $G$ sur $C$ est réalisable sur $K$.*

On remarque qu'ici le corps $K$ ne dépend pas de la représentation de $G$ choisie.

*Démonstration.* Soit $\chi$ dans $R(G)$. Par le théorème 2.1, on peut écrire :

$$\chi = \sum n_i \operatorname{Ind}_{H_i}^G(\varphi_i)$$

où les $\varphi_i$ sont des caractères de dimension 1 des sous-groupes $H_i$ de $G$. Par définition de $m$ et comme $K$ contient les racines $m$-ièmes de l'unité, $\varphi_i$ est dans $R_K(H_i)$. De là,

$\mathrm{Ind}_{H_i}^G(\varphi_i)$ appartient à $R_K(G)$. En effet, si $H$ est un sous-groupe de $G$ et $V$ est une représentation de $H$ sur $K$ de caractère $\varphi$, $\mathrm{Ind}_H^G(V)$ est une représentation de $G$ sur $K$ et son caractère, $\mathrm{Ind}_H^G(\varphi)$, est dans $R_K(G)$.

On déduit donc que $\chi$ appartient à $R_K(G)$, comme voulu. □

On peut se poser une autre question. Etant donné un corps algébriquement clos $C$ et $K$ un sous-corps de $C$, peut-on caractériser les représentations sur $C$ qui sont réalisables sur $K$ ?

## 3.3 Le cas réel

On va répondre à cette question, dans le cas où $C = \mathbb{C}$ et $K = \mathbb{R}$. On se donne une représentation complexe $V$ de $G$, de caractère $\chi$. On dira que la représentation est réelle si elle est réalisable sur $\mathbb{R}$.

**Proposition 3.6.** *Le caractère $\chi$ est à valeurs réelles si et seulement s'il existe une forme bilinéaire non dégénérée invariante par $G$ sur $V$.*

*Démonstration.* Partant d'une représentation $V$ de $G$, on peut mettre une structure de représentation sur le dual $V^*$ de $V$. Son caractère, que l'on note $\hat{\chi}$ vérifie alors : $\hat{\chi}(g) = \chi(g^{-1})$. Comme on travaille dans le corps des complexes, on a $\hat{\chi}(g) = \overline{\chi(g)}$.

Ainsi $\chi$ est à valeurs réelles si et seulement si $\chi = \hat{\chi}$ et les représentations $V$ et $V^*$ sont isomorphes en tant que représentations. Soit alors $f\colon V \longrightarrow V^*$ un isomorphisme de représentations. La forme bilinéaire $B(u, v) = f(u)(v)$ est alors non dégénérée et $G$-invariante sur $V$.

Réciproquement, si $B$ est une forme bilinéaire $G$-invariante sur $V$, on pose $f(u) = B(u, \cdot)$. $f$ est alors un isomorphisme (injectif car $B$ non dégénérée et on a $\dim(V) = \dim(V^*)$) entre les représentations $V$ et $V^*$. □

Mais être à valeurs réelles ne signifie pas être réelle. Il faut une hypothèse de plus sur la forme bilinéaire $G$-invariante.

**Proposition 3.7.** *La représentation $V$ est réelle si et seulement s'il existe une forme bilinéaire symétrique non dégénérée invariante par $G$ sur $V$.*

*Démonstration.* On suppose $V$ réelle. On écrit alors $V = \mathbb{C} \otimes_{\mathbb{R}} V_0$, où $V_0$ est une représentation de $G$ sur $R$. On choisit un produit scalaire $\varphi$ sur $V_0$, que l'on rend $G$-invariant comme suit :

$$\varphi'(u, v) = \sum_{g \in G} \varphi(g \cdot u, g \cdot v)$$

Par extension des scalaires, on a une forme bilinéaire symétrique non dégénérée invariante par $G$.

Réciproquement, si on dispose d'une telle forme $B$ sur $V$, on choisit $\langle \cdot, \cdot \rangle$ un produit scalaire hermitien $G$-invariant sur $V$ (on utilise le même procédé de moyenne). Pour tout $u \in V$, il existe alors un unique élément $\varphi(u) \in V$ tel que :

$$\forall v \in V,\ B(u, v) = \langle \varphi(u), v \rangle$$

Ceci découle du fait que $B(u,\cdot)$ est une forme linéaire et que $w \longmapsto \langle w,\cdot\rangle$ est un isomorphisme entre $V$ et $V^*$. Le morphisme $\varphi$ est alors anti-linéaire et bijectif et $\varphi^2$ est un isomorphisme de $V$. De plus,

$$\langle \varphi^2(u), v\rangle = B(\varphi(u), v) = B(v, \varphi(u)) = \langle \varphi(v), \varphi(u)\rangle$$

Ainsi,

$$\langle \varphi^2(u), v\rangle = \overline{\langle \varphi(u), \varphi(v)\rangle} = \overline{\langle \varphi^2(v), u\rangle} = \langle u, \varphi^2(v)\rangle$$

Le morphisme $\varphi^2$ est alors hermitien et positif (prendre $x = y$). On peut alors écrire $\varphi^2 = \psi^2$ avec $\psi$ hermitien positif et polynôme en $\varphi^2$. On pose alors $\sigma = \varphi\psi^{-1}$ et $\sigma^2 = \varphi^2\psi^{-2} = id$ car $\varphi$ et $\psi$ commutent. On peut donc écrire $V = V_0 + V_1$ où $V_0$ est l'espace propre associé à la valeur propre 1 de $\sigma$ et $V_1$ celui associé à la valeur propre $-1$. Puisque $\sigma$ est anti-linéaire, $\sigma(iV_0) = V_1$ et alors $V = V_0 \oplus iV_0$.

Mais le fait que $\langle\cdot,\cdot\rangle$ et $B$ sont $G$-invariants entraînent que $\varphi$, $\psi$ puis $\sigma$ commutent à l'action de $G$. Les sous-espaces $V_0$ et $iV_0$ sont donc stables par $G$ et $V = (V_0)_{\mathbb{C}}$ est réelle. □

On s'intéresse maintenant à des représentations irréductibles, auxquelles s'applique le lemme de Schur. Celui-ci donne alors l'unicité de la forme bilinéaire, à homothétie près.

**Théorème 3.8.** *Soit $V$ une représentation complexe de $G$ et $\chi$ son caractère. On note $S = \frac{1}{g}\sum_{x\in G}\chi(x^2)$.*

1. *$\chi$ est à valeurs réelles si et seulement si $S \neq 0$.*
2. *$V$ est réelle si et seulement si $S = 1$.*

*Démonstration.* Une forme $B$ bilinéaire et $G$-invariante correspond à un morphisme de représentations entre $V$ et $V^*$. Dans ce cas, le lemme de Schur assure que $B$ est non dégénérée et unique à homothétie près et $V \otimes V$ ne peut alors contenir qu'une fois la représentation triviale.

Comme $V \otimes V = \Lambda^2 V \oplus S^2 V$, la représentation triviale est soit dans $\Lambda^2 V$, soit dans $S^2 V$. On note $\chi_a$ le caractère de $\Lambda^2 V$ et $\chi_s$ celui de $S^2 V$. On a les formules suivantes :

$$\chi_s(x) = \frac{1}{2}\left(\chi(x)^2 + \chi(x^2)\right)$$
$$\chi_a(x) = \frac{1}{2}\left(\chi(x)^2 - \chi(x^2)\right)$$

Ainsi $S = \frac{1}{g}\sum_{x\in G}(\chi_s(x) - \chi_a(x)) = \langle 1, \chi_s\rangle - \langle 1, \chi_a\rangle$. Le résultat découle alors de 3.6 pour 1, et de 3.7 pour 2. □

On peut classifier en fonction de la valeur $S$ les représentations complexes irréductibles en trois types :

1. si $S = 0$, le caractère $\chi$ n'est pas à valeurs réelles et par restriction des scalaires, on définit une représentation irréductible sur $\mathbb{R}$, de dimension double et de caractère $\chi + \overline{\chi}$.

2. si $S = 1$, la représentation est réalisable sur $\mathbb{R}$
3. si $S = -1$, les valeurs de $\chi$ sont réelles mais la représentation n'est pas réalisable sur $\mathbb{R}$. Par restriction des scalaires, on définit une représentation sur $\mathbb{R}$, de dimension double et de caractère $2\chi$.

## 3.4 Représentations du groupe quaternionique

Dans cette partie, on étudie en détail l'exemple du groupe quaternionique, que l'on notera $Q$. Cette étude constitue un contre-exemple intéressant : elle montre qu'il n'existe pas, pour un groupe donné, de plus petit sous-corps, au sens de l'inclusion, sur lequel toute représentation serait réalisable.

**Définition 3.9.** *On définit le groupe quaternionique $Q$ comme le groupe d'ordre 8 constitué de $\{\pm 1, \pm i, \pm j, \pm k\}$ vérifiant les relations suivantes :*
- *$1$ est l'élément neutre*
- *$i^2 = j^2 = k^2 = -1$*
- *$ij = k$, $jk = i$, $ki = j$*

Ses classes de conjugaison sont $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$ et $\{k, -k\}$. Il existe donc 5 représentations complexes irréductibles de $Q$. On établit pour cela la table des caractères de $Q$.

Calculons d'abord ceux de dimension 1. Pour cela, il faut calculer le groupe dérivé $D(Q)$ de $Q$ et remonter sur $Q$ les représentations de $Q/D(Q)$. En considérant les classes de conjugaison de $Q$, on montre que $D(Q) \subset \{-1, 1\}$ et comme $Q/D(Q)$ est abélien alors que $Q$ ne l'est pas, on a $D(Q) = \{-1, 1\}$. $Q/D(Q)$ est d'ordre 4 et ne contient que des éléments d'ordre 2. Ainsi $Q/D(Q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On a donc 4 caractères de dimension 1, donnés par les caractères de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il reste alors un caractère de dimension 2. On complète la table des caractères par orthogonalité. On obtient la table suivante (voir table 1).

| | $\{1\}$ | $\{-1\}$ | $\{i, -i\}$ | $\{j, -j\}$ | $\{k, -k\}$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_i$ | 1 | 1 | 1 | $-1$ | $-1$ |
| $\chi_j$ | 1 | 1 | $-1$ | 1 | $-1$ |
| $\chi_k$ | 1 | 1 | $-1$ | $-1$ | 1 |
| $\chi_2$ | 2 | $-2$ | 0 | 0 | 0 |

TABLE 1: Table des caractères de $Q$

Les représentations de dimension 1 sont évidemment réalisables sur $\mathbb{Q}$. Le théorème 3.5 assure que la représentation de dimension 2 est réalisable sur $\mathbb{Q}[i]$. Comme, pour tout $x \in Q\backslash\{-1, 1\}$, $x^2 = -1$, on a $\sum_{x \in Q} \chi_2(x^2) = -8$. La représentation de dimension 2 n'est donc pas réalisable sur $\mathbb{R}$, en vertu du théorème 3.8. Elle permet tout de même de donner une représentation matricielle de dimension 4 sur $\mathbb{R}$ du corps des quaternions ($\mathbb{H} = \mathbb{R} \otimes \mathbb{Q}[Q]$, $\mathbb{Q}[Q]$ est l'algèbre des quaternions sur $\mathbb{Q}$, souvent notée $\mathbb{H}_{\mathbb{Q}}$).

Enfin, le théorème suivant décrit la réalisabilité de cette représentation sur les corps quadratiques :

**Théorème 3.10.** *La représentation irréductible de dimension 2 de $Q$ est réalisable sur $\mathbb{Q}[i\sqrt{d}]$ si et seulement si $d$ est un entier positif sans facteurs carrés et non congru à 7 modulo 8.*

*En particulier, il n'existe pas de plus petit sous-corps de $\mathbb{C}$, au sens de l'inclusion, tel que toute représentation d'un groupe soit réalisable sur ce corps.*

*Démonstration.* Par le lemme 3.11 ci-dessous, la représentation est réalisable si et seulement si -1 est somme de deux carrés dans $\mathbb{Q}[i\sqrt{d}]$. Par le lemme 3.12 ci-après, c'est le cas si et seulement si $d$ est somme de trois carrés entiers. Par [Ser95], la représentation est réalisable si et seulement si $d$ est non congru à 7 modulo 8 ($d$ est sans facteurs carrés). □

Dans toute la suite, $(V, \rho)$ désigne la représentation complexe irréductible de dimension 2 du groupe quaternionique, et $\chi$ son caractère. Matriciellement, on a :

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \rho(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \rho(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \rho(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

**Lemme 3.11.** *Soit $K$ un sous-corps de $\mathbb{C}$. La représentation $V$ est réalisable sur $K$ si et seulement si $-1$ est somme de 2 carrés.*

*Démonstration.* On suppose que $V$ est réalisable sur $K$. Soit $(V', \rho')$ la représentation correspondante sur le corps $K$. Comme $V$ est irréductible, $V'$ l'est aussi : si $V' = \mathbb{K}e_1 \oplus \mathbb{K}e_2$ se décompose en droites stables par $G$, alors $V = \mathbb{C} \otimes V' = \mathbb{C}e_1 \oplus \mathbb{C}e_2$ se décompose également en droites stables par $G$. Ainsi il existe un élément de $G$ qui n'agit pas par homothétie. On suppose que c'est $j$, quitte à renommer les éléments du groupe. Soit $e_1 \neq 0$ dans $V'$ et $e_2 = \rho'(j)(e_1)$. La famille $(e_1, e_2)$ est une base de $V'$ et dans cette base, $\rho'(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. De plus, $V'$ et $V$ ayant même caractère, $\rho'(i)$ est de trace nulle. De là, il existe $\alpha$, $\beta$ et $\gamma$ dans $K$ tels que $\rho'(i) = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$. De plus, comme $k = ij$, on a $\rho'(k) = \rho'(i)\rho'(j) = \begin{pmatrix} \beta & -\alpha \\ -\alpha & -\gamma \end{pmatrix}$. La matrice $\rho'(k)$ étant aussi de trace nulle, $\beta = \gamma$. Maintenant, comme $j^2 = -1$, on a $-I_2 = \rho'(j^2) = \rho'(j)^2 = (\alpha^2 + \beta^2)I_2$ et $-1 = \alpha^2 + \beta^2$.

Réciproquement, on suppose que $-1 = \alpha^2 + \beta^2$, avec $\alpha$ et $\beta$ éléments de $K$. Les matrices suivantes de $\mathcal{M}_2(K)$ donnent une représentation irréductible de $G$ sur $K^2$, qui est alors isomorphe à $V$ :

$$\rho'(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \rho'(i) = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix},$$
$$\rho'(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ \rho'(k) = \begin{pmatrix} \beta & -\alpha \\ -\alpha & -\beta \end{pmatrix}$$

□

**Lemme 3.12.** *Soit $d$ un entier strictement positif sans facteur carré. On peut écrire $-1$ comme somme de deux carrés dans $\mathbb{Q}[i\sqrt{d}]$ si et seulement si $d$ est somme de trois carrés entiers.*

La démonstration du lemme 3.12 utilise le lemme suivant.

**Lemme 3.13** (Théorème de Davenport-Cassels)**.** *Si un entier est somme de trois carrés rationnels alors il est somme de trois carrés entiers.*

*Démonstration.* Soit $n \in \mathbb{N}$. On pose $q(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - n\alpha_4^2$. On note $\varphi$ la forme polaire associée à $q$ : $\varphi(\alpha, \beta) = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 - n^2\alpha_4\beta_4$. On cherche à montrer que si $q(x) = 0$ avec $x \in \mathbb{Z}^4$ et $x_4 \neq 0$, alors il existe $y \in \mathbb{Z}^4$ avec $y_4 = 1$ tel que $q(y) = 0$.

On procède par récurrence descendante sur $x_4$. Si $x_4 = 1$, il n'y a rien à faire. On suppose $x_4 > 1$ (si $x_4 < 0$, on remplace $x_4$ par $-x_4$). Pour $i \in \{1, \dots, 4\}$, on choisit $m_i \in \mathbb{Z}$ tel que $\left|\frac{x_i}{x_4} - m_i\right| < \frac{1}{2}$. On remarque que $m_4 = 1$. Si $q(m) = 0$, on n'a rien à faire.

Sinon, on pose $y = q(m)x - 2\varphi(m, x)m$. C'est un élément de $\mathbb{Z}^4$ et comme $q(x) = 0$,

$$q(y) = q(m)^2 q(x) - 4q(m)\varphi(m, x)^2 + 4q(m)\varphi(m, x)^2 = 0$$

De plus,

$$\begin{aligned}
|y_4| &= x_4 \left| q(m) - 2\varphi\left(m, \frac{x}{x_4}\right) m_4 \right| \\
&= x_4 \left| q(m) - 2\varphi\left(m, \frac{x}{x_4}\right) + q\left(\frac{x}{x_4}\right) \right| \\
&= x_4 \left| q\left(m - \frac{x}{x_4}\right) \right| \\
&= x_4 \left| \left(m_1 - \frac{x_1}{x_4}\right)^2 + \left(m_1 - \frac{x_1}{x_4}\right)^2 + \left(m_1 - \frac{x_1}{x_4}\right)^2 \right| \\
&\leq \frac{3}{4} x_4
\end{aligned}$$

Enfin, $y_4 \neq 0$, sinon $x_i = m_i x_4$ et $q(m) = 0$. Ceci permet de conclure la récurrence descendante. □

*Démonstration de 3.12.* On suppose $d$ somme de trois carrés entiers. $d = n_1^2 + n_2^2 + n_3^2$, avec $n_1 \neq 0$. On a alors $-1 = \left(i\frac{n_1}{\sqrt{d}}\right)^2 + \left(i\frac{n_2}{\sqrt{d}}\right)^2 + \left(i\frac{n_3}{\sqrt{d}}\right)^2$ et $-1$ est somme de trois carrés dans $\mathbb{Q}[i\sqrt{d}]$.

Si $-1 = \alpha^2 + \beta^2 + \gamma^2$ dans $\mathbb{Q}[i\sqrt{d}]$ avec $\alpha \neq 0$, alors $-1 = \left(\frac{\alpha\gamma+\beta}{\alpha^2+\beta^2}\right)^2 + \left(\frac{\beta\gamma+\alpha}{\alpha^2+\beta^2}\right)^2$ et $-1$ est somme de deux carrés dans $\mathbb{Q}[i\sqrt{d}]$.

Réciproquement, on suppose $-1 = \alpha^2 + \beta^2$ dans $\mathbb{Q}[i\sqrt{d}]$. On écrit alors $\alpha = \alpha_1 + i\sqrt{d}\alpha_2$ et $\beta = \beta_1 + i\sqrt{d}\beta_2$. Ainsi on a les équations suivantes :

$$\begin{aligned} \alpha_1^2 + \beta_1^2 - d(\alpha_2^2 + \beta_2^2) &= -1 \\ \alpha_1\alpha_2 + \beta_1\beta_2 &= 0 \end{aligned}$$

On peut alors supposer $\alpha_2 \neq 0$ et on a :

$$\begin{aligned} d &= \frac{\beta_1^2\beta_2^2 + \beta_1^2\alpha_2^2 + \alpha_2^2}{\alpha_2^2(\alpha_2^2 + \beta_2^2)} \\ &= \frac{\beta_1^2(\alpha_2^2 + \beta_2^2)^2 + \alpha_2^2(\alpha_2^2 + \beta_2^2)}{\alpha_2^2(\alpha_2^2 + \beta_2^2)^2} \\ &= \left(\frac{\beta_1}{\alpha_2}\right)^2 + \left(\frac{\alpha_2}{\alpha_2^2 + \beta_2^2}\right)^2 + \left(\frac{\beta_2}{\alpha_2^2 + \beta_2^2}\right)^2 \end{aligned}$$

$d$ est alors somme de trois carrés rationnels, et par la proposition 3.13, $d$ est somme de trois carrés entiers. □

# 4 Anneaux de Dedekind et modules

Dans cette partie, on s'intéresse aux anneaux de Dedekind, à leurs idéaux et aux modules sur des anneaux de Dedekind. Donnons tout d'abord la définition d'un anneau de Dedekind.

**Définition 4.1.** *Soit $A$ un anneau commutatif unitaire et intègre. On dit que $A$ est un anneau de Dedekind s'il vérifie les propriétés suivantes :*

- *$A$ est noethérien.*
- *tout idéal premier non nul de $A$ est maximal.*
- *$A$ est intégralement clos, c'est-à-dire que tout élément de son corps des fractions entier sur $A$ est dans $A$.*

Les anneaux de Dedekind sont des objets qui apparaissent couramment. Par exemple, si $K$ est un corps de nombres, son anneau des entiers $\mathcal{O}_K$ est un anneau de Dedekind (voir à ce sujet [Mar77], théorème 14).

## 4.1 Idéaux d'un anneau de Dedekind

L'étude des idéaux d'un anneau de Dedekind est très intéressante puisque ces idéaux forment un groupe, modulo une relation d'équivalence que l'on va définir. Dans toute cette partie, $A$ désignera un anneau de Dedekind. Son corps des fractions sera noté $K$.

**Définition 4.2.** *On dit que $I$ est un idéal fractionnaire de $A$ si $I$ est un sous-$A$-module de $K$ et qu'il existe $d \in A$ tel que $dI \subseteq A$.*

*On peut définir le produit de deux idéaux fractionnaires $I$ et $J$ comme $IJ = \{\sum_{i=1}^{n} a_i b_i / n \in \mathbb{N}, a_i \in I, b_i \in J\}$. On vérifie que c'est bien un idéal fractionnaire de $A$.*

Il faut faire attention à la dénomination. Un idéal fractionnaire de $A$ n'est pas un idéal de $A$, mais il existe $d \in A$ tel que $dI$ soit un idéal de $A$. On peut donc écrire un idéal fractionnaire sous la forme $\frac{1}{d}J$, $J$ étant un idéal de $A$ et $d$ un élément de $A$.

**Définition 4.3.** *Soient $I$ et $J$ deux idéaux d'un anneau $A$. On dit que $I \mid J$ ($I$ divise $J$) si et seulement s'il existe un idéal $L$ de $A$ tel que $IL = J$.*

**Proposition 4.4.** *Soit $I$ un idéal fractionnaire de $A$. Il existe alors un idéal fractionnaire $J$ de $A$ tel que $IJ$ est principal.*

On se ramène tout d'abord au cas où $I$ est un idéal de $A$. En effet, si le résultat est montré pour les idéaux de $A$, on écrit $I = \frac{1}{d}I'$, $I'$ idéal de $A$. On choisit alors $J'$ tel que $I'J'$ soit principal. L'idéal fractionnaire $J = \frac{1}{d}J'$ convient alors.

**Lemme 4.5.** *Dans un anneau de Dedekind, tout idéal contient un produit d'idéaux premiers.*

*Démonstration.* Par l'absurde, supposons que l'ensemble des idéaux de $A$ ne contenant pas de produit d'idéaux premiers est non vide. Comme $A$ est noethérien, il existe $I$ maximal dans cet ensemble. L'idéal $I$ n'est pas premier et il existe alors $r$ et $s$ dans $A\backslash I$ tels que $rs \in I$.

Considérons alors les idéaux $I + (r)$ et $I + (s)$. Ils contiennent strictement $I$ et, par maximalité de $I$, contiennent un produit d'idéaux premiers. Or, par définition de $r$ et $s$, $(I + (r))(I + (s))$ est inclus dans $I$ et $I$ contient un produit d'idéaux premiers. On aboutit donc à une contradiction. □

**Lemme 4.6.** *Soit $I$ un idéal propre de $A$. Il existe alors $\gamma \in K\backslash A$ tel que $\gamma I \subseteq A$.*

*Démonstration.* Soit $a$ un élément non nul de $I$. Par le lemme 4.5, il existe $\mathfrak{p}_1 \dots, \mathfrak{p}_n$ tels que $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq (a)$, avec $n$ minimal. Chaque idéal propre étant contenu dans un idéal maximal, il existe $\mathfrak{p}$ premier tel que $I \subseteq \mathfrak{p}$. De là, $\mathfrak{p}$ contient le produit $\mathfrak{p}_1 \dots \mathfrak{p}_n$ et contient alors un des $\mathfrak{p}_i$ (sinon, il existe $r_i \in \mathfrak{p}_i\backslash\mathfrak{p}$ et $\mathfrak{p}$ contient $a_1 \dots a_n$ et donc l'un des $a_i$ car $\mathfrak{p}$ est premier). On suppose alors, par exemple, $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Comme $\mathfrak{p}_1$ est maximal, on a $\mathfrak{p} = \mathfrak{p}_1$.

Par minimalité de $n$, il existe $b \in \mathfrak{p}_2 \dots \mathfrak{p}_n\backslash(a)$. On pose $\gamma = \frac{b}{a}$ et on a $\gamma I \subseteq A$. En effet, si $x \in I$ alors $x \in \mathfrak{p}_1$ et $x \in \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n \subseteq (a)$. De là, $\gamma x \in A$. □

*Démonstration de 4.4.* Soit $I$ un idéal de $A$, $\alpha$ un élément non nul de $I$ et $J = \{\beta \in A / \beta I \subseteq (\alpha)\}$. L'ensemble $J$ est un idéal de $A$, non vide et $IJ \subseteq (\alpha)$. On considère $R = \frac{1}{\alpha}IJ$ qui est un idéal de $A$. Si $R = A$ alors il n'y a rien à faire.

Sinon, $R$ est un idéal propre de $A$ et on peut appliquer le lemme 4.6. Il existe $\gamma \in K\backslash A$ tel que $\gamma R \in A$. On va montrer que $\gamma$ est un entier sur $A$. Comme $\alpha \in I$, $R$ contient $J$ et ainsi $\gamma J \subseteq \gamma R \subseteq A$. Donc si $x \in \gamma J$ alors $xI \in \gamma IJ \subseteq \alpha\gamma R \subseteq (\alpha)$ et ainsi $\gamma J \subseteq J$.

Maintenant, comme $A$ est noethérien, $J$ est de type fini. Soient $a_1, \dots, a_n$ générant $J$. Le fait que $\gamma J \subseteq J$ se traduit par l'existence d'une matrice $M \in \mathcal{M}_n(A)$ telle que :

$$\gamma \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

En prenant le déterminant de $\gamma I_n - M$, on obtient une équation polynômiale à coefficients dans $A$ unitaire. Ainsi $\gamma$ est entier sur $A$ et $A$ étant intégralement clos, $\gamma \in A$. Ceci est absurde.

Donc $IJ = (\alpha)$. □

**Corollaire 4.7** (Loi de simplification)**.** *Soient $I$, $J$ et $L$ trois idéaux fractionnaires de $A$. Si $IJ = IL$ alors $I = L$.*

*Démonstration.* Par la proposition 4.4, il existe $M$ idéal fractionnaire de $A$ tel que $IM = (\alpha)$, avec $\alpha \in A$. De là, $\alpha J = \alpha L$ et alors $J = L$. □

**Corollaire 4.8.** *Dans un anneau de Dedekind, l'ensemble des idéaux fractionnaires forme un groupe commutatif, d'élément neutre $A$.*

En effet, la proposition 4.4 assure l'existence d'un inverse. On peut alors définir une notion importante dans les anneaux de Dedekind, celle de groupe de classe d'idéaux.

**Définition 4.9** (Groupe des classes d'idéaux)**.** *On appelle groupe des classes d'idéaux le groupe des idéaux fractionnaires quotienté par le sous-groupe des idéaux principaux. On le note $\mathcal{C}l(A)$.*

On remarque que tout élément de ce groupe contient un idéal de $A$. En effet, si on se donne une classe $[I]$, il existe un élément $d \in A$ tel que $dI$ est un idéal de $A$ et $[I] = [dI]$. Ce groupe permet alors de mettre en évidence le défaut de principalité d'un anneau de Dedekind. Il est en effet trivial si et seulement si l'anneau est principal.

On peut maintenant montrer l'existence et l'unicité de la décomposition d'un idéal en produit d'idéaux premiers.

**Proposition 4.10.** *Tout idéal non trivial de $A$ se décompose de manière unique comme produit d'idéaux premiers, à l'ordre des facteurs près.*

*Démonstration.* Commençons par l'unicité. Supposons $I = \mathfrak{p}_1 \dots \mathfrak{p}_n = \mathfrak{q}_1 \dots \mathfrak{q}_s$. On a alors $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq \mathfrak{p}_1$ et par primalité de $\mathfrak{p}_1$, il existe $i$ tel que $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Par maximalité de $\mathfrak{q}_i$, on a égalité. La loi de simplification et une récurrence permettent alors de conclure.

Pour l'existence, supposons l'ensemble des idéaux ne s'écrivant pas comme produit d'idéaux premiers non vide. L'anneau $A$ étant noethérien, il existe un élément $M$ maximal dans cet ensemble. Comme $M$ est propre, il est inclus dans un idéal premier $\mathfrak{p}$. On peut alors trouver un idéal $I$ tel que $I\mathfrak{p} = (\alpha)$ est principal. L'idéal $J = \frac{1}{\alpha} IM$ vérifie alors $J\mathfrak{p} = M$. De là, $M \subseteq J$ et si $M = J$, $M\mathfrak{p} = M$. Dans ce cas, par la loi de simplification, $\mathfrak{p} = A$, ce qui est absurde. De là, $M \subsetneq J$ et $J$ est produit d'idéaux premiers par maximalité de $M$. Comme $M = J\mathfrak{p}$, $M$ est aussi produit d'idéaux premiers, ce qui est absurde. □

**Corollaire 4.11.** *Soient $I$ et $J$ deux idéaux d'un anneau de Dedekind $A$. Les deux propositions suivantes sont équivalentes :*

*(i)* $J \subset I$

*(ii)* $I \mid J$

*Démonstration.* L'implication $(ii) \Rightarrow (i)$ est vraie quelque soit l'anneau $A$.

Réciproquement, on décompose $I$ et $J$ en facteurs premiers :

$$I = \prod_i \mathfrak{p}_i^{r_i}$$
$$J = \prod_i \mathfrak{p}_i^{s_i}$$

Comme $J \subset I$, on a, pour tout $i$, $r_i < s_i$. En multipliant les facteurs de $J$ n'apparaissant pas dans $I$, on construit un idéal $L$ tel que $IL = J$. □

En fait, les anneaux de Dedekind ont des idéaux légèrement plus complexes que ceux des anneaux principaux. On sait que ces idéaux sont de type fini car un anneau de Dedekind est noethérien, mais on a le résultat suivant, plus précis :

**Proposition 4.12.** *Tout idéal d'un anneau de Dedekind est engendré par au plus deux éléments.*

*Démonstration.* Soit $I$ un idéal d'un anneau de Dedekind. Puisque $I$ est de type fini, fixons $a_1, \ldots, a_n$ tels que $I = (a_1, \ldots, a_n)$. On pose $J = (a_1)$. Montrons alors que tout idéal de $A/J$ est principal. On peut écrire $J = \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_q^{\alpha_q}$. Si $i \neq j$, on a, par maximalité des idéaux premiers, $\mathfrak{p}_i + \mathfrak{p}_j = A$. De là, on écrit $1 = a_i + a_j$ avec $a_i \in \mathfrak{p}_i$ et $a_j \in \mathfrak{p}_j$. On a alors $1 = (a_i + a_j)^{\alpha_i + \alpha_j} \in \mathfrak{p}_i^{\alpha_i} + \mathfrak{p}_j^{\alpha_j}$ en développant avec le binôme de Newton. Ainsi les idéaux $\mathfrak{p}_i$ sont deux à deux premiers entre eux et on peut appliquer le théorème des restes chinois. On se ramène donc au cas où $J = \mathfrak{p}^\alpha$. Les idéaux propres de $A/\mathfrak{p}^\alpha$ sont les $\mathfrak{p}^j/\mathfrak{p}^\alpha$, avec $j \in \{1, \ldots, \alpha - 1\}$. Fixons $j$ et choisissons $x_j$ dans $\mathfrak{p}^j \backslash \mathfrak{p}^{j+1}$. On a alors $(x_j) + \mathfrak{p}^\alpha = \mathfrak{p}^j$ (c'est le pgcd de $(x_j)$ et $\mathfrak{p}^\alpha$). L'idéal $\mathfrak{p}^j/\mathfrak{p}^\alpha$ est alors engendré par la classe de $x_j$ et est principal.

L'idéal $I/J$ est alors principal. Soit $a \in I$ dont la classe modulo $J$ engendre $I/J$. Vérifions que $I = (a_1, a)$. Si $x \in I$, la classe de $x$ dans $I/J$ est multiple de la classe de $a$. En remontant dans $J = (a_1)$, on obtient $x \in (a_1, a)$. L'autre inclusion est évidente. □

## 4.2 Norme d'un élément, d'un idéal

On définit la notion de norme d'un élément d'un corps de nombres, puis celle de norme d'un idéal d'un anneau d'entiers d'un corps de nombres.

**Définition 4.13.** *Soit $K$ une extension de $\mathbb{Q}$ de degré fini $n$. L'espace $K$ est un $\mathbb{Q}$-espace vectoriel de dimension finie, et pour $x \in K$, l'opération $m_x$ de multiplication par $x$ est un endormorphisme de $K$. On définit la* ***norme*** *de $x$, notée $N(x)$, comme étant le déterminant de cet endomorphisme.*

**Proposition 4.14.** *Si $x$ est un élément non nul de $\mathcal{O}_K$, alors $|N(x)| = \mathrm{card}(\mathcal{O}_K/(x))$.*

*Démonstration.* $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $n$ (voir [Mar77], corollaire du théorème 9), et $(x)$ est un sous-$\mathbb{Z}$-module de $\mathcal{O}_K$. On peut donc trouver, par le théorème de la base adaptée une base $(e_1, \ldots, e_n)$ et des entiers $d_1, \ldots, d_n$ tels que $(d_1 e_1, \ldots, d_n e_n)$

soit une base de $(x)$. Le quotient $\mathcal{O}_K/(x)$ est alors isomorphe à $\bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z}$, donc est de cardinal $d_1 \dots d_n$.

Or, $(xe_1, \dots, xe_n)$ est aussi une base de $(x)$. On note $u$ le morphisme de $\mathbb{Z}$-modules de $\mathcal{O}_K$ sur $(x)$ défini par $u(e_i) = d_i e_i$ et $v$ celui de $(x)$ dans $(x)$ tel que $v(d_i e_i) = xe_i$. Comme $v$ envoie une base sur une base, $v$ est de déterminant 1 ou $-1$. Mais $v \circ u$ est la multiplication par $x$, et en prenant le déterminant, on obtient $|d_1 \dots d_n| = |N(x)|$. □

**Définition 4.15.** *Soit $I$ un idéal non nul de $\mathcal{O}_K$. On définit la **norme** de l'idéal $I$ comme la cardinal du quotient $\mathcal{O}_K/I$.*

La proposition précédente montre alors que la norme d'un idéal principal est égale à la norme de n'importe lequel de ses générateurs.

**Proposition 4.16.** *Soient $I$ et $J$ deux idéaux de $\mathcal{O}_K$. Alors $N(IJ) = N(I)N(J)$.*

*Démonstration.* Par la proposition 4.10, il suffit de traiter le cas de $I$ idéal et $\mathfrak{p}$ idéal premier. Comme $I\mathfrak{p} \subseteq I$, on a $\mathrm{card}(\mathcal{O}_K/I\mathfrak{p}) = \mathrm{card}(\mathcal{O}_K/I)\,\mathrm{card}(I/I\mathfrak{p})$. Il ne reste alors qu'à voir que $\mathrm{card}(I/I\mathfrak{p}) = \mathrm{card}(\mathcal{O}_K/\mathfrak{p})$.

Or $I/I\mathfrak{p}$ est un $\mathcal{O}_K/\mathfrak{p}$-espace vectoriel et ses sous-espaces vectoriels sont les $L/I\mathfrak{p}$ avec $I\mathfrak{p} \subseteq L \subseteq I$. Mais il n'y a aucun idéal strictement compris entre $I\mathfrak{p}$ et $I$ et l'espace vectoriel $I/I\mathfrak{p}$ est de dimension 1 sur $\mathcal{O}_K/\mathfrak{p}$, et le résultat est prouvé. □

## 4.3 Modules projectifs

On définit tout d'abord la notion de module projectif, pour ensuite donner un théorème de structure des modules projectifs de type fini sur un anneau de Dedekind.

**Définition 4.17.** *Soit $A$ un anneau. On dit qu'un $A$-module $P$ est projectif si pour tout $A$-modules $M$ et $M'$, tout morphisme $g$ surjectif de $M$ sur $M'$ et tout morphisme $f$ de $P$ dans $M'$, il existe un morphisme $h$ de $P$ dans $M$ tel que le diagramme suivant commute*

$$\begin{array}{ccccc} & & & & P \\ & & \swarrow^{h} & \downarrow{\scriptstyle f} & \\ M & \xrightarrow{g} & M' & \longrightarrow & 0 \end{array}$$

Donnons tout d'abord des exemples de modules projectifs.

**Proposition 4.18.** *Soit $(P_a)_a$ une famille de $A$-modules. Alors $P = \bigoplus_a P_a$ est projectif si et seulement si pour tout $a$, $P_a$ est projectif.*

*Démonstration.* Supposons $P_a$ projectif pour tout $a$. On se donne le diagramme suivant :

$$\begin{array}{ccccc} & & & & P \\ & & & \downarrow{\scriptstyle f} & \\ M & \xrightarrow{g} & M' & \longrightarrow & 0 \end{array}$$

On note $i_a$ l'injection canonique de $P_a$ dans $P$. En posant $f_a = f \circ i_a$, il existe $h_a$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccc} & & P_a & & \\ & \swarrow^{h_a} & \downarrow{\scriptstyle f_a} & & \\ M & \xrightarrow{g} & M' & \longrightarrow & 0 \end{array}$$

On pose alors $h = \bigoplus_a h_a$, ce qui permet de conclure quant à la projectivité de $P$.

Réciproquement, on suppose $P$ projectif. On se donne le diagramme suivant :

$$\begin{array}{ccccc} & & P_a & & \\ & & \downarrow{\scriptstyle f_a} & & \\ M & \xrightarrow{g} & M' & \longrightarrow & 0 \end{array}$$

On note $\pi_a$ la projection canonique de $P$ dans $P_a$. En posant $f = f_a \circ \pi_a$, il existe $h$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{h} & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & M' & \longrightarrow & 0 \end{array}$$

On pose alors $h_a = h \circ i_a$, ce qui permet de conclure quant à la projectivité de $P_a$. □

**Proposition 4.19.** *Tout module libre est projectif.*

*Démonstration.* Par la propriété 4.18, il suffit de montrer que $A$ est projectif. Soient $M$ et $M'$ deux $A$-modules, $g\colon M \to M'$ un morphisme surjectif et $f\colon A \to M'$ un morphisme. Par surjectivité de $g$, il existe $m \in M$ tel que $f(1) = g(m)$. $h\colon \left\{ \begin{array}{ccc} A & \longrightarrow & M \\ a & \longmapsto & am \end{array} \right.$ convient alors. □

**Proposition 4.20.** *Les propriétés suivantes sont équivalentes.*

1. *$P$ est projectif.*
2. *Si $M$ et $M'$ sont deux $A$-modules, toute suite exacte de la forme $0 \to M \to M' \to P \to 0$ est scindée.*
3. *il existe un $A$-module $S$ tel que $P \oplus S$ soit libre.*

*Démonstration.* $1 \Rightarrow 2$ : On se donne une suite exacte $0 \to M \to M' \to P \to 0$, on note $g\colon M' \to P$ le morphisme surjectif de cette suite. On considère :

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle id} & & \\ M' & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

Ceci nous donne une section par hypothèse.

$2 \Rightarrow 3$ : Il existe $F$ libre tel que $F \to P \to 0$ soit exacte (prendre pour $F$ un module libre de base une famille génératrice de $P$). De là, on dispose de la suite exacte $0 \to S \to F \to P \to 0$, qui est donc scindée. On en déduit $F = P \oplus S$.

$3 \Rightarrow 1$ : On suppose $F = P \oplus S$ avec $F$ libre. $F$ est alors projectif par 4.19 et $P$ aussi par 4.18. □

On s'intéresse maintenant aux anneaux de Dedekind et aux modules projectifs de type fini. On montre le théorème suivant :

**Théorème 4.21** (Modules projectifs de type fini)**.** *Soit $M$ un module projectif de type fini sur un anneau de Dedekind. Il existe alors un idéal $I$, unique à isomorphisme près, et un entier $n$, également unique tel que :*

$$M \simeq A^{n-1} \oplus I$$

Ce premier lemme justifie la présence d'un seul idéal dans le théorème 4.21.

**Lemme 4.22** (Somme directe d'idéaux fractionnaires)**.** *Soient $I$ et $J$ deux idéaux fractionnaires d'un anneau de Dedekind $A$. Alors $I \oplus J \simeq A \oplus IJ$.*

*Ainsi, si $I_1, \dots, I_n$ sont des idéaux fractionnaires, $\bigoplus_{i=1}^{n} I_i \simeq A^{n-1} \oplus I_1 \dots I_n$.*

*Démonstration.* On traite d'abord le cas où $I + J = A$. On considère $\pi : \begin{cases} I \oplus J & \longrightarrow & A \\ (i,j) & \longmapsto & i+j \end{cases}$. Le morphisme $\pi$ est d'image $A$ et de noyau $I \cap J = IJ$. On a alors la suite exacte $0 \to IJ \to I \oplus J \to A \to 0$ qui est scindée car $A$ est projectif. Donc $I \oplus J \simeq A \oplus IJ$.

On va alors se ramener au cas où $I + J = A$ en multipliant $I$ et $J$ par des éléments bien choisis de $K$. On peut supposer $I$ et $J$ idéaux de $A$ quitte à les multiplier par un élément de $A$. Par la proposition 4.10, on peut écrire $I = \prod \mathfrak{p}_i^{r_i}$ et $J = \prod \mathfrak{p}_i^{r'_i}$ avec des puissances positives ou nulles.

On cherche maintenant $a \in A$ tel que l' ordre de $\mathfrak{p}_i$ dans la décomposition de $(a)$ soit exactement $r_i$. Pour cela, choisissons $x_i \in \mathfrak{p}_i^{r_i+1} \backslash \mathfrak{p}_i^{r_i}$ (on a une inclusion stricte grâce à la loi de simplification, $\mathfrak{p}_i$ étant un idéal propre de $A$). Le théorème des restes chinois assure alors l'existence de $a$ avec $a \equiv x_i \ [\mathfrak{p}_i^{r_i+1}]$.

Maintenant, soit $L$ un idéal propre de $A$ tel que $IL = (a)$ (on complète la décomposition de $I$ pour obtenir celle de $(a)$). Les facteurs premiers de $L$ sont alors distincts des $\mathfrak{p}_i$ par le choix de $a$. On fait de même en choisissant un idéal $L'$ de $A$, et un élément $b \in A$ tels que $LL' = (b)$ et les facteurs premiers de $L'$ soient distincts de ceux de $L$ et des $\mathfrak{p}_i$. Ainsi $L'$ est premier avec $J$ par construction et $\frac{b}{a} I = LL' I I^{-1} L^{-1} = L'$. De là, $I \simeq L'$ et $L' + J = A$ : on est ramené au cas précédent. □

Ce second lemme donne l'existence et l'intérêt de l'étude des modules projectifs sur les anneaux de Dedekind. On verra en effet par la suite qu'un module de type fini est somme directe de sa composante de torsion et de sa composante sans torsion.

**Lemme 4.23.** *Soit $M$ un $A$-module de type fini non nul. Le module $M$ est projectif si et seulement s'il est sans torsion.*

*Par suite, si $n = \dim(M \otimes_A K) = \mathrm{rang}(M)$, il existe un idéal $I$ de $A$ tel que $M \simeq A^{n-1} \oplus I$.*

*Démonstration.* Supposons tout d'abord $M$ projectif. Il existe alors un $A$-module $S$ tel que $M \oplus S$ soit libre. Comme un module libre est sans torsion, $M$ est sans torsion aussi.

Réciproquement, supposons $M$ sans torsion. On fait une récurrence sur $n = \mathrm{rang}(M) = \dim(M \otimes_A K)$. Si $n = 1$, $M$ est un sous-A-module de type fini de $M \otimes_A K \simeq K$ et c'est alors un idéal fractionnaire de $A$. Soit $J$ idéal fractionnaire de $A$ donné par la proposition 4.4 tel que $IJ$ soit principal. On a alors $I \oplus J \simeq A \oplus IJ$ par le lemme 4.22. Le module $I \oplus J$ est ainsi libre, ce qui assure la projectivité de $I$.

Si $\mathrm{rang}(M) = n > 1$, on choisit $n-1$ éléments de $M$ engendrant un sous-espace vectoriel $V$ de $M \otimes_A K$ de dimension $n-1$. L'ensemble $N = \{m \in M / m \otimes 1 \in V\}$ est alors un sous-module de $M$ de rang $n-1$ (car $N \otimes_A K = V$) et de type fini. On dispose alors de la suite exacte

$$0 \to N \to M \to M/N \to 0$$

En la tensorisant par $K$, elle reste exacte. Or $M/N$ est de rang 1 et sans torsion, donc projectif. En effet, soit $x \in M$ et $a \in A \setminus \{0\}$ tel que $a\bar{x} = 0$. De là, $ax \in N$ et $x \in N$, ce qui montre que $\mathrm{Tor}(M/N) = \{0\}$. Ainsi cette suite exacte est scindée et $M = N \oplus M/N$ et on conclut par récurrence.

□

Il reste maintenant à voir l'unicité à isomorphisme près de l'idéal $I$ dans 4.21 pour terminer la classification de la partie sans torsion d'un module de type fini.

**Lemme 4.24.** *Si $A^{n-1} \oplus I \simeq A^{m-1} \oplus J$ alors $n = m$ et $I \simeq J$.*

*Démonstration.* Tout d'abord, $I \otimes_A K \simeq J \otimes_A K \simeq K$. Ainsi, en tensorisant $A^{n-1} \oplus I \simeq A^{m-1} \oplus J$ par $K$, on obtient $K^n \simeq K^m$ et alors $n = m$.

On prend maintenant la $n$-ième puissance extérieure de $A^{n-1} \oplus I \simeq A^{m-1} \oplus J$, c'est-à-dire $\bigwedge^n (A^{n-1} \oplus I) \simeq \bigwedge^n (A^{n-1} \oplus J)$. Ainsi on obtient :

$$\bigoplus_{p+q=n} \left( \bigwedge^p \left( A^{n-1} \right) \otimes \bigwedge^q (I) \right) \simeq \bigoplus_{p+q=n} \left( \bigwedge^p \left( A^{n-1} \right) \otimes \bigwedge^q (J) \right)$$

On utilise maintenant la proposition 4.12 pour simplifier cet isomorphisme. En effet, $\bigwedge^k I = 0$ pour $k \geq 3$. Il reste alors $I \oplus \left( \bigwedge^2 I \right)^{n-1} \simeq J \oplus \left( \bigwedge^2 J \right)^{n-1}$. Comme $I$ et $J$ sont engendrés par au plus deux éléments, les modules $\bigwedge^2 I$ et $\bigwedge^2 J$ sont donc de torsion alors que $I$ et $J$ sont sans torsion. En comparant les parties sans torsion, on obtient donc $I \simeq J$. □

Ceci termine la caractérisation des modules projectif de type fini sur un anneau de Dedekind.

## 4.4 Modules de type fini sur un anneau de Dedekind

On s'intéresse maintenant au théorème de structure des modules de type fini sur un anneau de Dedekind.

**Théorème 4.25.** *Soit $M$ un $A$-module de type fini non nul, $A$ étant un anneau de Dedekind. Il existe alors un unique entier $n \in \mathbb{N}$, un idéal $I$ non nul, unique à isomorphisme près, des idéaux premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_q$ uniques et des entiers $\alpha_1, \dots, \alpha_q$ uniques tels que :*

$$M \simeq \underbrace{A^{n-1} \oplus I}_{\text{sans torsion}} \oplus \underbrace{\bigoplus_{i=1}^{q} A/\mathfrak{p}_i^{\alpha_i}}_{\text{torsion}}$$

Si $M$ est un module sur un anneau de Dedekind et $\mathrm{Tor}(M)$ son module de torsion, la suite exacte $0 \to \mathrm{Tor}(M) \to M \to M/\mathrm{Tor}(M) \to 0$ est scindée ($M/\mathrm{Tor}(M)$ est sans torsion donc projectif par le lemme 4.23), ce qui assure que $M = \mathrm{Tor}(M) \oplus M/\mathrm{Tor}(M)$. Il ne reste alors qu'à étudier la partie de torsion pour démontrer le théorème 4.25.

Pour cela, on se ramène à étudier les modules sur $A/\mathfrak{p}^\alpha$, $\mathfrak{p}$ étant un idéal premier de $A$. En effet, si $M$ est un module de torsion de type fini, on note $\mathrm{Ann}(M) = \{a \in A \mid aM = 0\}$. Le fait que $M$ est de type fini assure que $\mathrm{Ann}(M)$ est un idéal non nul de $A$. On voit alors $M$ comme un $A/\mathrm{Ann}(M)$ module. En utilisant la proposition 4.10, on écrit $\mathrm{Ann}(M) = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_n^{\alpha_n}$ et on a alors, par le théorème des restes chinois :

$$M \simeq M/\mathrm{Ann}(M)M \simeq \bigoplus_{i=1}^{n} M/\mathfrak{p}_i^{\alpha_i} M$$

On étudie alors les $M/\mathfrak{p}_i^{\alpha_i}M$ qui sont des $A/\mathfrak{p}_i^{\alpha_i}$ modules.

**Lemme 4.26.** *Soit $\mathfrak{p}$ un idéal premier non nul d'un anneau de Dedekind $A$ et $\alpha \in \mathbb{N}^*$. Soit $M$ un module de type fini sur $A/\mathfrak{p}^\alpha$. Il existe alors des entiers uniques $a_1, \dots, a_n$ tels que :*

$$M \simeq \bigoplus_{i=1}^{\alpha} \left(A/\mathfrak{p}^i\right)^{a_i}$$

*Démonstration.* On fait une récurrence sur $\alpha$, le cas $\alpha = 1$ étant clair car $M$ est alors un $A/\mathfrak{p}$-espace vectoriel de dimension finie et est alors somme directe de $A/\mathfrak{p}$ (rappelons que $A$ étant de Dedekind, $\mathfrak{p}$ est maximal et donc $A/\mathfrak{p}$ est un corps).

On suppose maintenant $\alpha \geq 2$. On choisit $y_1, \dots, y_n$ une famille libre maximale de $M$, ce qui est possible car le module $M$ est de type fini. On considère alors le $A/\mathfrak{p}^{\alpha-1}$ module $M' = M/\left(y_1 A/\mathfrak{p}^\alpha \oplus \dots \oplus y_n A/\mathfrak{p}^\alpha\right)$. Par hypothèse de récurrence, on peut écrire $M' \simeq \bigoplus_{i=1}^{\alpha-1} \left(A/\mathfrak{p}^i\right)^{a_i}$ et on dispose de la suite exacte :

$$0 \to y_1 A/\mathfrak{p}^\alpha \oplus \dots \oplus y_n A/\mathfrak{p}^\alpha \to M \to \bigoplus_{i=1}^{\alpha-1} \left(A/\mathfrak{p}^i\right)^{a_i} \to 0$$

Vérifions que cette suite est scindée. On considère un facteur premier $M'' = A/\mathfrak{p}^m$ de $M'$ et $x \in M$ dont la projection dans $M''$ vaut 1. On choisit alors $\beta \in (\mathfrak{p}^m/\mathfrak{p}^\alpha) \setminus (\mathfrak{p}^{m+1}/\mathfrak{p}^\alpha)$. L'élément $\beta x$ est alors de $\mathfrak{p}^{r-m}$ torsion et est aussi dans $y_1 A/\mathfrak{p}^\alpha \oplus \ldots \oplus y_n A/\mathfrak{p}^\alpha$. Il existe alors $y \in y_1 A/\mathfrak{p}^\alpha \oplus \ldots \oplus y_n A/\mathfrak{p}^\alpha$ tel que $\beta(x-y) = 0$. En posant $z = x - y$, on dispose d'un élément tel que $\beta z = 0$ et $\mathfrak{p}^\alpha z = 0$. C'est alors un élément de $(\beta) + \mathfrak{p}^\alpha = \mathfrak{p}^m$-torsion et il existe ainsi un morphisme $g\colon M'' \to M$ avec $g(1) = z$. En sommant sur tous les facteurs directs, on scinde alors la suite exacte, et ainsi :

$$M \simeq \bigoplus_{i=1}^{\alpha-1} \left(A/\mathfrak{p}^i\right)^{a_i} \oplus (A\mathfrak{p}^\alpha)^n$$

Passons maintenant à l'unicité. Si $M \simeq \bigoplus_i (A/\mathfrak{p}^i)^{a_i}$ alors la dimension du $A/\mathfrak{p}$-espace vectoriel $\mathfrak{p}^j M/\mathfrak{p}^{j+1}M$ est $\sum_{i \geq j+1} a_i$ (cette somme est finie car $M$ est de type fini) et on a donc unicité des $a_i$. □

Ceci permet d'achever la démonstration du théorème de classification des modules de type fini sur des anneaux de Dedekind.

## 4.5 Un invariant sur les modules de type fini

Grâce au théorème 4.25, pour tout module $M$ de type fini on dispose d'un élément de $\mathcal{C}l(A)$ qui ne dépend que du module. Cette partie reprend la preuve de la partie 3.2 de [IH10].

**Définition 4.27** (Invariant de Steinitz)**.** *Soit $A$ un anneau de Dedekind et $M$ un $A$-module de type fini non nul. On peut alors écrire :*

$$M \simeq A^{n-1} \oplus I \oplus \bigoplus_{i=1}^{q} A/\mathfrak{p}_i^{\alpha_i}$$

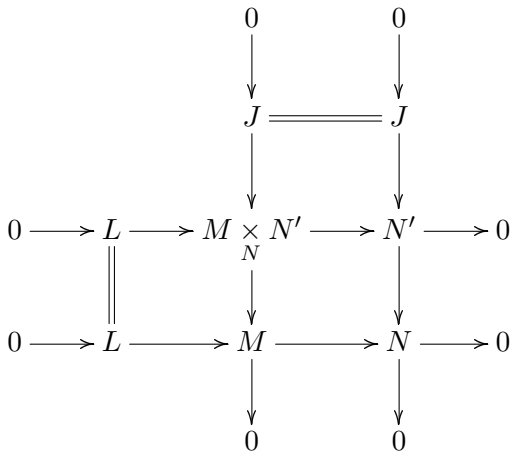
*On définit alors l'invariant de Steinitz par :* $\mathrm{St}(M) = [I][\mathfrak{p}_1]^{-\alpha_1} \ldots [\mathfrak{p}_q]^{-\alpha_q}$.

Il est clair, par unicité dans le théorème 4.25 et grâce au lemme 4.22 que l'invariant de Steinitz se comporte bien vis-à-vis de la somme directe : $\mathrm{St}(M \oplus M') = \mathrm{St}(M)\,\mathrm{St}(M')$. Mais il se comporte également bien vis-à-vis des suites exactes.

**Proposition 4.28.** *Soit $0 \to L \to M \to N \to 0$ une suite exacte de $A$-modules de type fini. Alors* $\mathrm{St}(M) = \mathrm{St}(L)\,\mathrm{St}(N)$.

*Démonstration.* Le théorème 4.25 permet d'écrire $N \simeq A^{n-1} \oplus I \oplus \bigoplus_{i=1}^{q} A/\mathfrak{p}_i^{r_i}$. On pose $N' = A^{n-1} \oplus I \oplus A$ et $J = \prod_{i=1}^{q} \mathfrak{p}_i^{r_i}$. Par définition de l'invariant de Steinitz, on a $\mathrm{St}(N') =$

$\mathrm{St}(N)\,\mathrm{St}(J)$. On considère alors le diagramme suivant :



le terme $M \underset{N}{\times} N'$ étant le produit fibré de $M$ et $N'$ au-dessus de $N$. Ce diagramme est commutatif, et comme $N'$ est sans torsion, il est projectif. La suite $0 \to L \to M \underset{N}{\times} N' \to N' \to 0$ est alors scindée et $M \underset{N}{\times} N' \simeq L \oplus N'$. De là, $\mathrm{St}(M \underset{N}{\times} N') = \mathrm{St}(L)\,\mathrm{St}(N')$. Ainsi $\mathrm{St}(M \underset{N}{\times} N') = \mathrm{St}(L)\,\mathrm{St}(N)\,\mathrm{St}(J)$ et il reste à vérifier que $\mathrm{St}(M \underset{N}{\times} N') = \mathrm{St}(J)\,\mathrm{St}(M)$.

Traitons d'abord le cas où $M$ est projectif. La suite exacte $0 \to J \to M \underset{N}{\times} N' \to M \to 0$ est alors scindée et $M \underset{N}{\times} N' \simeq M \oplus J$. On a bien $\mathrm{St}(M \underset{N}{\times} N') = \mathrm{St}(J)\,\mathrm{St}(M)$ et la proposition est montrée dans le cas où $M$ est projectif.

Maintenant, supposons $L$ projectif. Comme $M \underset{N}{\times} N' \simeq L \oplus N'$, $M \underset{N}{\times} N'$ est sans torsion. On peut donc appliquer le cas précédent à la suite exacte $0 \to J \to M \underset{N}{\times} N' \to M \to 0$. On obtient alors $\mathrm{St}(M \underset{N}{\times} N') = \mathrm{St}(J)\,\mathrm{St}(M)$ et le théorème est montré quand $L$ est projectif.

Revenons finalement au cas général. On applique la cas précédent à la suite exacte $0 \to J \to M \underset{N}{\times} N' \to M \to 0$ car $J$ est toujours sans torsion donc projectif. On a donc $\mathrm{St}(M \underset{N}{\times} N') = \mathrm{St}(J)\,\mathrm{St}(M)$ ce qui permet de conclure en toute généralité. □

On utilisera par la suite cet invariant afin de montrer la non intégralité de la représentation irréductible de dimension 2 des quaternions sur $\mathbb{Q}[i\sqrt{35}]$.

## 5 Un exemple de représentation non intégrale

Soit $K$ un corps de nombres, c'est-à-dire une extension finie de $\mathbb{Q}$. On se donne une représentation d'un groupe $G$ sur le corps $K$. On note $\mathcal{O}_K$ l'anneau des entiers algébriques de $K$.

**Définition 5.1.** *Soit $V$ un $K$-espace vectoriel. Soit $\Lambda$ un sous-$\mathcal{O}_K$-module de $V$. On dit que $\Lambda$ est un réseau de $V$ si $\Lambda \otimes_{\mathcal{O}_K} K = V$.*

On s'intéresse au problème d'intégralité d'une représentation $V$ d'un groupe fini $G$, réalisable sur un corps $K$. On essaie d'écrire les matrices définissant la représentation sur l'anneau $\mathcal{O}_K$ des entiers algébriques de $K$. Si on arrive à faire ceci, on dispose alors d'une famille libre de $V$ qui génère un réseau $G$-invariant de $V$, l'action de $G$ sur ce réseau étant donné par les matrices à coefficients dans $\mathcal{O}_K$. On peut alors voir la représentation comme un réseau libre de $V$. Ceci motive alors la définition suivante :

**Définition 5.2.** *Soient $G$ un groupe et $V$ représentation de $G$ sur $K$.*
*On dit que la représentation $(V, \rho)$ est intégrale sur $K$ s'il existe un réseau libre de $V$ stable sous l'action de $G$.*

On étudie alors l'intégralité ou la non-intégralité de la représentation $V$ sur $K$.

On se rend tout d'abord compte qu'il existe effectivement des $\mathcal{O}_K$-modules de type fini stables sous l'action de $G$. En effet, si $V$ est une représentation de $G$ sur $K$, on se donne une base $e_1, \dots, e_n$ de $V$ et on considère le module $\Lambda$ engendré sur $\mathcal{O}_K$ par la famille $(g \cdot e_i)_{g \in G, 1 \leq i \leq n}$.

Si l'anneau des entiers $\mathcal{O}_K$ est principal, alors le théorème de structure des modules de type fini sur les anneaux principaux permet de conclure, car un tel module est sans torsion. Mais $\mathcal{O}_K$ n'est pas en général un anneau principal, et ce n'est pas le cas quand $K = \mathbb{Q}[i\sqrt{35}]$. Par contre, c'est toujours un anneau de Dedekind (voir [Mar77] théorème 14 ou [Sam67] théorème 1 du paragraphe 3.4) et le théorème 4.25 permet de voir l'obstruction à la liberté du module.

Maintenant, on s'intéresse au cas particulier du groupe quaternionique $Q$ et de sa représentation irréductible de dimension 2. On a vu au théorème 3.10 que cette représentation est réalisable sur les corps quadratiques $\mathbb{Q}[i\sqrt{d}]$ quand $d$ est somme de 3 carrés. On va montrer le résultat suivant :

**Théorème 5.3.** *Soit $K = \mathbb{Q}[i\sqrt{35}]$. La représentation irréductible de dimension 2 du groupe quaternionique n'est pas intégrale sur $K$.*

On commence par calculer l'anneau des entiers de $\mathbb{Q}[i\sqrt{35}]$ et la norme d'un élément.

**Proposition 5.4.** *L'anneau des entiers de $\mathbb{Q}[i\sqrt{35}]$ est $\mathbb{Z}\left[\frac{1+i\sqrt{35}}{2}\right]$.*

*Démonstration.* Soit $x = r + si\sqrt{35}$. L'élément $x$ de $\mathbb{Q}[i\sqrt{35}]$ est un entier algébrique si et seulement si son polynôme minimal est à coefficients dans $\mathbb{Z}$ (voir [Mar77], théorème 1). Le polynôme minimal de $x$ est

$$P(X) = X^2 - 2rX + r^2 + 35s^2$$

On exige donc :

$$2r \in \mathbb{Z},\ r^2 + 35s^2 \in \mathbb{Z}$$

On distingue alors deux cas :

- Ou bien $r \in \mathbb{Z}$. Alors, comme 35 ne contient pas de facteur carré, $s$ est nécessairement dans $\mathbb{Z}$ aussi.

– Ou bien $r = R + \frac{1}{2}, R \in \mathbb{Z}$. Alors la seconde condition équivaut à $\frac{1}{4} + 35\frac{p^2}{q^2} \in \mathbb{Z}$, où $\frac{p}{q}$ est la forme irréductible du rationnel $s$ (avec $q \in \mathbb{N}^*$).

Dans ce cas, on a en particulier $4(\frac{1}{4} + 35\frac{p^2}{q^2}) \in \mathbb{Z}$. Par choix de $p$ et $q$, $q^2$ n'a pas de facteur commun avec $p^2$. Il n'en a pas non plus avec 35, qui n'a pas de facteur carré.

On en déduit donc que $q^2 \mid 4$. Comme $s \notin \mathbb{Z}$, $q \neq 1$, donc $q = 2$.

Ces deux situations peuvent être synthétisées sous la forme

$$x = a + b\frac{1 + i\sqrt{35}}{2}, a, b \in \mathbb{Z}$$

Réciproquement, on vérifie que le polynôme $(X - a - \frac{b}{2})^2 + 35\frac{b^2}{4}$ est bien à coefficients dans $\mathbb{Z}$ et annulateur de $x = a + b\frac{1+i\sqrt{35}}{2}$, quelques soient $a$ et $b$ dans $\mathbb{Z}$. □

**Proposition 5.5.** *Soit $x = a + ib\sqrt{35} \in \mathbb{Q}[i\sqrt{35}]$. Alors $N(x) = a^2 + 35b^2$.*

*Démonstration.* Dans la base $(1, i\sqrt{35})$, la matrice de la multiplication par $x$ est :

$$\begin{pmatrix} a & -35b \\ b & a \end{pmatrix}$$

Son déterminant est $N(x) = a^2 + 35b^2$. □

La preuve du théorème 5.3 repose sur le lemme suivant, et sur un calcul explicite pour un réseau particulier.

**Proposition 5.6.** *Soit $\Lambda$ un réseau $Q$-invariant de la représentation irréductible de dimension 2. Alors* $\mathrm{St}(\Lambda)$ *dans $\mathcal{C}l(\mathcal{O}_K)/\mathcal{C}l(\mathcal{O}_K)^2$ ne dépend pas du réseau $\Lambda$ choisi.*

La preuve se fait par récurrence grâce au lemme suivant :

**Lemme 5.7.** *Soient $\Lambda \subsetneq \Lambda'$ deux réseaux invariants sour l'action de la représentation de dimension 2 de $Q$. On est dans l'un des deux cas suivants :*
- *soit il existe un idéal $\mathfrak{p}$ premier tel que $\Lambda \subset \mathfrak{p}\Lambda' \subsetneq \Lambda'$.*
- *soit il existe un entier $r \geq 1$ tel que $\Lambda'/\Lambda \simeq \mathcal{O}_K/(2^r)$.*

On a tout d'abord besoin du lemme suivant, dont la preuve est un simple calcul.

**Lemme 5.8.** *L'idéal* $(2)$ *est premier dans $\mathbb{Z}\left[\frac{1+i\sqrt{35}}{2}\right]$*

*Démonstration.* Soient $a + b\frac{1+i\sqrt{35}}{2}$ et $c + d\frac{1+i\sqrt{35}}{2}$ dans $\mathbb{Z}\left[\frac{1+i\sqrt{35}}{2}\right]$. On a alors $a + b\frac{1+i\sqrt{35}}{2} \in (2)$ si et seulement si les entiers $a$ et $b$ sont pairs.

Calculons alors le produit de ces deux éléments :

$$\begin{aligned}\left(a + b\frac{1 + i\sqrt{35}}{2}\right)\left(c + d\frac{1 + i\sqrt{35}}{2}\right) &= ac + (bc + ad)\frac{1 + i\sqrt{35}}{2} + bd\left(\frac{1 + i\sqrt{35}}{2}\right)^2 \\ &= ac - 9bd + (bc + ad + bd)\frac{1 + i\sqrt{35}}{2}\end{aligned}$$

| $(c,d)$ \ $(a,b)$ | (0,0) | (0,1) | (1,0) | (1,1) |
|---|---|---|---|---|
| (0,0) | (0,0) | (0,0) | (0,0) | (0,0) |
| (0,1) | (0,0) | (1,1) | (0,1) | (1,0) |
| (1,0) | (0,0) | (0,1) | (1,0) | (1,1) |
| (1,1) | (0,0) | (1,0) | (1,1) | (0,1) |

TABLE 2: Valeurs de $(ac - 9bd, bc + ad + bd)$ modulo 2 en fonction de celles de $a, b, c, d$

On regarde alors modulo 2 et un calcul exhaustif effectué dans le tableau 2 permet de conclure.

□

*Démonstration de 5.7.* Soit $x \in V$. On note $\Lambda_x = \{y \in \Lambda \mid \exists \alpha \in K,\ y = \alpha x\}$ et $\Lambda'_x = \{y \in \Lambda' \mid \exists \alpha \in K,\ y = \alpha x\}$. Ils sont alors isomorphes à des idéaux de $\mathcal{O}_K$.

Comme $\Lambda \subsetneq \Lambda'$, quitte à choisir $x$ correctement, on peut supposer que $\Lambda_x \subsetneq \Lambda'_x$. On utilise alors la proposition 4.10 pour écrire :

$$\Lambda_x = \prod_i \mathfrak{p}_i^{r_i},\ \Lambda'_x = \prod_i \mathfrak{p}_i^{s_i}$$

La relation d'inclusion implique de plus que pour tout $i, s_i \leq r_i$, l'inclusion stricte assurant l'existence de $i_0$ tel que $s_{i_0} < r_{i_0}$. On a alors

$$\Lambda_x \subseteq \mathfrak{p}_{i_0} \Lambda'_x \subsetneq \Lambda'_x$$

On distingue alors deux cas.

- Ou bien il existe $x \in V$ et $\mathfrak{p}$ un idéal tels que $\Lambda_x \subseteq \mathfrak{p}\Lambda'_x \subsetneq \Lambda'_x$ et $\mathcal{O}_K/\mathfrak{p}$ est de caractéristique différente de 2. Alors $\Lambda'/\mathfrak{p}\Lambda'$ est un espace vectoriel su le corps $\mathcal{O}_K/\mathfrak{p}$, et constitue alors une représentation irréductible de $Q$. Comme la caractéristique de $\mathcal{O}_K/\mathfrak{p}$ est différente de 2, elle ne divise pas le cardinal de $Q$. Le théorème de Mashcke assure alors que cette représentation est celle de dimension 2 du groupe quaternionique (il suffit de regarder le caractère). Dans ce cas, $\Lambda/\mathfrak{p}\Lambda'$ étant une sous-représentation stricte de $\Lambda'/\mathfrak{p}\Lambda'$, elle est nécessairement nulle, et on a

  $$\Lambda \subset \mathfrak{p}\Lambda' \subsetneq \Lambda'$$

  On se trouve alors dans le premier cas.
- Ou bien, pour tout $x \in V$, pour tout idéal premier $\mathfrak{p}$ tel que $\Lambda_x \subseteq \mathfrak{p}\Lambda'_x \subsetneq \Lambda'_x$, le corps $\mathcal{O}_K/\mathfrak{p}$ est de caractéristique 2. Dans ce cas, nous allons montrer que l'idéal (2) convient. On a

  $$\Lambda'/\Lambda = \bigoplus_i \mathcal{O}_K/\mathfrak{p}_i^{r_i}$$

  où les $\mathcal{O}_K/\mathfrak{p}_i$ sont tous de caractéristique 2. En effet, soit $\mathfrak{p}_i$ l'un des idéaux premiers intervenant dans cette décomposition du quotient. Dans le quotient $\Lambda'/\Lambda$,

l'élément $y = (0, \dots, 1, 0, \dots, 0)$, où le 1 est en $i$-ème position, est de $\mathfrak{p}_i$-torsion. Un antécédent $x$ de $y$ dans $\Lambda'$ est de $\mathfrak{p}_i$-torsion dans $\Lambda'/\Lambda$. Il existe donc $x \in V$ tel que $\Lambda_x \subset \mathfrak{p}_i\Lambda'_x \subsetneq \Lambda'_x$. Par hypothèse, $\mathcal{O}_K/\mathfrak{p}_i$ est donc de caractéristique 2.
Autrement dit $(2) \subset \mathfrak{p}_i$, et ce pour tout $i$. Comme $(2)$ est premier dans l'anneau de Dedekind $\mathcal{O}_K$, $(2) = \mathfrak{p}_i$. Comme les $\mathfrak{p}_\mathfrak{i}$ sont distincts dans la décomposition, il existe $r \geq 1$ tel que :

$$\Lambda'/\Lambda \simeq \mathcal{O}_K/(2^r)$$

On se trouve alors dans le second cas.

□

*Démonstration de 5.6.* Soient $\Lambda$ et $\Lambda'$ deux réseaux $Q$-invariants. Comme ces réseaux sont de type finis, on peut trouver un entier $m$ tel que $m\Lambda \subseteq \Lambda'$. De plus, $\mathrm{St}(m\Lambda) = \mathrm{St}(\Lambda)$ et on peut alors supposer $\Lambda \subseteq \Lambda'$.

Maintenant, on remarque que le module quotient $\Lambda'/\Lambda$ est fini, ce qui permet de faire une récurrence sur son cardinal. Si $\Lambda' = \Lambda$, il n'y a rien à faire.

On suppose maintenant $\mathrm{card}(\Lambda'/\Lambda) > 1$. On applique alors la proposition 5.7.

– Si on se trouve dans le premier cas, soit $\mathfrak{p}$ premier tel que $\Lambda \subseteq \mathfrak{p}\Lambda' \subsetneq \Lambda'$. Comme $\mathrm{card}(\mathfrak{p}\Lambda'/\Lambda) < \mathrm{card}(\Lambda'/\Lambda)$, l'hypothèse de récurrence assure que $\mathrm{St}(\mathfrak{p}\Lambda') = \mathrm{St}(\Lambda)$ dans $\mathcal{C}l(\mathcal{O}_K)/\mathcal{C}l(\mathcal{O}_\mathcal{K})^2$. Il reste à voir que $\mathrm{St}(\mathfrak{p}\Lambda') = \mathrm{St}(\Lambda')$ dans $\mathcal{C}l(\mathcal{O}_K)/\mathcal{C}l(\mathcal{O}_\mathcal{K})^2$. Mais par le théorème 4.25, on peut écrire $\Lambda' \simeq A \oplus I$ et le lemme 4.22 assure que $\mathfrak{p}\Lambda' \simeq A \oplus \mathfrak{p}^2 I$ et donc $\mathrm{St}(\mathfrak{p}\Lambda) = [\mathfrak{p}]^2\,\mathrm{St}(\Lambda')$, ce qui permet de conclure dans ce cas.
– Si on se trouve dans le second cas, la proposition 4.28 appliqué à la suite exacte :

$$0 \to \Lambda \to \Lambda' \to \Lambda'/\Lambda \to 0$$

assure que $\mathrm{St}(\Lambda') = \mathrm{St}(\Lambda)\,\mathrm{St}(\Lambda'/\Lambda)$. Or il existe $r$ entier tel que $\Lambda'/\Lambda \simeq \mathcal{O}_K/(2^r)$ et ainsi $\mathrm{St}(\Lambda'/\Lambda) = \mathrm{St}(\mathcal{O}_K)\,\mathrm{St}((2^r))$ est trivial dans le groupe des classes d'idéaux. Donc $\mathrm{St}(\Lambda') = \mathrm{St}(\Lambda)$ dans $\mathcal{C}l(\mathcal{O}_K)$ donc en particulier dans $\mathcal{C}l(\mathcal{O}_K)/\mathcal{C}l(\mathcal{O}_K)^2$, ce qui permet de conclure dans ce cas.

Ainsi le résultat est prouvé par récurrence.

□

On effectue maintenant un calcul explicite de $\mathrm{St}(\Lambda)$ pour un certain réseau $\Lambda$, et on veut voir que ce n'est pas un carré dans $\mathcal{C}l(\mathcal{O}_K)$.

Calculons tout d'abord les matrices des éléments de $Q$ définissant l'action. Comme $35 = 5^2 + 3^2 + 1^2$, on obtient :

$$-1 = \left(\frac{5 + 3i\sqrt{35}}{34}\right)^2 + \left(\frac{3 - 5i\sqrt{35}}{34}\right)^2$$

Les calculs effectués dans la partie 3.4 donnent alors les matrices suivantes :

$$\rho(i) = \frac{1}{34}\begin{pmatrix} 5 + 3i\sqrt{35} & 3 - 5i\sqrt{35} \\ 3 - 5i\sqrt{35} & -5 - 3i\sqrt{35} \end{pmatrix}$$

$$\rho(k) = \frac{1}{34}\begin{pmatrix} 3 - 5i\sqrt{35} & -5 - 3i\sqrt{35} \\ -5 - 3i\sqrt{35} & -3 + 5i\sqrt{35} \end{pmatrix}$$

On considère alors le réseau $\Lambda$ engendré par le vecteur $\begin{pmatrix}17\\0\end{pmatrix}$ et ses conjugués par l'action de $G$ :

$$\Lambda = \left\langle e_1 = \begin{pmatrix}17\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\17\end{pmatrix}, e_3 = \begin{pmatrix}\frac{5+3i\sqrt{35}}{2}\\\frac{3-5i\sqrt{35}}{2}\end{pmatrix}, e_4 = \begin{pmatrix}\frac{3-5i\sqrt{35}}{2}\\\frac{-5-3i\sqrt{35}}{2}\end{pmatrix}\right\rangle$$

Mais un réseau est engendré par seulement trois vecteurs d'après le théorème 4.25 et la proposition 4.12. Dans notre cas :

$$e_4 - i\sqrt{35}e_3 = 3e_1 - 5e_2$$

Pour calculer $\mathrm{St}(\Lambda)$, on se ramène au calcul de l'invariant de Steinitz d'un idéal via la suite exacte suivante :

$$0 \to \mathcal{O}_K e_1 \oplus \mathcal{O}_K e_2 \to \Lambda \to \Lambda/\left(\mathcal{O}_K e_1 \oplus \mathcal{O}_K e_2\right) \simeq \mathcal{O}_K e_3/I \to 0$$

La proposition 4.28 donne alors $\mathrm{St}(\Lambda) = \mathrm{St}(\mathcal{O}_K e_3/I)\,\mathrm{St}(\mathcal{O}_K e_1 \oplus \mathcal{O}_K e_2) = \mathrm{St}(I)^{-1}$. Il ne reste plus qu'à calculer $\mathrm{St}(I)^{-1}$.

On note $\alpha = \frac{5+3i\sqrt{35}}{2}$ et $\beta = \frac{3-5i\sqrt{35}}{2}$. On a alors :

$$\begin{aligned} I &= \{x \in \mathcal{O}_K/17 | x\alpha \text{ et } 17|x\beta\} \\ &= (17)/((\beta) + (\alpha) + (17)) \end{aligned}$$

Les idéaux $(\alpha)$ et $(\beta)$ ne sont pas premiers car de norme respective $N(\alpha) = 5 \times 17$ et $N(\beta) = 13 \times 17$ qui ne sont pas des puissances de nombres premiers.

La proposition 4.10 et la multiplicativité de la norme donne alors des idéaux premiers $\alpha_5, \alpha_{17}, \beta_{13}, \beta_{17}$ de norme respective 5, 17, 13, 17 tels que :

$$\begin{aligned} (\alpha) &= \alpha_5\alpha_{17} \\ (\beta) &= \beta_{13}\beta_{17} \end{aligned}$$

L'idéal (17) est soit premier, soit produit de deux idéaux de norme 17. Or $\beta_{17} \supseteq (17)$ donc $\beta_{17}|(17)$ par le corollaire 4.11. Donc il existe un idéal premier $\mathfrak{p}$ de norme 17 tel que $(17) = \beta_{17}\mathfrak{p}$.

On pose $\mathfrak{p}'$ le pgcd de $(\beta)$ et de (17). Ainsi $\mathfrak{p}' = (17) + (\beta) = \beta_{17}(\beta_5 + \mathfrak{p})$. Or $\beta_5$ est de norme 5 et $\mathfrak{p}$ de norme 17. Ces deux idéaux sont alors premiers entre eux et $\mathfrak{p}' = \beta_{17}$. Mais on a la relation suivante :

$$\alpha = i\sqrt{35}\beta + 17 \times 5$$

ce qui assure que $(\alpha) \subseteq \beta_{17}$.

On a ainsi les décompositions suivantes :

$$(\alpha) = \beta_{17}\alpha_5,\ (\beta) = \beta_{17}\beta_{13},\ (17) = \beta_{17}\mathfrak{p}$$

ce qui donne $(\alpha) + (\beta) + (17) = \beta_{17}$.

Finalement, on obtient que $\mathrm{St}(\Lambda) = \mathrm{St}(\beta_{17})$ et il reste à montrer que $\beta_{17}$ n'est pas un carré dans $\mathcal{C}l(\mathcal{O}_K)$.

**Lemme 5.9.** *Soit $I$ un idéal de norme 17. Alors $I$ n'est pas un carré dans $\mathcal{O}_K$.*

*Démonstration.* Supposons $[I] = [J]^2$ dans $\mathcal{C}l(\mathcal{O}_K)$. Il existe alors $f$ et $g$ éléments de $\mathcal{O}_K$ tels que :

$$(f)I = (g)J^2$$

On a alors $17 = N(I) = N\left(\frac{f}{g}\right) N(J)^2$. Comme $N\left(\frac{f}{g}\right) = r^2 + 35s^2$ avec $r$ et $s$ rationnels, et comme $N(J)$ est un entier, on se ramène à résoudre l'équation diophantienne suivante :

$$17c^2 = a^2 + 35b^2, \ \text{pgcd}(a, b, c) = 1$$

La réduction modulo 5 donne alors $2c^2 \equiv a^2$ [5]. Si $c^2 \equiv 0$ [5] alors $c$ est divisible par 5 et $a$ également. Ainsi $a^2$ et $c^2$ sont divisible par 25 et $35b^2$ également. Ainsi 5 divise $b^2$ et alors 5 divise $a$, $b$ et $c$ qui sont premiers entre eux.

Donc $c^2$ est inversible modulo 5 et 2 est un carré modulo 5. Mais les carrés modulo 5 ne sont que 0, 1 et 4. Donc cette équation n'a pas de solution et $\mathfrak{p}$ n'est pas un carré dans $\mathcal{O}_K$ □

L'invariant de Steinitz de $\Lambda$ n'est donc pas trivial dans $\mathcal{C}l(\mathcal{O}_K)/\mathcal{C}l(\mathcal{O}_K)^2$ et ainsi aucun réseau ne peut être libre par la proposition 5.6. La représentation du groupe quaternionique n'est donc pas intégrale sur $\mathbb{Q}[i\sqrt{35}]$, ce qui démontre le théorème 5.3.

## Références


[Bra45] Richard Brauer : On the Representation of a Group of Order g in the Field of the g-Th Roots of Unity. *American Journal of Mathematics*, 67(4):pp. 461–471, 1945.

[CRW92] Gerald Cliff, Jürgen Ritter et Alfred Weiss : Group representation and integrality. *Journal für die reine und angewandte Mathematik*, 426, 1992.

[IH10] Diego Izquierdo et Yichao Huang : Le problème de Noether pour les groupes abéliens. 2010.

[Mar77] Daniel A. Marcus : *Number Fields.* Universitext (1979). Springer-Verlag, 1977.

[Sam67] Pierre Samuel : *Théorie algébrique des nombres.* Collection Méthodes. Hermann, 1967.

[Ser95] Jean-Pierre Serre : *Cours d'arithmétique.* PUF, 1995.

[Ser98] Jean-Pierre Serre : *Représentations linéaires des groupes finis.* Hermann, 1998.

[Ser06] Jean-Pierre Serre : Three letters to Walter Feit on group representations and quaternions. *Journal of Algebra*, 2006.