SIMILITUDE DE MATRICES ENTIÈRES ET IDÉAUX II

GRÉGORY BERHUY

Table des matières

1. Similitude de matrices entières et classe d'idéaux 1
2. Finitude du nombre de classes d'idéaux d'un ordre 9

1. Similitude de matrices entières et classe d'idéaux

Soit $f \in K[X]$ un polynôme irréductible de degré n, où K est un corps. La réduction de Frobenius nous dit qu'une matrice $M \in \mathrm{M}_n(K)$ telle que $\chi_M = \mu_M = f$ est semblable à une matrice compagnon.

En particulier, si f est irréductible, toute matrice $M \in \mathrm{M}_n(K)$ de polynôme caractéristique f est semblable à une matrice compagnon. En effet, puisque μ_f et χ_f ont mêmes diviseurs irréductibles et sont unitaires, on a nécessairement $\chi_f = \mu_f$ dans ce cas.

Si on remplace K par un anneau commutatif, le résultat devient faux, comme le montre l'exemple suivant.

Exemple 1.1. La matrice $M = \begin{pmatrix} 1 & -3 \\ 2 & -1 \end{pmatrix}$ est de polynôme caractéristique $X^2 + 5$, mais n'est pas semblable à la matrice compagnon associée à $X^2 + 5$, à savoir $C = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$.

En effet, supposons qu'il existe $P \in \mathrm{GL}_2(\mathbb{Z})$ telle que $PCP^{-1} = M$. En particulier, on a $PC = MP$. En écrivant $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on obtient un système linéaire, qui se réduit après quelques manipulations aux deux équations

$$b = a - 3c \quad \text{et} \quad d = 2a - c.$$

On a donc $P = \begin{pmatrix} a & a-3c \\ c & 2a-c \end{pmatrix}$, et donc

$$\det(P) = 2a^2 - 2ac + 3c^2 = a^2 + (a-c)^2 + 2c^2 \geq 0.$$

Date: 6 mars 2024.

Puisque $\det(P) = \pm 1$, on obtient $a^2 + (a-c)^2 + 2c^2 = 1$. En particulier, $1 \geq 2c^2$, et donc $c = 0$. Mais alors, $2a^2 = 1$, ce qui est impossible.

Le but de ce qui est suit est d'essayer de comprendre ce contre-exemple. Plus précisément, nous essayerons de répondre aux questions suivantes.

Étant donné un polynôme unitaire $f \in \mathbb{Z}[X]$:

(1) À quelles conditions une matrice $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_M = \mu_M = f$ est-elle semblable sur $\mathbb{Z}$ à C_f ?

(2) À quelles conditions toute matrice $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_M = \mu_M = f$ est-elle semblable sur $\mathbb{Z}$ à C_f ?

(3) Le nombre de classes de conjugaison de matrices $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_M = \mu_M = f$ est-il fini ou infini ?

Nous nous limiterons au cas où le polynôme caractéristique de M est irréductible, qui est déjà suffisamment compliqué, si bien que l'égalité $\chi_M = \mu_M$ est immédiate, et la condition précédente se récrit simplement $\chi_M = f$.

On se fixe donc un polynôme irréductible unitaire $f \in \mathbb{Z}[X]$ de degré n, et une racine $\alpha \in \mathbb{C}$ de f.

Lemme 1.2. *Soit $M \in \mathrm{M}_n(\mathbb{Z})$ une matrice de polynôme caractéristique f. Alors,*

α est une valeur propre simple de M^t, et il existe un vecteur propre $\mathbf{v}$ de M^t pour la valeur propre α dont les coordonnées sont dans $\mathbb{Q}(\alpha)$.

De plus, ce vecteur est unique à multiplication près par un élément de $\mathbb{Q}(\alpha)^n$.

Démonstration. Puisque $\chi_{M^t} = \chi_M = f$, α est une valeur propre complexe de M^t. Par définition, $M - \alpha I_n$ est une matrice de déterminant nul à coefficients dans $\mathbb{Q}(\alpha)$. La théorie des systèmes linéaires montre alors que le système $(M^t - \alpha)\mathbf{v}$ possède une solution non nulle dans $\mathbb{Q}(\alpha)^n$. Notons maintenant que toutes les racines complexes de f sont simples. En effet, comme f' est non nul de degré $< n$, et comme f est irréductible, f et f' sont premiers entre eux (les seuls diviseurs unitaires communs possibles étant 1 et f). Ainsi, le sous-espace propre de $\mathbb{C}^n$ associé à α est de dimension 1. En particulier, deux vecteurs propres dont les coordonnées sont dans $\mathbb{Q}(\alpha)$ sont proportionnels, avec un facteur de proportionnalité appartenant à $\mathbb{Q}(\alpha)$. $\square$

Notation. Si $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{Q}(\alpha)^n$ est un vecteur propre de M^t, on pose $I_{\mathbf{v}} = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$.

Ce groupe abélien jouit alors des propriétés suivantes.

Lemme 1.3. *On garde les notations précédentes. Alors :*

(1) *Pour tout vecteur propre* $\mathbf{v} \in \mathbb{Q}(\alpha)^n$ *de* M^t *pour la valeur propre* α*, on a* $\alpha I_{\mathbf{v}} \subset I_{\mathbf{v}}$*.*

En particulier, $I_{\mathbf{v}}$ *est un sous* $\mathbb{Z}[\alpha]$*-module de* $\mathbb{Q}(\alpha)$*.*

De plus, si $\mathbf{v} \in \mathbb{Z}[\alpha]^n$*,* $I_{\mathbf{v}}$ *est un idéal de* $\mathbb{Z}[\alpha]$*.*

(2) *Si* $\mathbf{v}, \mathbf{w} \in \mathbb{Q}(\alpha)^n$ *sont deux vecteurs propres de* M^t *pour la valeur propre* α *, alors il existe* $\lambda \in \mathbb{Q}(\alpha)^\times$ *tel que* $I_{\mathbf{v}} = \lambda I_{\mathbf{w}}$*.*

(3) *Pour tout vecteur propre* $\mathbf{v} \in \mathbb{Q}(\alpha)^n$ *de* M^t *pour la valeur propre* α*, il existe* $x \in \mathbb{Q}(\alpha)^\times$ *et un idéal* $\mathfrak{a}$ *de* $\mathbb{Z}[\alpha]$ *tels que* $I_{\mathbf{v}} = x\mathfrak{a}$*.*

Démonstration. Montrons (1).

Par choix de $\mathbf{v}$, on a $M^t\mathbf{v} = \alpha\mathbf{v}$, soit encore $\alpha\mathbf{v}^t = \mathbf{v}^t M$, ce qui se récrit

$$\alpha v_j = \sum_{i=1}^{n} a_{ij} v_i \quad \text{pour tout } j \in [\![1, n]\!] \,,$$

où $M = (a_{ij})_{i,j}$. En particulier, $\alpha v_j \in I_{\mathbf{v}}$ pour tout $j \in [\![1, n]\!]$. On en déduit aisément que $\alpha I_{\mathbf{v}} \subset I_{\mathbf{v}}$. Le reste est alors clair.

Le point (2) découle immédiatement du lemme précédent et de la définition de $I_{\mathbf{v}}$.

Montrons (3). Soit $\mathbf{w} \in \mathbb{Q}(\alpha)^n$ un vecteur propre de M^t pour la valeur propre α. Quitte à remplacer $\mathbf{w}$ par $m\mathbf{w}$ pour un entier $m \geq 1$ bien choisi, on peut suppose que $\mathbf{w} \in \mathbb{Z}[\alpha]^n$. Si maintenant $\mathbf{v} \in \mathbb{Q}(\alpha)^n$ est un vecteur propre arbitraire, le lemme précédent montre qu'il existe $\lambda \in \mathbb{Q}(\alpha)$ tel que $\mathbf{v} = \lambda\mathbf{w}$. On applique alors les deux points précédents pour conclure. □

Ce lemme permet donc d'associer à M un sous-module de type fini du $\mathbb{Z}[\alpha]$-module $\mathbb{Q}(\alpha)$ de la forme $x\mathfrak{a}$, où $\mathfrak{a}$ est un idéal de $\mathbb{Z}[\alpha]$, unique à multiplication par un élément non nul de $\mathbb{Q}(\alpha)$ près.

Ce type d'objet mérite un nom bien à lui.

Définition 1.4. Soit A un anneau intègre, de corps des fractions K. Un *idéal fractionnaire* de A est un sous-module de K de la forme $x\mathfrak{a}$, où $x \in K^\times$ et $\mathfrak{a}$ est un idéal de A.

Deux idéaux fractionnaires **non nuls** I_1 et I_2 de A seront dit *équivalents* s'il existe $\lambda \in K^\times$ tel que $I_1 = \lambda I_2$. La relation « être équivalents » définit une relation d'équivalence sur l'ensemble des idéaux fractionnaires non nuls de A.

La classe d'équivalence de I sera notée $[I]$, et l'ensemble quotient pour cette relation d'équivalence sera noté $\mathscr{C}\ell_0(A)$.

Exemples 1.5.

(1) Avec les notations précédentes, $I_{\mathbf{v}}$ est un idéal fractionnaire non nul de $\mathbb{Z}[\alpha]$.
(2) Tout idéal d'un anneau intègre A est un idéal fractionnaire de A.

Remarques 1.6. Soit A un anneau intègre. Alors :

(1) Si $I = \lambda\mathfrak{a}$, où $\lambda \in K^\times$ et $\mathfrak{a}$ est un idéal de A, alors $[I] = [A] \in \mathscr{C}\ell_0(A)$ si, et seulement si, $\mathfrak{a}$ est un idéal principal. En effet, si $\mathfrak{a}$ est principal, engendré par a, alors $I = \lambda aA$ et par conséquent, $[I] = [A]$. Réciproquement, supposons que $[I] = [A]$. Il existe donc $\mu \in K^\times$ tel que $\lambda\mathfrak{a} = \mu A$. On a donc $\mathfrak{a} = xA$, avec $x = \lambda\mu^{-1} \in K^\times$. Mais, $x \in xA = \mathfrak{a}$ et donc $\mathfrak{a}$ est principal, engendré par x.

   Ce qui précède montre alors que l'ensemble $\mathscr{C}\ell_0(A)$ est trivial (i.e réduit à $\{[A]\}$) si, et seulement si, A est un anneau principal.
(2) Si I et J sont deux idéaux fractionnaires de A, le A-module IJ engendré par les éléments de la forme $xy, x \in I, y \in J$ est encore un idéal fractionnaire de A. De plus, ce produit est associatif, commutatif, de neutre A. L'ensemble des idéaux fractionnaires non nuls de A, muni du produit, est alors un monoïde commutatif, de neutre A. Ce n'est en général pas un groupe.

   Il est facile de voir le produit est compatible avec la relation d'équivalence. Il induit alors une structure de monoïde commutatif sur $\mathscr{C}\ell_0(A)$, de neutre $[A]$. Là encore, ce n'est en général pas un groupe.

Lemme 1.7. *Soit $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_M = f$, et soit $\mathbf{v} \in \mathbb{Q}(\alpha)^n \in \setminus\{0\}$ tel que $M^t\mathbf{v} = \alpha\mathbf{v}$. La classe $[I_v] \in \mathscr{C}\ell_0(\mathbb{Z}[\alpha])$ ne dépend que de la classe de conjugaison de M.*

Démonstration. On a déjà constaté que $[I_{\mathbf{v}}]$ était indépendante du choix de $\mathbf{v}$. Soit $P \in \mathrm{GL}_n(\mathbb{Z})$. Nous allons montrer que les classes des idéaux fractionnaires associées à M et PMP^{-1} sont les mêmes.

Pour cela, remarquons que P^{-t} est alors inversible et à coefficients dans $\mathbb{Z}$. Mais alors, si $\mathbf{v} \in \mathbb{Q}(\alpha) \in \setminus\{0\}$ est un vecteur propre de M^t associé à α, alors $\mathbf{w} = P^{-t}\mathbf{v} \in \mathbb{Q}(\alpha) \in \setminus\{0\}$ et c'est un vecteur propre de $(PMP^{-1})^t = P^{-t}M^tP^t$ associé à α.

D'après le point précédent, la classe associé à PMP^{-1} est celle de $I_{\mathbf{w}}$. Par définition de $\mathbf{w}$, les coordonnées de $\mathbf{w}$ sont des combinaisons $\mathbb{Z}$-linéaires des coordonnées de $\mathbf{v}$. On a donc $I_{\mathbf{w}} \subset \mathbf{I}_{\mathbf{v}}$. Mais on a également $\mathbf{v} = P^t\mathbf{w}$. Le même raisonnement montre alors que $I_{\mathbf{v}} \subset I_{\mathbf{w}}$, d'où finalement $I_{\mathbf{v}} = I_{\mathbf{w}}$, ce qui suffit à conclure. $\square$

Exemple 1.8. Soit $M = C_f$. On vérifie alors aisément que $\mathbf{v} = \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}$ est un vecteur propre de M^t pour la valeur propre α. Ainsi, $I_{\mathbf{v}} = \mathbb{Z}[\alpha]$ et la classe d'idéal associée à la classe de conjugaison entière de C_f est la classe triviale dans $\mathscr{C}\ell_0(\mathbb{Z}[\alpha])$.

Nous avons déjà suffisamment d'outils pour comprendre le contre exemple du début.

Exemple 1.9. Soit $M = \begin{pmatrix} 1 & -3 \\ 2 & -1 \end{pmatrix}$. On a $\chi_M = X^2 + 5$, et on peut donc prendre $\alpha = i\sqrt{5}$. On vérifie que $\mathbf{v} = \begin{pmatrix} 2 \\ -1 + i\sqrt{5} \end{pmatrix}$ est un vecteur propre de M^t associé à α. On a $I_{\mathbf{v}} = 2\mathbb{Z} + (-1 + i\sqrt{5})\mathbb{Z}$.

Or, il est bien connu que cet idéal n'est pas principal (exercice). La classe $[I_{\mathbf{v}}]$ n'est donc pas triviale, d'après la remarque 1.6 (1). Or, l'exemple 1.8 montre que la classe de conjugaison de la matrice compagnon associée à $X^2 + 5$ est la classe triviale. Ainsi, M ne peut être conjuguée à une matrice compagnon.

Nous voulons maintenant aller en sens inverse, et associer une classe de conjugaison d'une matrice entière à une classe d'idéal.

Pour cela, il nous faut étudier de plus près les idéaux de $\mathbb{Z}[\alpha]$. Comme cela ne coûte pas plus cher, on va donner quelques résultats sur une classe plus générale d'anneaux.

Définition 1.10. Un *ordre* est un anneau intègre $\mathcal{O}$ qui est aussi un $\mathbb{Z}$-module libre de rang fini.

Exemple 1.11. Avec les notations précédentes, $\mathbb{Z}[\alpha]$ est un ordre, de $\mathbb{Z}$-base $(1, \alpha, \ldots, \alpha^{n-1})$.

Lemme 1.12. *Soit $\mathcal{O}$ un ordre, et soit $n \geq 1$ son rang sur $\mathbb{Z}$. Alors, tout idéal $\mathfrak{a}$ de $\mathcal{O}$ non nul est un $\mathbb{Z}$-module libre de rang n et l'anneau quotient $\mathcal{O}/\mathfrak{a}$ est fini.*

Démonstration. Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}$, et soit $a \in \mathfrak{a} \setminus \{0\}$. Comme le morphisme canonique $\mathcal{O}/a\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{a}$ est surjectif, il suffit de montrer que $\mathcal{O}/a\mathcal{O}$ est fini. Mais $\mathcal{O}$ étant un anneau intègre, si $(e_1, \ldots, e_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}$, $(ae_1, \ldots, ae_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}$. Le théorème de structure de $\mathbb{Z}$-modules de type fini montre alors que $\mathcal{O}/a\mathcal{O}$ est fini. Mais alors, $\mathcal{O}/\mathfrak{a}$ est fini et ce même théorème montre que $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang n. $\square$

Le lemme précédent montre en particulier que tout idéal d'un ordre est de type fini. En particulier, tout idéal fractionnaire I non nul de

$\mathbb{Z}[\alpha]$s'écrit $I = \lambda\mathfrak{a}$, où $\lambda \in \mathbb{Q}(\alpha)^\times$ et $\mathfrak{a}$ est un idéal arbitraire de $\mathbb{Z}[\alpha]$ (cf. remarque 1.6 (1)). Comme $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang n d'après le lemme précédent, I aussi (par intégrité de $\mathbb{Q}(\alpha)$).

Soit $\mathscr{B} = (v_1, \dots, v_n)$ une $\mathbb{Z}$-base de I. Comme I est un sous-module du $\mathbb{Z}[\alpha]$-module $\mathbb{Q}(\alpha)$, on a $\alpha I \subset I$, si bien que la multiplication par α induit un endomorphisme $\ell_\alpha : I \longrightarrow I$.

On a alors le lemme suivant.

Lemme 1.13. *Soit I un idéal fractionnaire non nul de $\mathbb{Z}[\alpha]$, soit $\mathscr{B} = (v_1, \dots, v_n)$ une $\mathbb{Z}$-base de I, et soit $M_{I,\mathscr{B}} = \mathrm{Mat}(\ell_\alpha; \mathscr{B})$. Alors :*

(1) *α est une valeur propre complexe de $M_{I,\mathscr{B}}^t \in \mathrm{M}_n(\mathbb{Z})$ et $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{Q}(\alpha)^n$ en est un vecteur propre pour la valeur propre α.*

(2) *La matrice $M_{I,\mathscr{B}}$ est de polynôme caractéristique f,*

(3) *La classe de conjugaison de $M_{I,\mathscr{B}}$ ne dépend que de la classe $[I]$.*

Démonstration. Montrons (1). Écrivons $M_{I,\mathscr{B}} = \mathrm{Mat}(\ell_\alpha; \mathscr{B}) = (a_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$. Par définition, on a donc $\alpha v_j = \sum_{i=1}^{n} a_{ij} v_i$, où $a_{ij} \in \mathbb{Z}$, et ceci pour tout $j \in [\![1, n]\!]$. Cela se récrit $\mathbf{v}^t M_{I,\mathscr{B}} = \alpha \mathbf{v}^t$, si bien que $\mathbf{v}$ est un vecteur propre de $M_{I,\mathscr{B}}^t$ pour la valeur propre α, à coefficients dans $\mathbb{Q}(\alpha)$, puisque $v_j \in I \subset \mathbb{Q}(\alpha)$.

Le polynôme caractéristique de $M_{I,\mathscr{B}}$, qui est à coefficients dans $\mathbb{Q}$ (et même dans $\mathbb{Z}$), annule donc α. Il est donc divisible par $\mu_{\alpha,\mathbb{Q}}$, à savoir f (puisque f est irréductible et unitaire annulé par α). En comparant les degrés, on conclut, ce qui démontre (2).

Montrons (3). Notons tout d'abord que si $\mathscr{C}$ est une autre $\mathbb{Z}$-base de I, alors la matrice P de $\mathscr{C}$ dans la base $\mathscr{B}$ est une matrice de $\mathrm{GL}_n(\mathbb{Z})$, et on a $M_{I,\mathscr{C}} = P^{-1} M_{I,\mathscr{B}} P$, ce qui démontre que la classe de conjugaison de $M_{I,\mathscr{B}}$ ne dépend pas de $\mathscr{B}$. Si maintenant J est un idéal fractionnaire équivalent à I, on a donc $J = xI$ pour un certain $x \in \mathbb{Q}(\alpha)^\times$. Mais alors, si $\mathscr{B}$ est une $\mathbb{Z}$-base de I, $x\mathscr{B}$ est une $\mathbb{Z}$-base de J. D'après ce qui précède, on peut choisir cette base pour calculer la classe de conjugaison associée à J. Mais il est clair que $\mathrm{Mat}(\ell_\alpha; x\mathscr{B}) = \mathrm{Mat}(\ell_\alpha; \mathscr{B})$, où ℓ_α est la multiplication par α dans $J = xI$ dans le membre de gauche, et dans I dans le membre de droite. On a donc $M_{J,\lambda\mathscr{B}} = M_{I,\mathscr{B}}$. $\square$

L'étape suivante est de montrer que les deux constructions précédentes sont inverses l'une de l'autre. Pour cela, on a besoin d'un dernier lemme.

Lemme 1.14. *Soit $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_M = f$, et soit $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{Q}(\alpha)^n \in \setminus\{0\}$ tel que $M^t\mathbf{v} = \alpha\mathbf{v}$. Alors, $(v_1, \ldots, v_n)$ est une famille $\mathbb{Q}$-libre et $\mathbb{Z}$-libre.*

Démonstration. Il suffit bien entendu de démontrer la $\mathbb{Q}$-liberté. Une relation de dépendance $\mathbb{Q}$-linéaire entre les coordonnées de $\mathbf{v}$ s'écrit $\mathbf{x}^t\mathbf{v} = 0$, avec $\mathbf{x} \in \mathbb{Q}^n$. On doit montrer que $\mathbf{x} = 0$.

Or, on sait qu'il existe $S \in \mathrm{GL}_n(\mathbb{Q})$ telle que $SMS^{-1} = C_f$. On a alors $S^{-t}M^tS^t = C_f^t$, et $S^{-t}\mathbf{v}$ est un vecteur propre de C_f^t. Un tel vecteur propre est proportionnel à $\begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}$ d'après l'exemple 1.8, donc ses coordonnées sont $\mathbb{Q}$-libres. En particulier, les égalités

$$\mathbf{x}^t\mathbf{v} = (S\mathbf{x})^t(S^{-t}\mathbf{v}) = 0$$

impliquent que $S\mathbf{x} = 0$, puisque $S\mathbf{x} \in \mathbb{Q}^n$. Mais, S étant inversible, on en déduit que $\mathbf{x} = 0$. □

On peut maintenant démontrer le théorème principal de ce paragraphe.

Théorème 1.15 (Latimer-McDuffee)**.** *Soit $f \in \mathbb{Z}[X]$ un polynôme irréductible unitaire de degré $n \geq 1$, et soit $\alpha \in \mathbb{C}$ une racine de f fixée. Alors, on a une bijection entre l'ensemble des classes de similitude entière des matrices $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_M = f$ et l'ensemble $\mathscr{C}\ell_0(\mathbb{Z}[\alpha])$ des classes d'idéaux fractionnaires de $\mathbb{Z}[\alpha]$.*

Cette bijection est donnée par

$$\begin{array}{rcl} \mathrm{Conj}_{\mathbb{Z}}(M) & \longmapsto & [I_{\mathbf{v}}] \\ \mathrm{Conj}_{\mathbb{Z}}(M_{I,\mathscr{B}}) & \longleftarrow\!\shortmid & [I] \end{array}$$

où $\mathbf{v}$ est un vecteur propre de M^t à coordonnées dans $\mathbb{Q}(\alpha)$, et où $\mathscr{B}$ est une $\mathbb{Z}$-base de I.

Via cette bijection, la classe de conjugaison de C_f correspond à la classe triviale $[\mathbb{Z}[\alpha]]$.

Démonstration. Il suffit de montrer que les deux constructions sont inverses l'une de l'autre. Soit $M \in \mathrm{M}_n(\mathbb{Z})$ vérifiant $\chi_f = M$, et soit $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ un vecteur propre de M^t à coordonnées dans $\mathbb{Q}(\alpha)$. D'après le lemme 1.14, $\mathscr{B} = (v_1, \ldots, v_n)$ est une $\mathbb{Z}$-base de $I_{\mathbf{v}}$. La classe de conjugaison associée à $I_{\mathbf{v}}$ est alors la classe de conjugaison de $\mathrm{Mat}(\ell_\alpha; \mathscr{B})$.

Or, par définition de $\mathbf{v}$, on a

$$\alpha v_j = \sum_{i=1}^{n} a_{ij} v_i \quad \text{pour tout } j \in [\![1, n]\!],$$

où $M = (a_{ij})_{i,j}$. Mais alors, $\mathrm{Mat}(\ell_\alpha; \mathscr{B})) = M$.

Si maintenant I est un idéal fractionnaire de $\mathbb{Z}[\alpha]$, choisissons une $\mathbb{Z}$-base $\mathscr{B} = (v_1, \ldots, v_n)$ de I. On doit montrer que la classe associée à $M_{I,\mathscr{B}}$ est $[I]$. Or, le lemme 1.13 montre que $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{Q}(\alpha)^n$ est un vecteur propre de $M^t_{I,\mathscr{B}}$ pour la valeur propre α. Mais alors, $I_{\mathbf{v}} = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n = I$ puisque $(v_1, \ldots, v_n)$ est une $\mathbb{Z}$-base de I, ce qui démontre le résultat voulu. □

Le corollaire suivant découle immédiatement du théorème précédent et de la remarque 1.6 (1).

Corollaire 1.16. *Soit $f \in \mathbb{Z}[X]$ un polynôme irréductible unitaire de degré $n \geq 1$, et soit $\alpha \in \mathbb{C}$ une racine de f fixée. Alors :*

(1) *Soit $M \in \mathrm{M}_n(\mathbb{Z})$ telle que $\chi_M = f$. Soit $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{Z}[\alpha]^n$ un vecteur propre de M^t associé à α. Alors, M est semblable sur $\mathbb{Z}$ à C_f si, et seulement si, $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ est un idéal principal de $\mathbb{Z}[\alpha]$.*
(2) *Toute matrice $M \in \mathrm{M}_n(\mathbb{Z})$ telle que $\chi_M = f$ est semblable sur $\mathbb{Z}$ à C_f si, et seulement si, $\mathbb{Z}[\alpha]$ est un anneau principal.*

Remarque 1.17. La démonstration de la correspondance permet de dégager une méthode pour décider si deux matrices $M, N \in \mathrm{M}_n(\mathbb{Z})$ de polynôme caractéristique f sont conjuguées, et de calculer une matrice inversible qui conjugue l'une en l'autre. Soient $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$, $\mathbf{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{Q}(\alpha)^n$ des vecteurs propres de M^t et N^t respectivement pour la valeur propre α.

Si $[I_{\mathbf{v}}] \neq [I_{\mathbf{w}}]$, les matrices M et N ne sont pas conjuguées. Si $[I_{\mathbf{v}}] = [I_{\mathbf{w}}]$, il existe $\lambda \in \mathbb{Q}(\alpha)^\times$ tel que $I_{\mathbf{v}} = \lambda I_{\mathbf{w}}$ Alors, $\mathscr{B} = (v_1, \ldots, v_n)$ est une $\mathbb{Z}$-base de $I_{\mathbf{v}}$, tandis que $\lambda\mathscr{B}$ et $\mathscr{C} = (w_1, \ldots, w_n)$ sont deux $\mathbb{Z}$-bases de $I_{\mathbf{w}}$. La matrice P de $\lambda\mathscr{B}$ dans la base $\mathscr{C}$ est donc une matrice de $\mathrm{GL}_n(\mathbb{Z})$.

Comme on l'a déjà constaté, $M_{I_{\mathbf{w}},\mathscr{C}} = N$. Mais, on a aussi $M_{I_{\mathbf{w}},\lambda\mathscr{B}} = M_{\lambda I_{\mathbf{v}},\lambda\mathscr{B}} = M$. La formule du changement de base appliquée à l'endomorphisme de multiplication par α dans $I_{\mathbf{w}}$ donne alors $PMP^{-1} = N$.

2. Finitude du nombre de classes d'idéaux d'un ordre

Le but de ce paragraphe est d'établir la finitude de l'ensemble des classes de similitude entières de matrices $M \in \mathrm{M}_n(\mathbb{Z})$ telle que $\chi_M = f$.

Le théorème de Latimer-McDuffee nous dit que cela revient à établir la finitude de l'ensemble des classes d'idéaux fractionnaires de $\mathbb{Z}[\alpha]$. Comme ce n'est pas plus compliqué, nous allons établir cette finitude pour un ordre $\mathcal{O}$.

Lemme 2.1. *Soit $\mathcal{O}$ un ordre. Alors, pour tout $a \in \mathcal{O}$ non nul, $|\mathcal{O}/a\mathcal{O}| = |\det(\ell_a)|$, où ℓ_a est l'endomorphisme de multiplication par a dans le $\mathbb{Z}$-module libre $\mathcal{O}$.*

Démonstration. Puisque $\mathcal{O}$ et $a\mathcal{O}$ sont tous deux des $\mathbb{Z}$-modules de rang n, d'après le théorème de la base adaptée, il existe une $\mathbb{Z}$-base $(w_1, \dots, w_n)$ de $\mathcal{O}$ et des entiers strictement positifs $q_1, \dots, q_n$ tels que $(q_1 w_1, \dots, q_n w_n)$ est une $\mathbb{Z}$-base de $a\mathcal{O}$.

Comme $(aw_1, \dots, aw_n)$ est aussi une $\mathbb{Z}$-base de $a\mathcal{O}$, la matrice P de $(q_1 w_1, \dots, q_n w_n)$ dans la base $(aw_1, \dots, aw_n)$ est une matrice de $\mathrm{GL}_n(\mathbb{Z})$, donc de déterminant ± 1. Soit M la matrice de ℓ_a dans la base $(w_1, \dots, w_n)$, c'est-à-dire la matrice de $(aw_1, \dots, aw_n)$ dans la base $(w_1, \dots, w_n)$. Alors, MP est la matrice de $(q_1 w_1, \dots, q_n w_n)$ dans la base $(w_1, \dots, w_n)$, c'est-à-dire la matrice $\mathrm{diag}(q_1, \dots, q_n)$.

On a donc $q_1 \cdots q_n = \det(MP) = \det(M)\det(P) = \pm\det(M) = \pm\det(\ell_a)$, d'où $q_1 \cdots q_n = |\det(\ell_a)|$. Mais, on a

$$\mathcal{O}/a\mathcal{O} = \bigoplus_{i=1}^{n} \mathbb{Z}w_i / \bigoplus_{i=1}^{n} \mathbb{Z}q_i w_i \simeq \prod_{i=1}^{n} \mathbb{Z}/q_i\mathbb{Z},$$

d'où $|\mathcal{O}/a\mathcal{O}| = q_1 \cdots q_n$. Ceci achève la démonstration. □

Rappelons que, d'après le lemme 1.12, pour tout idéal $\mathfrak{a}$ non nul de $\mathcal{O}$, $|\mathcal{O}/\mathfrak{a}|$ est fini, et l'énoncé suivant a un sens.

Lemme 2.2. *Il existe une constante $c > 0$, ne dépendant que de $\mathcal{O}$, telle que tout idéal $\mathfrak{a}$ non nul de $\mathcal{O}$ contient un élément $a \in \mathfrak{a}$ non nul vérifiant*

$$|\mathcal{O}/a\mathcal{O}| \leq c|\mathcal{O}/\mathfrak{a}|.$$

Démonstration. Soit $k \geq 1$ l'unique entier tel $k^n \leq |\mathcal{O}/\mathfrak{a}| < (k+1)^n$. Soit $(w_1, \ldots, w_n)$ une $\mathbb{Z}$-base de $\mathcal{O}$. On pose

$$\mathscr{E} = \{x = \sum_{j=1}^{n} m_j w_j \mid |m_j| \leq k \text{ pour tout } j\}$$

et soit

$$\mathscr{E}^+ = \{x = \sum_{j=1}^{n} m_j w_j \mid 0 \leq m_j \leq k \text{ pour tout } j\}.$$

Soit M_j la matrice de ℓ_{w_j} dans la base $(w_1, \ldots, w_n)$. Ces matrices commutant deux à deux, elles sont co-trigonalisables dans $\mathbb{C}$. Il existe donc $Q \in \mathrm{GL}_n(\mathbb{C})$ telle que $Q^{-1} M_j Q = \mathrm{diag}(\lambda_1^{(j)}, \ldots, \lambda_n^{j})$.

Posons $c = \prod_{i=1}^{n} (\sum_{j=1}^{n} |\lambda_i^{(j)}|)$.

Pour tout $x \in \mathscr{E}$, on a donc

$$|\det(\ell_x)| = |\prod_{i=1}^{n} |\sum_{j=1}^{n} m_j \lambda_i^{(j)}| \leq k^n c \leq c|\mathcal{O}/\mathfrak{a}|.$$

Parmi les $(k+1)^n$ éléments de $\mathscr{E}^+$, il y a au moins deux éléments x_1, x_2 distincts qui sont congrus modulo $\mathfrak{a}$, puisque $|\mathcal{O}/\mathfrak{a}| < (k+1)^n$. Posons $a = x_1 - x_2$. Alors d'une part, $a \in \mathfrak{a} \setminus \{0\}$, et d'autre part, $a \in \mathscr{E}$, si bien que

$$|\det(\ell_a)| \leq c|\mathcal{O}/\mathfrak{a}|.$$

On conclut en utilisant le lemme précédent. □

On peut maintenant démontrer le résultat attendu.

Théorème 2.3. *Le nombre de classes d'idéaux fractionnaires de $\mathcal{O}$ est fini.*

Démonstration. Soit $c > 0$ la constante définie due lemme précédent.

Soit I un idéal fractionnaire non nul de $\mathcal{O}$. On a donc $I = \lambda\mathfrak{a}$, où $\lambda \in K^\times$ et $\mathfrak{a}$ est un idéal de $\mathcal{O}$. D'après le lemme précédent, il existe $a \in \mathfrak{a} \setminus \{0\}$ tel que $|\mathcal{O}/a\mathcal{O}| \leq c|\mathcal{O}/\mathfrak{a}|$, soit encore $|\mathfrak{a}/a\mathcal{O}| \leq c$.

Notons que, puisque $a\mathcal{O} \subset \mathfrak{a}$, on a $\mathcal{O} \subset a^{-1}\mathfrak{a}$. La multiplication par a^{-1} induisant un isomorphisme de $\mathbb{Z}$-modules $a^{-1}\mathfrak{a}/\mathcal{O} \simeq \mathfrak{a}/a\mathcal{O}$, on en conclut que la classe de I peut être représentée par un idéal fractionnaire J contenant $\mathcal{O}$ tel $|J/\mathcal{O}| \leq c$.

Soit $m = |J/\mathcal{O}|$. Alors, $mJ \subset \mathcal{O}$, et donc $J \subset m^{-1}\mathcal{O}$. Bref, $\mathcal{O} \subset J \subset m^{-1}\mathcal{O}$. Or, l'ensemble de tels $\mathbb{Z}$-modules J est en bijection avec les sous-modules de $m^{-1}\mathcal{O}/\mathcal{O}$. Mais, ce dernier quotient est fini d'après un lemme précédent, puisque $m^{-1}\mathcal{O}/\mathcal{O}$ est isomorphe à $\mathcal{O}/m\mathcal{O}$. À m fixé,

il y a donc un nombre fini de possibilités pour J. Comme le nombre de possibilités pour m est fini, on obtient la conclusion demandée. $\square$

Le théorème de Latimer-McDuffee nous donne alors immédiatement le corollaire suivant.

Corollaire 2.4. *Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré $n \geq 1$. Alors, le nombre de classes de similitude entière de matrices $M \in \mathrm{M}_n(\mathbb{Z})$ telle que $\chi_M = f$ est fini.*