SIMILITUDE DE MATRICES ENTIÈRES ET IDÉAUX

GRÉGORY BERHUY

1. Échauffement

On rappelle que si $\pi = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$, la matrice compagnon de π est la matrice $C_\pi \in \mathrm{M}_n(K)$ définie par

$$C_\pi = \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & & \vdots \\ & & \ddots\ 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix}.$$

Le point de départ de cet article est le théorème suivant.

Théorème 1.1. *Soit K un corps, soit E un K-espace vectoriel de dimension finie non nulle, et soit $\pi \in K[X]$ un polynôme irréductible unitaire. Enfin, soit $u \in \mathscr{L}(E)$ tel que $\mu_u = \pi$. Alors, il existe une base $\mathbf{e}$ de E telle que*

$$\mathrm{Mat}(u;\mathbf{e}) = \begin{pmatrix} C_\pi & & \\ & \ddots & \\ & & C_\pi \end{pmatrix},$$

où C_π est la matrice compagnon associée à π.

En particulier, deux endomorphismes de E de polynôme minimal égal à π sont semblables, et deux matrices de $\mathrm{M}_n(K)$ de polynôme minimal égal à π sont semblables.

Démonstration. Soit $L = K[X]/(\pi)$. Comme $K[X]$ est principal et π est irréductible, L est un corps. Notons que pour tous $P, Q \in K[X]$ et tout $v \in E$, on a

$$(P + Q\pi)(u)(v) = P(u)(v) + (Q(u) \circ \pi(u))(v) = P(u)(v),$$

puisque $\pi(u) = \mu_u(u) = 0$. Ainsi, la loi externe

$$\begin{aligned} L \times E &\longrightarrow E \\ (\overline{P}, v) &\longmapsto \overline{P} \bullet v = P(u)(v) \end{aligned}$$

est bien définie. On vérifie aisément qu'elle munit le groupe abélien $(E, +)$ d'une structure de L-espace vectoriel.

Date: 31 janvier 2019.

Remarquons que, pour tout $\lambda \in K$, et tout $v \in E$, on a

$$\lambda \cdot v = (\lambda \mathrm{Id}_E)(v) = \overline{\lambda} \bullet v.$$

Il s'ensuit que si $(v_1, \ldots, v_m)$ est une famille K-génératrice de E, elle est aussi L-génératrice. Ainsi, E un L-espace vectoriel de dimension finie. Soit $\mathbf{v} = (v_1, \ldots, v_n)$ une L-base de E. Alors, la famille $\mathbf{e}$ définie par

$$\mathbf{e} = (e_1, u(e_1), \ldots, u^{d-1}(e_1), \ldots, e_n, u(e_n), \ldots, u^{d-1}(e_n)),$$

avec $d = \deg(\pi)$, est une K-base de E.

Commençons par remarquer que pour tout $\overline{P} \in L$, il existe un unique polynôme $R \in K[X]$ tel que $\deg(R) \leq d-1$ et $\overline{P} = \overline{R}$. En effet, l'existence est obtenue par division euclidienne, et l'unicité provient du fait que si $\overline{R} = \overline{0}$, alors $\pi \mid R$. En particulier, si R est non nul, on a $\deg(R) \geq d$.

Soit maintenant $v \in E$. Puisque $\mathbf{v}$ est génératrice, il existe $\overline{P}_1, \ldots, \overline{P}_n \in L$ tels que

$$v = \sum_{j=1}^{n} \overline{P}_j \bullet v_j.$$

D'après ce qui précède, on peut suppose que $\deg(P_j) \leq d-1$. Si $P_j = \sum_{i=0}^{d-1} \lambda_{ij} X^i$, on a alors

$$v = \sum_{i=0}^{d-1} \sum_{j=1}^{n} \lambda_{ij} u^i(v_j),$$

ce qui démontre que $\mathbf{e}$ est une famille K-génératrice de E.

Supposons maintenant que $\sum_{i=0}^{d-1} \sum_{j=1}^{n} \lambda_{ij} u^i(v_j) = 0$, avec $\lambda_{ij} \in K$. Si on pose $P_j = \sum_{i=0}^{d-1} \lambda_{ij} X^i$, l'égalité précédente se récrit

$$\sum_{j=1}^{n} \overline{P}_j \bullet v_j = 0.$$

Comme $\mathbf{v}$ est une L-base de E, on en déduit que $\overline{P}_j = \overline{0}$ pour tout $j \in [\![1, n]\!]$. Comme $\deg(P_j) \leq d-1$, on a ainsi $P_j = 0$ pour tout $j \in [\![1, n]\!]$, et on en déduit que tous les coefficients λ_{ij} sont nuls. Par conséquent, $\mathbf{e}$ est K-libre, et c'est donc une K-base de E.

Comme $\pi(u) = 0$, on a $u^d = -a_0 \mathrm{Id}_E - a_1 u - \cdots - a_{d-1} u^{d-1}$. Il s'ensuit aisément que $\mathrm{Mat}(u; \mathbf{e})$ possède la forme voulue. Le dernier point est clair. □

Remarque 1.2. Ce résultat est faux si π n'est pas irréductible. Par exemple, les matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ont même polynôme minimal $X(X-1)$, mais ne sont pas semblables car elles n'ont pas le même polynôme caractéristique.

Si on trouve que c'est un peu tricher, on peut considérer les matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

qui ont toutes deux un polynôme minimal égal à X^2, et un polynôme caractéristique égal à X^4, mais qui ne sont pas semblables.

Corollaire 1.3. *Soit $M \in \mathrm{M}_n(K)$. On suppose que le polynôme minimal de M est irréductible. Alors, M et M^t sont semblables.*

Démonstration. Pour tout $P \in K[X]$, on a

$$P(M) = 0 \iff P(M)^t = 0 \iff P(M^t).$$

Ainsi, M et M^t ont mêmes polynômes annulateurs. Il s'ensuit que M et M^t ont même polynôme minimal. On applique alors le théorème précédent. □

Remarque 1.4. Le résultat de ce corollaire est vrai plus généralement sans aucune hypothèse sur le polynôme minimal.

Que se passe-t-il si on remplace K par $\mathbb{Z}$? Avant de répondre à la question, il faut introduire le bon contexte.

Une matrice $M \in \mathrm{M}_n(\mathbb{Z})$ définit un morphisme de groupes

$$\begin{aligned} f_M \colon \mathbb{Z}^n &\longrightarrow \mathbb{Z}^n \\ \omega &\longmapsto M\omega \end{aligned},$$

et on voit aisément que tout morphisme de groupes $\mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ est de la forme f_M pour une unique matrice $M \in \mathrm{M}_n(\mathbb{Z})$. Pour cela, on utilise le fait que tout élément de $\mathbb{Z}^n$ s'écrit de manière unique comme combinaison $\mathbb{Z}$-linéaire des vecteurs de la base canonique.

On vérifie alors que f_M est un automorphisme si, et seulement si, $M \in \mathrm{GL}_n(\mathbb{Z}) \overset{def}{=} \mathrm{M}_n(\mathbb{Z})^\times$. Remarquons au passage que l'on a

$$\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathrm{M}_n(\mathbb{Z}) \mid \det(M) = \pm 1\}.$$

En effet, si $MN = NM = I_n$ pour un certain $N \in \mathrm{M}_n(\mathbb{Z})$, alors $\det(M)\det(N) = 1 \in \mathbb{Z}$ et $\det(M) = \pm 1$. Inversement, si $M \in \mathrm{M}_n(\mathbb{Z})$

et $\det(M) = \pm 1$, alors $\det(M)^{-1}\mathrm{com}(M)^t \in \mathrm{M}_n(\mathbb{Z})$, et les égalités

$$\det(M)I_n = \mathrm{com}(M)^t M = M\mathrm{com}(M)^t$$

montrent que M est inversible dans $\mathrm{M}_n(\mathbb{Z})$, d'inverse $\det(M)^{-1}\mathrm{com}(M)^t$.

On dira alors que deux endomorphismes de u, u' $\mathbb{Z}^n$ sont semblables sur $\mathbb{Z}$ s'il existe un automorphisme v de $\mathbb{Z}^n$ tel que $u' = v \circ u \circ v^{-1}$. Deux matrices $M, M' \in \mathrm{M}_n(\mathbb{Z})$ sont dites semblables sur $\mathbb{Z}$ s'il existe $S \in \mathrm{GL}_n(\mathbb{Z})$ telle que $M' = SMS^{-1}$.

On peut donc se poser les questions suivantes : soit $\pi \in \mathbb{Z}[X]$ un polynôme unitaire, irréductible dans $\mathbb{Q}[X]$. Soient $M, M' \in \mathrm{M}_n(\mathbb{Z})$ de polynôme minimal π. Les matrices M et M' sont-elles semblables ? les matrices M et M^t sont-elles semblables ?

Les exemples suivants montrent que la réponse aux deux questions est négative en général.

Exemples 1.5.

(1) Les matrices $M_1 = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 1 & -3 \\ 2 & -1 \end{pmatrix}$ ont un polynôme minimal égal à $X^2 + 5$, mais ne sont pas semblables sur $\mathbb{Z}$.

En effet, soit $S \in \mathrm{GL}_2(\mathbb{Z})$ telle que $SM_1S^{-1} = M_2$. En particulier, on a $SM_1 = M_2S$. En écrivant $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on obtient un système linéaire, qui se réduit après quelques manipulations aux deux équations

$$-a = b + 3c = 0 \quad \text{et} \quad -2a = c + d = 0.$$

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

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

Puisque $\det(S) = \pm 1$, 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.

En revanche, si $S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $S_2 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$, alors on a les égalités $S_1M_1S_1^{-1} = M_1^t$ et $S_2M_2S_2^{-1} = M_2^t$.

(2) Si $M = \begin{pmatrix} 1 & -5 \\ 3 & -1 \end{pmatrix}$, alors M et M^t ne sont pas semblables sur $\mathbb{Z}$.

En effet, soit $S \in \mathrm{GL}_2(\mathbb{Z})$ telle que $SMS^{-1} = M^t$. En écrivant $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on obtient cette fois les deux équations

$$b = c \quad \text{et} \quad 5a + 2b + 3d = 0.$$

On a donc $2(a+b)+3(a+d)=0$. On en déduit aisément que $a+b=3k, a+d=-2k, k\in\mathbb{Z}$. On a alors $S=\begin{pmatrix} a & -a+3k \\ -a+3k & -a-2k\end{pmatrix}$, et donc

$$\det(S)=-(2a^2-4ak+9k^2)=-(a^2+(a-2k)^2+5k^2)\leq 0.$$

Puisque $\det(S)=\pm 1$, on obtient $a^2+(a-2k)^2+5k^2=1$. Comme précédemment, on a $k=0$, puis $2a^2=1$, ce qui est impossible.

Déterminer toutes les classes de conjugaison de matrices entières n'est pas si facile. Nous allons rester modestes, et traiter le cas des matrices 2×2, de polynôme minimal X^2+d, avec $d\geq 1$.

On peut commencer par se demander s'il y en a un nombre fini, ce qui a priori n'est pas clair.

Soit $M\in \mathrm{M}_2(\mathbb{Z})$ de polynôme minimal X^2+d. On a donc $\mathrm{tr}(M)=0$ et $\det(M)=d$, si bien que M est de la forme

$$[a,b,c]_d \overset{def}{=} \begin{pmatrix} b & -c \\ a & -b\end{pmatrix},\ a,b,c\in\mathbb{Z},\ ac-b^2=d.$$

Si $D=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, S_\varepsilon=\begin{pmatrix}0 & \varepsilon\\ 1 & 0\end{pmatrix}$, avec $\varepsilon=\pm 1$, et $T_k=\begin{pmatrix}1 & -k\\ 0 & 1\end{pmatrix}, k\in\mathbb{Z}$, on vérifie que $D, S_\varepsilon, T_k\in \mathrm{GL}_2(\mathbb{Z})$, et que l'on a les relations suivantes, pour tous $a,b,c,k\in\mathbb{Z}$:

(1) $D[a,b,c]_dD^{-1}=[-a,b,-c]_d$;
(2) $S_1[a,b,c]_dS_1^{-1}=[-c,-b,-a]_d$ et $S_{-1}[a,b,c]_dS_{-1}^{-1}=[c,-b,a]_d$;
(3) $T_k[a,b,c]_dT_k^{-1}=[a,b-ka,c-2kb+k^2a]_d$.

On a alors le résultat suivant.

Lemme 1.6. *Soit $d\geq 1$ un entier. Alors, toute matrice $M\in \mathrm{M}_2(\mathbb{Z})$ de polynôme minimal X^2+d est semblable sur $\mathbb{Z}$ à une unique matrice $[a,b,c]_d$, avec $a,b,c\in\mathbb{Z}$ vérifiant les conditions suivantes :*

(i) $ac-b^2=d$;
(ii) $0<a\leq c,\ -\frac{a}{2}<b\leq\frac{a}{2}$ *et* $b>0$ *dès que* $a=c$.

En particulier, $1\leq a\leq 2\sqrt{\frac{d}{3}}$, *et il y a un nombre fini de classes de similitude de telles matrices.*

Démonstration. On sait déjà qu'une telle matrice M est de la forme $[a,b,c]_d$, avec $a,b,c\in\mathbb{Z}$ et $ac-b^2=d$. Remarquons que a et c sont non nuls, puisque sinon on aurait $d=-b^2\geq 0$. On va maintenant

décrire un algorithme pour obtenir une matrice $M_{a',b',c'}$ semblable à $M = M_{a,b,c}$, où $a', b'c'$ vérifient les conditions demandées.

Initialisation. On pose $[a', b,', c]_d = [a, b, c]_d$. Si $a', b,', c'$ vérifient les conditions demandées, on a fini. Sinon, on passe à l'étape 1.

Étape 1. Si $a' > 0$, on ne fait rien. Si $a' < 0$, on fait

$$[a', b', c']_d \longleftarrow [-a', b', -c']_d$$

en conjuguant par D.

On passe à l'étape suivante.

Étape 2. Si $a' \leq c'$, on ne fait rien. Si $a' > c'$, on fait

$$[a', b', c']_d \longleftarrow [c', -b', a']_d$$

en conjuguant par S_{-1}.

On passe à l'étape suivante.

Étape 3. Si $-\frac{a'}{2} < b' \leq \frac{a'}{2}$, on ne fait rien. Si $b' \leq -\dfrac{a'}{2}$ ou $b' > \dfrac{a'}{2}$, on prend $k \in \mathbb{Z}$ tel que $-\frac{a'}{2} < b' - ka' \leq \frac{a'}{2}$, et on fait

$$[a', b', c']_d \longleftarrow [a', b - k'a, c + k(a' - 2b')]_d$$

en conjuguant par T_k.

Si $a' > c'$, on repart à l'étape 2. Si $a' = c'$, on passe à l'étape 4.

Étape 4. Si $b' > 0$, on ne fait rien. Sinon, on fait

$$[a', b', c']_d \longleftarrow [c', -b', a']_d$$

en conjuguant par S_{-1}.

FIN.

Remarquons que la valeur de a' après l'étape 3 est la valeur de a' obtenue après l'étape 2. Si à la fin de l'étape 3, on a encore $a' > c'$, une nouvelle étape 2 va remplacer a' par une valeur strictement inférieure. Cela garantit que l'on arrivera à la fin de l'étape 3 à une valeur $a' \leq' c$ en au plus $|a'|$ itérations de l'étape 2. On arrive donc au début de l'étape 4 avec une matrice $M_{a',b',a'}$, où $0 < a'$ et $-\dfrac{a'}{2} < b' \leq \dfrac{a'}{2}$. Si $b' < 0$, l'étape 4 remplace b' par $-b'$, et on a donc $-\dfrac{a'}{2} \leq -b' < \dfrac{a'}{2}$. Comme $-b' > 0$ et $-\dfrac{a'}{2} < 0$, on a donc bien $-\dfrac{a'}{2} < -b' < \dfrac{a'}{2}$.

Notons qu'à chaque étape, l'algorithme produit une matrice semblable à la matrice utilisée au début de l'étape. En particulier, la matrice finale est semblable à $[a, b, c]_d = M$. Deux matrices semblables ayant même polynôme minimal et même déterminant, la matrice $[a', b', c']_d$ a donc un polynôme minimal égal à X^2+d et on a nécessairement $a'c'-b'^2 = d$.

L'algorithme produit donc une matrice vérifiant les conditions voulues. L'unicité est pénible à démontrer, et est admise.

Si maintenant $a, b, c \in \mathbb{Z}$ vérifient les conditions (i) et (ii), on a en particulier

$$a^2 \leq ac = d + b^2 \leq d + \frac{a^2}{4},$$

d'où $a^2 \leq \frac{4d}{3}$ et $1 \leq a \leq 2\sqrt{\frac{d}{3}}$, puisque $a > 0$. Il y a donc un nombre fini de valeurs possibles pour a, donc un nombre fini de valeurs pour b. Comme $c = \frac{d + b^2}{a}$, on a aussi un nombre fini de valeurs pour c.

Comme toute matrice $M \in \mathrm{M}_2(\mathbb{Z})$ de polynôme minimal $X^2 + d$ est semblable à une matrice $[a, b, c]_d$, avec $a, b, c \in \mathbb{Z}$ vérifiant (i) et (ii), cela démontre le dernier point. □

Définition 1.7. Soit $d \geq 1$ un entier. Une matrice $[a, b, c]_d \in \mathrm{M}_2(\mathbb{Z})$ où $a, b, c \in \mathbb{Z}$ vérifient les conditions (i) et (ii) du lemme 1.6 est dite *réduite*.

Ainsi, toute matrice $M \in \mathrm{M}_2(\mathbb{Z})$ de polynôme minimal $X^2 + d$ est semblable à une unique matrice réduite.

Exemples 1.8. Soit $d \geq 1$ un entier, et soit $[a, b, c]_d$ une matrice réduite.

Si $d = 1, 2$, on obtient $1 \leq a < 2$, i.e. $a = 1$, d'où $b = 0$, puis $c = d$. La seule matrice réduite est donc $[1, 0, d]_d = \begin{pmatrix} 0 & -d \\ 0 & 1 \end{pmatrix}$, i.e. la matrice compagnon de $X^2 + d$, et toutes les matrices de $\mathrm{M}_n(\mathbb{Z})$ de polynôme minimal $X^2 + d$ sont semblables.

Si $d \geq 3$, nous allons montrer qu'il y a au moins deux classes de similitude distinctes.

Si $d = 2m, m \geq 2$, alors les matrices $[1, 0, d]_d$ et $[2, 0, m]_d$ ne sont pas semblables.

En effet, si $S = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ vérifie $S[1, 0, d]_d S^{-1} = [m, 0, 2]_d$, alors on a $y = -mz$ et $t = 2x$, d'où

$$\det(S) = 2x^2 + mz^2 \geq 2(x^2 + z^2),$$

car $m \geq 2$.

Puisque x et z ne peuvent être tous les deux nuls (car $S \neq 0$), on obtient $\det(S) \geq 2$ et ainsi on ne peut avoir $\det(S) \pm 1$.

Si $d = 2m - 1, m \geq 2$, alors les matrices $[1, 0, d]_d$ et $[2, 1, m]_d$ ne sont pas semblables.

En effet, si $S = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ vérifie $S[1,0,d]_d S^{-1} = [2,1,m]_d$, alors on a $t = x - 2z$ et $y = x - mz$, d'où

$$\det(S) = 2x^2 - 2xz + mz^2 = x^2 + (x-z)^2 + (m-1)z^2 \geq x^2 + z^2.$$

Comme $\det(S) = \pm 1$, on a $x = 0$ ou $x = \pm 1$. Si $x = \pm 1$, alors $z = 0$ et $\det(S) = 2$. Si $x = 0$, alors $\det(S) = mz^2$. Comme dans ce cas $z \neq 0$, on a $\det(S) \geq m \geq 2$. Dans tous les cas, on ne peut avoir $\det(S) = \pm 1$.

Remarque 1.9. De manière générale, on peut démontrer que deux matrices réduites sont semblables si, et seulement si, elles sont égales. En particulier, toute matrice de $\mathrm{M}_2(\mathbb{Z})$ de polynôme minimal $X^2 + d$ est semblable à une unique matrice réduite.

Cela permet aussi de retrouver le résultat du point (2) sans calculs.

Afin de répondre à la question sur la similitude entre et sa transposée, il faut pousser l'étude un peu plus loin.

2. Matrices entières et idéaux

Soit $d \geq 1$. Dans ce qui suit, on pose

$$A_d = \mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$$

et

$$K_d = \mathbb{Q}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Q}\},$$

avec $\alpha = i\sqrt{d}$. On ne suppose pas que d soit sans facteurs carrés pour l'instant.

Pour tout $P \in \mathbb{Z}[X]$ (resp. $P \in \mathbb{Q}[X]$), par division euclidienne, il existe $Q \in \mathbb{Z}[X]$ (resp. $Q \in \mathbb{Q}[X]$) et $a, b \in \mathbb{Z}$ (resp. $a, b, \in \mathbb{Q}$) tels que

$$P = Q(X^2 + d) + a + bX.$$

En particulier, $P(\alpha) = a + b\alpha$, et $P(\alpha) = 0$ si, et seulement si, $X^2 + d \mid P$ (il est clair que $a + b\alpha = \iff a = b = 0$, puisque α est imaginaire pur).

Par conséquent, les deux morphismes d'évaluation en α $\mathbb{Z}[X] \longrightarrow \mathbb{C}$ et $\mathbb{Q}[X] \longrightarrow \mathbb{C}$ ont pour image A_d et K_d, et leurs noyaux sont engendrés par $X^2 + d$ dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$ respectivement. Ainsi, A_d et K_d sont des sous-anneaux de $\mathfrak{c}$, et on a des isomorphismes d'anneaux

$$A_d \simeq \mathbb{Z}[X]/(X^2 + d) \quad \text{et} \quad K_d \simeq \mathbb{Q}[X]/(X^2 + d).$$

En particulier, A_d est intègre et K_d est un corps. Remarquons aussi que tout élément de K_d peut s'écrire sous la forme $z = \dfrac{z'}{m}$, avec $z' \in A_d$ et $m \geq 1$.

Avant de continuer, introduisons une définition et une notation commode.

Définition 2.1. Soit G un groupe abélien, noté additivement. On dit qu'une famille $(g_1, \dots, g_n)$ d'éléments de G est une $\mathbb{Z}$-*base* de G si tout élément de G s'écrit de manière unique comme combinaison $\mathbb{Z}$-linéaire finie de $g_1, \dots, g_n$.

On le note $G = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_n$.

Exemples 2.2.

(1) Le groupe abélien $\mathbb{Z}^n$ possède une $\mathbb{Z}$-base pour tout $n \geq 1$, à savoir la base canonique.

(2) Une $\mathbb{Z}$-base n'existe pas toujours. En fait, si G possède une $\mathbb{Z}$-base, il est facile de voir (en procédant comme dans le cas des espaces vectoriels) que $G \simeq \mathbb{Z}^n$, pour un certain entier $n \geq 0$.

En particulier, un groupe abélien fini non trivial ne possède pas de $\mathbb{Z}$-base.

(3) Le groupe abélien $\mathbb{Q}$ ne possède pas de $\mathbb{Z}$-base.

En effet, si $(g_1, \dots, g_n)$ est une $\mathbb{Z}$-base de $\mathbb{Q}$, alors $n \geq 1$ (car $\mathbb{Q} \neq 0$). De plus, des éléments d'une $\mathbb{Z}$-base sont nécessairement non nuls. Supposons que $n \geq 2$. Si $g_i = \dfrac{r_i}{s_i}, r_i, s_i \in \mathbb{Z} \setminus \{0\}$ premiers entre eux, on a

$$(r_1 s_2)g_1 - (r_2 s_1)g_2 = 0g_1 + 0g_2,$$

d'où une contradiction avec l'unicité de l'écriture. Par conséquent, $n = 1$.

Mais alors, si p est un nombre premier ne divisant pas s_1, alors on ne peut avoir $\dfrac{1}{p} = mg_1, m \in \mathbb{Z}$. Sinon, on aurait $s_1 = mpr_1$ et $p \mid s_1$.

Revenons à notre propos.

Soit $M \in \mathrm{M}_2(\mathbb{Z})$ une matrice de polynôme minimal $X^2 + d$. Comme $\mu_M = X^2 + d = (X - \alpha)(X + \alpha) \in K_d[X]$, M est diagonalisable sur K_d. En particulier, le sous-espace propre de K_d^2 associé à α est de dimension 1. Quitte à multiplier par un entier, on voit il existe toujours au moins un vecteur propre de M à coordonnées dans A_d.

On a alors le lemme suivant.

Lemme 2.3. *Soit $d \geq 1$. Soit $M \in \mathrm{M}_2(\mathbb{Z})$ une matrice de polynôme minimal $X^2 + d$, et soit $\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in A_d^2$ un vecteur propre de M pour la valeur propre α. Alors, le sous-groupe $\mathfrak{a}_\omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ de A_d engendré par ω_1 et ω_2 est un idéal non nul de A_d. De plus, on a*

$$\mathfrak{a}_\omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2.$$

Enfin, si $\omega' \in A_d^2$ est un autre vecteur propre de M pour la valeur propre α, il existe $z, z' \in A_d$ tels que

$$z'\mathfrak{a}_\omega = z\mathfrak{a}_{\omega'}.$$

Démonstration. Soit $\omega = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \in K_d^2$ un vecteur propre de M associé à la valeur propre α.

Par hypothèse, $\mathfrak{a}_\omega \subset A_d$. Par définition, $\mathfrak{a}_\omega$ est un sous-groupe de A_d, clairement non nul, puisqu'une des deux coordonnées de ω est non nulle. De plus, comme tout élément de A_d est de la forme $a + b\alpha, a, b \in \mathbb{Z}$, il suffit de montrer que $\alpha\omega_1$ et $\alpha\omega_2$ sont des éléments de $\mathfrak{a}_\omega$ pour conclure.

Or, comme $M \in \mathrm{M}_2(\mathbb{Z})$ et $\alpha\omega = M\omega$, on voit que $\alpha\omega_1$ et $\alpha\omega_2$ sont des combinaisons $\mathbb{Z}$-linéaires de ω_1, ω_2. Ainsi, $\mathfrak{a}_\omega$ est un idéal de A_d.

Notons que ω_1 et ω_2 ne sont pas $\mathbb{Q}$-liés. En effet, dans le cas contraire, on aurait $\omega = zv$, avec $z \in A_d \setminus \{0\}$ et $v \in \mathbb{Q}^2$ non nul. Mais alors, on aurait $Mv = \alpha v$, ce qui est impossible puisque $Mv \in \mathbb{Q}^2$ et αv est un vecteur dont au moins une coordonnée est imaginaire pure.

Comme (ω_1, ω_2) forme une famille $\mathbb{Q}$-libre, pour tous $m, n \in \mathbb{Z}$, on a donc

$$m\omega_1 + n\omega_2 = 0 \Longrightarrow m = n = 0.$$

On en déduit facilement que $\mathfrak{a}_\omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

Si $\omega' \in A_d^2$ est un autre vecteur propre associé à la valeur propre α, il existe $u \in A_d$ non nul tel que $\omega' = u\omega$. . Si on écrit $u = \dfrac{z}{z'}$, avec $z, z' \in A_d$ (en fait, on peut prendre $z' \in \mathbb{Z}$, comme on l'a déjà vu), on a $z\omega' = z'\omega$. Notons que $z\omega'$ et $z'\omega$ sont deux vecteurs propres de M associés à α, et à coordonnées dans A_d. On a alors facilement

$$z'\mathfrak{a}_\omega = \mathfrak{a}_{z'\omega} = \mathfrak{a}_{z\omega'} = z'\mathfrak{a}_\omega.$$

□

Exemple 2.4. Si $M = [a, b, c]_d = \begin{pmatrix} b & -c\\ a & -b\end{pmatrix}$, alors $\omega_0 = \begin{pmatrix} b+\alpha\\ a\end{pmatrix} \in A_d^2$ est un vecteur propre de M associé à α, puisque l'on a

$$M\omega_0 = \begin{pmatrix} b^2 - ac + b\alpha\\ a\alpha\end{pmatrix} = \begin{pmatrix} -d + b\alpha\\ a\alpha\end{pmatrix} = \begin{pmatrix} \alpha^2 + b\alpha\\ a\alpha\end{pmatrix} = \alpha\omega_0.$$

On a alors $I_{\omega_0} = \mathbb{Z}(b + \alpha) \oplus \mathbb{Z}a$.

Le résultat du lemme précédent suggère la définition suivante.

Définition 2.5. Deux idéaux non nuls $\mathfrak{a}_1$ et $\mathfrak{a}_2$ de A_d sont *équivalents* s'il existe $z_1, z_2 \in A_d \setminus \{0\}$ tels que $z_2\mathfrak{a}_1 = z_1\mathfrak{a}_2$.

On le note $\mathfrak{a}_1 \sim \mathfrak{a}_2$. C'est clairement une relation d'équivalence sur l'ensemble des idéaux non nuls de A_d.

L'ensemble quotient est noté $\mathscr{C}\ell(-d)$, et la classe d'équivalence d'un idéal non nul $\mathfrak{a}$ sera notée $[\mathfrak{a}]$.

Remarque 2.6. Il est clair que le produit de deux idéaux non nuls de A_d est un idéal non nul de A_d. De plus, si $\mathfrak{a}_1, \mathfrak{a}_1', \mathfrak{a}_2, \mathfrak{a}_2'$ sont des idéaux non nuls de A_d, il est facile de constater que si $\mathfrak{a}_1 \sim \mathfrak{a}_1'$ et si $\mathfrak{a}_2 \sim \mathfrak{a}_2'$, alors $\mathfrak{a}_1\mathfrak{a}_2 \sim \mathfrak{a}_1'\mathfrak{a}_2'$.

Autrement, le produit d'idéaux est compatible avec la relation d'équivalence, et on peut définir une loi produit sur $\mathscr{C}\ell(-d)$ par

$$[\mathfrak{a}_1][\mathfrak{a}_2] = [\mathfrak{a}_1\mathfrak{a}_2],$$

pour toutes classes d'idéaux $[\mathfrak{a}_1], [\mathfrak{a}_2] \in \mathscr{C}\ell(-d)$.

Ce produit est associatif, commutatif, et de neutre $[A_d]$.

Notons également au passage que pour tout idéal non nul $\mathfrak{a}$ de A_d, on a $[\mathfrak{a}] = [A_d] \in \mathscr{C}\ell(-d)$ si, et seulement si, $\mathfrak{a}$ est un idéal principal non nul.

En effet, si $\mathfrak{a} = (z), z \in A_d \setminus \{0\}$, alors $1\mathfrak{a} = zA_d$, d'où $[\mathfrak{a}] = [A_d]$. Inversement, si $[\mathfrak{a}] = [A_d]$, il existe $z_1, z_2 \in A^\times$ non nuls tels que $z_2\mathfrak{a} = z_1A$. En particulier, $z_1 = z_2x$, pour un certain $x \in \mathfrak{a} \subset A_d$. Mais alors, $z_2\mathfrak{a} = z_2xA_d$, et par intégrité, on obtient aisément $\mathfrak{a} = xA_d = (x)$.

En particulier, $\mathscr{C}\ell(-d)$ est trivial si, et seulement si, A_d est un anneau principal.

On a alors le résultat suivant.

Lemme 2.7. *Soit $d \geq 1$. Soit $M \in \mathrm{M}_2(\mathbb{Z})$ une matrice de polynôme minimal $X^2 + d$, et soit $\omega = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \in A_d^2$ un vecteur propre de M pour la valeur propre α. Alors, la classe $c(M) = [\mathfrak{a}_\omega] \in \mathscr{C}\ell(-d)$ est indépendante du choix de ω, et ne dépend que de la classe de conjugaison de M.*

Démonstration. On garde les notations de l'énoncé Le fait que $[\mathfrak{a}_\omega]$ soit indépendante du choix de ω découle directement du lemme 2.3 et de la définition de $\mathscr{C}\ell(-d)$. Si maintenant $M' = SMS^{-1}$, avec $S \in \mathrm{GL}_2(\mathbb{Z})$, alors S_ω est un vecteur propre de M' associé à la valeur propre α, à coordonnées dans A_d. On a donc $c(M') = [\mathfrak{a}_{S\omega}]$.

Or, comme les coordonnées de $S\omega$ sont des combinaisons $\mathbb{Z}$-linéaires des coordonnées de ω, on en déduit que $\mathfrak{a}_{S\omega} \subset \mathfrak{a}_\omega$. Remarquons maintenant que $\omega = S^{-1}(S\omega)$, et donc que les coordonnées de ω sont aussi des combinaisons $\mathbb{Z}$-linéaires des coordonnées de $S\omega$, d'où $\mathfrak{a}_\omega \subset \mathfrak{a}_{S\omega}$. Par conséquent, $\mathfrak{a}_{S\omega} = \mathfrak{a}_\omega$ et $c(SMS^{-1}) = c(M)$. □

On peut donc associer à une classe de conjugaison de matrices une classe d'idéaux. On va maintenant montrer que l'on peut aller en sens

inverse. On commence par démontrer qu'un idéal non nul de A_d possède une $\mathbb{Z}$-base à deux éléments.

Lemme 2.8. *Tout idéal non nul de A_d est de la forme $\mathfrak{a} = s(a, b+\alpha)$, avec $s, a \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z}$ tels que $a \mid b^2 - d$. Dans ce cas, on a $\mathfrak{a} = \mathbb{Z}s(b+\alpha) \oplus \mathbb{Z}sa$.*

En particulier, tout idéal $\mathfrak{a}$ non nul de A_d possède une $\mathbb{Z}$-base à deux éléments.

Démonstration. Soit $\mathfrak{a}$ un idéal non nul de A_d. Remarquons que $\mathfrak{a}$ contient au moins un élément qui n'appartient pas à $\mathbb{Z}$. En effet, si $z = x + y\alpha \in \mathfrak{a} \setminus \{0\}$, alors soit $y \neq 0$, auquel cas $z \notin \mathbb{Z}$, soit $x = 0$, mais alors $y \neq 0$ et $\alpha z = y\alpha \subset \mathfrak{a}$ n'est pas dans $\mathbb{Z}$.

Il existe donc un élément $z_0 = r + s\alpha \in \mathfrak{a}$, avec $s \in \mathbb{Z}$ non nul, de valeur absolue minimale. Quitte à remplacer z par $-z$, on peut supposer que $s \geq 1$.

Si maintenant $z = u + v\alpha, u, v \in \mathbb{Z}$, on va montrer que $s \mid v$. Soit $k = \operatorname{pgcd}(v, s)$, et soient $m, n \in \mathbb{Z}$ tels que $mv + ns = k$. On a alors $mz + nz_0 = (mu + nr) + k\alpha \in \mathfrak{a}$. Comme $k \geq 1$ et $k \mid s$, on a $k \geq s$, et par minimalité de s, on en déduit $k = s$. Mais alors $s \mid v$. Écrivons $v = ws, w \in \mathbb{Z}$. On a alors $z = u + ws\alpha$ et $z - wz_0 = r - wu \in \mathfrak{a}$. On en déduit l'inclusion

$$\mathfrak{a} \subset \{t + \ell z_0 \mid \ell \in \mathbb{Z}, t \in \mathfrak{a} \cap \mathbb{Z}\}.$$

L'inclusion inverse étant évidente, on a égalité. Comme $\mathfrak{a} \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, il est principal, et on a $\mathfrak{a} \cap \mathbb{Z} = g\mathbb{Z}$, avec $g \in \mathbb{Z}$. Notons que $|z_0|^2 = z_0\overline{z}_0 \in \mathfrak{a} \cap \mathbb{Z} \setminus \{0\}$ car z_0 est non nul. Ainsi, $\mathfrak{a} \cap \mathbb{Z}$ est non nul, donc g est non nul.

Ainsi, $\mathfrak{a} = \mathbb{Z}z_0 + \mathbb{Z}g$. Comme $g \in \mathfrak{a}$, $g\alpha \in \mathfrak{a}$, et donc $s \mid g$. De plus, $z_0\alpha \in \mathfrak{a}$, soit $-sd + r\alpha \in \mathfrak{a}$, d'où $s \mid r$. Bref, on peut écrire $z_0 = s(b+\alpha)$ et $g = sa$, avec $a, b \in \mathbb{Z}$, où a est non nul. Enfin, on a $z_0(b - \alpha) = s(b+\alpha)(b-\alpha) = s(b^2 - d) \in \mathfrak{a} \cap \mathbb{Z} = g\mathbb{Z}$, d'où $g \mid s(b^2 - d)$, et ainsi $a \mid b^2 - d$. Finalement, $\mathfrak{a} = s(\mathbb{Z}(b+\alpha) + \mathbb{Z}a)$. De plus, $(s(b+\alpha), sa)$ est clairement $\mathbb{Q}$-libre (car $s \neq 0$) et on a

$$\mathfrak{a} = \mathbb{Z}s(b+\alpha) \oplus \mathbb{Z}sa.$$

Mais alors, on a $\mathfrak{a} \subset s(a, b+\alpha)$. Comme $\mathfrak{a}$ contient sa et $s(b+\alpha)$, on a aussi l'inclusion inverse, d'où $\mathfrak{a} = (a, b+\alpha)$. □

On peut maintenant associer une classe de conjugaison à toute classe d'idéaux. Soit $\mathfrak{a}$ un idéal non nul de A_d, et soit (ω_1, ω_2) une $\mathbb{Z}$-base de $\mathfrak{a}$. Comme $\alpha\omega_1, \alpha\omega_2 \in \mathfrak{a}$, ils s'écrivent de manière unique comme combinaison $\mathbb{Z}$-linéaire de ω_1 et ω_2. Il existe donc $M_{\mathfrak{a},\omega} \in \mathrm{M}_2(\mathbb{Z})$ tel que $M_{\mathfrak{a},\omega}\omega = \alpha\omega$, où $\omega = \begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix}$.

Remarquons d'abord que si (ω_1, ω_2) est une $\mathbb{Z}$-base de $\mathfrak{a}$, et si $\omega = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$, alors pour toute matrice $N \in \mathrm{M}_2(\mathbb{Z})$, $N\omega \Longrightarrow N = 0$.

En effet, si $N = \begin{pmatrix}x & y\\ z & t\end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$, et si $N\omega = 0$, alors $x\omega_1 + y\omega_2 = z\omega_1 + t\omega_2 = 0$, d'où $x = y = z = t = 0$ et $N = 0$.

En particulier, la matrice $M_{\mathfrak{a},\omega}$ est unique.

Notons aussi que conjuguer la relation $M_{\mathfrak{a},\omega}\omega = \alpha\omega$ donne $M_{\mathfrak{a},\omega}\overline{\omega} = -\alpha\overline{\omega}$. Ainsi, α et $-\alpha$ sont deux valeurs propres distinctes de $M_{\mathfrak{a},\omega}$. Comme on est en dimension 2, cela implique que $M_{\mathfrak{a},\omega}\omega$ est diagonalisable sur K_d, et son polynôme minimal est donc $(X-\alpha)(X+\alpha) = X^2+d$ (le polynôme minimal ne dépend pas du corps de base où on se place).

Lemme 2.9. *La classe de conjugaison $\mu(\mathfrak{a})$ de $M_{\mathfrak{a},\omega}$ est indépendante du choix de (ω_1, ω_2), et ne dépend que de la classe $[\mathfrak{a}]$.*

Démonstration. Soit (ω_1', ω_2') une autre $\mathbb{Z}$-base de $\mathfrak{a}$, et soit $M_{\mathfrak{a},\omega'} \in \mathrm{M}_2(\mathbb{Z})$ l'unique matrice telle que $M_{\mathfrak{a},\omega'}\omega' = \alpha\omega'$.

Comme $\omega_j' \in \mathfrak{a}$, ω_j' est combinaison $\mathbb{Z}$-linéaire de ω_1, ω_2. Il existe donc $S \in \mathrm{M}_2(\mathbb{Z})$ telle que $\omega' = S\omega$, avec des notations évidentes. En échangeant les rôles des deux $\mathbb{Z}$-bases, on voit qu'il existe $S' \in \mathrm{M}_2(\mathbb{Z})$ telle que $\omega = S'\omega'$. On a donc $(SS' - I_2)\omega = 0$. Comme (ω_1, ω_2) est une $\mathbb{Z}$-base, on a $SS' - I_2 = 0$. On montre de même que $S'S = I_2$, d'où $S \in \mathrm{GL}_2(\mathbb{Z})$.

On a alors

$$M_{\mathfrak{a},\omega'}\omega' = M_{\mathfrak{a},\omega'}S\omega = \alpha\omega' = \alpha S\omega = S(\alpha\omega) = SM_{\mathfrak{a},\omega}\omega.$$

On a ainsi $(M_{\mathfrak{a},\omega'}S - SM_{\mathfrak{a},\omega})\omega = 0$, d'où $M_{\mathfrak{a},\omega'}S - SM_{\mathfrak{a},\omega} = 0$, et par conséquent $M_{\mathfrak{a},\omega'} = SM_{\mathfrak{a},\omega}S^{-1}$.

Ainsi, la classe de conjugaison $\mu(\mathfrak{a})$ ne dépend pas du choix de (ω_1, ω_2). Soit maintenant $z \in A_d$ non nul. Alors, $(z\omega_1, z\omega_2)$ est une $\mathbb{Z}$-base $z\mathfrak{a}$. Mais alors, on a $M_{\mathfrak{a},z\omega} = M_{\mathfrak{a},\omega}$, puisque si $M_{\mathfrak{a},\omega}\omega = \alpha\omega$, alors $M_{\mathfrak{a},\omega}(z\omega) = \alpha(z\omega)$. On a donc $\mu(z\mathfrak{a}) = \mu(\mathfrak{a})$.

Si maintenant $\mathfrak{a}'$ est un idéal non nul de A_d équivalent à $\mathfrak{a}$, il existe $z, z' \in A_d$ non nuls tels que $z'\mathfrak{a} = z\mathfrak{a}'$. Mais alors, on a

$$\mu(\mathfrak{a}') = \mu(z\mathfrak{a}') = \mu(z'\mathfrak{a}) = \mu(\mathfrak{a}).$$

□

Les lemmes 2.7 et 2.9 montrent que les deux applications bien définies

$$\begin{array}{rccc}\overline{c}\colon & \mathscr{C}(d) & \longrightarrow & \mathscr{C}\ell(-d)\\ & \mathrm{Conj}(M) & \longmapsto & c(M)\end{array}$$

et

$$\begin{array}{rccc} \overline{\mu}\colon & \mathscr{C}\ell(-d) & \longrightarrow & \mathscr{C}(d) \\ & [\mathfrak{a}] & \longmapsto & \mathrm{Conj}(\mathfrak{a}) \end{array},$$

où $\mathscr{C}(d)$ est l'ensemble des classes de conjugaison de matrices $M \in \mathrm{M}_2(d)$ de polynôme minimal X^2+d.

On a alors le résultat suivant.

Théorème 2.10. *Soit $d \geq 1$. Les applications $\overline{c}$ et $\overline{\mu}$ induisent une correspondance bijective entre l'ensemble $\mathscr{C}(d)$ des classes de conjugaison de matrices $M \in \mathrm{M}_2(d)$ de polynôme minimal X^2+d, et l'ensemble des classes d'idéaux $\mathscr{C}\ell(-d)$.*

En particulier, $\mathscr{C}\ell(-d)$ est fini.

De plus, si $M = [a,b,c]_d$, alors la classe de conjugaison de M est envoyée sur la classe de l'idéal $\mathbb{Z}(b+\alpha)\oplus\mathbb{Z}a$, et la classe de conjugaison de $[1,0,d]_d$ est envoyée sur la classe triviale.

Démonstration. Si $M \in \mathrm{M}_2(\mathbb{Z})$ est de polynôme minimal X^2+d, $\overline{c}(\mathrm{Conj}(M))$ est la classe de $\mathfrak{a} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, où $\omega = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ est un vecteur propre de M associé à α. Mais alors, par construction,la classe de $\overline{\mu}[\mathfrak{a}_\omega]$ est envoyée sur la classe de conjugaison d'une matrice dont un vecteur propre pour la valeur propre α est ω. Or, M est une telle matrice, d'où $\overline{\mu}\circ\overline{c} = \mathrm{Id}$.

Si maintenant $\mathfrak{a}$ est un idéal non nul de A_d et si (ω_1,ω_2) est une $\mathbb{Z}$-base de $\mathfrak{a}$, alors $\overline{\mu}([\mathfrak{a}])$ est la classe de conjugaison d'une matrice M dont ω est un vecteur propre associé à α. Mais, alors $\overline{c}(\mathrm{Conj}(M))$ est la classe de l'idéal dont les éléments sont les combinaisons $\mathbb{Z}$-linéaires des coordonnées d'un vecteur propre de M à coefficients de A_d associé à α. Or, ω est un tel vecteur propre, et l'idéal obtenu est $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, c'est-à-dire $\mathfrak{a}$. Par conséquent, $\overline{c}\circ\overline{\mu} = \mathrm{Id}$.

Ceci établit la bijection attendue. La finitude de $\mathscr{C}\ell(-d)$ découle alors du lemme 1.6.

Enfin, si $M = [a,b,c]_d$, l'exemple 2.4 montre que

$$\overline{c}(\mathrm{Conj}(M)) = [\mathbb{Z}(b+\alpha)\oplus\mathbb{Z}a].$$

Ceci achève la démonstration. □

Corollaire 2.11. *Soit $d \geq 1$. Alors, toutes les matrices de $\mathrm{M}_2(\mathbb{Z})$ de polynôme minimal X^2+d sont conjuguées si, et seulement si, l'anneau A_d est principal.*

Démonstration. Cela découle du théorème précédent et de la fin de la remarque 2.6. □

On peut maintenant réinterpréter les exemples 1.8.

Exemple 2.12. Si $d = 1, 2$, il est bien connu que A_d est un anneau principal. L'ensemble $\mathscr{C}\ell(-d)$ est donc trivial, et il n'y a qu'une classe de conjugaison de matrices de $M_2(\mathbb{Z})$ de polynôme minimal $X^2 + d$.

Si $d \geq 3$, l'exemple 1.8 nous dit que l'anneau A_d ne peut être principal, ce que l'on va maintenant montrer directement.

Pour cela, vérifions que 2 est un élément irréductible non premier.

On montre facilement que $z \in A_d^\times \iff |z|^2 = 1 \iff z = \pm 1$. Ainsi, 2 est non nul, non inversible. Si maintenant $2 = z_1 z_2, z_i \in A_d$, alors $4 = |z_1|^2 |z_2|^2$, d'où $|z_1|^2 = 1, 2, 4$. Dans le premier cas, z_1 est inversible, et dans le troisième, on a $|z_2|^2$ est inversible. Dans le deuxième cas, si $z_1 = x + y\alpha$, on a $x^2 + dy^2 = 2$. Si $y \neq 0$, on a $x^2 = dy^2 \geq d > 2$, donc $y = 0$ et $x^2 = 2$, ce qui est impossible. Bref, le deuxième cas ne se produit pas, et 2 est irréductible dans A_d.

En revanche, (2) n'est pas un idéal premier.

En effet, si $d = 2m, m \geq 2$, on a $\alpha^2 = -d = -2m \in (2)$, mais $\alpha \notin (2)$, car $(2) = \{x + y\alpha \mid x, y \in frm{-}e\mathbb{Z}\}$.

Si $d = 2m - 1, m \geq 2$, on a $(1+\alpha)(1-\alpha) = 1 - \alpha = d + 1 = 2m \in (2)$, mais $1 + \alpha \notin (2)$.

En regardant de plus près la correspondance et l'exemple 1.8, on conclut d'ailleurs que l'idéal $(2, \alpha)$ n'est pas principal si $d \geq 3$ est pair, et que l'idéal $(2, 1 + \alpha)$ est non principal si $d \geq 3$ est impair, ce que l'on peut vérifier directement.

Si $\mathfrak{a}$ est un idéal non nul de A_d, on note

$$\overline{\mathfrak{a}} = \{\overline{x} \mid x \in \mathfrak{a}\},$$

où $\overline{\ }$ désigne la conjugaison complexe. Clairement, c'est un idéal non nul de A_d. On peut maintenant donner une première réponse au problème de conjugaison entre une matrice et sa transposée.

Lemme 2.13. *Soit $M \in \mathrm{M}_2(\mathbb{Z})$ dont le polynôme minimal est $X^2 + d$, correspondant à la classe d'un idéal non nul $\mathfrak{a}$ de A_d. Alors, M^t correspond à la classe de $\overline{\mathfrak{a}}$.*

En particulier, M et M^t sont conjuguées si, et seulement si, $\mathfrak{a}$ et $\overline{\mathfrak{a}}$ sont équivalents.

Démonstration. Si $M = [a, b, c]_d$, sa classe de conjugaison correspond à la classe de $\mathfrak{a} = \mathbb{Z}(b + \alpha) \oplus \mathbb{Z}a$. Alors,

$$\overline{\mathfrak{a}} = \mathbb{Z}(b - \alpha) \oplus \mathbb{Z}a = \mathbb{Z}(-b + \alpha) \oplus \mathbb{Z}a.$$

Par conséquent, $[a, -b, c]_d$ est envoyée sur $\overline{\mathfrak{a}}$; sa classe de conjugaison correspond donc à $[\overline{\mathfrak{a}}]$. Or, d'après les relations introduites avant le lemme 1.6, on a

$$S_1 [a, -b, c]_d S_1^{-1} = [-c, b, -a]_d = M^t,$$

et donc $[a,-b,c]_d$ est conjuguée à M^t. On a donc le premier point. Le reste est alors clair. □

Ceci est très loin d'être satisfaisant. Afin de continuer plus avant, on va faire une hypothèse supplémentaire sur d.

Dorénavant, on suppose que d est sans facteurs carrés, et que $-d \not\equiv 1[4]$.

On a alors le lemme suivant.

Lemme 2.14. *Soit $d \geq 1$ sans facteurs carrés, tel que $-d \not\equiv 1[4]$, et soit $\mathfrak{a}$ un idéal non nul de A_d. Alors, l'idéal $\mathfrak{a}\overline{\mathfrak{a}}$ est principal, engendré par un unique entier strictement positif.*

Plus précisément, si $\mathfrak{a} = s(a, b+\alpha)$, où $s, a \in \mathbb{Z}$ sont non nuls, $b \in \mathbb{Z}$ et $a \mid b^2 - d$, alors $\mathfrak{a}\overline{\mathfrak{a}} = (s^2 a)$.

Démonstration. D'après le lemme 2.8, on a $\mathfrak{a} = s(s, b+\alpha)$, avec $s, a \in \mathbb{Z}$ non nuls, $b \in \mathbb{Z}$ et $a \mid b^2 - d$.

Écrivons $b^2 - d = ac$. On commence par démontrer que $a, 2b$ et c sont premiers dans leur ensemble.

Comme d est sans facteurs carrés, a, b, c sont premiers dans leur ensemble. De plus, a et c ne peuvent être tous les deux pairs. Sinon, on aurait $ac \equiv 0[4]$. Mais, d étant sans facteurs carrés, on aurait nécessairement b impair, et donc $b^2 \equiv 1[4]$, d'où la contradiction $d \equiv -1[4]$. Ainsi, a ou c est impair, ce qui implique qu'en fait $a, 2b$ et c sont premiers dans leur ensemble.

Passons à la démonstration proprement dite. On a facilement que l'idéal $\mathfrak{a}\overline{\mathfrak{a}}$ est engendré par

$$x_1 = s^2(b+\alpha)(b-\alpha), x_2 = s^2(b+\alpha)a, x_3 = s^2(b-\alpha)a, x_4 = s^2a^2.$$

En particulier, $\mathfrak{a}\overline{\mathfrak{a}} \subset (as^2)$.

De plus, on a $x_1 = s^2(b^2-d) = acs^2$ et $x_2 + x_3 = 2bs^2$. Par conséquent, $\mathfrak{a}\overline{\mathfrak{a}}$ contient le sous-groupe de $\mathbb{Z}$ engendré par $c(as^2), 2b(as^2), a(as^2)$. Comme $a, 2b$ et c sont premiers entre eux, ce sous-groupe n'est rien d'autres que $as^2\mathbb{Z}$. Bref, $\mathfrak{a}\overline{\mathfrak{a}}$ contient as^2, donc contient (as^2). Ainsi, $\mathfrak{a}\overline{\mathfrak{a}} = (as^2)$.

Quitte à remplacer as^2 par son opposé, on en déduit que $\mathfrak{a}\overline{\mathfrak{a}}$ est engendré par un entier strictement positif. Maintenant, si $\mathfrak{a}\overline{\mathfrak{a}} = (m) = (n)$, avec $m, n > 0$, alors m et n sont égaux à un inversible de A_d près. Mais $A_d^\times = \{\pm 1\}$, et comme m et n sont strictement positifs, ils sont égaux. □

Définition 2.15. Soit $\mathfrak{a}$ un idéal non nul de A_d. La *norme* de $\mathfrak{a}$ est l'unique générateur strictement positif de $\mathfrak{a}\overline{\mathfrak{a}}$. On le note $N(\mathfrak{a})$.

Le lemme suivant résume les propriétés utiles de la norme.

Lemme 2.16. *Soit $d \geq 1$ sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Pour tous idéaux non nuls $\mathfrak{a}, \mathfrak{b}$ de A_d, et tout $z \in A_d \setminus \{0\}$, on a :*

(1) $N((z)) = |z|^2$;
(2) $N(\mathfrak{a}) = 1$ *si, et seulement si,* $\mathfrak{a} = A_d$;
(3) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.
(4) *Si* $\mathfrak{a} = s(a, b + \alpha)$, *avec* $s, a \in \mathbb{Z}$ *non nuls,* $b \in \mathbb{Z}$ *et* $a \mid b^2 - d$, *alors* $N(\mathfrak{a}) = s^2 a$.

Démonstration. Montrons (1). Si $z \in A_d$ est non nul, on a $\overline{(z)} = (\overline{z})$. Par conséquent, $(z)(\overline{z}) = (z\overline{z}) = (|z|^2)$. Comme $|z|^2$ est un entier strictement positif, on utilise alors la définition pour conclure.

En prenant $z = 1$, on obtient $N(A_d) = 1$. Inversement, si $\mathfrak{a}$ est un idéal non nul de norme 1, alors par définition, on a $\mathfrak{a}\overline{\mathfrak{a}} = (1) = A_d$. En particulier, $A_d = \mathfrak{a}\overline{\mathfrak{a}} \subset \mathfrak{a}$, d'où $\mathfrak{a} = A_d$, d'où (2).

Si $\mathfrak{a}, \mathfrak{b}$ sont deux idéaux non nuls de A_d, on vérifie que l'on a les égalités

$$\mathfrak{ab}\overline{\mathfrak{ab}} = \mathfrak{ab}\overline{\mathfrak{a}}\,\overline{\mathfrak{b}} = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{b}\overline{\mathfrak{b}}.$$

Par conséquent,

$$\mathfrak{ab}\overline{\mathfrak{ab}} = (N(\mathfrak{a}))(N(\mathfrak{b})) = (N(\mathfrak{a})N(\mathfrak{b})).$$

Comme $N(\mathfrak{a})N(\mathfrak{b})$ est un entier strictement positif, la définition de la norme permet de conclure. Le dernier point découle du lemme 2.14 et de la définition de la norme. □

La norme permet de démontrer parfois la non principalité des idéaux à peu de frais.

Exemple 2.17. Soit $d \geq 3$ sans facteurs carrés, et tel que $-d \not\equiv 1[4]$. On pose $\mathfrak{a} = (2, \alpha)$ si $d = 2m$ et $\mathfrak{a} = (2, 1 + \alpha)$ si $d = 2m - 1$.

Si $d = 2m$, on a $2 \mid 0^2 + d$, et si $d = 2m - 1$, on a $2 \mid 1^2 + d$. D'après le lem 2.16, dans les deux cas, on a $N(\mathfrak{a}) = 2$. Si on avait $\mathfrak{a} = (z), z \in A_d$, on aurait $N(\mathfrak{a}) = 2 = |z|^2$, par le lemme 2.16. Or, on a déjà constaté que l'équation $|z|^2 = 2, z \in A_d$, n'a pas de solutions. On retrouve donc la non principalité de $\mathfrak{a}$ déjà établies (avec certes des hypothèses supplémentaires sur d).

On a alors le théorème suivant.

Théorème 2.18. *Soit $d \geq 1$ sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Alors, le produit d'idéaux induit sur $\mathscr{C}\ell(-d)$ une structure de groupe abélien fini, dont le neutre est la classe $[A_d]$. De plus, pour tout idéal $\mathfrak{a}$ non nul, on a $[\mathfrak{a}]^{-1} = [\overline{\mathfrak{a}}]$.*

Enfin, toute classe de $\mathscr{C}\ell(-d)$ est représenté par un idéal $\mathfrak{a}$ vérifiant $N(\mathfrak{a}) \leq 2\sqrt{\dfrac{d}{3}}$.

Démonstration. On sait déjà que $\mathscr{C}\ell(-d)$ est fini d'après le théorème 2.10, et que le produit d'idéaux induit sur $\mathscr{C}\ell(-d)$ une loi associative, commutative, de neutre $[A_d]$ par la remarque 2.6. Pour montrer que $\mathscr{C}\ell(-d)$ est un groupe, il reste à voir que tout élément de $\mathscr{C}\ell(-d)$ est inversible. Or, le lemme 2.14 montre que pour tout idéal non nul $\mathfrak{a}$ de A_d, on a $[\mathfrak{a}][\overline{\mathfrak{a}}] = [\mathfrak{a}\overline{\mathfrak{a}}] = [A_d]$, ce qui permet de conclure.

D'autre part, le théorème 2.10 montre que tout élément de $\mathscr{C}\ell(-d)$ est de la forme $\overline{c}(\mathrm{Conj}(M))$, pour une matrice $M \in \mathrm{M}_2(\mathbb{Z})$ de polynôme minimal $X^2 + d$. Or, une telle matrice M est semblable à une matrice $[a, b, c]_d$ réduite, et dans ce cas, $1 \leq a \leq 2\sqrt{\dfrac{d}{3}}$, d'après le lemme 1.6. Or, l'élément de $\mathscr{C}\ell(-d)$ correspondant à la classe de similitude de $[a, b, c]_d$ est $\mathbb{Z}(b + \alpha) \oplus \mathbb{Z}a$, qui est de norme a, par le lemme 2.16. Ceci achève la démonstration. □

Le théorème 2.18 et le lemme 2.14 sont faux si $-d \equiv 1[4]$, comme le montre l'exemple suivant.

Exemple 2.19. Prenons $d = 3$, et soit $\mathfrak{a} = (2, 1 + \alpha)$. Alors, il n'existe pas d'idéal $\mathfrak{b}$ non nul tel que $\mathfrak{ab}$ soit principal. Autrement dit, $[\mathfrak{a}]$ n'a pas d'inverse dans $\mathscr{C}\ell(-3)$.

Pour le voir, commençons par remarquer que $\mathfrak{a}^2 = \mathfrak{a}$. En effet, on a

$$\mathfrak{a}^2 = (4, 2(1+\alpha), -2+2\alpha)) = (4, 2(1+\alpha), 2(1-\alpha)) = (4, 2(1+\alpha), 2(1+\alpha)+2(1-\alpha)),$$

c'est-à-dire

$$\mathfrak{a}^2 = (4, 2(1 + \alpha), 4) = (4, 2(1 + \alpha)) = 2\mathfrak{a}.$$

Autrement dit, $[\mathfrak{a}]^2 = [\mathfrak{a}]$. Supposons maintenant qu'il existe un idéal non nul $\mathfrak{b}$ tel que $\mathfrak{ab}$ soit principal. On a donc

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{ab}] = [A_3] \in \mathscr{C}\ell(3).$$

Mais alors,

$$[\mathfrak{a}] = [\mathfrak{a}][A_3] = [\mathfrak{a}]^2[\mathfrak{b}] = [\mathfrak{a}][\mathfrak{b}] = [A_3],$$

et par conséquent $\mathfrak{a}$ est principal. Or, ce n'est pas le cas d'après l'exemple 2.12.

On peut maintenant revenir au problème de conjugaison entre une matrice et sa transposée.

Proposition 2.20. *Soit $d \geq 1$ sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Soit $M \in \mathrm{M}_2(\mathbb{Z})$ dont le polynôme minimal est $X^2 + d$, correspondant à la classe d'un idéal non nul $\mathfrak{a}$ de A_d.*

Alors, M et M^t sont semblables si, et seulement si, $[\mathfrak{a}]$ est d'ordre au plus 2 dans $\mathscr{C}\ell(-d)$, c'est-à-dire si, seulement s, $\mathfrak{a}^2$ est principal.

En particulier, toute matrice de $\mathrm{M}_2(\mathbb{Z})$ *de polynôme minimal* X^2+d *est semblable à sa transposée si, et seulement si,* $\mathscr{C}\ell(-d) \simeq (\mathbb{Z}/2\mathbb{Z})^r$ *pour un certain* $r \geq 0$.

Démonstration. D'après le lemme 2.13, M et M^t sont semblables si, et seulement si $\mathfrak{a}$ et $\overline{\mathfrak{a}}$ sont équivalents. Cela revient à dire que $[\mathfrak{a}] = [\overline{\mathfrak{a}}] = [\mathfrak{a}]^{-1}$, soit encore $[\mathfrak{a}]^2 = [A_d]$. Ceci est encore équivalent à $[\mathfrak{a}^2] = [A_d]$, i.e. $\mathfrak{a}^2$ est principal.

Le dernier point provient du fait bien connu qu'un groupe (abélien) fini dont tous les éléments sont d'ordre au plus est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^r$ pour un certain $r \geq 0$. □

On continue ces considérations en démontrant que $\mathscr{C}\ell(-d)$ est d'ordre pair.

Proposition 2.21. *Soit* $d \geq 3$ *sans facteurs carrés et tel que* $-d \not\equiv 1[4]$. *Alors,* $\mathscr{C}\ell(-d)$ *est d'ordre pair.*

En particulier, il existe une matrice $M \in \mathrm{M}_2(d)$ *de polynôme minimal* X^2+d, *non semblable à* $\begin{pmatrix} 0 & -d \\ 1 & 0 \end{pmatrix}$ *qui est semblable à sa transposée.*

Démonstration. Il suffit de démontrer que $\mathscr{C}\ell(-d)$ possède un élément d'ordre 2.

Supposons que $d = 2m$, avec $m \geq 3$. Comme d est sans facteurs carrés, m est impair. On sait déjà que $\mathfrak{a} = (2, \alpha)$ n'est pas principal, d'après l'exemple 2.12. De plus, on a $\mathfrak{a}^2 = (4, 2\alpha, -2m)$. Comme $\mathfrak{a}^2$ contient 4 et $2m$, il contient $4\mathbb{Z} + 2m\mathbb{Z}$. Puisque m est impair, le pgcd de 4 et -2m est 2. Par conséquent $2 \in \mathfrak{a}^2$, et $(2) \subset \mathfrak{a}^2$. De plus, on a clairement $\mathfrak{a}^2 \subset (2)$, d'où $\mathfrak{a}^2 = (2)$. Par conséquent, $\mathfrak{a}^2$ est principal, et $[\mathfrak{a}]$ est d'ordre 2.

Supposons que $d = 2m-1$, avec $m \geq 2$. Comme $-d \equiv 1[4]$, m est impair. D'après l'exemple 2.12, $\mathfrak{a} = (2, 1+\alpha)$ n'est pas principal. De plus, on a

$$\mathfrak{a}^2 = (4, 2(1+\alpha), 2-2m+2\alpha) = (4, 2(1+\alpha), -2m) \subset (2).$$

Comme précédemment, puisque m est impair, $\mathfrak{a}^2$ contient alors 2, et $\mathfrak{a}^2 = (2)$. Le reste est alors clair. □

On va maintenant démontrer que $\mathscr{C}\ell(-5) \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathscr{C}\ell(-14) \simeq \mathbb{Z}/4\mathbb{Z}$, ce qui explique a posteriori les exemples 1.5.

Exemples 2.22.

(1) Supposons que $d = 5$. Dans ce cas, on vérifie facilement qu'il n'y a que deux matrices réduites, à savoir $[1, 0, -5]_5$ et $[2, 1, 3]_5$,

c'est-à-dire

$$\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & -3 \\ 2 & -1 \end{pmatrix}.$$

Comme on sait que ces deux matrices ne sont pas semblables (cf. exemple 1.5 (1)), on en déduit que $\mathscr{C}\ell(-5)$ possède deux éléments. Par conséquent, $\mathscr{C}\ell(5) \simeq \mathbb{Z}/2\mathbb{Z}$. En particulier, toute matrice de $\mathrm{M}_2(\mathbb{Z})$ de polynôme minimal X^2+5 est semblables à sa transposée, ce qui confirme ce que l'on a constaté dans l'exemple 1.5 (1).

(2) Supposons maintenant que $d = 14$. Dans ce cas, quelques petits calculs rapides montrent qu'il y a quatre matrices réduites, à savoir

$$\begin{pmatrix} 0 & -14 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -7 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -5 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -5 \\ 3 & -1 \end{pmatrix}.$$

On a donc $|\mathscr{C}\ell(-14)| = 1, 2, 3$ ou 4. La proposition précédente nous dit alors que $|\mathscr{C}\ell(-14)| = 2$ ou 4.

Soit $\mathfrak{a} = (3, 1+\alpha)$. Comme l'ordre de $[\mathfrak{a}]$ divise l'ordre de $\mathscr{C}\ell(14)$, il divise 4 (quelque soit le cas dans lequel on est). Montrons que $\mathfrak{a}^2$ n'est pas principal. Cela démontrera en particulier que $[\mathfrak{a}]$ n'est pas d'ordre 1 ou 2, et donc que $[\mathfrak{a}]$ est d'ordre 4. Cela imposera alors que $\mathscr{C}\ell(-14)$ est d'ordre 4, et donc cyclique, engendré par $[\mathfrak{a}]$.

Puisque $3 \mid 1^2 + 14$, le lemme 2.16 montre que $N(\mathfrak{a}) = 3$. Le lemme 2.16 implique alors que $N(\mathfrak{a}^2) = N(\mathfrak{a})^2 = 9$. Supposons que $\mathfrak{a}^2 = (z)$ pour un certain $z \in A_d$ non nul. Le même lemme montre alors que l'on aurait $N(\mathfrak{a}^2) = |z|^2$. Ainsi, on aurait $|z|^2 = 9$. Les calculs usuels montrent alors nécessairement que $z = \pm 3$. Quitte à remplacer z par $-z$, on peut suppose $z = 3$.

On doit donc avoir

$$\mathfrak{a}^2 = (3) = (9, 3(1+\alpha), -13 + 2\alpha).$$

En particulier, on a $-13 + 2\alpha \in (3)$, soit $3 \mid -13 + 2\alpha$, ce qui n'est pas possible, car 2 n'est pas un multiple entier de 3. Ainsi, $\mathfrak{a}^2$ n'est pas principal, et on a fini.

Notons que la classe de l'idéal $\mathfrak{a}$ correspond à la matrice $\begin{pmatrix} 1 & -5 \\ 3 & -1 \end{pmatrix}$. Comme $[\mathfrak{a}]$ n'est pas d'ordre 2, on retrouve le fait que cette matrice n'est pas semblable à sa transposée, ce que l'on avait démontré dans l'exemple 1.5 (2).

On connaît 35 valeurs de $d \geq 1$, avec d sans facteurs carrés et $-d \not\equiv 1[4]$, pour lesquelles $\mathscr{C}\ell(-d) \simeq (\mathbb{Z}/2\mathbb{Z})^r$, la plus grande étant 1365. On sait d'autre part qu'il y a au plus une autre valeur de d qui convienne,

et sous l'hypothèse de Riemann généralisée, on démontre que ces 35 valeurs sont en fait les seules.

La plus petite valeur de d n'apparaissant pas dans la liste est d'ailleurs $d = 14$.

Afin de pouvoir faire des calculs, il convient de mieux comprendre le groupe $\mathscr{C}\ell(-d)$. En particulier, il serait bon de connaître un système de générateurs. C'est l'objet du paragraphe suivant.

3. Factorisation d'idéaux en produit d'idéaux premiers

Dans ce paragraphe, on va démontrer que tout idéal non nul de A_d se factorise en produit d'idéaux premiers, de manière unique à l'ordre des facteurs près.

Commençons par introduire une notion de divisibilité entre idéaux.

Définition 3.1. Soit A un anneau commutatif, et soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A. On dit que $\mathfrak{a}$ *divise* $\mathfrak{b}$ s'il existe un idéal $\mathfrak{c}$ de A tel que $\mathfrak{b} = \mathfrak{ac}$.

On le note $\mathfrak{a} \mid \mathfrak{b}$.

On commence par deux lemmes techniques.

Lemme 3.2. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Alors :*

(1) *pour tous idéaux $\mathfrak{a}, \mathfrak{b}$ et tout idéal non nul $\mathfrak{c}$ de A_d, on a $\mathfrak{ac} = \mathfrak{bc} \Longrightarrow \mathfrak{a} = \mathfrak{b}$;*

(2) *pour tout idéaux $\mathfrak{a}, \mathfrak{b}$ de A_d, on a $\mathfrak{a} \mid \mathfrak{b}$ si, et seulement si, $\mathfrak{a} \supset \mathfrak{b}$.*

Démonstration. Gardons les notations de l'énoncé, et montrons (1). Si $\mathfrak{ac} = \mathfrak{bc}$, alors $\mathfrak{ac}\overline{\mathfrak{c}} = \mathfrak{bc}\overline{\mathfrak{c}}$. Le lemme 2.14 montre alors que $m\mathfrak{a} = m\mathfrak{b}$, avec $m = N(\mathfrak{c})$. On en déduit facilement que $\mathfrak{a} = \mathfrak{b}$ (l'anneau A_d étant de caractéristique nulle, $m \in 0$, et on peut utiliser l'intégrité de l'anneau).

Montrons (2). Si $\mathfrak{a} \mid \mathfrak{b}$, il existe $\mathfrak{c}$ tel que $\mathfrak{b} = \mathfrak{ac}$. Comme $\mathfrak{ac} \subset \mathfrak{a}$, on a bien $\mathfrak{b} \subset \mathfrak{a}$. Supposons maintenant que $\mathfrak{b} \subset \mathfrak{a}$. Si $\mathfrak{a} = 0$, alors $\mathfrak{b} = 0$, et on a $\mathfrak{a} \mid \mathfrak{b}$, puisque $(0) = (0)(0)$. Supposons $\mathfrak{a}$ non nul. Alors, on a $\overline{\mathfrak{a}}\mathfrak{b} \subset (m)$, où $m = N(\mathfrak{a})$. Soit $\mathfrak{c} = \{z \in A_d \mid mz \in \overline{\mathfrak{a}}\mathfrak{b}\}$. C'est clairement un idéal de A_d, et de plus $m\mathfrak{c} = \overline{\mathfrak{a}}\mathfrak{b}$. En effet, par définition, on a $m\mathfrak{c} \in \overline{\mathfrak{a}}\mathfrak{b}$. De plus, si $z' \in \overline{\mathfrak{a}}\mathfrak{b}$, il existe $z \in A_d$ tel que $z' = mz$ d'après l'inclusion ci-dessus. Mais alors, $z \in \mathfrak{c}$ et $z' \in m\mathfrak{c}$.

Bref, on a $\overline{\mathfrak{a}}\mathfrak{b} = m\mathfrak{c}$, puis $m\mathfrak{b} = m\mathfrak{ac}$ en multipliant par $\mathfrak{a}$. Mais alors $\mathfrak{b} = \mathfrak{ac}$, d'où $\mathfrak{a} \mid \mathfrak{b}$. □

On s'intéresse maintenant aux propriétés des idéaux premiers.

Lemme 3.3. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$, et soit $\mathfrak{p}$ un idéal non nul de A_d. Alors, les propriétés suivantes sont équivalentes :*

(1) *$\mathfrak{p}$ est un idéal premier ;*
(2) *$\mathfrak{p}$ est un idéal maximal ;*
(3) *$\mathfrak{p} \neq A_d$, et pour tous idéaux $\mathfrak{a}, \mathfrak{b}$, on a $\mathfrak{p} = \mathfrak{ab} \Longrightarrow \mathfrak{a} = A_d$ ou $\mathfrak{b} = A_d$.*

Dans ce cas,les seuls diviseurs de $\mathfrak{p}$ sont A_d et $\mathfrak{p}$, et pour tous idéaux $\mathfrak{a}, \mathfrak{b}$, on a $\mathfrak{p} \mid \mathfrak{ab} \Longrightarrow \mathfrak{p} \mid \mathfrak{a}$ ou $\mathfrak{p} \mid \mathfrak{b}$.

Démonstration. Soit $\mathfrak{p}$ un idéal non nul. Supposons que $\mathfrak{p}$ soit un idéal premier, et soit $m = N(\mathfrak{p})$. Alors, $(m) = \mathfrak{p}\overline{\mathfrak{p}} \subset \mathfrak{p}$, et on a donc un morphisme d'anneaux surjectifs $A/(m) \longrightarrow A/\mathfrak{p}$. Comme A est isomorphe à $\mathbb{Z}^2$ comme groupe abélien, $A/(m)$ est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^2$ comme groupe abélien. En particulier, $A/(m)$ est fini, et par suite $A/\mathfrak{p}$ est fini. Mais, $\mathfrak{p}$ étant premier, $A/\mathfrak{p}$ est intègre. Or, un anneau intègre fini est un corps, et $\mathfrak{p}$ est maximal.

Remontrons ce dernier point rapidement. Si B est un anneau fini intègre, pour tout $b \in B$ non nul, l'application

$$\begin{aligned} B &\longrightarrow B \\ x &\longmapsto bx \end{aligned}$$

est injective par intégrité. Comme B est fini, elle est donc surjective. En particulier, il existe $b' \in B$ tel que $bb' = 1_B$, et b est donc inversible.

Supposons maintenant que $\mathfrak{p}$ soit maximal. Alors, $\mathfrak{p} \neq A_d$. Supposons maintenant que $\mathfrak{p} = \mathfrak{ab}$. Si $\mathfrak{a} \neq A_d$, alors,$\mathfrak{p} \subset \mathfrak{a}$, et par maximalité, $\mathfrak{a} = \mathfrak{p}$. Mais alors $\mathfrak{p} = \mathfrak{pb}$, et par le lemme 3.2, on a $\mathfrak{b} = A_d$.

Supposons enfin que $\mathfrak{p}$ vérifie (3). Alors, $\mathfrak{p} \neq A_d$. Soient $x, y \in A_d$ tels que $xy \in \mathfrak{p}$. On a donc $(x)(y) \subset \mathfrak{p}$. Par le lemme 3.2, on a $\mathfrak{p} \mid (x)(y)$, et par hypothèse, on a $\mathfrak{p} \mid (x)$ ou $\mathfrak{p} \mid (y)$, c'est-à-dire $(x) \subset \mathfrak{p}$ ou $(y) \subset \mathfrak{p}$. Mais alors, $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$, et $\mathfrak{p}$ est premier.

Supposons enfin que $\mathfrak{p}$ vérifie une des trois conditions équivalentes. Soit $\mathfrak{a}$ un diviseur de $\mathfrak{p}$. Alors, on peut écrire $\mathfrak{p} = \mathfrak{ab}$, pour un certain idéal $\mathfrak{b}$. Par (2), on a $\mathfrak{a} = A_d$ ou $\mathfrak{b} = A_d$. Mais le second cas implique $\mathfrak{p} = \mathfrak{a}A_d = \mathfrak{a}$. On a donc bien $\mathfrak{a} = A_d$ ou $\mathfrak{p}$.

Soient maintenant $\mathfrak{a}, \mathfrak{b}$ tels que $\mathfrak{p} \mid \mathfrak{ab}$. Alors, $\mathfrak{ab} \subset \mathfrak{p}$. Comme $\mathfrak{p} \subset \mathfrak{a}+\mathfrak{p}$, on a $\mathfrak{a}+\mathfrak{p} = \mathfrak{p}$ ou $\mathfrak{a}+\mathfrak{p} = A_d$ d'après ce qui précède. Dans le premier cas, on a $\mathfrak{a} \subset \mathfrak{p}$ car $\mathfrak{a} \subset \mathfrak{a}+\mathfrak{p}$, et donc $\mathfrak{p} \mid \mathfrak{a}$ par le lemme 3.2. Dans le second cas, on a

$$\mathfrak{b} \subset \mathfrak{b}(\mathfrak{a}+\mathfrak{p}) \subset \mathfrak{ab}+\mathfrak{p}.$$

Comme $\mathfrak{p} \mid \mathfrak{ab}$, on a $\mathfrak{ab} \subset \mathfrak{p}$ et ainsi $\mathfrak{b} \subset \mathfrak{p}+\mathfrak{p} \subset \mathfrak{p}$, d'où $\mathfrak{p} \mid \mathfrak{b}$. □

Corollaire 3.4. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Alors, tout idéal non nul de A_d dont la norme est un nombre premier est un idéal premier.*

Démonstration. Soit $\mathfrak{p}$ un idéal de A_d tel que $N(\mathfrak{p}) = p$, avec p premier. Supposons que $\mathfrak{a}$ soit un idéal de A_d vérifiant $\mathfrak{a} \mid \mathfrak{p}$. Alors, il existe $\mathfrak{b}$ tel que $\mathfrak{p} = \mathfrak{ab}$. Par le lemme 2.16, on a

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{p}) = p,$$

d'où $N(\mathfrak{a}) = 1$ ou $N(\mathfrak{a}) = p$. Dans le premier cas, ce même lemme montre que $\mathfrak{a} = A_p$. Dans le second cas, on a $N(\mathfrak{b}) = 1$, et donc $\mathfrak{b} = A_d$, et par conséquent $\mathfrak{p} = \mathfrak{a}A_d = \mathfrak{a}$. D'après le lemme précédent, $\mathfrak{p}$ est premier. □

On peut maintenant démontrer le théorème fondamental sur les idéaux de A_d.

Théorème 3.5. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Alors, tout idéal non nul s'écrit comme produit d'idéaux premiers, et la décomposition est unique à permutation près des facteurs.*

Démonstration. On démontre l'existence par récurrence sur la norme des idéaux. Pour tout $n \geq 1$, soit (H_n) la propriété :

(H_n) tout idéal non nul $\mathfrak{a}$ de A_d vérifiant $N(\mathfrak{a}) \leq n$ se décompose en produit d'idéaux premiers.

Si $n = 1$, on a $N(\mathfrak{a}) = 1$, et donc $\mathfrak{a} = A_d$ par le lemme 2.16. Ainsi, $\mathfrak{a}$ est un produit vide d'idéaux premiers, et (H_1) est donc vraie.

Supposons avoir montré (H_n) pour un entier $n \geq 1$, et soit $\mathfrak{a}$ un idéal non nul de A_d tel que $N(\mathfrak{a}) \leq n + 1$. Si $\mathfrak{a}$ est premier, on a notre décomposition. Sinon, il existe deux idéaux $\mathfrak{b}, \mathfrak{c} \neq A_d$ tel que $\mathfrak{a} = \mathfrak{bc}$, d'après le lemme 3.3. Notons que $N(\mathfrak{b}) < N(\mathfrak{a})$ et $N(\mathfrak{c}) < N(\mathfrak{a})$. En effet, si $N(\mathfrak{b}) = N(\mathfrak{a})$, on a $N(\mathfrak{c}) = 1$, puis $\mathfrak{c} = A_d$ par le lemme 2.16, ce qui est exclus. Si $N(\mathfrak{c}) = N(\mathfrak{a})$, on obtient de même la contradiction $\mathfrak{b} = A_d$. Ainsi, on a $N(\mathfrak{b}) \leq n$ et $N(\mathfrak{c}) \leq n$, donc par hypothèse de récurrence, $\mathfrak{b}$ et $\mathfrak{c}$ s'écrivent comme un produit d'idéaux premiers. Il en est donc de même de $\mathfrak{bc} = \mathfrak{a}$. Par conséquent, (H_{n+1}) est établie ce qui achève la récurrence, et la démonstration de l'existence d'une décomposition.

Pour la démonstration de l'unicité, on procède exactement comme dans $\mathbb{N}$. C'est possible car on peut simplifier par un idéal non nul, et car un idéal premier vérifie des propriétés similaires à un nombre premier (les seuls diviseurs de $\mathfrak{p}$ sont A_d et $\mathfrak{p}$, et si $\mathfrak{p}$ divise un produit d'idéaux, il divise un des facteurs). □

Ceci n'est évidemment plus vrai si $-d \equiv 1[4]$.

Exemple 3.6. Soit $d = 3$, et soit $\mathfrak{a} = (2, 1 + \alpha)$. Alors, on a vu que $\mathfrak{a}$ est non principal, et que $\mathfrak{a}^2 = 2\mathfrak{a}$. Si on avait existence et unicité d'une décomposition en produit d'idéaux premiers, on pourrait décomposer (2) et $\mathfrak{a}$, et simplifier chaque facteur de $\mathfrak{a}$ pour obtenir la contradiction $\mathfrak{a} = (2)$.

On déduit du théorème 2.18 et de ce qui précède le résultat suivant.

Théorème 3.7. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Alors, $\mathscr{C}\ell(-d)$ est engendré par les classes d'idéaux premiers dont la norme est inférieure à $2\sqrt{\frac{d}{3}}$.*

Démonstration. On sait que toute classe de $\mathscr{C}\ell(-d)$ est représentée par un idéal non nul $\mathfrak{a}$ de norme inférieure à $2\sqrt{\frac{d}{3}}$. Si $\mathfrak{p}$ est un diviseur premier de $\mathfrak{a}$, on a $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$, et alors $N(\mathfrak{a}) = N(\mathfrak{p})N(\mathfrak{b})$. Mais alors, $N(\mathfrak{p}) \leq N(\mathfrak{a}) \leq 2\sqrt{\frac{d}{3}}$. Comme $\mathfrak{a}$ est produit d'idéaux premiers, on en déduit le résultat voulu. □

Nous allons poursuivre notre étude et expliquer maintenant comme trouver tous les idéaux premiers de l'anneau A_d. On commence par montrer qu'un idéal premier contient un unique nombre premier p.

Lemme 3.8. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$, et soit $\mathfrak{p}$ un idéal premier non nul de A_d. Alors, il existe un unique nombre premier p tel que $(p) \subset \mathfrak{p}$.*

Si p est un tel nombre premier, on a $N(\mathfrak{p}) = p$ ou p^2.

Démonstration. L'idéal $\mathfrak{p} \cap \mathbb{Z}$ est un idéal non nul de $\mathbb{Z}$ (si $z \in \mathfrak{p}$ est non nul, alors $|z|^2 = z\overline{z}$ est un élément non nul de $\mathfrak{p} \cap \mathbb{Z}$). Or, il est facile de constater que $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Comme il est non nul, il existe un nombre premier p tel que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Mais alors, $p \in \mathfrak{p}$, d'où $(p) \subset \mathfrak{p}$ et par suite $\mathfrak{p} \mid (p)$. Il existe alors un idéal $\mathfrak{a}$ non nul tel que $(p) = \mathfrak{p}\mathfrak{a}$. D'après le lemme 2.16, on a alors

$$N(\mathfrak{p})N(\mathfrak{a}) = p^2,$$

et comme p est premier, on a $N(\mathfrak{p}) = 1, p$ ou p^2. Le premier cas est exclu, car cela impliquerait $\mathfrak{p} = A_d$, ce qui est impossible puisque $\mathfrak{p}$ est premier.

Soit maintenant un nombre premier q tel que $(q) \subset \mathfrak{p}$. Alors, $q \in \mathfrak{p}$. Ainsi, $q \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, et par conséquent $p \mid q$. Comme p et q sont premiers, on obtient alors $q = p$. □

Pour déterminer tous les idéaux premiers, il suffit donc de savoir trouver tous les idéaux premiers $\mathfrak{p}$ contenant un nombre premier p fixé, c'est-à-dire tous les diviseurs premiers de (p). Il faut donc factoriser l'idéal (p).

La proposition suivant donne une réponse complète.

Proposition 3.9. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$, et soit p un nombre premier. Alors :*

(1) *si $p \nmid d$ et $-d$ n'est pas un carré modulo p, alors (p) est l'unique idéal premier de A_d contenant p ;*

(2) *si $p \nmid d$ est un carré modulo p et p est impair, et si $\omega \in \mathbb{Z}$ vérifie $-d \equiv \omega^2[p]$, alors $\mathfrak{p} = (p, \omega+\alpha)$ et $\overline{\mathfrak{p}} = (p, \omega-\alpha)$ sont distincts, et sont les seuls idéaux premiers de A_d contenant (p). De plus, on a $(p) = \mathfrak{p}\overline{\mathfrak{p}}$.*

(3) *si $p \mid d$ ou si $p = 2$ (les deux cas ne s'excluant pas nécessairement), alors $\mathfrak{p} = (p, \alpha)$ est l'unique idéal premier de A_d contenant p, et $(p) = \mathfrak{p}^2$;*

Démonstration. Notons que dans le premier cas, p est impair, puisque tout entier est un carré modulo 2, et donc les trois cas s'excluent bien mutuellement.

On a déjà constaté que l'on avait un isomorphisme d'anneaux $A_d \simeq \mathbb{Z}[X]/(X^2+d)$. Quelques applications des divers théorèmes de factorisation montrent que l'on a des isomorphismes d'anneaux

$$A/(p) \simeq \mathbb{Z}[X]/(p, X^2+d) \simeq \mathbb{F}_p[X]/(X^2+\tilde{d}),$$

où $\tilde{d}$ est la classe de d modulo p.

Si d n'est pas un carré modulo p, le polynôme $X^2+\tilde{d}$ n'a pas de racines, et est donc irréductible (puisqu'il est de degré 2). Puisque $\mathbb{F}_p[X]$ est principal, $\mathbb{F}_p[X]/(X^2+\tilde{d})$ est un corps, et (p) est maximal, et donc premier.

Supposons que d soit un carré modulo p (on ne suppose rien de plus pour l'instant) et soit $\omega \in \mathbb{Z}$ vérifie $-d \equiv \omega^2[p]$. Posons $\mathfrak{p} = (p, \omega + \alpha)$.Comme $p \mid (\pm\omega)^2 + d$, par le lemme 2.14, on a donc

$$N(\mathfrak{p}) = N(\overline{\mathfrak{p}}) = p,$$

et $\mathfrak{p}$ et $\overline{\mathfrak{p}}$ sont donc des idéaux premiers d'après le corollaire 3.4.

Notons que $\mathfrak{p}$ ne dépend pas du choix de ω, puisque $(p, \omega + mp + \alpha) = (p, \omega + \alpha)$. En particulier, si $p \mid d$, on peut prendre $\omega = 0$. Dans ce cas, $\mathfrak{p} = (p, \omega) = \overline{\mathfrak{p}}$ et $(p) = \mathfrak{p}^2$.

Supposons maintenant que $p = 2$. Alors, on a

$$\overline{\mathfrak{p}} = (2, -\omega + \alpha) = (2, 2\alpha + \omega - \alpha) = (2, \omega - \alpha) = \overline{\mathfrak{p}},$$

et $(2) = \mathfrak{p}^2$.

Il reste à démontrer que si $p \nmid d$ et p est impair, on a $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Comme $p \mid (\pm\omega)^2 + d$, par le lemme 2.14, on a $\mathfrak{p} = \mathbb{Z}p \oplus \mathbb{Z}(\omega + \alpha)$ et $\overline{\mathfrak{p}} = \mathbb{Z}p \oplus (-\omega + \alpha)$. Si $\mathfrak{p} = \overline{\mathfrak{p}}$, on a donc $-\omega + \alpha = up + v(\omega + \alpha)$, avec $u, v \in \mathbb{Z}$. On en déduit alors $v = 1$, puis $-\omega = up + \omega$. Ainsi, $p \mid 2\omega$. Or, p est impair, et comme $p \nmid d$, on a aussi $p \nmid \omega$, d'où une contradiction. □

Ce résultat permet de réduire encore un peu plus la famille génératrice de $\mathscr{C}\ell(-d)$.

Théorème 3.10. *Soit $d \geq 1$ un entier sans facteurs carrés, tel que $-d \not\equiv 1[4]$. Alors, le groupe $\mathscr{C}\ell(-d)$ est engendré par les classes des idéaux premiers divisant p, où p décrit l'ensemble des nombres premiers vérifiant au moins une des conditions suivantes :*

(1) $p \leq \sqrt[4]{\dfrac{4d}{3}}$ *si p est impair, $p \nmid d$, et $-d$ n'est pas un carré modulo p ;*

(2) $p \leq \sqrt{\dfrac{4d}{3}}$ *si p est impair, $p \nmid d$, et $-d$ est un carré modulo p ;*

(3) $p \leq \sqrt{\dfrac{4d}{3}}$ *si $p \mid d$ ou $p = 2$.*

Démonstration. Pour s'en convaincre, il suffit d'utiliser le théorème 3.7 et le résultat précédent, en calculant la norme des diviseurs premiers de (p) dans chaque cas. □

Remarque 3.11. Si p est un carré modulo p, il n'est pas nécessaire de prendre les classes des deux diviseurs premiers de p ; un seul suffit. En effet, on a $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, et par conséquent $[\overline{\mathfrak{p}}] = [\mathfrak{p}]^{-1}$.

Exemple 3.12. Prenons $d = 30$. On a $\sqrt[4]{\dfrac{4d}{3}} \approx 2.78$ et $\sqrt{\dfrac{4d}{3}} \approx 7.75$. On peut donc se restreindre dans un premier aux nombres premiers ≤ 7, c'est-à-dire $2, 3, 5, 7$. De plus, $-30 \mod 5[7]$ et les carrés de $(\mathbb{Z}/7\mathbb{Z})^\times$ sont les classes de $1, 2, 4$. Par conséquent, -30 n'est pas un carré modulo 7, et on peut éliminer 7.

Bref, il suffit de considérer les idéaux premiers divisant $p = 2, 3$ et 5, c'est-à-dire

$$\mathfrak{p}_2 = (2, \alpha), \ \mathfrak{p}_3 = (3, \alpha), \ \mathfrak{p}_5 = (5, \alpha).$$

Comme $\mathfrak{p}_p^2 = (p)$ $(p = 2, 3, 5)$, leurs classes dans $\mathscr{C}\ell(-30)$ sont d'ordre au plus 2.

On sait alors que $\mathscr{C}\ell(-30) \simeq (\mathbb{Z}/2\mathbb{Z})^r$, avec $r \leq 3$ (en effet, $\mathscr{C}\ell(-30)$ est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel, possédant une famille génératrice à 3 éléments).

Pour $p = 2, 3, 5$, l'idéal $\mathfrak{p}_p$ n'est pas principal. En effet, s'il l'était, il existerait $z \in A_{30}$ tel que $\mathfrak{p}_p = (z)$. D'après le lemme 2.16, on aurait $|z|^2 = p$. Or, si $x, y \in \mathbb{Z}$ vérifient $x^2 + 30y^2 = p$, alors nécessairement $y = 0$, d'où la contradiction $x^2 = p$.

Maintenant, on a $\alpha^2 = -30 = -2{\cdot}3{\cdot}5$, d'où

$$(\alpha)^2 = (\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5)^2.$$

En décomposant (α) en produits d'idéaux premiers, on en déduit que $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$, d'où $[p_5] = [\mathfrak{p}_2]^{-1}[\mathfrak{p}_3]^{-1}$. On est maintenant réduit à deux générateurs, à savoir $[\mathfrak{p}_2]$ et $[\mathfrak{p}_3]$. Il reste finalement à décider si ces deux classes sont égales ou non.

Si $[\mathfrak{p}_2] = [\mathfrak{p}_3]$, alors $[\mathfrak{p}_2\mathfrak{p}_3] = [\mathfrak{p}_2]^2 = [(2)] = [A_{30}]$. Comme $\mathfrak{p}_2\mathfrak{p}_3$ est de norme 6, cela implique qu'il est engendré par un élément de A_{30} dont le carré du module est 6. Comme précédemment, on voit qu'un tel élément n'existe pas.

Au bout du compte, on a $\mathscr{C}\ell(-30) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, où les générateurs sont $[\mathfrak{p}_2]$ et $[\mathfrak{p}_3]$.

On aurait pu aller plus rapidement en estimant le nombre de matrices réduites. Si $d = 30$, on trouve les quatre matrices

$$[0, 0, 30]_{30}, [2, 0, 15]_{30}, [3, 0, 5]_{30}, [5, 0, 6]_{30}.$$

Cela donne $\mathscr{C}\ell(-30) \leq 4$, et si on croit au fait (avéré) que deux matrices réduites distinctes ne sont pas semblables, on obtient $\mathscr{C}\ell(-30) = 4$.

Pour vraiment comprendre les idéaux premiers de A_d, il reste à savoir déterminer quand un entier donné est un carré modulo p ou non. On démontre (et nous admettrons) qu'il existe une unique application

$$\begin{aligned} \mathbb{Z} \times (2\mathbb{N} + 1) &\longrightarrow \mathbb{Z} \\ (m, n) &\longmapsto \left(\frac{m}{n}\right) \end{aligned}$$

vérifiant les propriétés suivantes :

(1) pour tout $n \geq 1$ impair, et tout $m \in \mathbb{Z}$, on a $\left(\frac{m}{n}\right) \in \{0, 1, -1\}$;

(2) pour tout $m \in \mathbb{Z}$, $\left(\frac{m}{1}\right) = 1$;

(3) pour tout $n \geq 1$ impair, et tout $m, k \in \mathbb{Z}$, $\left(\frac{m + kn}{n}\right) = \left(\frac{m}{n}\right)$;

(4) pour tout $n \geq 1$ impair, et tout $m \in \mathbb{Z}$, $\left(\frac{m}{n}\right) \neq 0$ si, et seulement si, m est premier à n ;

(5) pour tout $n \geq 1$ impair, et tout $m, m' \in \mathbb{Z}$, $\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$;

(6) pour tout $n \geq 1$ impair, et tout $m \in \mathbb{Z}$ premier à n, $\left(\frac{m^2}{n}\right) 1$;

(7) pour tout p premier impair, et tout $m \in \mathbb{Z}$ premier à p, $\left(\frac{m}{p}\right) = 1$ si, et seulement si, m est un carré modulo p ;

(8) pour tous $n, m \geq 1$ premiers entre eux, $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right)$;

(9) pour tout $n \geq 1$ impair, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ et $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Toutes ces propriétés permettent de déterminer si un entier est un carré modulo p, sans avoir à factoriser les entiers (il suffit juste de savoir factoriser par 2).

Exemples 3.13.

(1) Déterminons si 70 est un carré modulo 197. On a

$$\left(\frac{70}{197}\right) = \left(\frac{2}{197}\right)\left(\frac{35}{197}\right) = -\left(\frac{35}{197}\right) = -\left(\frac{197}{35}\right),$$

d'où

$$\left(\frac{70}{197}\right) = -\left(\frac{-13}{35}\right) = -\left(\frac{-1}{35}\right)\left(\frac{13}{35}\right) = \left(\frac{13}{35}\right) = \left(\frac{35}{13}\right) = \left(\frac{-4}{13}\right),$$

soit

$$\left(\frac{70}{197}\right) = \left(\frac{-1}{13}\right)\left(\frac{2^2}{13}\right) = \left(\frac{-1}{13}\right) = 1.$$

Par conséquent, 70 est un carré modulo 197. On peut d'ailleurs vérifier que l'on a $55^2 \equiv 70$ [197].

(2) Calculons $\left(\frac{13898}{8911}\right)$. On a

$$\left(\frac{13898}{8911}\right) = \left(\frac{-3924}{8911}\right) = \left(\frac{-1}{8911}\right)\left(\frac{2}{8911}\right)^2\left(\frac{981}{8911}\right).$$

On a ainsi

$$\left(\frac{13898}{8911}\right) = -\left(\frac{981}{8911}\right) = -\left(\frac{8911}{981}\right) = -\left(\frac{82}{981}\right).$$

d'où

$$\left(\frac{13898}{8911}\right) = -\left(\frac{2}{981}\right)\left(\frac{41}{981}\right) = \left(\frac{41}{981}\right) = \left(\frac{981}{41}\right).$$

On a alors
$$\left(\frac{13898}{8911}\right) = \left(\frac{981}{41}\right) = \left(\frac{-3}{41}\right) = \left(\frac{-1}{41}\right)\left(\frac{3}{41}\right) = \left(\frac{3}{41}\right).$$
Enfin, on obtient
$$\left(\frac{13898}{8911}\right) = \left(\frac{41}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$
Ainsi, 13898 n'est pas un carré modulo 8911.

L'application $\left(\frac{-}{n}\right)$ s'appelle le *symbole de Jacobi modulo n*. Lorsque p est premier, on l'appelle plutôt *symbole de Legendre modulo p*.

Ce symbole permet aussi de fournir une formule explicite pour l'ordre du groupe $\mathscr{C}\ell(-d)$. Puisque $\mathbb{Z}[i]$ est principal, le groupe $\mathscr{C}\ell(-1)$ est trivial. Pour $d \geq 2$, on a la formule suivante.

Théorème 3.14. *Soit $d \geq 2$ un entier sans facteurs carrés tel que $-d \not\equiv 1[4]$. Alors, on a*
$$|\mathscr{C}\ell(-d)| = -\frac{1}{4d}\sum_{k=0}^{2d-1}(-1)^k\left(\frac{d}{2k+1}\right)(2k+1).$$

Remarque 3.15. Lorsque d est de plus impair, cette égalité peut se récrire comme suit :
$$|\mathscr{C}\ell(-d)| = \frac{1}{4d}\sum_{k=0}^{d-1}(-1)^k\left(\frac{2k+1}{d}\right)(4d-4k-2).$$

4. Application à l'équation de Bachet

Le groupe $\mathscr{C}\ell(-d)$ a bien entendu un intérêt qui va au-delà du problème des classes de conjugaison de matrices entières. Montrons comment on peut résoudre des équations diophantiennes grâce à cet outil.

On s'intéresse à l'équation $t^3 = x^2 + d,\ x, t \in \mathbb{Z}$. On suppose ici que $d \geq 1$ est sans facteurs carrés, et que $-d \equiv 1[4]$. Cette équation se récrit
$$t^3 = (x-\alpha)(x+\alpha) \in A_d.$$

Une première idée serait de démontrer que $x-\alpha$ et $x+\alpha$ sont premiers entre eux, puis d'en déduire en utilisant l'existence et l'unicité d'une décomposition en irréductibles que $x-\alpha$ et $x+\alpha$ sont des cubes. Malheureusement, cette démarche ne fonctionne que pour $d = 1, 2$, puisque ce sont les seules valeurs pour lesquelles A_d est principal (et même factoriel).

En revanche, on va pouvoir utiliser (grâce à l'hypothèse sur d) l'existence et l'unicité de la décomposition en idéaux premiers.

Posons $\mathfrak{a} = (x+\alpha)$, et montrons que $\mathfrak{a}$ et $\overline{\mathfrak{a}}$ sont premiers entre eux. Dans le cas contraire, ils auraient un diviseur premier $\mathfrak{p}$ en commun. On aurait donc $\mathfrak{a} \subset \mathfrak{p}$ et $\overline{\mathfrak{a}} \subset \mathfrak{p}$. En particulier, $x \pm \alpha \in \mathfrak{p}$, puis $2\alpha \in \mathfrak{p}$. En multipliant par $-\alpha$, on obtient alors $-2d \in \mathfrak{p}$. Comme $t^3 = (x-\alpha)(X+\alpha)$, on a $t^3 \in \mathfrak{p}$, puis $t \in \mathfrak{p}$ car $\mathfrak{p}$ est premier. Ainsi, $t\mathbb{Z}+2d\mathbb{Z} \subset \mathfrak{p}$.

Montrons que t et $2d$ sont premiers entre eux dans $\mathbb{Z}$, ce qui conduira à la contradiction $1 \in \mathbb{Z} = t\mathbb{Z} + 2d\mathbb{Z} \subset \mathfrak{p}$ (puisque $\mathfrak{p}$ est premier, on a $\mathfrak{p} \neq A_d$). Montrons tout d'abord que t est impair. Si t est pair, $t^3 \equiv 0[4]$. On a donc $-d \equiv x^2[4]$. Or $-d \equiv 2, 3[4]$ (on ne peut avoir $-d \equiv 0[4]$ car d est sans facteurs carrés). Comme $x^2 \equiv 0, 1[4]$, on obtient une contradiction. Ainsi, t est impair. Il reste alors à montrer que t est premier à d pour conclure. Si t et d possèdent un diviseur premier commun p, alors $p \mid x^2$, donc $p \mid x$. Mais, $p \mid t$ et on obtient alors $p^2 \mid d$, d'où une contradiction par hypothèse sur d. Finalement, t et $2d$ sont premiers entre eux.

Bref, $\mathfrak{a}$ et $\overline{\mathfrak{a}}$ sont premiers entre eux, et leur produit est un cube. En décomposant en produit d'idéaux premiers, et en utilisant l'unicité de la décomposition, on obtient que $\mathfrak{a} = \mathfrak{b}^3$, pour un certain idéal $\mathfrak{b}$ de A_d.

Supposons maintenant que $3 \nmid |\mathscr{C}\ell(-d)|$. Dans ce cas, comme

$$[\mathfrak{b}]^3 = [\mathfrak{b}^3] = [\mathfrak{a}] = [(x+\alpha)] = 1 \in \mathscr{C}\ell(-d),$$

on en déduit $[\mathfrak{b}] = 1$, i.e. $\mathfrak{b}$ est principal. Si on écrit $\mathfrak{b} = (z), z \in A_d$, on en déduit $(x+\alpha) = (z^3)$. Or, A_d est intègre, et on a $A_d^\times = \{\pm 1\}$. Ainsi, $x + \alpha = \pm z^3$. Si $z = u + v\alpha, u, v \in \mathbb{Z}$, en développant et en identifiant parties réelles et imaginaires, on obtient

$$x = \pm u(u^2 - 3dv^2) \quad \text{et} \quad \pm 1 = (3u^2 - dv^2)v.$$

La seconde équation implique que $v = \pm 1$ (et donc $v^2 = 1$). On a alors $d = 3u^2 \pm 1$ et $x = \pm u(u^2 - 3d)$. Notons que l'on a aussi

$$(t)^3 = (t^3) = (\mathfrak{b}\overline{\mathfrak{b}})^3,$$

puis par unicité de la décomposition

$$(t) = \mathfrak{b}\overline{\mathfrak{b}} = (z\overline{z}),$$

d'où encore $t = \pm z\overline{z} = \pm(u^2 + d)$. Comme $t^3 = x^2 + d \geq 0$, on a finalement $t \geq 0$ et $t = u^2 + d$. Bref, on a démontré le théorème suivant.

Théorème 4.1. *Soit $d \geq 1$ un entier sans facteurs carrés tel que $-d \not\equiv 1[4]$. On suppose que $3 \nmid |\mathscr{C}\ell(-d)|$. Alors, l'équation $t^3 = x^2 + d, t, x \in \mathbb{Z}$ a des solutions si, et seulement si, il existe $u \in \mathbb{Z}$ tel que $d = 3u^2 \pm 1$. Dans ce cas, les solutions sont $(x, t) = (\pm u(u^2 - 3d), u^2 + d)$.*

5. Compléments

On a des résultats totalement similaires lorsque $-d \equiv 1[4]$, mais il faut considérer les matrices 2×2 de polynôme minimal $X^2 + X + \dfrac{d+1}{4}$ et les idéaux de l'anneau $\mathbb{Z}[\frac{-1+i\sqrt{d}}{2}]$.

Tout ceci s'inscrit dans un cadre plus général. Si K est un corps qui est aussi un $\mathbb{Q}$-espace vectoriel de dimension finie $n \geq 1$, on note $\mathcal{O}_K$ l'ensemble des éléments de K annulés par un polynôme unitaire à coefficients dans $\mathbb{Z}$. On montre alors que $\mathcal{O}_K$ est un anneau, et que tout idéal non nul de $\mathcal{O}_K$ peut se factoriser de manière unique en produit de puissances d'idéaux premiers. De plus, tout idéal non nul de $\mathcal{O}_K$ possède une $\mathbb{Z}$-base à n éléments. De plus, $\mathscr{C}\ell(\mathcal{O}_K)$ (qui est défini de manière similaire à $\mathscr{C}\ell(-d)$) est un groupe abélien fini.

En particulier, si $\mathcal{O}_K$ est de la forme $\mathbb{Z}[\alpha] = \{P(\alpha) \mid P \in \mathbb{Z}[X]\}$, on a à nouveau une correspondance entre $\mathscr{C}\ell(\mathcal{O}_K)$ et l'ensemble des classes de similitude de matrices entière de polynôme minimal μ_α, où μ_α est le polynôme minimal de l'endomorphisme de multiplication par α dans le $\mathbb{Q}$-espace vectoriel K.

Cette situation n'est pas très fréquente, mais on a quand même quelques familles d'exemples intéressants :

(i) Si $K = \mathbb{Q}[\sqrt{\Delta}]$, avec $\Delta \in \mathbb{Z}$ non nul sans facteurs carrés, alors $\mathcal{O}_K = \mathbb{Z}[\sqrt{\Delta}]$ si $\Delta \not\equiv 1[4]$, et $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{\Delta}}{2}]$ si $\Delta \equiv 1[4]$.

(ii) Si $K = \mathbb{Q}[\zeta_n]$, alors $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ $(n \geq 1)$.

Le point (i) explique alors tous les résultats obtenus dans ce texte, en prenant subtilement $\Delta = -d$.

Il est intéressant de noter qu'il n'y a qu'un nombre fini de valeurs de Δ pour lesquelles $\mathcal{O}_K$ est un anneau principal ($K = \mathbb{Q}[\sqrt{\Delta}]$) lorsque $\Delta < 0$. On a déjà vu que pour $\Delta \not\equiv 1[4]$, $\Delta = -1, -2$ sont les seules valeurs possibles, mais il y en a sept autres lorsque $\Delta \equiv 1[4]$, à savoir $-3, -7, -11, -19, -43, -67$ et -163. En revanche, on ne sait toujours pas à l'heure actuelle s'il y a une infinité d'entiers $\Delta > 0$ sans facteurs carrés tel que $\mathcal{O}_K$ soit principal lorsque $K = \mathbb{Q}[\sqrt{\Delta}]$. À vrai dire, on ne sait même pas s'il y a une infinité de corps K tel que $\mathcal{O}_K$ soit principal.