RAPPORT DE RECHERCHE

L R I

GRAPHES, HYPERGRAPHES, DROITE PROJECTIVE, QUATERNIONS

DELORME C

Unité Mixte de Recherche 8623
CNRS-Université Paris Sud – LRI

10/2007

Rapport de Recherche N° 1477

CNRS – Université de Paris Sud
Centre d'Orsay
LABORATOIRE DE RECHERCHE EN INFORMATIQUE
Bâtiment 490
91405 ORSAY Cedex (France)

Graphes, hypergraphes, droite projective, quaternions

C. Delorme *

October 15, 2007

Abstract

We build some highly symmetrical graphs and compute some of their parameters. The construction involves some algebraic and geometric tools. Some well-known graphs, such as Biggs triple graphs, Biggs and Hoare sextet graphs, Ramanujan graphs, are thus placed in a common frame

Résumé

On se propose ici de décrire certaines façons de construire des graphes sommets-transitifs en indiquant leurs caractéristiques communes. Ces graphes font intervenir des objets algébriques et géométriques simples. Ils permettent de voir la parenté de certains graphes connus (graphes de triplets de Biggs, graphes de sextets de Biggs et Hoare, graphes de Ramanujan, etc.) en les plaçant dans un cadre commun

1 La droite projective sur un anneau

On prend un anneau commutatif et unitaire R.

Un point de la droite projective $PG(1,R)$ est une classe d'équivalence de couples d'éléments de R, les deux éléments du couple engendrant R en tant qu'idéal; autrement dit, si $\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ est un couple convenable, il existe des éléments u, v de R tels que $ua_1 + va_2 = 1$. Quand à la relation d'équivalence, elle se définit par l'action des homothéties, c'est-à-dire que deux couples $\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$ sont équivalents s'il existe un élément inversible u de R tel que $ua_1 = b_1$ et $ua_2 = b_2$.

*LRI, Bât 490, Université Paris-XI, F-91400 ORSAY

1.1 Fonctorialité

Un morphisme d'anneaux unitaires $\rho : R_1 \to R_2$ induit fonctoriellement une application naturelle $PG(1,\rho) : PG(1,R_1) \to PG(1,R_2)$. Cela veut dire que le composé de deux morphismes d'anneaux unitaires induit la composée des applications induites par les deux morphismes, et que l'identité d'un anneau induit l'identité sur la droite correspondante. L'image de la classe de $\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ est la classe de $\begin{bmatrix} \rho(a_1) \\ \rho(a_2) \end{bmatrix}$. Les compatibilités nécessaires se vérifient sans peine et sans amusement.

1.2 Dénombrement

Quand R est le corps fini $\mathbf{F}_q$ à q éléments, la droite projective a $q+1$ éléments : les classes des $\begin{bmatrix} x \\ 1 \end{bmatrix}$ et la classe de $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Quand R est $\mathbf{Z}/p^k\mathbf{Z}$, il y a $p^k + p^{k-1}$ éléments sur la droite. Plus généralement, les deux règles suivantes permettent de traiter tous les anneaux commutatifs et unitaires finis.

- si R est un anneau fini et local (c'est-à-dire ayant un seul idéal maximal) de corps résiduel (le quotient de R par son unique idéal maximal) le corps $\mathbf{F}_q$ à q éléments, il est facile de voir que R a q^k éléments pour un certain entier k et que la droite projective a $q^k + q^{k-1}$ éléments.

- si R est l'anneau produit $R_1 \times R_2$, la droite projective $PG(1,R)$ s'identifie naturellement à l'ensemble produit $PG(1,R_1) \times PG(1,R_2)$.

Que ces règles suffisent résulte très simplement du théorème suivant :
Théorème *Tout anneau fini est le produit de ses composantes locales.*
Preuve du théorème

Il suffit de voir que si R est fini et non local, c'est un produit d'anneaux de cardinal moindre. On fait alors une petite récurrence et le tour est joué. Soit donc r dans un des idéaux maximaux, mais pas dans tous. On trouve par finitude deux puissances de r égales, soit $r^u = r^{u+v}$ avec $0 < v$. Alors $w = r^{uv}$ est idempotent (*i.e.* $w^2 = w$), et différent de 0 et 1. Donc l'anneau R est isomorphe au produit de ses deux quotients R/wR et $R/(1-w)R$ avec les projections évidentes. En effet $(\overline{x_1}, \overline{x_2})$ est l'image de $x_1(1-w) + x_2 w$ pour tous x_1 et x_2 de R

Ainsi la droite sur $\mathbf{Z}/6\mathbf{Z}$ a 12 éléments, celle sur $\mathbf{Z}/12\mathbf{Z}$ en a 24.

1.3 Points bien distincts

Deux points, représentés par les couples $\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ et $\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$, sont *bien distincts* si le déterminant $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$ est inversible dans R.

Par exemple si R est un corps, tous les points sont bien distincts; si R est $\mathbf{Z}/4\mathbf{Z}$, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ est bien distinct de $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$, mais pas de $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$.

Fonctorialité

L'application naturelle associée à un morphisme d'anneau préserve les paires de points bien distincts. On a même mieux :

- si R est un anneau local, la relation "x n'est pas bien distinct de y" est une relation d'équivalence, la même que "x et y ont même image dans la droite projective du corps résiduel".
- si R est l'anneau produit $R_1 \times R_2$, les paires de points bien distincts sont caractérisées par le fait que leurs images par les projections naturelles dans $PG(1, R_1)$ et $PG(1, R_2)$ sont elles-mêmes des paires de points bien distincts.

2 Graphes de triplets ordonnés

Les sommets de $\Gamma(R)$ sont les triplets ordonnés (a, b, c) formés d'éléments mutuellement bien distincts de $PG(1, R)$.

Les arêtes issues du triplet (a, b, c) le joignent aux triplets (a', b, c), (a, b', c), (a, b, c') de sorte que les birapports $[a, a', b, c]$, $[b, b', a, c]$, $[c, c', a, b]$ valent -1. Le premier de ces birapports est

$$[a, a', b, c] = \frac{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a'_1 & b_1 \\ a'_2 & b_2 \end{vmatrix}} \div \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a'_1 & c_1 \\ a'_2 & c_2 \end{vmatrix}}$$

Les autres se calculent similairement. On observe que si a, b, c sont des images de couples d'entiers, il en va de même pour a', b', c'. Donc il est inutile de prendre autre chose que des $\mathbf{Z}/n\mathbf{Z}$ pour avoir des graphes connexes .

Il est opportun de constater que les morphismes d'anneaux induisent fonctoriellement des morphismes de graphes. Cela ne présente pas de difficulté.

2.1 Dénombrement des sommets

Le nombre de ces triplets est $q^3 - q$ pour un corps à q éléments. Pour les anneaux commutatifs finis, on pourra s'appuyer sur les deux règles :

- si R est un anneau local, de corps résiduel $\mathbf{F}_q$, ayant q^k éléments, le nombre des triplets est $(q^3 - q)q^{3k-3}$
- si R est l'anneau produit $R_1 \times R_2$, le nombre des triplets pour R est le produit des nombres de triplets pour R_1 et R_2.

Par exemple pour $\mathbf{Z}/3\mathbf{Z}$ cela donne 24, pour $\mathbf{Z}/4\mathbf{Z}$ cela donne 48, pour $\mathbf{Z}/12\mathbf{Z}$ cela fera 1152 triplets.

2.2 Sommet-transitivité

Le groupe projectif $PGL(2, R)$ opère sur les points de la droite projective. L'opération est simple à décrire : elle se représente par

$$\left(M, \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right) \mapsto M \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$$

où M est une matrice 2×2 inversible (définie à homothétie près). Elle se comporte aussi de manière fonctorielle. Plus en détail, tout morphisme $\rho : R_1 \to R_2$ d'anneaux commutatifs unitaires induit fonctoriellement un morphisme de groupes $PGL(2, \rho) : PGL(2, R_1) \to PGL(2, R_2)$, et le morphisme d'ensembles (ou application) déjà vu $PG(1, \rho) : PG(1, R_1) \to PG(1, R_2)$. Abrégeons ici en ρ_G et ρ_D ces deux applications (G comme groupe et D comme droite). Le caractère fonctoriel de l'opération de $PGL(2, \bullet)$ sur $PG(1, \bullet)$ comporte aussi l'égalité : $\rho_G(g).\rho_D(x) = \rho_D(g.x)$

Ce groupe opère transitivement sur les triplets : en effet, on envoie le triplet $\left(\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}\right)$ vers $\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} u \\ v \end{bmatrix}\right)$ en utilisant la matrice inverse de $\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$ pour un certain choix des représentants, puis ceci vers $\left(\begin{bmatrix} u^{-1} \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ v^{-1} \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right)$ avec une matrice diagonale. Ce triplet est le même que $\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right)$

Le stabilisateur d'un point quelconque est réduit à l'identité : seules les matrices scalaires conservent chacune des trois droites engendrées par les trois vecteurs $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ et $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

Le graphe $\Gamma(R)$ ainsi obtenu est sommet-transitif car l'opération du groupe $PGL(2,R)$ respecte les arêtes. Là encore c'est du petit calcul sans difficulté.

2.3 Le point de vue des graphes de Cayley

Le graphe $\Gamma(R)$ n'est autre qu'un graphe de Cayley du groupe $PGL(2,R)$. On numérote le triplet (a,b,c) par l'élément α de $PGL(2,R)$ qui envoie le triplet ordonné $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\right)$ sur (a,b,c). Alors les trois voisins de (a,b,c) sont numérotés par les $\alpha\sigma_i$ où les σ_i sont les numéros des trois voisins de $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\right)$.

Les σ_i sont représentés par les matrices

$$\begin{bmatrix}-1&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\2&-1\end{bmatrix},\begin{bmatrix}-1&2\\0&1\end{bmatrix}$$

2.4 Structure du graphe $\Gamma(\mathbf{Z})$

La condition "être bien distinct" est sévère dans $\mathbf{Z}$ car $\mathbf{Z}$ a peu d'éléments inversibles. Il apparaît que les triplets sont toujours à l'ordre et au signe près du style $t=\left(\begin{bmatrix}a_1\\a_2\end{bmatrix}\begin{bmatrix}b_1\\b_2\end{bmatrix}\begin{bmatrix}a_1+b_1\\a_2+b_2\end{bmatrix}\right)$. Si le plus grand en valeur absolue des dénominateurs des éléments de t, soit $\delta(t)$, n'est pas 1, alors t a un unique voisin t' avec $\delta(t')<\delta(t)$. Donc il y a un unique chemin de t vers les triplets où $\delta=1$. Ceux-là forment un chemin infini dans les deux sens, où la place de $\begin{bmatrix}1\\0\end{bmatrix}$ est fixe, et où les deux autres éléments sont $\begin{bmatrix}n\\1\end{bmatrix}$ et $\begin{bmatrix}n+1\\1\end{bmatrix}$, avec n parcourant $\mathbf{Z}$, les places de l'entier pair et de l'entier impair qui figurent parmi n et $n+1$ étant fixes aussi.

Ceci prouve que le graphe $\Gamma(\mathbf{Z})$ a 6 composantes connexes, reconnaissables à leur projection dans le graphe $\Gamma(\mathbf{Z}/2\mathbf{Z})$, qui a 6 points isolés. Ces composantes sont des arbres infinis réguliers de degré 3.

2.5 Composantes connexes des graphes $\Gamma(\mathbf{Z}/n\mathbf{Z})$

Dans ce paragraphe R sera $\mathbf{Z}/n\mathbf{Z}$.

On observera que le produit des trois déterminants issus d'un triplet (a,b,c)

$$\begin{vmatrix}a_1&b_1\\a_2&b_2\end{vmatrix}\begin{vmatrix}b_1&c_1\\b_2&c_2\end{vmatrix}\begin{vmatrix}c_1&a_1\\c_2&a_2\end{vmatrix}$$

est connu aux carrés près dans R^*. On peut donc définir une fonction ϕ qui à un triplet associe la classe du produit dans le groupe quotient de R^* par le sous-groupe des carrés de R^* (on note R^* le groupe multiplicatif des éléments inversibles de R)

Pour des sommets adjacents t, t', on a $\phi(t) = -\phi(t')$. Cela limite les composantes connexes : des triplets t et t' qui donnent $\phi(t) \neq \phi(t')$ et $\phi(t) \neq -\phi(t')$ ne peuvent pas être connectés.

Cela donne aussi une bipartition si -1 n'est pas un carré dans R.

On note aussi que si n est pair le morphisme issu de la projection naturelle $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ donne un découpage en 6 pièces isomorphes qui se projettent sur les 6 points de $\Gamma(\mathbf{Z}/2\mathbf{Z})$

On utilise une propriété des matrices à coefficients dans un anneau principal.

Théorème *Soit M une matrice 2×2 à coefficients entiers, dont le déterminant est $1 + nm$. Il existe une matrice M' à coefficients entiers, de déterminant 1 et congrue à M modulo n (autrement dit $M - M'$ a tous ses coefficients multiples de n).*

Preuve du théorème

On sait qu'il existe des matrices A et B à coefficients entiers et de déterminant 1 telles que $AMB = \begin{bmatrix} k & 0 \\ 0 & k' \end{bmatrix}$ où k est le pgcd des coefficients de M et $kk' = 1 + nm$ (voir [3]). On ajoute au besoin la matrice $\begin{bmatrix} 0 & n \\ 0 & 0 \end{bmatrix}$ pour avoir un pgcd des coefficients égal à 1, et on recommence. On a alors la matrice $A'AMBB' = \begin{bmatrix} 1 & 0 \\ 0 & 1+nm \end{bmatrix}$. Elle est congrue à Id modulo n. En revenant en arrière, on voit que M est congrue modulo n à une matrice de déterminant 1.

Si les trois déterminants d'une matrice 2×3 ont un produit carré modulo n, on peut en multipliant les colonnes modulo n faire en sorte que les déterminants soient tous $\equiv 1$ modulo n, puis choisir les représentants entiers des a_i et b_i pour que $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = 1$ et il est ensuite facile d'ajuster la dernière colonne pour que les déterminants vaillent 1. Alors il est clair que le graphe $\Gamma(\mathbf{Z})$ se projette surjectivement sur le graphe $\Gamma_1(R)$ des triplets donnant un produit dans $(\pm 1)\{\text{carrés de } R^*\}$.

Si n est pair, les 6 composantes donnent 6 composantes pour Γ_1; et si n est impair, Γ_1 est connexe.

2.6 Quotients

On peut ensuite faire le quotient par le sous-groupe A_3 d'automorphismes engendré par : $(a, b, c) \mapsto (b, c, a)$. Cela conserve la bipartition éventuelle dûe à "-1 pas carré". On peut aussi faire le quotient par S_3. Cette bipartition disparaît alors.

Les quotients ne sont plus des graphes de Cayley. Les sommets sont cette fois les αH où H est le sous-groupe engendré par les matrices $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ pour A_3 et $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ pour S_3. Les arêtes sont les images par la projection naturelle des arêtes du graphe que l'on quotiente. Comme la conjugaison par ces deux sous-groupes conserve l'ensemble des 3 homographies σ_i et comme les rapports $\sigma_i \sigma_j^{-1}$ ne sont pas dans ces sous-groupes A_3 et S_3 (sauf si $R = \mathbf{Z}/2\mathbf{Z}$), le degré reste trois.

Le quotient par S_3 lorsque n est premier est précisément le graphe de triplets décrit par Biggs [2]

2.7 Maille des graphes $\Gamma(\mathbf{Z}/n\mathbf{Z})$

Le birayon formé des triplets contenant $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ se referme en cycles de longueur ppcm(2,n) dans le graphe des triplets ordonnés et dans son quotient par A_3, il se referme en cycles de longueur n dans le quotient par S_3. Donc la maille g est au plus $\mathrm{ppcm}(2, n)$.

Le maille est minorée par les k tels que $\mathrm{fib}(k+2) \geq \mathrm{ppcm}(2, n)$, car les triplets à distance k du birayon formé des triplets contenant $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ont leurs dénominateurs qui ne dépassent pas le $(d+2)^{\text{i-ème}}$ nombre de Fibonacci (voir [2])

$$\mathrm{fib}(d+2) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{d+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{d+2} \right)$$

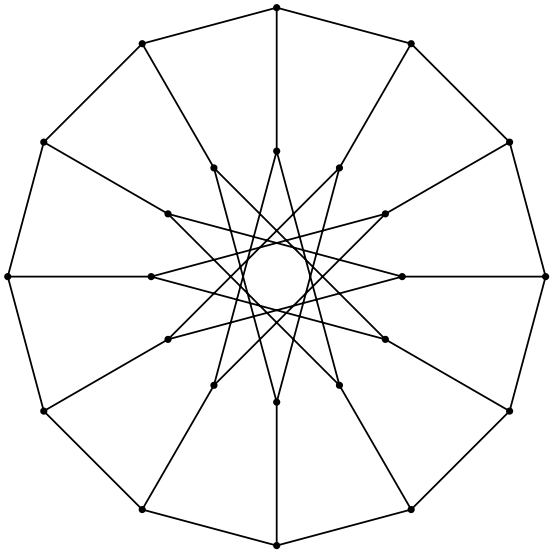
Dans les quotients, la minoration de la maille se fait avec les k tels que $\mathrm{fib}(k+2) \geq n$.

3 Exemples

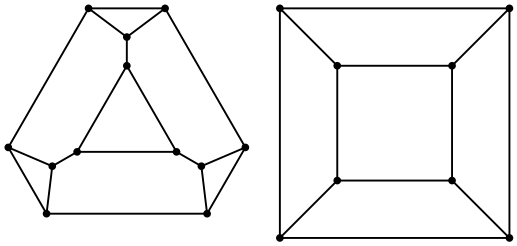
On va décrire plus en détail les graphes $\Gamma(\mathbf{Z}/n\mathbf{Z})$ pour les petites valeurs de n.

Pour $n = 2$, le graphe Γ est formé de 6 points isolés. Les quotients par T (engendré par une des transpositions de triplets), par A_3 et S_3 contiennent respectivement 3, 2, 1 points isolés

Pour $n = 3$, le graphe Γ est ceci:

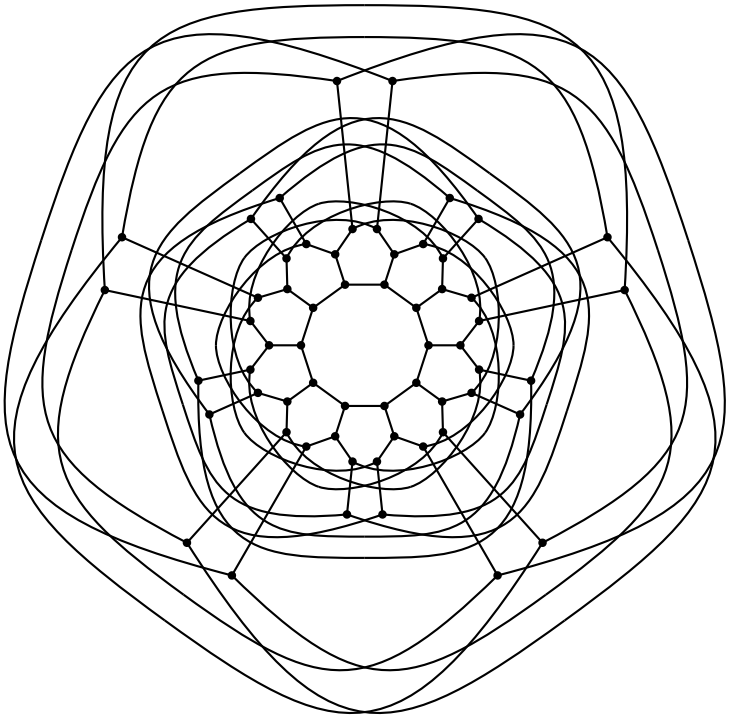


Le quotient par T est le graphe du tétraèdre tronqué, celui par A_3 est le graphe du cube, celui par S_3 est K_4.

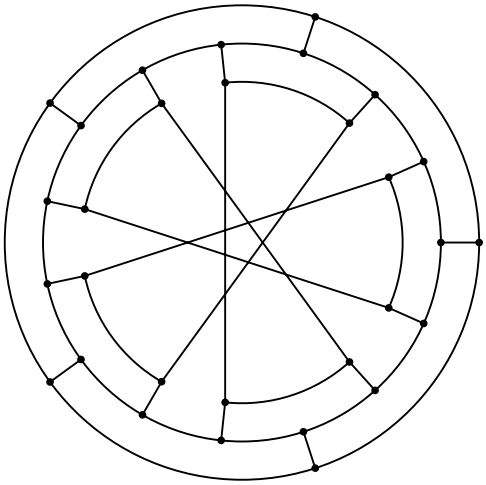


Pour $n = 4$, le graphe Γ est formé de six copies du cube. Les quotients en contiennent respectivement 3, 2 et 1.

Pour $n = 5$, le graphe Γ est formé de deux copies de ceci:



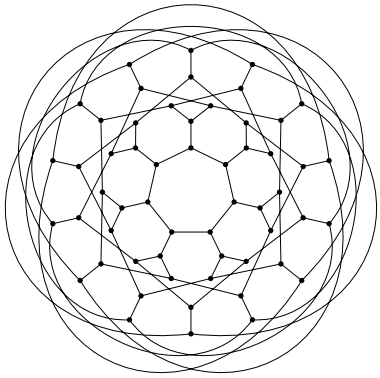
Le quotient par T est formé de deux copies de ceci:



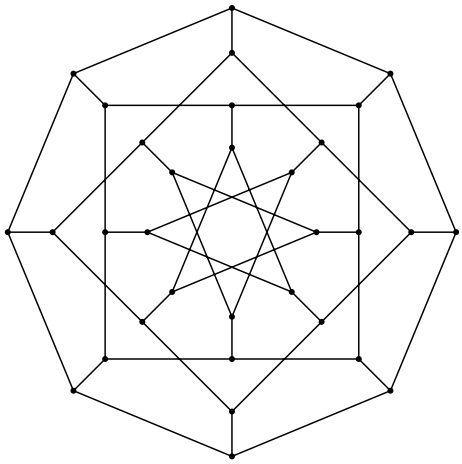
Le quotient par A_3 est formé de deux dodécaèdres, celui par S_3 de deux graphes de Petersen.

Pour $n = 6$, on obtient respectivement 6, 3, 2 et 1 copie du graphe $\Gamma(\mathbf{Z}/3\mathbf{Z})$.

Pour $n = 7$, le quotient par S_3 est ceci:



Pour $n = 8$, on obtient respectivement 12, 6, 4, 2 copies de ceci:



4 Hypergraphes et autres graphes

De la même façon, on pourra former des hypergraphes de degré 3 où les arêtes sont du style $\{(a, b, c), a \in A\}$, les birapports $[a, a', b, c]$ étant dans un sous-groupe G de R^* quand (a, b, c) et (a', b, c) sont dans une même arête. Le même sous-groupe G servira à former des arêtes avec (a, c) fixes et (a, b) fixes, en permutant les rôles des trois triplets. L'ordre du sous-groupe G est la taille des arêtes.

Une condition nécessaire évidente de connexité est cette fois que R reçoit

épimorphiquement $\mathbf{Z}[G]$, et on observe que le produit des trois déterminants dans le quotient de R^* par le sous-groupe engendré par G et les carrés de R^* est invariant sur les composantes connexes.

Là encore il est possible de prendre les quotients par A_3 et S_3 pour obtenir d'autres hypergraphes de degré 3.

On peut aussi former des graphes de degré maximum $3k$ en remplaçant les arêtes des hypergraphes définis ci-dessus par des graphes où les arêtes marquent les $((a,b,c),(a',b,c))$ où le birapport est dans un sous-ensemble S de G à k éléments , stable par passage à l'inverse. Là, le produit des trois déterminants est multiplié par les classes des éléments de S dans le quotient de R^* par les carrés de R^*. Ce qui peut dégager une bipartition, ou une partition des sommets du même style.

4.1 Structure de $\Sigma(\mathbf{Z}[j])$

Un exemple simple s'obtient avec G cyclique d'ordre 3. Les anneaux locaux finis dont le groupe multiplicatif contient G sont les quotients de l'anneau principal $\mathbf{Z}[j]$ (où j est racine cubique primitive de 1) par ses divers idéaux primaires (c'est à dire contenus dans un seul idéal maximal). On obtient ainsi des hypergraphes de degré 3 avec des arêtes à 3 sommets. Ces hypergraphes peuvent aussi se voir comme des graphes bipartis $\Sigma(R)$ réguliers de degré 3. La maille des graphes $\Sigma(R)$ ne dépasse pas 12, car il est déjà 12 dans $\Sigma(\mathbf{Z}[j])$.

On notera aussi que $\Sigma(\mathbf{Z}[j]/(1-j)\mathbf{Z}[j])$ est formé de 24 arêtes disjointes (des arêtes triples si on y tient !). L'anneau $\mathbf{Z}[j]/(1-j)\mathbf{Z}[j]$ est en effet isomorphe à $\mathbf{Z}/3\mathbf{Z}$. Le graphe $\Sigma(\mathbf{Z}[j])$ comporte 24 pièces, qui se projettent sur ces 24 arêtes. On observera que $\mathbf{Z}[j]$ n'a que six éléments inversibles, à savoir $\pm 1,\ \pm j,\ \pm j^2$. Cela impose que les triplets autorisés soient de la forme $\left(\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \begin{bmatrix} a_1+\epsilon b_1 \\ a_2+\epsilon b_2 \end{bmatrix}\right)$ où ϵ est un de ces six éléments. La connexité des pièces se voit alors en remarquant que tout triplet t dont le plus grand module des dénominateurs $\delta(t)$ dépasse 1 a un voisin t' avec $\delta(t') < \delta(t)$.

Comme $\mathbf{Z}[j]/(1-j)\mathbf{Z}[j]$ est principal on démontrera comme plus haut que se rassemblent dans une seule composante connexe de $\Sigma(R)$ tous les triplets de points de la droite sur $R = \mathbf{Z}[j]/n\mathbf{Z}[j]$, où n est premier avec $1-j$ ou 3 (ce qui revient au même), et dont le produit des déterminants est dans les carrés de R^*.

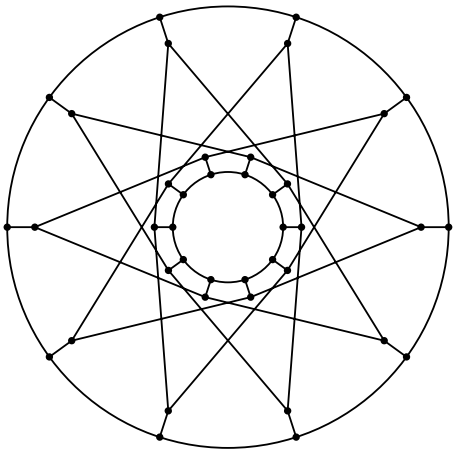
4.2 Exemples

Voici les graphes obtenus pour quelques idéaux de petite norme de $\mathbf{Z}[j]$.

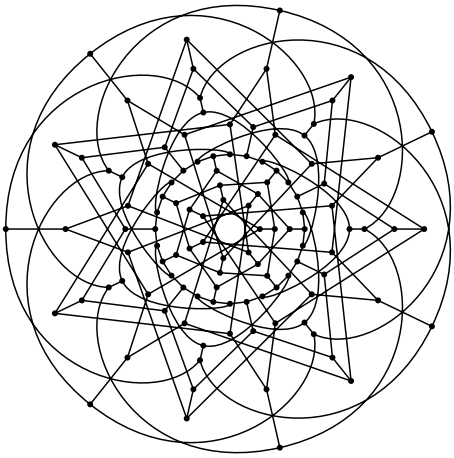
Pour $n = 2$, l'anneau $\mathbf{Z}[j]/2\mathbf{Z}[j]$ est le corps à 4 éléments. Il y a 60 triplets ordonnés et 60 ensembles de trois triplets différant par un élément à une place donnée.

En prenant le quotient par S_3, on trouve le graphe biparti à 20 sommets qui décrit les inclusions des parties à 2 et 3 éléments d'un ensemble à 5 éléments.

En prenant le quotient par A_3 on obtient ceci:



Pour l'idéal de norme 7 engendré par $j - 2$, on obtient un graphe biparti à 672 sommets; le quotient par S_3 est ceci:



Pour l'idéal de norme 9 engendré par 3, on obtient 24, 12, 8 ou 4 copies du graphe d'incidence des 27 points de $\mathbf{F}_3^3$ avec les 27 blocs de trois points dont les distances de Hamming mutuelles valent 1 (autrement dit les 27 droites parallèles aux trois axes de coordonnées).

5 Graphes et hypergraphes issus des polyèdres réguliers

Les graphes de sextets de Biggs et Hoare [4] peuvent être présentés de la façon suivante :

On prend le groupe engendré par les huitièmes de tour autour de trois axes orthogonaux. Il contient le sous-groupe isomorphe à S_4 des rotations de l'octaèdre de rayon 1 ayant ces axes pour axes de rotation d'ordre 4.

En assimilant la sphère unité de $\mathbf{R}^3$ à la droite projective sur $\mathbf{C}$, les divers octaèdres deviennent les sextets, et le groupe s'identifie à un sous-groupe G de $PGL(2,R)$, où R est l'anneau $\mathbf{Z}[\frac{1}{2}][X]/(X^4+1)$, à savoir le groupe engendré par l'ensemble S des huitièmes de tour autour des diagonales de l'octaèdre. On pourra former le quotient du graphe de Cayley associé à G et S par le sous-groupe stabilisant globalement le sextet de départ (ce qui donne un graphe de degré 3) et par les sous-groupes de classes de matrices de la forme $I+M$, où les 4 coefficients de M appartiennent à un idéal J de R, ce qui donne des graphes finis de degré 3. Quand J est un idéal premier de R, on trouve précisément les graphes décrits dans [4].

On peut faire le même travail avec les autres axes de rotation, et les autres polyèdres réguliers, en ajoutant d'autres angles, ce qui donne des graphes et hypergraphes de divers degrés et divers rangs.

Le dénombrement des sommets du graphe est simple : on a déjà calculé, le nombre des matrices de $PGL(2,R/J)$ voir 2.2 et les groupes de rotation des polyèdres réguliers ont pour ordres :

• 12 pour le groupe du tétraèdre, qui est isomorphe à A_4

• 24 pour le groupe commun au cube, à l'octaèdre et au cuboctaèdre

• 60 pour le groupe commun au dodécaèdre, à l'icosaèdre et à l'icosidodécaèdre, qui est isomorphe à A_5.

On utilisera aussi le groupe d'ordre 4 des demi-tours autour de 3 axes mutuellement orthogonaux.

L'outil essentiel pour le calcul des matrices des rotations est le fait que des rotations de même axe commutent, et donc leurs matrices et la matrice identité sont linéairement liées.

Les rotations d'ordre 2 correspondent aux matrices de trace nulle, celles d'ordre m se déterminent par des matrices M où

$$(\mathrm{tr}(M))^2 = 4\cos^2(\frac{\pi}{m})\det(M)$$

Toutefois, les quaternions donnent un outil de calcul plus pratique.

6 Les quaternions entiers

On prend l'algèbre libre $\mathbf{H}$ de dimension 4 sur $\mathbf{Z}$ engendrée par $1, i, j, k$ et déterminée par $i^2 = j^2 = k^2 = -1$ et $ij = k = -ji$ et l'associativité de la multiplication. Cette algèbre est isomorphe à une sous-algèbre de celle des matrices 4×4 par l'injection

$$a + bi + cj + dk \mapsto \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

Cette algèbre est intègre: on note de plus un morphisme multiplicatif de $\mathbf{H}$ vers $\mathbf{N}$, la "norme", obtenue en multipliant le quaternion par son conjugué:

$$a + bi + cj + dk \mapsto \begin{cases} a^2 + b^2 + c^2 + d^2 \\ \text{ou} \\ (a + bi + cj + dk)(a - bi - cj - dk) \\ \text{ou} \\ \sqrt{\det \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}} \end{cases}$$

Cette application est surjective: c'est le théorème des 4 carrés. Quand au nombre de façons de représenter un entier impair par quatre carrés, c'est 8 fois la somme de ses diviseurs (théorème de Jacobi).

6.1 Les quaternions sur un anneau R

Soit R un anneau commutatif. On forme l'anneau de quaternions $\mathbf{H} \otimes_{\mathbf{Z}} R$, c'est une algèbre, de dimension 4 sur R.

Si R est de caractéristique impaire, cette algèbre est isomorphe à $M_2(R)$. On associe, par exemple à i, j, k les matrices $\begin{bmatrix} u & v \\ v & -u \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -v & u \\ u & v \end{bmatrix}$, où $u^2 + v^2 = -1$ (c'est toujours possible en caractéristique impaire) et bien sûr à 1 la matrice identité. Lorsque la caractérisque a ses facteurs premiers $\equiv 1 \pmod 4$, on peut même prendre $v = 0$.

Quand R est le corps des réels, on obtient le corps des quaternions habituel.

6.2 Les groupes des polyèdres

Le quotient du groupe multiplicatif des quaternions réels par son centre, qui est le groupe multiplicatif des réels, est isomorphe au groupe $SO(3)$ des rotations vectorielles de l'espace à trois dimensions par l'isomorphisme déduit par passage au quotient du morphisme qui au quaternion non nul $a + bu$, où u est un quaternion de carré -1 associe la rotation d'axe dirigé par u et d'angle θ tel que $\sin(\theta) = \frac{2b}{a^2+b^2}$ et $\cos(\theta) = \frac{a^2-b^2}{a^2+b^2}$, ce qui correspond à l'effet sur les quaternions de trace nulle (assimilés au vecteurs de $\mathbf{R}^3$) de la conjugaison $v \mapsto uvu^{-1}$

Le groupe des 3 demi-tours est l'image du groupe des 8 quaternions de norme 1 : $\{\pm 1, \pm i, \pm j, \pm k\}$.

Le groupe du tétraèdre est engendré par les images des 16 quaternions de norme 4 que voici : $\pm 1 \pm i \pm j \pm k$.

Le groupe du cube est est engendré par les images des 12 quaternions de norme 2 que voici : $\pm 1 \pm i, \pm 1 \pm j, \pm 1 \pm k$.

Le groupe de l'icosaèdre est engendré par les quaternions de norme 4 déjà vus pour le tétraèdre et par $1 + i\varphi + j\varphi^{-1}$ où φ est le nombre d'or $\frac{1+\sqrt{5}}{2}$. Ce dernier est aussi de norme 4 et représente une rotation d'ordre 3.

6.3 Graphes issus du cube

On peut former un graphe de degré 3 en ajoutant les 12 huitièmes de tour autour des axes passant par les centres de faces (avec les 24 quaternions $\pm 1 \pm i(1 \pm \sqrt{2}), \pm 1 \pm j(1 \pm \sqrt{2}), \pm 1 \pm k(1 \pm \sqrt{2})$), et en formant le quotient par le groupe du cube. Cette construction est celle des graphes de sextets de Biggs et Hoare [4].

On peut former un graphe de degré 4 avec les demi-tours autour des diagonales du cube.

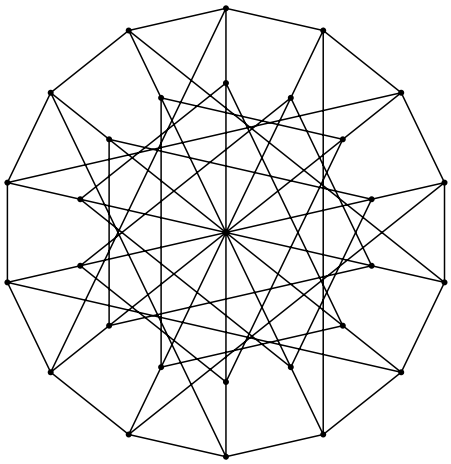
On peut former un hypergraphe de degré 3 et 3-uniforme avec les tiers de tour autour des axes passant par les milieux des faces (12 quaternions $\pm 1 \pm i\sqrt{3}, \pm 1 \pm j\sqrt{3}, \pm 1 \pm k\sqrt{3}$). Et à partir de là un graphe biparti de degré 3. On peut former les quotients de cet hypergraphe par le groupe des 3 symétries ou le groupe du tétraèdre ou le groupe du cube.

On peut former un graphe de degré 6 en intoduisant les 12 quarts de tour autour des axes passant par les milieux d'arêtes (24 quaternions $\pm\sqrt{2} \pm i \pm j, \pm\sqrt{2} \pm j \pm k, \pm\sqrt{2} \pm k \pm i$), et en formant le quotient par le groupe du cube. Comme les arêtes se rassemblent en triangles disjoints, on peut en tirer un hypergraphe de degré 3 et 3-uniforme et aussi un graphe biparti 3-régulier.

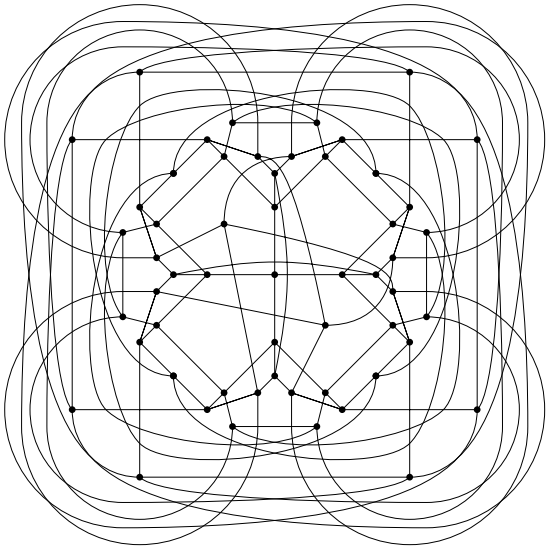
Exemple Dans l'anneau $\mathbf{Z}[j]$, 2 est un carré. En prenant l'idéal engendré

par $2-j$, de norme 7, on obtient 14 positions du cube, les rotations d'ordre 8 autour des axes d'ordre 3 fournissent le graphe de Heawood, les 4 rotations d'ordre 2 autour des axes ternaires donnent son complémentaire dans le graphe biparti complet qui le contient, et enfin, les rotations d'ordre 4 autour des axes binaires donnent les arêtes restantes, qui forment deux copies de K_7 après passage au quotient par le groupe du cube. L'hypergraphe correspondant à un de ces K_7 est le plan de Fano, et le graphe biparti le graphe de Heawood à nouveau.

Le quotient par le groupe du tétraèdre est le graphe antipodal ci-dessous



Exemple Pour $p = 11$, on obtient le graphe de degré 4, diamètre 5 et maille 5 ci dessous:



6.4 Graphes issus du tétraèdre

En ajoutant les 6 quarts de tours autour des axes passant par les milieux d'arêtes, on reste dans le groupe du cube.

On peut former un graphe de degré 4 avec les demi-tours autour des axes passant par un sommet du tétraèdre. Cela revient au même que les diagonales du cube.

On peut former un hypergraphe de degré 3 et 3-uniforme avec les tiers de tour autour des axes passant par les milieux des arêtes opposées. (12 quaternions $\pm 1 \pm i\sqrt{3}, \pm 1 \pm j\sqrt{3}, \pm 1 \pm k\sqrt{3}$). Et à partir de là un graphe biparti de degré 3. (dejà vu avec le cube).

6.5 Graphes issus de l'icosaèdre

On peut former un graphe de degré 10 en ajoutant les 10 demi-tours autour des axes passant par les milieux des faces. (20 quaternions, les 8 qui se trouvaient déjà dans le tétraèdre, $\pm i \pm j \pm k$, et les 12 nouveaux $\pm i\varphi \pm j\varphi^{-1}, \pm j\varphi \pm k\varphi^{-1}, \pm k\varphi \pm i\varphi^{-1}$ On peut en faire le quotient par le groupe aux 3 symétries, celui du tétraèdre, celui de l'icosaèdre.

On peut former des graphes avec les 30 quarts de tour autour des axes joignant les milieux d'arêtes opposées. (60 quaternions les 12 $\pm 1 \pm i, \pm 1 \pm j, \pm 1 \pm k$ et les 48 $\pm 2 \pm i\varphi \pm j \pm k\varphi^{-1}, \pm 2 \pm j\varphi \pm k \pm i\varphi^{-1}, \pm 2 \pm k\varphi \pm i \pm j\varphi^{-1}$) Le quotients par le groupe de l'icosaèdre a pour degré 5.

On peut former un graphe de degré 6 avec les demi-tours autour des axes passant par les sommets (12 quaternions $\pm i \pm j\varphi, \pm j \pm k\varphi, \pm k \pm i\varphi$). On peut en faire le quotient par le groupe aux 3 symétries, celui du tétraèdre, celui de l'icosaèdre.

7 Graphes de Ramanujan

Nous allons prendre ici une définition un peu plus générale que celle de [6] Etant donné un entier impair p, on forme le monoïde multiplicatif des quaternions de norme une puissance de p avec
• si $p^k \equiv 1 \bmod 4$ la coordonnée de 1 impaire et les trois autres coordonnées paires
• si $p^k \equiv 3 \bmod 4$, la coordonnée de 1 paire et les 3 autres impaires.

On prend le quotient du monoïde ainsi obtenu par les homothéties de rapport $\pm p^k$, ce qui donne un sous-groupe G_p de $PGL(\mathbf{Z}[\frac{1}{p}])$. Le graphe X^p est le graphe de Cayley de ce groupe, avec les arêtes provenant des quaternions de norme p. C'est en fait un graphe de degré $\sum_{d|p} d$, qui est un arbre si p est premier (théorème de Dickson).

Ensuite, soit q un entier impair premier avec p. On prend le quotient de ce groupe par la congruence modulo q (c'est à dire par le sous groupe distingué de ses éléments de la forme "orbite de $I + qM$ par les homothéties de rapport $\pm p^k$ ". Ce quotient est un sous-groupe de $PGL(\mathbf{Z}/q\mathbf{Z})$, qui admet $PSL(\mathbf{Z}/q\mathbf{Z})$ pour sous-groupe d'indice 1 ou 2 selon que p est un carré ou non dans $\mathbf{Z}/q\mathbf{Z}$. Le graphe $X^{p,q}$ est le graphe de Cayley défini avec les images des représentations choisies de p dans ce groupe.

8 graphes $X^{3,q}$ et quotients

En particulier, pour $p = 3$, $X^{3,q}$ a pour degré 4, car l'ensemble S des 8 quaternions intéressants de norme 3, à savoir les $\pm i \pm j \pm k$, vérifie $GSG = GS$ quand G est l'un quelconque des trois groupes (à homothétie de rapport 2 près).

Le groupe qui donne X_3 est celui des rotations engendrées par les demi-tours autour des axes ternaires du tétraèdre. Les quotients donnent les positions accessibles aux figures admettant seulement les axes de symétries binaires du tétraèdre, au tétraèdre, au cube, en composant ces rotations.

Voici les résultats avec q premier (pour la simplicité de programmation)

Graphe $X^{3,q}$			
q	diamètre	maille	ordre
5	6	6	120
7	6	8	336
11	8	9	660
13	8	9	1092
17	11	12	4896
19	11	12	6840
23	10	12	6072

quotient par les 3 demi-tours			
q	diamètre	maille	ordre
5	4	6	30
7	6	6	84
11	8	5	165
13	7	7	273
17	8	10	1224
19	10	10	1710
23	10	9	1518
29	10	12	6090
31	11	12	7440
37	12	9	6327

quotient par le groupe du tétraèdre			
q	diamètre	maille	ordre
5	3	4	10
7	4	6	28
11	4	5	55
13	5	7	91
17	8	8	408
19	9	10	570
23	7	9	506
29	10	10	2030
31	10	10	2480
37	8	9	2109
41	12	12	5740
43	12	12	6622
47	12	12	4324
53	13	12	12402

quotient par le groupe du cube			
q	diamètre	maille	ordre
5	1	3	5
7	3	4	14
11	4	5	55
13	5	7	91
17	6	8	204
19	6	9	285
23	6	6	253
29	9	7	1015
31	8	10	1240
37	8	9	2109
41	9	12	2870
43	9	7	3311
47	9	12	2162
53	10	12	6201
59	10	13	8555
61	10	13	9455
67	11	14	12529
71	10	9	7455
73	10	9	8103

A Anneaux principaux

Il est bien connu que $\mathbf{Z}$ est principal.

L'anneau $\mathbf{Z}[j] = \mathbf{Z}[X]/(X^2+X+1)$ est euclidien pour la norme habituelle (carré du module), donc principal. Il en va de même pour les anneaux $\mathbf{Z}[i\sqrt{2}]$ et $\mathbf{Z}[i]$.

L'anneau $\mathbf{Z}[X]/(X^4+1) = \mathbf{Z}[\alpha]$ est euclidien, car la différence entre une combinaison rationnelle des α^m, $m = 0, 1, 2, 3$ et la combinaison entière "la plus proche", soit $a + b\alpha + ci + di\alpha$ avec les rationnels a, b, c, d tous au plus égaux à $1/2$ en valeur absolue, cette différence a pour conjugué sur $\mathbf{Z}[i]$ la combinaison $a-b\alpha+ci-di\alpha$, leur produit vaut $(a^2+2bd-c^2)+(d^2+2ac-b^2)i$, dont le conjugué sur $\mathbf{Z}$ est $(a^2+2bd-c^2)-(d^2+2ac-b^2)i$. Le produit, qui est la norme sur Q, vaut $(a^2+c^2)^2+(b^2+d^2)^2+4bd(a^2-c^2)+4ac(d^2-b^2)$. Ceci est au plus 1, et ne peut valoir 1 que si chacun des termes de la somme vaut $1/4$. Mais alors $a^2+c^2 = 1/2$, donc $|a| = |c| = 1/2$, donc $a^2-c^2 = 0$ et la norme est < 1. Voir [7] ou [1].

Pour d'autres anneaux, on pourra utiliser le fait qu'un localisé de prin-

cipal est aussi principal, et le célèbre résultat suivant:

Théorème de Hermite et Minkowski *Si l'anneau intègre A de dimension finie sur $\mathbf{Z}$ a r_1 plongements réels et $2r_2$ plongements non réels dans $\mathbf{C}$, toute classe d'idéaux contient un idéal de norme au plus k avec :*

$$k = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D|^{1/2}$$

où $n = r_1 + 2r_2$ est la dimension de l'anneau et D son discriminant sur $\mathbf{Z}$. Ce discriminant est le déterminant de la matrice symétrique $\mathrm{Tr}_{\mathbf{Z}}(e_i e_j)$ où $\{e_i\}$ est une base de A sur $\mathbf{Z}$.

A.1 Exemples

L'anneau $\mathbf{Z}[\alpha]$ où $\alpha^2 = i$ a pour base $1, \alpha, i, i\alpha$; de plus, $n = 4$ et $r_2 = 2$. La matrice des traces est $\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & -4 & 0 \\ 0 & -4 & 0 & 0 \end{pmatrix}$ donc $D = 256$ et $k = \frac{24}{\pi^2} < 3$, donc chaque classe a un idéal de norme au plus 2. Mais le seul idéal de norme 2, qui est engendré par $1 - \alpha$, est principal. Donc tous les idéaux sont principaux. Voir [5].

L'anneau $\mathbf{Z}[\omega]$, où ω est une racine primitive cinquième de l'unité, a pour base $1, x, x^2, x^3$; de plus $n = 4$ et $r_2 = 2$. La matrice des traces est $\begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 4 \\ -1 & -1 & 4 & -1 \end{pmatrix}$ donc $D = 125$ et $k = \frac{15\sqrt{5}}{2\pi^2} < 2$. et l'anneau est principal.

L'anneau $\mathbf{Z}[j][\sqrt{2}]$ a pour base $1, j, \sqrt{2}, j\sqrt{2}$. La matrice des traces est $\begin{pmatrix} 4 & -2 & 0 & 0 \\ -2 & -2 & 0 & 0 \\ 0 & 0 & 8 & -4 \\ 0 & 0 & -4 & -4 \end{pmatrix}$, donc $D = 288$ et $k = \frac{18\sqrt{2}}{\pi^2} < 3$. Comme il n'y a pas d'idéal de norme 2 (vu que l'idéal engendré par 2 est carré de celui engendré par $\sqrt{2}$ et que le quotient de l'anneau par ce dernier idéal est le corps à 4 éléments), l'anneau est principal

References

[1] R. Akhtar, Cyclotomic Euclidean number fields, Senior thesis, 1995, Harvard University.

[2] N.L. Biggs, Graphs with large girth, Ars Combinatoria 25-C (1988) p. 73–80

[3] G. Birkoff, S. MacLane, Algebra, MacMillan, New-York 1967

[4] N.L. Biggs, M. J. Hoare, The sextet construction for cubic graphs, Combinatorica 3 (1983) p. 153–165

[5] H. Hasse, Zahlentheorie, 3. berichtigte Aufl., Berlin: Akademie Verlag 1969

[6] A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan graphs, Combinatorica 8 (1988) p. 261–277

[7] J. M. Masley, On Euclidean rings of integers in cyclotomic fields, J. Reine Angew. Math. 272 (1975) p. 45-48