NOMBRES ET ALGÈBRE

Jean-Yves MÉRINDOL

EDP SCIENCES

17, avenue du Hoggar
Parc d'Activité de Courtabœuf, BP 112
91944 Les Ulis Cedex A, France

Grenoble Sciences

Grenoble Sciences poursuit un triple objectif :

- réaliser des ouvrages correspondant à un projet clairement défini, sans contrainte de mode ou de programme,
- garantir les qualités scientifique et pédagogique des ouvrages retenus,
- proposer des ouvrages à un prix accessible au public le plus large possible.

Chaque projet est sélectionné au niveau de Grenoble Sciences avec le concours de referees anonymes. Puis les auteurs travaillent pendant une année (en moyenne) avec les membres d'un comité de lecture interactif, dont les noms apparaissent au début de l'ouvrage. Celui-ci est ensuite publié chez l'éditeur le plus adapté.

(Contact : Tél. : (33)4 76 51 46 95 - E-mail : Grenoble.Sciences@ujf-grenoble.fr)

Deux collections existent chez EDP Sciences :

- la ***Collection Grenoble Sciences***, connue pour son originalité de projets et sa qualité
- ***Grenoble Sciences - Rencontres Scientifiques***, collection présentant des thèmes de recherche d'actualité, traités par des scientifiques de premier plan issus de disciplines différentes.

Directeur scientifique de Grenoble Sciences

Jean BORNAREL, Professeur à l'Université Joseph Fourier, Grenoble 1

Comité de lecture pour ***"Nombres et algèbre"***

- **Jean-Luc CHABERT**, Professeur à l'Université de Picardie
- **José BERTIN**, Professeur à l'Université Joseph Fourier, Grenoble 1
- **Bernard CHARLES**, Professeur à l'Université des Sciences et Techniques du Languedoc, Montpellier 2

Grenoble Sciences bénéficie du soutien du **Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche** et de la **Région Rhône-Alpes**.
Grenoble Sciences est rattaché à l'**Université Joseph Fourier de Grenoble**.

Illustration de couverture : ***Alice GIRAUD***

ISBN 2-86883-820-0
© EDP Sciences, 2006

EXTRAITS

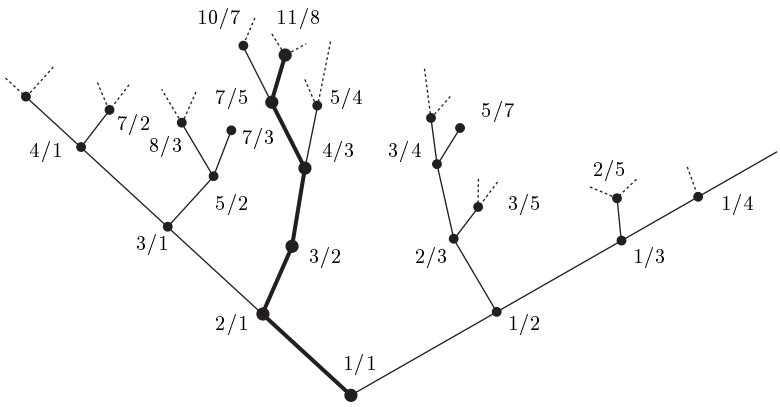
1.8.1. Un exemple : l'arbre de Stern-Brocot

Cette partie reprend avec quelques variantes les résultats déjà obtenus dans la partie sur les fractions continues en les exposant dans le langage des arbres. On sait d'après 1.64 que $\mathrm{SL}_2(\mathbf{N})$ est un monoïde libre de base $\{h, b\}$. L'objet que nous étudions ici est l'arbre $\vec{\Gamma}_{\{h,b\}}(\mathrm{SL}_2(\mathbf{N}))$, que l'on appelle « l'arbre de Stern-Brocot » et que l'on va désormais noter $\vec{\Gamma}_{sb}$.

Cet arbre a été introduit par le mathématicien Moritz Stern en 1858 dans un article au *Journal de Crelle* : *Über eine Zahlentheoretische Funktion.* Presque simultanément, et indépendamment, l'horloger Achille Brocot introduisait la même idée dans la *Revue Chronométrique* (1860). Ce dernier est un constructeur réputé (ses horloges sont toujours recherchées et de grand prix) et un inventeur de nombreuses améliorations en horlogerie (échappement, suspension, calendrier perpétuel). Ceci l'a amené à travailler sur les engrenages et les rouages et à essayer d'obtenir les meilleures approximations possibles de rationnels par des rouages de taille raisonnable (c'est-à-dire sans trop de dents). Les fractions continues sont particulièrement adaptées à ce problème : on le verra par exemple en 11.72. L'arbre de Stern-Brocot donne un procédé simple pour trouver ces fractions.

On reprend les considérations de 1.5. En particulier, le monoïde $\mathrm{SL}_2(\mathbf{N})$ opère sur l'ensemble $\mathbf{P}^1(\mathbf{Q}) = \mathbf{Q}^{>0} \cup \{0\} \cup \{\infty\}$. Considérons l'application ϕ de $\mathrm{SL}_2(\mathbf{N})$ vers $\mathbf{Q}^{>0}$ qui associe à $g \in \mathrm{SL}_2(\mathbf{N})$ la fraction $\phi(g) = g(1)$. Puisque $\phi(h^p) = h^p(1) = p+1$ et $\phi(b^q) = b^q(1) = \frac{1}{q+1}$, si $g = h^{q_1} b^{q_2} \dots b^{q_{2n}}$ (où ces exposants sont non nuls sauf peut-être le premier et le dernier), $\phi(g) = g(1)$ est la fraction dont le développement en fraction continue est $[q_1; q_2, \dots, q_{2n} + 1]$.

Puisque tout $q \in \mathbf{Q}^{>0}$ a un unique développement en fraction continue, cette application ϕ est une bijection entre le monoïde libre $\mathrm{SL}_2(\mathbf{N})$ et $\mathbf{Q}^{>0}$. Cette bijection ϕ permet de considérer que les sommets de $\vec{\Gamma}_{sb} = \vec{\Gamma}_{\{h,b\}}(\mathrm{SL}_2(\mathbf{N}))$ sont indexés par les rationnels de $\mathbf{Q}^{>0}$. Par définition même, il y a deux arêtes de $\vec{\Gamma}_{sb}$ qui ont $g(1)$ comme origine. Leurs extrémités sont le sommet $gb(1)$ et $gh(1)$.



que l'on voit comme une matrice à coefficients dans A. Montrer que les deux lignes de cette matrice carrée sont libres. Montrer que deux colonnes quelconques sont liées.

Trouver un exemple de même nature pour tout anneau $\mathbf{Z}/pqr\mathbf{Z}$ où p, q et r sont trois premiers distincts.

Soit $A = \mathbf{Z}[X_{i,j}]$ l'anneau des polynômes à coefficients entiers en les neuf indéterminées $X_{i,j}$ où i et j varient entre 1 et 3.

En déduire que les matrices

$$U = \begin{pmatrix} X_{1,1} & X_{1,2} & X_{1,3} \\ X_{2,1} & X_{2,2} & X_{2,3} \\ X_{3,1} & X_{3,2} & X_{3,3} \end{pmatrix}$$

et ${}^tU$ ne sont pas équivalentes dans $M_{3\times 3}(A)$.

Montrer qu'elles sont élémentairement équivalentes, donc équivalentes, dans $M_{3\times 3}(K)$ où $K = \mathbf{Q}(X_{i,j})$ est le corps des fractions de A.

La méthode du pivot de Gauss a un intérêt théorique, mais aussi pratique, et elle est à la base de nombreuses méthodes de calcul numérique ou formel. Ainsi, la preuve de 6.12 donne un moyen de calculer le déterminant de la matrice A. En effet, si les diviseurs élémentaires sont $d_1, d_2, \ldots, d_r$, alors $\det(A) = 0$ si $r < n$ et $\det(A) = d_1 d_2 \cdots d_n$ sinon. Si $n \geq 3$, et si A est assez générale, cet algorithme (sous réserve d'en améliorer la mise en forme) est bien plus efficace que celui donné par le développement suivant les lignes ou les colonnes de A. Vous pouvez le tester vous-même pour $n = 3$ ou 4. Noter qu'il est inutile, pour calculer le déterminant, de se ramener au cas où $d_i \mid d_{i+1}$.

6.3. Modules sur les anneaux principaux

Soit A un anneau principal. Le théorème des diviseurs élémentaires va nous permettre de donner la structure des sous-modules et des modules quotients des A-modules libres.

6.3.1. Sous-modules des modules libres : les réseaux

Un réseau est un sous-A-module d'un module libre de dimension finie. Si l'on veut mentionner l'anneau A, on parle de A-réseau. Par exemple, les A-réseaux dans A sont exactement les idéaux de A. Ce vocabulaire provient du cas $A = \mathbf{Z}$. Un réseau est alors un sous-groupe additif de $\mathbf{Z}^n$, sous-groupes qui interviennent naturellement en cristallographie. Les physiciens ont en effet observé qu'un cristal est obtenu par répétition d'un motif élémentaire (c'est une molécule qui forme ce qu'on appelle la maille du cristal) par des translations dans $\mathbf{R}^3$ qui forment un sous-groupe isomorphe à $\mathbf{Z}^3$. C'est à cause de la présence de ces translations qui permettent de répéter le motif de base que l'on parle de « réseaux cristallins ».

Le travail théorique réalisé par les cristallographes du XIXe siècle, principalement[2] Auguste BRAVAIS (23 août 1811 – 30 mars 1863), a consisté à déterminer tous les groupes des isométries de $\mathbf{R}^3$ qui contiennent un tel sous-groupe de translations. BRAVAIS donne les bases de cette classification en regroupant les cristaux en 14 types. On va résoudre ici un problème beaucoup plus simple, point de départ élémentaire de la classification de BRAVAIS : on cherche à comprendre (si l'anneau A est $\mathbf{Z}$) quels sont tous les sous-modules de $\mathbf{Z}^n$, sans chercher à « augmenter » ces sous-groupes de translations par d'autres symétries.

Le théorème des diviseurs élémentaires, convenablement interprété et légèrement généralisé, va nous conduire, lorsque A est principal, à la classification des réseaux de A^n.

THÉORÈME 6.24 *Soient A un anneau principal, n un entier et M un sous-module de A^n.*

Il existe des éléments $b_1, b_2, \cdots, b_n$ de A^n, un entier r et des éléments $d_1, d_2, \cdots, d_r$ de A où $d_1 \mid d_2 \mid \cdots \mid d_r$ tels que $(b_1, b_2, \cdots, b_n)$ soit une base ordonnée de A^n et $(d_1 b_1, \cdots, d_r b_r)$ soit une base ordonnée de M. En particulier, M est un module libre de type fini de rang $r \leq n$.

L'entier r et les idéaux $d_1 A \supset d_2 A \supset \cdots \supset d_r A$ sont uniquement déterminés par ces conditions.

PREUVE

1) *Première étape : M admet une partie génératrice finie*

Il s'agit donc démontrer que M est de type fini, et c'est le point le plus délicat de la preuve. Si M est fini, c'est clair (prendre M comme partie génératrice de lui même).

Sinon, soient $A^{(M)}$ le A-module libre engendré par M et $\phi : A^{(M)} \to A^n$ le morphisme de A-modules qui envoie $[m]$ vers m. Son image est M. La matrice (infinie) S de ce morphisme ϕ dans les bases canoniques des A-modules libres A^n et $A^{(M)}$ est de format $n \times M$. Sa colonne m est composée des coefficients de m dans la base canonique de A^n.

On peut multiplier à gauche S par des matrices de $\mathrm{SL}_n(A)$ (ce qui revient à faire des opérations élémentaires sur les lignes de S).

Il nous faut étendre la définition des opérations élémentaires sur les colonnes pour tenir compte du fait qu'il y a (si M est infini) un nombre infini de telles colonnes. On pourrait procéder colonne par colonne, et itérer le processus, mais ceci ne mettrait

2 BRAVAIS a communiqué ses résultats dans une série de trois mémoires présentés à l'Académie des Sciences, de février 1849 à août 1850. La détermination, à conjugaison près par les affinités directes, de tous les sous-groupes discrets du groupe des isométries affines de $\mathbf{R}^3$ est due au minéralogiste Ievgraf Stepanovitch FEDOROV et au mathématicien Arthur SCHÖNFLIESS vers 1892. Il y a 230 tels sous-groupes dont 11 apparaissent par paires « éniantomorphes » : il s'agit de réseaux conjugués modulo le groupe des affinités (directes et indirectes) sans l'être modulo le sous-groupe des affinités directes. En dimension 2, on sait depuis longtemps qu'il existe 17 réseaux à conjugaison près (et que l'éniantomorphisme n'apparaît pas).

EXERCICE 6.78 *Soient E un $\mathbf{k}$-espace vectoriel de dimension finie et $(u_i)_{i\in I}$ une famille de $\mathbf{k}$-endomorphismes de E. On suppose qu'il existe une base de E dans laquelle tous les u_i soient simultanément diagonaux. Montrer que les u_i commutent deux à deux.*

EXERCICES 6.79

1) Soient u un endomorphisme de E et F un sous-espace stable. On suppose que $u\mid_F$ et $\overline{u} : E/F \to E/F$ sont triangularisables. Montrer que u est triangularisable.

Donner des exemples où $u\mid_F$ et $\overline{u}$ sont diagonalisables sans que u ne le soit. Montrer que si $u\mid_F$ et $\overline{u}$ sont diagonalisables avec des valeurs propres distinctes, u est diagonalisable.

2) Soient u (resp. v) un endomorphisme de l'espace vectoriel E (resp. F) de dimension finie. Montrer que si u et v sont diagonalisables (resp. triangularisables), il en est de même de $u \otimes v$.

3) Soit u un endormorphisme diagonalisable de polynôme caractéristique $\chi_u(X) = \prod_{k=1}^{r}(X-d_k)^{n_k}$. On suppose que l'on a choisi l'indexation des d_k de sorte que $n_1 \geq n_1 \geq \cdots \geq n_r > 0$. Posons $a_i = n_i - n_{i+1}$ (i entre 1 et $r-1$) et $a_r = n_r$.

Montrer que les invariants de similitude de u sont :

$$\left[(X-d_1)^{[a_1]}, [(X-d_1)(X-d_2)]^{[a_2]}, \ldots, [(X-d_1)\cdots(X-d_r)]^{[a_r]}\right]$$

où le symbole $P^{[a]}$ signifie que l'invariant P est répété a fois.

On renvoie à 7.41 pour la décomposition de JORDAN, qui est un résultat plus précis sur la réduction des endomorphismes triangularisables.

6.5.5. INVERSE D'UNE MATRICE

Nous allons montrer que le théorème de CAYLEY-HAMILTON donne un moyen théorique et pratique pour calculer l'inverse d'une matrice.

Soient A une matrice carrée de taille n à coefficients dans un corps $\mathbf{k}$ et $\chi_A = X^n - c_1X^{n-1} - \cdots - c_kX^k - \cdots - c_n$ son polynôme caractéristique. Quitte à passer à un corps de décomposition de χ_A (voir 9.16), on peut supposer que ce polynôme χ_A est scindé et on note $\lambda_1, \ldots, \lambda_n$ la liste de ses racines, en les répétant avec leurs multiplicités, de sorte que

$$\chi_A(X) = X^n - c_1X^{n-1} - \cdots - c_kX^k - \cdots - c_n = (X-\lambda_1)\cdots(X-\lambda_n).$$

Le théorème de CAYLEY-HAMILTON nous apprend que

$$A^n = c_1A^{n-1} + \cdots + c_{n-1}A + c_n1_n.$$

Si $c_n = (-1)^{n-1}\det A \neq 0$, ce qui revient à demander que A soit inversible, on en déduit que

$$A^{-1} = (1/c_n)[A^{n-1} - c_1A^{n-2} - \cdots - c_{n-1}1_n].$$

Cette méthode permet d'obtenir A^{-1}, sous réserve d'avoir calculé les puissances $A^2, A^3, \cdots, A^{n-1}$ et les coefficients $c_1, \ldots, c_{n-1}$.

En développant le produit donnant χ_A en fonction des λ_i, on trouve que chaque terme c_k vaut $(-1)^k e_k$ où e_k est le k-ième polynôme symétrique élémentaire en les λ_i. Notons $p_k = \sum_{i=1}^n \lambda_i^k$ le k^e polynôme de Newton en les λ_i (voir 3.2.2).

D'après les relations de Newton (voir 3.23), on a[6], pour tout entier m, les relations suivantes entre les sommes de Newton p_j et les coefficients c_k :

$$mc_m = p_m - p_{m-1}c_1 - \cdots - p_{m-p}c_p - \ldots - p_1 c_{m-1}.$$

On sait que A est triangularisable dans le corps de décomposition de χ_A et que les valeurs sur la diagonale de cette matrice triangulaire sont les λ_i (voir 6.70). Si P est une matrice inversible telle que $P^{-1}AP$ est triangulaire, on constate que $\operatorname{tr} A = \operatorname{tr} P^{-1}AP = \lambda_1 + \cdots + \lambda_n = c_1 = p_1$. Pour la même raison, $\operatorname{tr} A^k = \operatorname{tr} P^{-1}A^kP = \lambda_1^k + \cdots + \lambda_n^k = p_k$.

Ainsi, en calculant les puissances $A^2, A^3, \cdots, A^{n-1}$, on obtient $p_2, \ldots, p_n$ par un simple calcul de traces, puis on en déduit de proche en proche les c_k en utilisant les relations de Newton, ce qui donne un moyen[7] de calculer A^{-1}.

Cette idée a été présentée par l'astronome Urbain Jean Joseph Le Verrier (11 mars 1811 – 23 septembre 1877) dans un article[8] de 1840 intitulé *Sur les variations séculaires des éléments des orbites pour les sept planètes principales.* Il appliquait cette méthode à des matrices carrées 4×4 dont les coefficients provenaient des observations astronomiques : la matrice qui l'intéresse est composée de réels entre $-17,6$ et $4,31$, connus avec une précision de 10^{-7}. Si une calculette programmable sait maintenant traiter ceci sans grande difficulté, l'inversion à la main d'une matrice de cette taille dont les coefficients sont des décimaux assez compliqués n'est pas facile et cette méthode est la bienvenue.

Ces méthodes ont permis à U.J.J. Le Verrier, et à John Couch Adams, d'accomplir un exploit qui les ont fait rentrer dans l'histoire de l'astronomie et de la science. Les astronomes réalisaient depuis le début du XIXe siècle que la trajectoire réelle d'Uranus (planète découverte par William Herschel en 1781) n'était pas conforme aux prédictions de la mécanique céleste newtonienne et que ces écarts pouvaient venir des perturbations causées par une planète encore inconnue. En 1846, indépendamment l'un de l'autre, Le Verrier et Adams ont déterminé par le calcul (en inversant les matrices *ad hoc*) une position et une masse possible pour cette nouvelle planète. Si Adams s'est heurté à l'incrédulité des astronomes anglais qui ont refusé de réaliser à Greenwich les observations qu'il suggérait, Le Verrier a su être plus convaincant et un jeune astronome allemand, Johann Gottfried Galle, a utilisé un instrument très performant de l'observatoire de Berlin pour observer le ciel aux endroits indiqués par le calcul. C'est le 23 septembre 1846 que J. Galle, en collaboration avec Heinrich Louis d'Arrest, a pu observer une planète inconnue. Cet astre, qui correspondait assez bien

6 Attention aux signes : $c_k = (-1)^k e_k$.

7 A noter que l'on évite ainsi tout calcul direct de déterminants de mineurs extraits, ce qui serait très couteux en temps-machine.

8 *J. de Math.* s. I **5**, 230.

aux positions $(i, n-i)$ (n est la taille des matrices que l'on considère). La multiplication à droite par Δ donne une bijection entre les matrices $T = (t_{i,j})$ de TOEPLITZ ($t_{i,j}$ ne dépend que de $i - j$) et les matrice de HANKEL. On a donné ici le résultat avec des matrices de TOEPLITZ tout en maintenant la référence (traditionnelle) aux matrices de HANKEL.

11.4.3. DÉVELOPPEMENT DES RÉELS EN FRACTIONS CONTINUES

On a étudié en 1.8.1 le monoïde libre $\mathrm{SL}_2(\mathbf{N})$ engendré par les matrices élémentaires h et b et son action sur $\mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. Ce monoïde libre agit aussi sur $\mathbf{P}^1(\mathbf{k}) = \mathbf{k} \cup \{\infty\}$ où $\mathbf{k}$ est un corps commutatif quelconque. On va ici s'intéresser à son action sur $\mathbf{P}^1(\mathbf{R})$. Si x est un réel, on pose $h(x) = 1 + x$ et

$$b(x) = \frac{1}{1 + \dfrac{1}{x}}$$

et on prolonge ceci, par les règles habituelles, pour $x = \infty$.

Soit x un réel et supposons que x ne soit pas un rationnel. On sait que $x = \lfloor x \rfloor + y$ où y est un réel satisfaisant à $0 \leq y < 1$. Puisque x n'est pas entier, $y \neq 0$, de sorte que $1/y$ est un réel de $]1, \infty)$. Ainsi tout réel positif x_0 qui n'est pas rationnel s'écrit, de façon unique, sous la forme $x_0 = d_0 + \frac{1}{x_1}$ où d_0 est un entier naturel et x_1 est un réel de $[1, \infty)$. Le réel x_1 n'est pas rationnel, sinon x le serait, ce qui montre que l'on peut continuer cette procédure et obtenir ainsi une suite $(d_n)_{n \in \mathbf{N}}$ telle que :

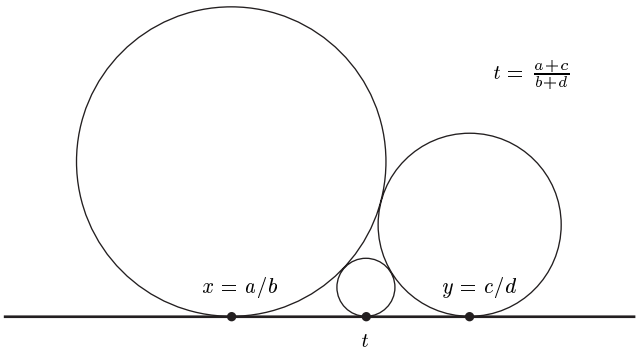
$x = x_0$ et $x_n = d_n + \frac{1}{x_{n+1}}$ avec $1 \leq x_{n+1}$ et $d_n \in \mathbf{N}$. Il est possible que $d_0 = 0$, mais dès que $n \geq 1$, $d_n \geq 1$.

On reconnait ici le procédé déjà décrit en 1.5 pour $\mathbf{Q}$ à ceci près que la suite des réduites est maintenant infinie.

$$[d_0; d_1, \ldots, d_n, \ldots] = d_0 + \cfrac{1}{d_1 + \cfrac{1}{d_2 + \cfrac{1}{\ddots + \cfrac{1}{d_{n-1} + \cfrac{1}{d_n + \cfrac{1}{\ddots + \cfrac{1}{\ddots}}}}}}} \tag{37}$$

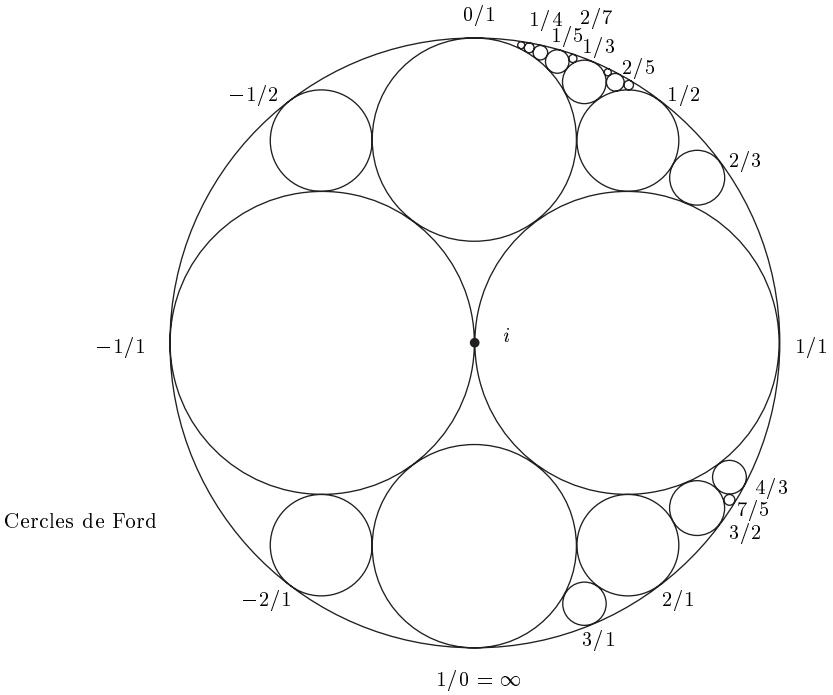
C'est ce qu'on appelle le développement en fraction continue de x.

EXERCICE 11.67 *Montrer que le développement en fraction continue de $\frac{1+\sqrt{5}}{2}$ est donné par la suite constante 1. Donner le développement en fraction continue de $\sqrt{2}$ (voir 1.57 pour le lien avec les formats des feuilles).*



que le groupe d'isotropie de i est isomorphe à $\mathbf{S}^1$ devient évident[23] : les rotations ordinaires de centre 0 respectent bien cette figure.

On aboutit ainsi à un nouveau modèle de la géométrie hyperbolique où le demi-plan est remplacé par le disque unité. Les diverses figures que l'on vient de définir dans H (domaine fondamental de $\mathrm{PSL}_2(\mathbf{Z})$, cercles de FORD) se transportent en des figures dans D, particulièrement esthétiques et souvent utilisées par l'artiste Maurits C. ESCHER (17 juin 1898 – 27 mars 1972).



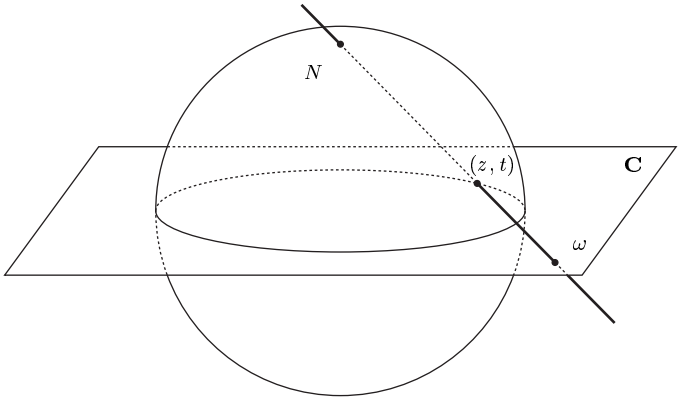
Cercles de Ford

23 En profiter pour prouver sans calcul que les cercles hyperboliques sont les cercles euclidiens ordinaires.

12.7. La sphère de Riemann

Considérons l'espace vectoriel réel (de dimension 3) $V = \mathbf{C} \times \mathbf{R}$, ensemble des couples (z, t). Le plan d'équation $t = 0$ sera appelé le plan horizontal et la droite d'équation $z = 0$ sera désignée sous le nom de droite verticale. L'ensemble des points (z, t) de V satisfaisant à $|z|^2 + t^2 = 1$ est la sphère unité de V, que l'on notera $\mathbf{S}^2$.

Soit $N = (0, 1)$. La projection stéréographique $p : \mathbf{S}^2 - \{N\} \to \mathbf{C}$ est la restriction à $\mathbf{S}^2 - \{N\}$ de la projection de $V - \{N\}$ sur le plan plan horizontal, à partir de N.



Si $(z, t) \neq N$ est un point de $\mathbf{S}^2$, on cherche le point ω de H tel que les points $N = (0, 1), (z, t)$ et $(\omega, 0)$ soient alignés. Un calcul immédiat (voir par exemple les premières lignes de 12.3.1) montre que cette condition géométrique est équivalente à :

$$\omega = p(z) = \frac{z}{1-t} \quad \text{et, inversement, à} \quad z = \frac{2\omega}{1+|\omega|^2}, t = \frac{|\omega|^2 - 1}{|\omega|^2 + 1}. \tag{52}$$

Il est tentant de prolonger cette application p en décidant que $p(N) = \infty$. Utilisons pour cela la droite projective $\mathbf{P}^1(\mathbf{C})$, quotient de $\mathbf{C}^2 - \{0\}$ par les homothéties (voir les notations en 10.1.3).

L'application p de $\mathbf{S}^2 - \{N\}$ vers $\mathbf{C}$ se prolonge alors en une application de $\mathbf{S}^2$ vers $\mathbf{P}^1(\mathbf{C})$ donnée par

$$p(z, t) = [z : 1 - t] = [1 + t : \overline{z}]$$

(montrer cette dernière égalité en utilisant que $t^2 + |z|^2 = 1$). Cette application envoie donc le pôle Nord vers $p(0, 1) = [1 : 0] = \infty$.

Remarquons que

$$[z : w] = [z\overline{w} : |w|^2] = \big[\frac{2z\overline{w}}{|z|^2 + |w|^2} : \frac{2|w|^2}{|z|^2 + |w|^2}\big],$$

ce qui montre que l'application inverse $q : \mathbf{P}^1(\mathbf{C}) \to \mathbf{S}^2$ est donnée par la formule :

$$q([z : w]) = \big(2\frac{\Re e z\overline{w}}{|z|^2 + |w|^2}, 2\frac{\Im m z\overline{w}}{|z|^2 + |w|^2}, \frac{|z|^2 - |w|^2}{|z|^2 + |w|^2}\big). \tag{53}$$

13.2. Groupes finis

On sait que tout groupe d'ordre p premier est cyclique. Il est naturel de s'intéresser à la classification, à isomorphisme près, de tous les groupes finis d'un ordre donné. C'est un problème complexe, et rapidement inextricable. On ne va donner ici que quelques indications.

13.2.1. Les p-groupes

Une des idées de base, simple mais efficace si on sait l'utiliser avec finesse, est de faire agir le groupe que l'on veut étudier sur divers ensembles et de tenir compte du fait que le cardinal de chaque orbite divise l'ordre du groupe. Ce renseignement est précieux si le cardinal de G est la puissance d'un nombre premier :

Définition 13.11 *Soit p un nombre premier. Un p-groupe est un groupe fini non trivial dont l'ordre est une puissance de p.*

Les groupes cycliques $\mathbf{Z}/p^r\mathbf{Z}$ et leurs produits (pour diverses valeurs de r) sont des p-groupes abéliens. Ce sont d'ailleurs les seuls qui soient abéliens (voir en 7.36), de sorte que le nombre de classes d'isomorphismes des p-groupes abéliens d'ordre p^r est le nombre $p(r)$ de partitions de r. Il est beaucoup plus délicat de classer tous les p-groupes non abéliens. Le nombre de classes d'isomorphismes de p-groupes d'ordre p^r augmente extrêmement vite avec r. L'estimation asymptotique, établie par Graham Higman et Charles C. Sims entre 1960 et 1965, est qu'il en existe $p^{2r^3/27+O(r^{8/3})}$. Voici, à titre d'exemple, le tableau qui donne les nombres N de classes de 2-groupes de cardinal 2^r (ce sont les seuls actuellement connus) :

2^r	4	8	16	32	64	128	256	512	1024
N	2	5	14	51	267	2328	56092	10494213	49487365422

La diversité des p-groupes est exceptionnelle. Les 2-groupes d'ordre représentent plus 99% des groupes d'ordre jusqu'à 2000 : il existe[2] « seulement », à isomorphisme près, 423 164 062 groupes d'ordres $\neq 1024$ et inférieurs à 2000, contre plus de 49.10^9 d'ordre 1024.

Le point de départ élémentaire de ces classifications est le suivant :

Proposition 13.12 *Le centre d'un p-groupe n'est pas trivial.*

2 C'est un résultat du type millénium visant à trouver vers l'an 2001 tous les groupes d'ordre plus petits que 2001. La difficulté principale est concentré dans les ordres 2^{10} et 3.2^9. Voir l'annonce de Hans Ulrich Besche, Bettina Eck et E.A O' Brien parue dans *Electronic research annoncement de l'AMS*, **7**, 1–4 (2001).