ἡ ὕβρις

Le journal mathématique de l'ENS de Cachan

Quis hic locus, quae regio, quae mundi plaga?
Vbi sum? Sub ortu solis an sub cardine
glacialis ursae? Numquid Hesperii maris
extrema tellus hunc dat Oceano modum?
Quas trahimus auras? Quod solum fesso subest?

Sénèque, Hercule Furieux

Éditorial

Peut-on imaginer un étudiant en probabilités discutant mathématiques avec un camarade spécialisé en géométrie algébrique ? Difficilement. D'autres ont même des constats plus amer : selon J.P Kahane et M. Chouchan, *Most mathematicians suffer from narrowness. They have only a fragmented view of mathematics and,* a fortiori, *of its history, its applications and its relationship with human society.* Nous voulons rétablir la communication.

Nous allons d'une part présenter des domaines que tous ne connaissent pas, d'autre part souligner l'interaction entre ces différents domaines. Nous ne voulons pas donner une vue égocentrique des mathématiques : l'utilisation par d'autres disciplines et les éventuelles influences en retour nous intéressent. Nous pensons à la physique théorique, mais il n'y a pas que ça...

Ce journal est le vôtre, nous attendons vos remarques et, surtout, vos articles. Vous pouvez consultez quelques recomandations typographiques et détails utililes pour la rédaction d'un article sur la page Web du journal, `http://www.rip.ens-cachan.fr:8080/~hubris`. Vous pouvez nous joindre à l'adresse électronique `hubris@RIP.ENS-Cachan.Fr`.

Ce trimestre, nous vous invitons à vous interroger sur l'axiome du choix, que l'on utilise parfois sans le savoir, à découvrir la K-théorie et à vous pencher sur le groupe $\mathrm{PGL}(2, \mathbf{C})$ et sur son utilité en géométrie.

Ce numéro est écrit par des élèves, nos talents pédagogiques et notre compréhension de la mathématique ne sont qu'embryonnaires. Les articles sont probablement mal écrits et regorgent d'erreurs. Soyez indulgents.

Une dernière précision : le titre du journal, ἡ ὕβρις, se lit *hubris* – c'est le terme grec désignant la démesure.

Enfin, nous tenons à remercier J.-M. Ghidaglia, J. Mazars, qui nous ont soutenus ainsi que les rédacteurs des articles déjà écrits et de ceux qui nous parviendrons bientôt.

Répétons-le encore une fois : ce journal est le vôtre, nous attendons vos articles. N'hésitez pas à nous contacter.

Gabriel Dos Reis
Vincent Zoonekynd

Sommaire

Lemme de Baire et axiome du choix

Raphael BOMBOY

Introduction

Le point de départ de cet article est, je crois, une question qui surgit lors d'une leçon d'agreg à laquelle je n'assistais pas. Rappelons qu'un anneau noethérien est un anneau dans lequel tout idéal est de type fini. Ce qui équivaut à dire que toute suite croissante d'idéaux de cet anneau est stationnaire. La question était : cette équivalence utilise-t-elle l'axiome du choix ? L'ouvrage (par ailleurs excellent) de Daniel Perrin [Per82], et par suite l'agrégatif au tableau ce jour là, affirmait que non. Eric Halberstadt fit remarquer que si et fut je crois mal compris. De là vient mon envie d'écrire cet article, article qui m'obligea à des investigations qui m'emmenèrent plus loin qu'initiallement prévu, et furent à l'origine de questions dont j'ignore encore la réponse (si quelqu'un sait quelque chose à ce sujet...).

L'essentiel de ce qui va suivre vient de mes discussions avec Eric Jaligot, Maurice Pouzet et mes collègues agrégatifs, qu'ils en soient remerciés.

Au fait, quel est le lien de tout ceci avec le lemme de Baire ? Patience, j'y reviendrai.

Le lemme de Baire

Je ne fais ici que rappeler le lemme de Baire et sa démonstration la plus classique. Ceux qui connaissent déjà ceci peuvent se rendre au paragraphe suivant.

Lemme. *Soit E un espace de Banach, $(O_n)_{n\in\mathbf{N}}$ une famille dénombrable d'ouverts denses de E. Alors $\cap_{i\in\mathbf{N}}O_n$ est dense dans E.*

Démonstration : Il suffit de montrer que pour tout ouvert O de E, $O\bigcap(\cap_{i\in\mathbf{N}}O_n)$ n'est pas vide.

Soit donc O un ouvert de E. O_1 étant dense dans E, $O\cap O_1$ n'est pas vide et on peut choisir $x_0\in E$ et $r_0<1$ tels que $B(x_0,r_0)\subset O\cap O_1$ ($B(x_0,r_0)$ désigne la boule ouverte de centre x_0 et de rayon r_0).

On construit par récurrence une suite $((x_n,r_n))_{n\in\mathbf{N}}$ telle que pour tout $n\in\mathbf{N}$, $B(x_{n+1},r_{n+1})\subset B(x_n,r_n/2)\bigcap(\cap_{1\leqslant i\leqslant n+1}O_i)$ et $r_n<1/n$. Pour cela, supposons cette suite construite jusqu'a l'ordre n. O_{n+1} étant dense dans E, $B(x_n,r_n)\cap O_{n+1}$ n'est pas vide et on peut choisir $x_{n+1}\in E$ et $r_{n+1}<1/(n+1)$ tels que $B(x_{n+1},r_{n+1})\subset B(x_n,r_n/2)\cap O_{n+1}$.

On vérifie alors facilement que la suite $(x_n)_{n\in\mathbf{N}}$ est de cauchy, donc qu'elle converge car E est complet. Sa limite l est dans $\cap_{n\in N}O_n$ car pour tout $n\in\mathbf{N}$, $l\in\overline{B(x_n,r_n/2)}\subset B(x_n,r_n)$. □

L'axiome du choix

On ne peut rien démontrer si on ne part pas d'une hypothèse de départ ; depuis Euclide, les mathématiciens utilisent tous plus ou moins une méthode axiomatique, c'est à dire qu'il partent d'un ensemble d'axiomes qu'ils jugent intuitivement évident et se donnent ensuite un ensemble de règles de démonstration (les logiciens disent règles d'inférences) qui leur permettent de démontrer de nouveaux théorèmes à partir de ces axiomes. Cela ne signifie pas qu'ils ont en permanence ces axiomes et ces règles d'inférences en tête lors de leur pratique quotidienne des mathématiques, mais qu'ils sont à peu près persuadés que s'ils y mettaient le temps voulu, ils pourraient formaliser entiérement leurs démonstrations.

On ne peut pas non plus définir tout les objets mathématiques à partir de rien, c'est à dire qu'on doit se donner un certain nombre d'objets de base dont la définition est intuitivement évidente. Au début du siècle eu lieu une tentative pour construire tout les objets mathématiques à partir des seules notions d'ensemble et d'appartenance ; c'est ce point de vue qui c'est imposé, et on définit aujourd'hui $\mathbf{N}$ comme étant le plus petit ordinal infini, $\mathbf{Z}$ comme ensemble des classes d'une relation d'équivalence sur $\mathbf{N}^2$, $\mathbf{Q}$ comme ensemble des classes d'une relation d'équivalence sur $\mathbf{Z}^2$, $\mathbf{R}$ à partir de l'ensemble des coupures de $\mathbf{Q}$, etc.

Si nous construisons les mathématiques à partir de la théorie des ensembles, ils nous faut axiomatiser celle-ci. Certains des axiomes couramment admis depuis le début du siècle ne sont pas discutés, ce sont ceux de Zermelo-Fraenkel ; pour ceux-ci, voir par exemple [CL94],[Kri72] ou [Jec78]. Un autre des axiomes proposés au début du siècle a été plus contesté : c'est l'axiome du choix, que nous énonçons ici.

Axiome (du choix). *Soit X un ensemble d'ensembles tous non vides. Alors il existe une fonction f, définie sur X et à valeurs dans $\cup_{x\in X}x$ telle que pour tout $x\in X$, $f(x)\in x$ (une telle fonction sera appelée fonction de choix).*

Remarque. En thérie des ensembles, tout est un ensemble. La notion d'« ensemble d'ensembles » est donc un pléonasme. Dans la définition ci-dessus, j'aurais pu dire « Soit X un ensemble dont tout les éléments sont non vides... » .

L'axiome du choix est bien un axiome, c'est à dire qu'on ne peut ni le démontrer, ni l'infirmer (c'est à dire démontrer son contraire) à partir des axiomes de Zermelo-Fraenkel (du moins si ceux-ci non contradictoires). Des explications s'imposent ici : comment peut-on démontrer que quelque chose n'est pas démontrable ? Pour cela, il faut faire ce qu'on appelle de la logique mathématique, c'est à dire commencer par définir formellement ce qu'est une formule (c'est un suite finie de symbole dans un alphabet donné), la démontrabilité et la vérité d'une formule, etc., et le définir formellement dans le cadre que nous nous sommes donné, c'est à dire à partir de la notion d'ensemble. Ces objets sont alors des objets mathématiques, comme peuvent l'être $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, un groupe ou un espace vectoriel, et on peut donc démontrer des théorèmes les concernant, par exemple qu'une formule n'est pas conséquence d'un ensemble d'axiomes donné.

Certains pensent qu'on trompe le lecteur en parlant ainsi des mathématiques en termes mathématiques ; il n'y a pourtant là-dessous aucun sophisme. Les objets qu'on manipule modèlisent le raisonnement mathématique, comme $\mathbf{R}^3$ modélise l'espace physique qui nous entoure ; mais leur signification intuitive n'infère pas sur la rigueur des raisonnements qu'on peut tenir à leur sujet. Ce sont bien des objets mathématiques, et la logique mathématique est une branche des mathématiques, pas de la métaphysique. Notons d'ailleurs que cette branche contient aujourd'hui des résultats non triviaux, qu'elle s'est scindée en plusieurs directions, et qu'elle s'est éloignée de ses motivations initiales pour se rapprocher d'autres domaines des mathématiques, comme l'algèbre ou l'informatique théorique. C'est un indice de son sérieux et de son intérêt, et on peut penser que la logique éliminera le doute que font peser certains sur la validité de ses raisonnements grâce à l'efficacité de ses résultats (c'est vrai parce que ça *marche*).

La démonstration de l'indépendance de l'axiome du choix avec les axiomes de Zermelo-Fraenkel contient de belles idées, mais elle est compliquée. Elle nécessite de bien avoir compris la notion de modèle et le théorème de complétude du calcul des prédicats, qui assure que des formules sont non contradictoires si et seulement si elles ont un modèle commun. La construction d'un modèle commun aux axiomes de Zermelo Fraenkel et à l'axiome du choix (grâce aux ensembles constructibles de Gödel) et d'un modèle commun aux axiomes de Zermelo Fraenkel et à la négation de l'axiome du choix (grâce au Forcing de Paul Cohen) est longue et parfois fastidieuse techniquement (pour tout cela, voir [Jec77b]). Même ainsi, ces modèles étant construits à partir d'un modèle – dont on admet l'existence – des axiomes de Zermelo-Fraenkel, on n'obtient qu'un résultat de consistance relative, c'est à dire qu'on ne prouve l'indépandendance de l'axiome du choix et des axiomes de Zermelo-Fraenkel que si ceux-ci sont consistants, c'est à dire non contradictoires. Or, un célèbre théorème du à Gödel affirme que leur consistence est indémontrable.

L'axiome du choix a eu plus de mal à être accepté comme intuitivement évident que d'autres axiomes, la fonction de choix pouvant être difficile à se représenter dans le cas de certains ensemble non dénombrables, par exemple si X est l'ensemble des parties de $\mathbf{R}$. Ceux qui mettent en doute l'axiome du choix tentent de montrer qu'il implique des résultats surprenants ; l'exemple qu'on donne généralement est celui de ce qu'on appelle le paradoxe de Banach-Tarsky, qui affirme qu'une sphère de $\mathbf{R}^3$ peut être décomposée en un nombre fini de morceaux tels qu'en recombinant ces morceaux comme un puzzle, on obtienne deux sphères disjointes de même volume que la sphère initiale (C'est vrai, mais les morceaux en question ont des formes franchement pathologiques : on ne peut pas définir dessus une notion de volume et ils n'ont pas un nombre fini de composantes connexes.) Mais l'axiome du choix à finit par s'imposer, en ce sens qu'on l'emploie à peu près partout : pour montrer le théorème de Krull, le théorème de la base incomplète, l'existence de la clôture algébrique d'un corps, que tout sous-groupe d'un groupe libre est libre, qu'une réunion dénombrable de sous-ensembles de réels négligeables pour la mesure de Lebesgue est négligeable,etc. En fait, c'est même pire que ça : pour chacun des exemples que je viens de donner, on peut montrer qu'ils sont indépendants des axiomes de Zermelo-Fraenkel. C'est à dire que sans l'axiome du choix, on peut construire des modèles dans lesquels tout les idéaux ne sont pas inclus dans un idéal maximal, tout les espaces vectoriels n'ont pas de bases, tout les corps n'ont pas de clôture algébrique, des groupes libres ont des sous-groupes non libres, on peut trouver un ensemble de réels qui est non négligeable, mais réunion d'un nombre dénombrable d'ensembles négligeables...vous voulez encore vous passer de l'axiome du choix ?

Lemme de Baire et axiome du choix

Revenons à nos moutons : la démonstration du lemme de Baire située plus haut utilise-t-elle l'axiome du choix ? Quand j'ai posé la question, on m'a souvent répondu non, et on s'est généralement justifié par une explication du type « Pour contruire la suite (x_n, r_n) jusqu'à l'ordre n, on n'a besoin de ne faire qu'un nombre fini de choix. Or, l'existence d'une fonction de choix se démontre trivialement quand X est fini » .

C'est faux, et voici pourquoi. Le problème vient de ce qu'une définition par récurrence est quelque chose de délicat, bien plus délicat qu'une démonstration par récurrence. Plus précisément, lorsque vous faites une définition par récurrence vous utilisez, probablement sans s'en rendre compte comme je l'ai fait moi même pendant des années, le résultat suivant :

Proposition. *Soit E un ensemble et F une fonction définie sur l'ensemble des couples $(n, \{x_0, ..., x_{n-1}\})$ où $n \in \mathbf{N}$ et $\{x_1, ..., x_{n-1}\}$ est un n-uplet d'éléments de E (avec la convention qu'un 0-uplet est l'ensemble vide). Alors il existe une unique suite $(x_n)_{n\in n}$ telle que pour tout $n \in N$, $x_n = F((n, \{x_0, ..., x_{n-1}\}))$.*

Démonstration Pour l'unicité, supposons qu'il existe deux suite $(x_n)_{n\in\mathbf{N}}$, $(y_n)_{n\in\mathbf{N}}$ distinctes vérifiant la condition ci-dessus. Soit n le plus petit entier tel que $x_n \neq y_n$. On a alors $x_m = y_m$ pour tout $m < n$, d'où $x_n = F((n, \{x_0, ..., x_{n-1}\})) = F((n, \{y_0, ..., y_{n-1}\})) = y_n$, une contradiction.

Pour l'existence, montrons que pour tout $n \in \mathbf{N}$, on peut construire un $n+1$-uplet $\{x_0, ..., x_n\}$ tel que pour tout $m \leqslant n$, $x_m = F(m, \{x_0, ..., x_{m-1}\})$. Supposons que cela soit faux : soit n le plus petit entier tel qu'on ne peut construire de tel $n+1$-uple. Il existe un n-uplet $\{x_0, ..., x_{n-1}\}$ tel que pour tout $m \leqslant n$, $x_m = F((m, \{x_0, ..., x_{m-1}\}))$; $\{x_0, ..., x_{n-1}, F((n, \{x_0, ..., x_{n-1}\}))\}$ est alors un $n+1$-uplet satisfaisant la même condition, d'où une contradiction.

De plus, de même que ci-dessus, pour tout $n \in \mathbf{N}$, on a unicité d'un tel n-uplet. C'est ce qui nous permet de conclure. En effet, pour tout entiers m,n tels que $m < n$, on a alors, si $\{x_1, ..., x_m\}$ et $\{y_1, ..., y_n\}$ sont les $m+1$-uplets et $n+1$-uplets définis comme ci-dessus, $\{x_1, ..., x_m\} = \{y_1, ..., y_n\}$. Pour tout $n \in \mathbf{N}$, on peut donc définir x_n comme étant le n^{eme} élément commun à tout les débuts de suite définis comme ci-dessus d'une longueur supérieure à n, et on vérifie facilement que la suite $(x_n)_{n\in\mathbf{N}}$ vérifie $x_n = F((n, \{x_0, ..., x_{n-1}\}))$ pour tout $n \in \mathbf{N}$.

Dans cette démonstration, il est essentiel que pour un n donné, x_n soit défini de manière unique à partir de n et $\{x_0, ..., x_{n-1}\}$. Sans cela vous pourrez bien définir pout tout n un n-uplet $\{x_0, ..., x_{n-1}\}$ tel que pour tout $m \leqslant n-1$, $x_m = F((m, \{x_0, ..., x_{m-1}\}))$, mais vous ne serez pas sur de l'unicité de ce n-uplet, et vous ne pourrez donc pas prendre l'union de tout ces débuts de suite pour former une suite $(x_n)_{n\in\mathbf{N}}$ telle que pour tout $n \in \mathbf{N}$, $x_n = F((n, \{x_0, ..., x_{n-1}\}))$.

Dans la démonstration du lemme de Baire que nous avons donnée, on n'a pas unicité du choix possible de x_n et r_n à chaque étape. Cette démonstration est-elle fausse ? Pas de panique, l'axiome du choix nous permet de nous en tirer. En effet, pour tout ouvert O, pour tout $n \in \mathbf{N}$, l'ensemble des couples (x, r) tels que $B(x, r) \subset O \bigcap (\cap_{1\leqslant i\leqslant n} O_i)$ et $r < 1/n$ est non vide. L'axiome du choix assure donc l'existence d'une fonction de choix f sur l'ensemble des ensembles de ce type, et pour tout $n \in \mathbf{N}$, si on a construit la suite (x_n, r_n) jusquà l'ordre n, on peut poser $(x_{n+1}, r_{n+1}) = f(\{(x, r); B(x, r) \subset O \bigcap (\cap_{1\leqslant i\leqslant n} O_i) \text{ et } r < 1/n\})$.

De l'axiome du choix partout

Lorsque j'eu compris pourquoi le lemme de Baire utilisait l'axiome du choix, ma grande surprise à été de découvrir que ce type de raisonnement – construire une suite par récurrence en choisissant à chaque étape un élément parmi un ensemble non vide – se retrouvait très fréquemment. On l'utilise en particulier :

- pour démontrer le théorme de projection sur un convexe fermé dans un Hilbert.
- Pour démontrer le théorème des fermés emboités dans un Banach.
- Pour démontrer qu'un espace métrique satisfait la propriété de Borel-Lebesgue si et seulement si il satisfait celle de Bolzano-Weierstrass.

On l'utilise également (j'avais promis qu'on y reviendrait) pour montrer qu'un anneau est noethérien si et seulement si toute suite croissante d'idéaux de cet anneau est stationnaire. Voici cette démonstration, du moins le sens qui utilise l'axiome du choix (pour l'autre, voir [Per82]).

Démonstration Montrons que si toute suite croissante d'idéaux est stationnaire, tout idéal est de type fini. Pour cela, supposons qu'on ait un idéal I qui ne soit pas de type fini. Choisissons $x_0 \in I$; on a alors $\langle x_0 \rangle \subsetneq I$ ($\langle x_0 \rangle$ désigne l'idéal engendré par x_0).

On construit alors par récurrence une suite $x_0, ...x_n, ...$ d'éléments de I telle que $\langle x_0 \rangle \subsetneq \langle x_0, x_1 \rangle \subsetneq$

... $\subsetneq$ $\langle x_0, ..., x_n\rangle$ $\subsetneq$ .... Pour cela, supposons cette suite construite jusqu'à l'ordre n. On a alors $\langle x_0, ..., x_n\rangle \subsetneq I$, d'où on peut choisir $x_{n+1} \in I$ tel que $\langle x_0, ..., x_n\rangle \subsetneq \langle x_0, ..., x_{n+1}\rangle$, ce qui conclut.

Evidemment, cette démonstration est aussi fausse que ma première démonstration du lemme de Baire ; et on peut la rendre juste de la même façon en utilisant une fonction de choix définie sur l'ensemble des ensembles du type $I - \langle X\rangle$, où X est une partie finie de I. En fait, une fois qu'on a compris comment fonctionne ce genre de démonstration, il est effectivement moins lourd de les écrire sous la forme ci-dessus en considérant à chaque fois que les terme « on choisit » sont une méta-définition pour « on prend l'élément image par la fonction de choix imposée dès le départ et définie sur un ensemble adapté de l'ensemble défini par le début de notre suite » l'ensemble adapté en question dépendant évidemment de la démonstration que vous êtes en train de faire.

L'utilisation inconsciente – ou peut-être camouflée pour ne pas faire peur aux étudiants – de cet axiome est très répendue dans ce genre de situation, des manuels réputés d'analyse ne font pas remarquer que le lemme de Baire ou le théorème de projection sur un convexe fermé emploie l'axiome du choix, alors qu'ils insistent sur le fait que le théorème de Hahn-Banach utilise le lemme de Zorn, équivalent célèbre de cet axiome.

Axiome du choix dénombrable, axiome du choix dépendant

Une des tentations de ceux qui se mefiaient de l'axiome du choix a été d'en trouver des formes plus faibles, mais suffisantes pour démontrer les résultats dont on avait besoin. Voici deux de ces plus célèbres versions faibles.

Axiome (du choix dépendant). *Soit X un ensemble, R une relation binaire sur X telle que pour tout $x \in X$, l'ensemble des $y \in X$ tels que xRy est non vide. Alors il existe une suite $x_0, ..., x_n, ...$ d'éléments de X telle que pour tout $n \in \mathbf{N}$, $x_n R x_{n+1}$.*

Axiome (du choix dénombrable). *Soit X un ensemble dénombrable dont tout les éléments sont non vides. Alors X admet une fonction de choix.*

Proposition. *L'axiome du choix implique l'axiome du choix dépendant ; l'axiome du choix dépendant implique l'axiome du choix dénombrable.*

Démonstration Montrons que l'axiome du choix implique l'axiome du choix dépendant. Soit X un ensemble non vide, R une relation binaire sur X telle que pour tout $x \in X$, il existe $y \in X$ tel que xRy. Soit Z l'ensemble des ensembles du type $X_x = \{y \in X;\ xRy\}$, où $x \in X$. Tout élément de Z est non vide, donc Z admet une fonction de choix f. On construit alors par récurrence une suite $x_0, .., x_n, ...$ d'éléments de X en posant $x_{n+1} = f(X_{x_n})$, et cette suite convient (c'est encore une fois le même genre de démonstration que pour le lemme de Baire).

Admettons maintenant l'axiome du choix dépendant. Soit X un ensemble dénombrable dont tout les éléments sont non vides. X étant dénombrable, on peut énumérer ses éléments $x_1, ..., x_n, ...$ Soit S l'ensemble des suites finis $t = (t_1, ...t_n)$ à valeurs dans $\cup_{1 \leqslant i \leqslant n} x_i$ telle pour tout $i \leqslant n$, $t_i \in x_i$. Pour tout $t \in S$, on définit $|t|$ comme étant la longueur de t.

Soit R la relation binaire définie sur S par sRt si et seulement si t est plus longue d'un élément que s et s est formée des $|s|$ premiers éléments de t. Pour tout $s \in S$, il existe $t \in S$ tel que sRt (il suffit de rajouter un élément de $x_{|s|+1}$ à la fin de s). D'après l'axiome du choix dépendant, on peut dons construire une suite de suite finie $s_1, ..., s_n, ...$ telle que si $m < n$, s_m est un segment initial de s_n. En prenant l'union de toute ces suites, on obtient donc une suite $s_1, ..., s_n, ...$ telle que pour tout $n \in \mathbf{N}$, $s_n \in x_n$, ce qui donne une fonction de choix sur X en posant $f(x_n) = s_n$.

Ces implications sont des implications strictes : l'axiome du choix dénombrable n'implique pas l'axiome du choix dépendant, et l'axiome du choix dépendant n'implique pas l'axiome du choix général. Cela se montre par les mêmes méthodes que les résultats d'indépendance de l'axiome du choix avec les axiomes de Zermelo-Fraenkel, et nous ne aventurerons pas en ces eaux dangereuses.

Proposition. *Le lemme de Baire est une conséquence de l'axiome du choix dépendant.*

Démonstration Soit O un ouvert de E. On définit une relation binaire sur l'ensemble des couples (B, n), où $n \in \mathbf{N}$ et B est une boule ouverte de E de rayon inférieur à $1/n$, par $(B(x, r), m)R(B(y, s), n)$ si et seulement si $n = m + 1$ et $B(y, s) \subset B(x, r/2) \bigcap (\cap_{1 \leqslant i \leqslant n} O_i) \bigcap O$. Cette relation vérifie les conditions qui permettent d'appliquer l'axiome du choix dépendant, et la suite de boules $B(x_n, r_n)$ qu'elle définie est telle que pour tout $n \in \mathbf{N}$, $B(x_{n+1}, r_{n+1}) \subset B(x_n, r_n/2)$, $r_n \leqslant 1/n$ et $B(x_n, r_n) \subset O \bigcap (\cap_{1 \leqslant i \leqslant n} O_i)$. On conclut alors de la manière habituelle.

Par contre, l'axiome du choix dénombrable ne suffit pas à priori à démontrer le lemme de Baire en général ; en effet, dans la démonstration du lemme de Baire, la fonction de choix qu'on utilise est définie sur un ensemble X indicié non pas par $\mathbf{N}$, mais par l'ensemble des couple (O, n), où $n \in \mathbf{N}$ et O est un ouvert de E ; X n'est donc pas dénonbrable. En revanche, si E est séparable, on peut démontrer le lemme de Baire dans E en utilisant le choix dénombrable : il suffit d'adapter la démonstration en prenant une base dénombrable d'ouverts.

Exercice. Établir :

- l'équivalence de la noethérianité et de la condition de chaîne fini sur les idéaux à l'aide de l'axiome du choix dépendant.
- le théorème des fermés emboités dans un Banach et l'équivalence des propriétés de Borel-Lebesgue et de Bolzano-Weierstrass pour un espace métrique à l'aide du choix dépendant, du choix dénombrable si les espaces considérés sont complets.
- le théorème de projection sur un convexe fermé dans un Hilbert à l'aide du choix dénombrable.

Un peu de mathématiques alternatives

L'axiome du choix a une conséquence désagréable en théorie de la mesure : il permet de construire un sous ensemble de $[0;1]$ non mesurable pour la mesure de Lebesgue (voir [Jec78]). En revanche, il existe des axiomes, contradictoires avec l'axiome du choix, qui permettent de démontrer que tout sous-ensemble de $[0;1]$ est mesurable ; voici le plus célèbre.

Soit ω^ω l'ensemble des suites à valeurs dans $\mathbf{N}$. A un sous ensemble A de ω^ω, on associe le jeu G_A suivant : deux joueurs choisissent à tour de rôle un entier naturel. Soit $a_1, ..., a_n, ...$ la suite des choix du premier joueur, $b_1, ..., b_n, ...$ celle du second. Si la suite $a_1, b_1, ..., a_n, b_n, ...$ est dans A, le premier joueur a gagné ; sinon, il a perdu. (Il n'y a aucune différence formelle entre l'ensemble A et le jeu G_A : G_A est juste une interprétation intuitive de cet ensemble.)

Une stratégie pour le premier joueur est une fonction σ définie sur l'ensemble des suites finies de $\mathbf{N}$; cette stratégie et gagnante, si pour toute suite $b_1, ..., b_n, ...$, la suite $\sigma(\varnothing), b_1, \sigma(b_1), ..., b_n, \sigma(b_1, ..., b_n), ...$ est dans A, c'est à dire si le premier joueur dispose d'une manière de jouer en fonction seulement de ce que l'autre a joué avant lui qui le fasse gagner à chaque coup.

Évidement, on peut également définir une stratégie et une stratégie gagnante pour le second joueur. On dit que le jeu A est déterminé si un des deux joueur a une stratégie gagnante.

Axiome (de détermination). *Pour tout $A \subset \omega^\omega$, G_A est déterminé.*

L'axiome de détermination a une conséquence importante : *il permet de démontrer que tout sous-ensemble de $[0;1]$ est mesurable pour la mesure de Lebesgue complétée (voir [Jec77b]).* Ceci prouve qu'il est contradictoire avec l'axiome du choix général, qui permet lui de construire un ensemble de réels non mesurables. Mais l'axiome de détermination permet de démontrer une version plus faible de l'axiome du choix :

Théorème. *L'axiome de détermination implique que tout ensemble dénombrable d'ensembles tous non vide de cardinalité inférieure à $2^{\aleph_0}$ admet une fonction de choix.*

Démonstration Un ensemble de cardinalité inférieure à $2^{\aleph_0}$ peut s'injecter dans l'ensemble des suites d'entiers naturels (on code donc chaque élément par une suite). Désormais, j'identifierai chaque ensemble de cardinalité inférieure à $2^{\aleph_0}$ avec un ensemble de suites à valeurs dans $\mathbf{N}$.

Soit donc $X = (x_0, ..., x_n, ...)$ un ensemble dénombrable d'ensembles de suites à valeurs dans $\mathbf{N}$. On définit alors le jeu suivant : soit $(a_0, ..., a_n, ...)$ la suite des choix du premier joueur, $(b_0, ..., b_n, ...)$ celle du second. Le second joueur à gagné si et seulement si $(b_1, ..., b_n, ...) \in x_{a_0}$.

Le premier joueur ne peut pas avoir de stratégie gagnante à ce jeu : quel que soit le nombre b_0 qu'il joue en premier, il ne peut avoir de stratégie qui lui permette de répondre à la suite $(b_1, ..., b_n, ...)$ où $(b_1, ..., b_n, ...)$ est un élément quelconque de x_{a_0}.

D'après l'axiome de détermination, le second joueur a donc une stratégie gagnante σ. (Attention : si on ne suppose ni l'axiome de détermination, ni l'axiome du choix, le fait que le premier joueur n'ait pas de stratégie gagnante n'implique pas que le second en ait une). σ nous donne alors une fonction de choix sur X (a chaque $n \in \mathbf{N}$, on associe l'élément de x_n qu'on obtient quand le premier joueur joue n suivit d'une suite infinie de 0 et le second sa stratégie gagnante).

Cette version faible de l'axiome du choix suffit pour montrer le lemme de Baire sur $\mathbf{R}$; elle suffit également pour montrer qu'une union dénombrable d'ensembles négligeables pour la mesure de Lebesgue est négligeable. Si on admet donc l'axiome de détermination, on peut construire une théorie de la mesure et une analyse dans laquelle les propriétés essentielles de la droite réelle restent conservées, mais dans laquelle tout ensemble de réel est mesurable.

A priori, cela relève d'un délire de logicien : en explorant deux mathématiques différentes à partir de deux axiomatiques différentes, on réduit les mathématiques à un jeu formel, alors qu'elles ont un sens, sens intuitif qu'on ne peut conserver qu'en partant d'axiomes « moralement » exacts. Pourtant, certains axiomes contradictoires avec l'axiome du choix ont permit de construire des mathématiques élégantes, qui permettent d'éclairer la signification des axiomes en question. Imposer ces axiomes revient à restreindre la notion d'ensemble de façon à éliminer les sous-ensembles pathologiques de $\mathbf{R}$; les résultats ainsi obtenus ont des applications en théorie de la mesure ou topologie. Il s'agit là d'un domaine qui s'appelle la *theorie descriptive des ensembles*, dont je ne dirai rien de plus parce que je n'y connais rien (mais si Alain pouvais nous faire un topo sur le sujet, ça serait très bien).

Question. *L'axiome de détermination est-il consistant avec l'axiome du choix dépendant ? Avec l'axiome du choix dénombrable ?*

Avant toute chose, il faudrait se demander si l'axiome de détermination est consistant avec ceux de Zermelo-Frankel : c'était encore au stade de conjecture dans les ouvrages que j'ai lu, et je ne sais pas où on en est actuellement.

Si l'axiome de détermination est consistant avec l'axiome du choix dépendant, on peut se passer d'une démonstration du lemme de Baire à l'aide de l'axiome de détermination en se plaçant dans un modèle de ces deux axiomes, dans lequel le lemme de Baire sera vrai pour un Banach quelconque.

Une autre conséquence de l'axiome du choix utilisée en analyse est le théorème de l'ultrafiltre.

Définition. *Soit E un espace topologique, X l'ensemble des ouverts sur cet espace. Un filtre sur E est un sous-ensemble F de X tel que si $O \in F$ et $O \subset O'$, $O' \in F$ et que si $O_1, O_2 \in F$, $O_1 \cup O_2 \in F$.*

Un filtre propre est un filtre qui n'est pas égal à X tout entier.

Un filtre maximal est un filtre propre maximal pour l'inclusion.

Théorème (de l'ultrafiltre). *Tout filtre est inclus dans un filtre maximal*

Pour la démonstration, très classique voir [Sch93].

Le théorème de l'ultrafiltre suffit à démontrer le théorème de Tychonoff, qui affirme qu'un produit d'espace compact est compact (voir [Sch93]).

D'autre part, c'est un énoncé strictement plus faible que l'axiome du choix (voir [Jec77b]).

Question. *Le théorème de l'ultrafiltre est-il consistant avec l'axiome de détermination ? Avec l'axiome du choix dépendant ? Celui du choix dénombrable ?*

Si le théorème de l'ultrafiltre est consistant avec l'axiome de détermination, on peut obtenir une analyse dans laquelle tout ensemble de réels est mesurable et le théorème de Tychonoff reste vrai ; avec l'axiome du choix dépendant en plus, le lemme de Baire reste vrai également dans le cas général. Mais je ne sais pas si c'est aussi intéressant que de montrer les conséquences du théorème de la page précédente.

Pour en savoir plus...

[Bar77] J. Barwise (ed.), *Handbook of mathematical logic*, North Holland, 1977.

[Bha94] Vandana Bhandari, *L'axiome du choix*, 1994.

[CL94] René Cori and Daniel Lascar, *Logique mathématique, t2*, Masson, 1994.

[Hal74] Paul R. Halmost, *Naive set theory*, Springer, 1974.

[Jec77a] Thomas J. Jech, About The Axiom Of Choice, 345–370, In Barwise [Bar77], 1977, pp. 345–370.

[Jec77b] Thomas J. Jech, *The axiom of choice*, North Holland, 1977.

[Jec78] Thomas J. Jech, *Set theory*, Academic Press, 1978.

[Kri72] Jean-Louis Krivine, *Théorie axiomatique des ensembles*, PUF, 1972.

[Kun80] Kenneth Kunen, *Set theory*, North Holland, 1980.

[Mic64] Jan Micielsky, *On the axiom of determinatness*, Fund. Math. **54** (1964).

[Per82] Daniel Perrin, *Cours d'algèbre*, Publication de l'ENSJF, 1982.

[Sch93] Laurent Schwartz, *Analyse I: théorie des ensembles et topologie*, Hermann, 1993.

K-théorie

Vincent ZOONEKYND

Résumé

Pour étudier un anneau, la K-théorie considére la catégorie des modules de type fini sur cet anneau : l'ensemble des objets est muni d'une structure de monoïde. Pour faciliter les calculs, on remplace ce monoïde par le groupe abélien le plus proche. On s'est ramené à l'étude d'un objet plus simple.
Nous définirons les groupes de K-théorie négatifs, qui sont des *invariants* des anneaux considérés. Ils sont reliés par une *suite exacte* qui permet (parfois) de les calculer de proche en proche.
Cet article se veut une présentation succinte de la K-théorie, destinée, destinée à rassurer ceux qui sont effrayés par les mots de cohomologie ou de K-théorie : il s'agit dans ces deux cas de remplacer des objets compliqués (anneaux, espaces topologiques) pas des objets plus simples (groupes abéliens, espaces vectoriels).

Introduction

On rencontre des anneaux dans des domaines très divers : l'étude de $\mathbf{Z}$ est liée à celle des nombres premiers, l'étude des espaces topologiques compacts ou de la géométrie non commutative se ramène à celle des $C^\star$-algèbres, l'analyse fonctionnelle se ramène souvent à l'étude d'opérateurs d'un espace de Hilbert, *i.e.*, éléments de l'algèbre de ses endomorphismes.

K_0 d'un anneau

Groupe de Grothendieck. Soit M un semi-groupe commutatif, il existe un groupe abélien KM, appelé *groupe de Grothendieck* et un morphisme de monoïdes $M \longrightarrow KM$ tel que pour tout groupe H et tout morphisme $M \longrightarrow H$ il existe un unique morphsime de groupe $KM \longrightarrow H$ tel que

$$\begin{tikzcd} M \arrow[r] \arrow[dr] & KM \arrow[d, dotted] \\ & H \end{tikzcd}$$

Il suffit de prendre l'ensemble de $(x, y) \in M^2$ modulo la relation d'équivalence

$$(x, y) \sim (u, v) \quad \text{si} \quad \exists t \in M \quad x + v + t = u + y + t.$$

Par exemple, $K\mathbf{N} = \mathbf{Z}$ et $K(\mathbf{N} \cup \{\infty\}) = 0$.

***K_0A*.** Soit A un anneau. L'ensemble (c'en est bien un) des classes d'isomorphie des A-modules projectifs (*i.e.*, facteurs directs d'un module libre) de type fini forme un monoïde. Son groupe de Grothendieck est appelé *premier groupe de K-théorie de A* et est noté $K_0(A)$. Par exemple, $K_0\mathbf{R} = \mathbf{Z}$: c'est la dimension des espaces vectoriels.

Remarque. Pour calculer le groupe de Grothendieck à partir de cette définition, il est bon de connaître la structure des modules projectifs de type fini sur notre anneau. Le calcul est donc à peu près immédiat si A est un corps ou un anneau principal. Nous disposons néanmoins d'une description plus concrète de K_0A.

***K_0* et idempotents.** Notons $\mathrm{GL}(A) = \varinjlim \mathrm{GL}_n A$ le groupe des matrices carrées inversibles finies d'ordre quelconque (on multiplie des matrices d'ordre différent en rajoutant des 1 sur la diagonale de la plus petite), $M(A) = \varinjlim M_n(A)$ l'algèbre (sans unité) des matrices finies d'ordre quelconque (on additionne ou multiplie des matrices de tailles différentes en complétant la plus petite par des zéros) et $\mathrm{Idem}\, A$ l'ensemble des éléments idempotents de $M(A)$. $\mathrm{GL}(A)$ agit par automorphismes intérieurs sur $\mathrm{Idem}\, A$. L'ensemble des orbites de cette action est un semi-groupe pour la loi $p \cdot q = \left(\begin{smallmatrix} p & 0 \\ 0 & q \end{smallmatrix}\right)$, qui est isomorphe au semi-groupe des modules projectifs de type fini sur A. On peut calculer K_0A par ce biais.

Invariance de Morita. Un corollaire du résultat précédent est : $K_0A = K_0M_n(A)$.

Exemples. Comme un module projectif de type fini sur un corps, un anneau principal ou un anneau local est libre, avec un rang bien défini, le premier groupe de K-théorie est dans un tel cas $\mathbf{Z}$.

Si A est un anneau de Dedekind et $\mathscr{C}\ell A$ son groupe des classes, on peut montrer que tout module projectif de type fini est de la forme $A^n \oplus I$, où I est un idéal de A, et donc :

$$KA = \mathbf{Z} \times \mathscr{C}\ell A.$$

***K_0* relatif.** Si I est un idéal bilatère de l'anneau A, posons

$$D(A, I) = \{(x, y) \in A \times A \ : \ x - y \in I\}.$$

On a une suite exacte $0 \longrightarrow I \longrightarrow D(A,I) \longrightarrow A \longrightarrow 0$. On définit alors :

$$K_0(A,I) = \mathrm{Ker}(\mathrm{pr}_{1*} : K_0 D(A,I) \longrightarrow K_0 A).$$

Théorème. On a une suite exacte :

$$K_0(A,I) \xrightarrow{\mathrm{pr}_{1*}} K_0 A \xrightarrow{q_*} K_0(A/I).$$

Excision. Si I est un anneau non nécessairement unitaire, notons I_+ l'anneau $= I \oplus \mathbf{Z}$ où la multiplication est donnée par $(x,n)\cdot(y,m) = (xy+ny+mx, mn)$: c'est un anneau unitaire. Posons $K_0 I = \mathrm{Ker}(K_0 I_+ \longrightarrow K_0\mathbf{Z})$. Si I était déjà unitaire, cela coïncide avec la définition antérieure. Le théorème d'excision dit que $K_0(A,I) = K_0 I$, *i.e.*, la K-théorie relative ne dépend pas de l'anneau mais uniquement de l'idéal.

***K*-théorie topologique et théorème de Swann.** Un *fibré vectoriel* sur un espace topologique X (que nous supposerons compact) est une application continue $\pi : E \longrightarrow X$ telle que tout $x \in X$ possède un voisinage ouvert U, avec des isomorphismes $\varphi_U : \pi^{-1}U \simeq U \times \mathbf{R}^n$. Cela permet de munir les fibres $\pi^{-1}(\{x\})$ d'une structure d'espace vectoriel — on demande que cette structure ne dépende pas du choix de U, *i.e.*, que les $\varphi_U \circ \varphi_V^{-1}$ soient linéaires sur les fibres :

$$\begin{tikzcd} (U\cap V)\times\mathbf{R}^n \arrow[dr] & \pi^{-1}(U\cap V) \arrow[l, "\varphi_V"'] \arrow[r, "\varphi_U"] \arrow[d] & (U\cap V)\times\mathbf{R}^n \arrow[dl] \\ & U\cap V. & \end{tikzcd}$$

Un *morphisme de fibrés vectoriels* est une application continue entre les espaces totaux $E \longrightarrow F$ commutant aux projections

$$\begin{tikzcd} E \arrow[rr] \arrow[dr] & & F \arrow[dl] \\ & X. & \end{tikzcd}$$

On définit $K^0 X$ comme le groupe de Grothendieck des classes d'isomorphie de fibrés vectoriels sur X. C'est le premier groupe de K-théorie topologique.

Théorème de Swann. Soit X un espace compact. On a un isomorphisme $K^0 X \simeq K_0 \mathscr{C}(X)$.

Périodicité de Bott. On définit alors la K-théorie (à support compact) d'un espace topologique non nécessairement compact X : $K^0_c X := K_0 \mathscr{C}_c(X)$ (attention, on prend les fonctions continues à support compact), puis la K-théorie négative,

$$K^{-i} X = K^0_c(X \times \mathbf{R}^i) = K_0 \mathscr{C}_c(X \times \mathbf{R}^i),$$

qui s'avère être périodique : $K^{n+8}X \simeq K^n X$ (la période est égale à 2 dans le cas complexe). En prolongeant par périodicité, on obtient la K-théorie positive.

Démonstration : Si E est un fibré vectoriel, l'espace de ses sections

$$\Gamma(X,E) = \{s : X \longrightarrow E, p \circ s = \mathrm{Id}_X\}$$

est un $\mathscr{C}(X)$-module.

Montrons que c'est un module de type fini. Considérons un recouvrement trivialisant fini, les fonctions coordonnées engendrent les $\Gamma(U,E)$; en les multipliant par une partition de l'unité, on obtient des sections globales qui engendrent $\Gamma(X,E)$.

Montrons que c'est un module projectif. Soient $s_1, \ldots, s_k$ des générateurs de $\Gamma(X,E)$. Le morphisme

$$\varphi : \left\{ \begin{array}{ccc} X \times \mathbf{C}^k & \longrightarrow & E \\ (x, v_1, \ldots, v_k) & \longmapsto & \sum v_i s_i(x) \end{array} \right.$$

est surjectif sur les fibres. Posons $E' = \mathrm{Ker}\,\varphi$. Si on choisit une métrique hermitienne sur E (il suffit d'en prendre sur des ouverts trivialisants et de les recoller avec une partition de l'unité), φ possède un adjoint, injectif, $E \longrightarrow X \times \mathbf{C}^k$, d'image $(E')^\perp \simeq E$. On a donc $X \times \mathbf{C}^k \simeq E \oplus E'$, d'où

$$\Gamma(X,E) \oplus \Gamma(X,E') \simeq \Gamma(X \times \mathbf{C}^k) \simeq \mathscr{C}(X)^k.$$

Soit P un module projectif : Montrons qu'il est de cette forme. En écrivant $P \oplus Q = \mathscr{C}(X, \mathbf{C}^n)$, on peut voir les éléments de P comme des fonctions $X \longrightarrow \mathbf{C}^n$. Posons $E = \{(x, v_1, \ldots, v_n) \in X \times \mathbf{C}^n \;:\; \exists s \in P,\ s(x) = (v_1, \ldots, v_n)\}$. On laisse au lecteur le soin de vérifier que la projection sur le premier facteur $E \longrightarrow X$ est un fibré vectoriel. $\square$

Structure d'anneau. On peut vérifier que le produit tensoriel des fibrés vectoriels induit une structure d'anneau sur $K_0 A$.

K_1 des anneaux

Nous avons vu l'intérêt de l'étude de la catégorie des modules pour celle d'un anneau. Mais une catégorie est essentiellement déterminée par ses *morphismes*, or, pour construire K_0, nous nous sommes limités aux objets.

Construction concrète de K_1. Notons $E(A,n)$ le sous-groupe de $\mathrm{GL}(A)$ engendré par les matrices élémentaires, *i.e.*, ne contenant des 1 sur la diagonale et ayant au plus un autre terme non nul et posons $E(A)=\bigcup E(A,n)\subset \mathrm{GL}(A)$. Nous définissons alors K_1 comme le plus grand quotient abélien de $\mathrm{GL}(A)$:

$$K_1A=(\mathrm{GL}(A))_{\mathrm{ab}}=\mathrm{GL}(A)/E(A).$$

Démonstration : Si $e_{i,j}(a)$ sont les matrices élémentaires, $e_{ij}(a)=[e_{ik}(a),e_{kl}(1)]$, et donc $E(A)=[E(A),E(A)]\subset[\mathrm{GL}(A),\mathrm{GL}(A)]$. Si $A,B\in \mathrm{GL}(A,n)$, on a :

$$\begin{pmatrix} ABA^{-1}B^{-1} & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix} AB & 0\\ 0 & B^{-1}A^{-1}\end{pmatrix}\begin{pmatrix} A^{-1} & 0\\ 0 & A\end{pmatrix}\begin{pmatrix} B^{-1} & 0\\ 0 & B\end{pmatrix}$$

$$\begin{pmatrix} A & 0\\ 0 & A^{-1}\end{pmatrix} = \begin{pmatrix} 1 & A\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 0\\ -A^{-1} & 1\end{pmatrix}\begin{pmatrix} 1 & A\\ 0 & 1\end{pmatrix}\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}$$

$$\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix} 1 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix} 1 & -1\\ 0 & 1\end{pmatrix}$$

Or, toute matrice trigonale est dans $E(A)$. D'où $[\mathrm{GL}(A),\mathrm{GL}(A)]=E(A)$, puis

$$\mathrm{GL}(A)_{\mathrm{ab}}=\frac{\mathrm{GL}(A)}{[\mathrm{GL}(A),\mathrm{GL}(A)]}=\frac{\mathrm{GL}(A)}{E(A)}. \qquad \square$$

Exemples. Si A est un anneau commutatif, le déterminant induit une surjection $K_1A\longrightarrow A^\times$. Si A est un corps commutatif, c'est un isomorphisme. Si A est un anneau local (non nécessairement commutatif), on peut définir un déterminant non commutatif induisant un isomorphisme $K_1A\simeq A^\times_{\mathrm{ab}}$. Si A est un anneau euclidien, $K_1A=A^\times$.

K_1 relatif. Posons

$$K_1(A,I)=\mathrm{Ker}(K_1D(A,I)\longrightarrow K_1A).$$

On peut montrer que c'est isomorphe à $\mathrm{GL}(A,I)/E(A,I)$, où $\mathrm{GL}(A,I)$ est le noyau de $\mathrm{GL}\,A\longrightarrow \mathrm{GL}(A/I)$ et $E(A,I)$ est le plus petit sous-groupe normal de $\mathrm{GL}\,A$ contenant les $e_{ij}(a)$, $a\in I$. On dispose d'une suite exacte :

$$\begin{tikzcd} K_1(A,I) \arrow[r] & K_1A \arrow[r] & K_1(A/I) \arrow[d, "\partial"] \\ K_0(A/I) & K_0A \arrow[l] & K_0(A,I) \arrow[l] \end{tikzcd}$$

K_1 d'une catégorie. Soit $\mathfrak{C}$ une catégorie abélienne, nous définissons $K_0\mathfrak{C}$ comme le groupe de Grothendieck des classes d'isomorphie d'objets de $\mathfrak{C}$ et $K_1\mathfrak{C}$ comme le groupe abélien engendré par les (P,α), où P est un objet de $\mathfrak{C}$ et α un automorphisme de P modulo les relations $(P,\alpha)=(P_1,\alpha_1)+(P_2,\alpha_2)$ si

$$\begin{tikzcd} 0 \arrow[r] & P_1 \arrow[r] \arrow[d, "\alpha_1"'] & P \arrow[r] \arrow[d, "\alpha"'] & P_2 \arrow[r] \arrow[d, "\alpha_2"] & 0 \\ 0 \arrow[r] & P_1 \arrow[r] & P \arrow[r] & P_2 \arrow[r] & 0. \end{tikzcd}$$

K-théorie négative

Invariance par homotopie. La K-théorie topologique est invariante par homotopie : si $A=\mathscr{C}(X)$ et $A'=\mathscr{C}(X\times\mathbf{R})$, alors $K_0A\simeq K_0A'$. Sur le plan algébrique, comme $A[X]$ est dense dans A', on peut espérer un isomorphisme entre K_0A et $K_0A[t]$, induit par l'application

$$\left\{\begin{array}{ccc} A[t] & \longrightarrow & A\\ t & \longmapsto & 0.\end{array}\right.$$

C'est bien le cas sous certaines conditions (si A est régulier à gauche). Dans le même ordre d'idées, $A[t,t^{-1}]$ est dense dans $\mathscr{C}(X\times\mathbf{S}^1)$. Ces deux anneaux, $A[t]$ et $A[t,t^{-1}]$ interviennet dans la construction des groupes de K-théorie négative.

K-théorie négative. On peut montrer que

$$K_0A=\mathrm{Coker}(K_1A[t]\oplus K_1A[t^{-1}]\longrightarrow K_1A[t,t^{-1}],$$

on définit donc par récurence :

$$K_{n-1}A=\mathrm{Coker}(K_nA[t]\oplus K_nA[t^{-1}]\longrightarrow K_nA[t,t^{-1}].$$

On dispose alors d'une suite exacte longue

$$\begin{tikzcd} \cdots \arrow[r] & K_0A \arrow[r] & K_0(A/I) \arrow[r] & K_{-1}I \arrow[d] \\ \cdots & K_{-2}I \arrow[l] & K_{-1}(A/I) \arrow[l] & K_{-1}A \arrow[l] \end{tikzcd}$$

Contrairement à la K-théorie topologique, ces groupes ne sont pas périodiques, il faut donc trouver autre chose pour définir la K-théorie positive.

Le K_2

K_0 classifiait les objets, *i.e.*, généralisait la théorie de la dimension ; K_1 étudiait le fait que $\mathrm{GL}(A)$ n'est pas engendré par les matrices élémentaires ; K_2 s'intéresse aux relations non triviales entre les matrices élémentaires : c'est ce que K_2A mesure.

Groupe de Steinberg. $\mathrm{St}\,A$ est le groupe engendré par les $x_{ij}(a)$, $a \in A$, modulo les relations

$$\begin{gathered} x_{ij}(a)x_{ij}(b) = x_{ij}(ab) \\ x_{ij}(a)x_{kl}(b) = e_{kl}(b)e_{ij}(a) \quad \text{si } j \neq k \text{ et } i \neq l \\ x_{ij}(a)x_{jk}(b)x_{ij}(a)^{-1}x_{jk}(b)^{-1} = e_{ik}(ab) \\ x_{ij}(a)x_{ki}(b)x_{ij}(a)^{-1}x_{ki}(b)^{-1} = x_{kj}(-ba) \end{gathered}$$

Les deux dernières s'entendent pour i, j et k différents. Comme le groupe $E(A)$ des matrices élémentaires vérifie aussi ces relations, on a un morphisme $\mathrm{St}\,A \longrightarrow E(A)$. On pose alors

$$K_2A = \mathrm{Ker}(\mathrm{St}\,A \longrightarrow E(A)).$$

Groupes de K-théorie supérieure

Nous n'aborderons pas ici la K-théorie positive : on peut construire K_nA, pour $n \geqslant 0$, comme groupes d'homotopie d'un espace topologique construit à partir de A.

Applications

Avant tout, les groupes de K-théorie sont des *invariants* : si A et B sont des anneaux isomorphes, alors K_0A et K_0B sont aussi isomorphes (mais ce n'est pas une condition suffisante d'isomorphie). En particulier, pour montrer que A et B ne sont pas isomorphes, il suffit de montrer que K_0A et K_0B ne sont pas isomorphes.

La K-théorie est aussi un outil dans certaines démonstrations (par exemple, l'existence de H-structure sur certaines sphères).

La K-théorie intervient dans la démonstration du théorème de l'indice d'Atiyah–Singer (un analogue du théorème de Riemann–Roch) qui permet de calculer l'indice d'un opérateur de Fredholm (ou d'un complexe d'opérateurs), ou les dimensions d'espaces de cohomologie.

Pour en savoir plus...

[BB85] B. Booss and B. Bleecker, *Topology and analysis : the Atiyah–Singer index formula and gauge-theoretic physics*, Springer Verlag, 1985.

[Bla86] B. Blackadar, *K-theory for operator algebras*, Springer Verlag, 1986.

[Kar78] M. Karoubi, *K-theory : an introduction*, Springer Verlag, 1978.

[Mil71] J.W. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, 1971.

[Ros94] J. Rosenberg, *Algebraic K-theory and its applications*, Springer Verlag, 1994.

Première rencontre avec $\mathrm{PGL}_2(\mathbf{C})$

Gabriel Dos Reis

Introduction

Initialement cet article devait porter sur la géométrie hyperbolique ; au cours de la rédaction, il s'est avéré qu'il était plus raisonnable de rédiger un autre article dans lequel seraient rappelés les quelques faits classiques de géométrie inversive souvent très vite oubliés. Cet article n'est donc pas un traitement exaustif du groupe $\mathrm{PGL}_2(\mathbf{C})$. Il sert simplement de texte introductif à l'article sur la géométrie hyperbolique plane. D'ailleurs beaucoup de choses ont été volontairement passées sous silence. Afin de mettre en exergue le caractère « omniprésent » de ce groupe, deux approches, qui se complètent merveilleusement bien, sont proposées : une approche analytico-topologique et une approche algébrique. J'espère réveiller et attiser la curiosité du lecteur sur ce groupe. On aura l'occasion de l'apprécier encore plus lorsqu'on verra son intervention en géométrie hyperbolique.

La sphère de Riemann

L'ensemble $\mathbf{C}$ des nombres complexes n'est autre chose que le plan euclidien muni d'une structure de corps. Il est dommage que d'une part beaucoup d'applications extrêmement simples (par exemple, $z \mapsto 1/z$) ne soient pas définies sur $\mathbf{C}$ tout entier ; et que d'autre part ce dernier ne soit pas compact. Or tout le monde sait combien les théorèmes dits de compacité sont assez utiles, pratiques et simples de maniement. Ces désagréments luttent en faveur de l'achèvement du plan $\mathbf{C}$; ce que nous allons nous dépêcher de faire.

La projection stéréographique

On considère la sphère

$$S^2 = \{x \in \mathbf{R}^3,\ |x| = x_1^2 + x_2^2 + x_3^2 = 1\}$$

de $\mathbf{R}^3$ dans lequel est plongé $\mathbf{C}$ identifié à $\mathbf{R}^2 \times \{0\}$. Les points $\mathrm{N}(0,0,1)$ et $\mathrm{S}(0,0,-1)$ seront appelés pôle nord et pôle sud. La *projection stéréographique de pôle nord* est l'application qui à tout point $\mathrm{P}(x_1,x_2,x_3)$ de la sphère S^2 associe le point $\pi(\mathrm{P})$ intersection de la droite (NP) avec le plan $\mathbf{C}$, d'affixe z. Il est clair que π est une bijection de $S^2 \setminus \{\mathrm{N}\}$ sur $\mathbf{C}$. Un rapide calcul montre que

$$z = \pi(x_1,x_2,x_3) = \frac{x_1 + \mathrm{i}x_2}{1 - x_3}$$

et que son inverse est donnée par

$$\begin{aligned} \pi^{-1} : \mathbf{C} &\to S^2 \setminus \{\mathrm{N}\} \\ z &\mapsto \left(\frac{z+\bar z}{|z|^2+1}, \frac{-\mathrm{i}(z-\bar z)}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1} \right). \end{aligned}$$

La continuité de π et de son inverse est flagrante sur ces formules, ainsi $\pi : \mathbf{C} \to S^2 \setminus \{\mathrm{N}\}$ est un homéomorphisme. Noter que $\pi(\mathrm{P})$ quitte tout compact de $\mathbf{C}$ lorsque le point P se rapproche du pôle nord. Ceci incite à poser $\pi(\mathrm{N}) = \infty$ où ∞ est un point pris en déhors de $\mathbf{C}$. Le nouvel espace $\mathbf{C}_\infty = \mathbf{C} \cup \{\infty\}$ ainsi obtenu s'appelle la *sphère de Riemann*. Il reste à préciser sa topologie ; il n'y a pas de mystère : les ouverts de $\mathbf{C}_\infty$ sont les images des ouverts de $\mathbf{C}$ et les complémentaires des parties compactes de $\mathbf{C}$. Il est clair que la topologie de $\mathbf{C}_\infty$ est prise afin que π (étendue) soit un homéomorphisme de S^2 sur $\mathbf{C}_\infty$. D'où la proposition suivante.

Proposition. — *La sphère de Riemann $\mathbf{C}_\infty$ est compacte.*

Le but avoué dans la construction précédente est de convoler les propriétés topologico-algébriques de la sphère S^2 et du corps $\mathbf{C}$ en une unique structure. En théorie des fonctions de la variable complexe, on définit les notions de continuté, d'holomorphie, d'analyticité et de méromorphie ; les prochains paragraphes ont pour but de montrer comment ses notions se transportent sur $\mathbf{C}_\infty$ et comment certains théorèmes utiles se généralisent assez naturellement. Pour ce faire la première étape consiste à « démocratiser » la sphère de Riemann, *i.e.,* à donner le même statut à tous les points de $\mathbf{C}_\infty$.

Demi-tour dans la sphère de Riemann

Si $\mathcal{D}$ est un ouvert de $\mathbf{C}_\infty$ ne contenant pas le point ∞ alors $\mathcal{D} \subset \mathbf{C}$ et l'on peut parler de fonctions holomorphes sur $\mathcal{D}$ au sens classique du terme. Notre souhait est que le compactifié $\mathbf{C}_\infty$ soit « homogène » en un certain sens. Afin d'éliminer toute discrimination à l'égard du point ∞ on introduit l'application

$$\begin{aligned} J : \mathbf{C}_\infty &\to \mathbf{C}_\infty \\ z &\mapsto \frac{1}{z} \end{aligned}$$

application bien définie sur $\mathbf{C} \setminus \{0\}$, dont les autres valeurs sont fixées par la convention : $J(0) = \infty$ et $J(\infty) = 0$. Il n'est pas dur de voir que J est une bijection involutive continue de $\mathbf{C}_\infty$. Quelle est la signification géométrique exacte de l'application J ? Soit

P le point d'affixe $z = x + \mathrm{i}y$ et P* le point d'affixe $J(z) = (x - \mathrm{i}y)/|z|^2$. Alors le point $\mathrm{Q} = \pi^{-1}(\mathrm{P}) \in S^2$ a pour coordonnées

$$x_1 = \frac{z+\bar{z}}{|z|^2+1}, \quad x_2 = \frac{-\mathrm{i}(z-\bar{z})}{|z|^2+1}, \quad x_3 = \frac{|z|^2-1}{|z|^2+1}$$

et celles de $\mathrm{Q}^* = \pi^{-1}(\mathrm{P}^*)$ sont

$$x_1^* = \frac{(z+\bar{z})\,|z|^{-2}}{|z|^{-2}+1} = x_1,$$
$$x_2^* = \frac{-\mathrm{i}(\bar{z}-z)\,|z|^{-2}}{|z|^{-2}+1} = -x_2,$$
$$x_3^* = \frac{|z|^{-2}-1}{|z|^{-2}+1} = -x_3.$$

Ainsi donc J induit le demi-tour par rapport à l'axe passant par les points -1 et 1 dans S^2. Puisque nous avons déjà identifié S^2 à $\mathbf{C}_\infty$ nous ne ferons pas de distinction entre J et $\pi^{-1}J\pi$ comme spécifiées dans le diagramme commutatif ci-dessous.

$$\begin{tikzcd} S^2 \arrow[r, "\pi^{-1}J\pi"] \arrow[d, "\pi"'] & S^2 \arrow[d, "\pi"] \\ \mathbf{C}_\infty \arrow[r, "J"'] & \mathbf{C}_\infty \end{tikzcd}$$

Le principal intérêt de cette application est de faire faire un demi-tour à la sphère S^2 pour ramener en 0 ce qui se passe à l'infini. Elle va donc nous permettre de prolonger les notions d'analyse complexe sur S^2.

Comportement des fonctions à l'infini

Nous pouvons maintenant définir ce qu'est une fonction holomorphe, méromorphe sur $\mathbf{C}_\infty$. Si f est une application définie sur $\mathcal{D} \setminus \{\infty\}$, $\mathcal{D}$ voisinage de ∞, on dira que f est continue en ∞ si $f \circ J$ est continue en 0. De même f sera holomorphe, méromorphe en ∞ si $f \circ J$ l'est en 0. On appellera *domaine* de $\mathbf{C}_\infty$ tout ouvert non-vide connexe de $\mathbf{C}_\infty$. Le vocabulaire étant précisé, il est possible d'étendre de substanciels théorèmes sur les fonctions holomorphes.

Théorème. — ***Soit f une fonction analytique sur $\mathcal{D} \subset \mathbf{C}_\infty$, et (z_n) une suite de points de zéros de f. Si la suite (z_n) admet un point d'accumulation dans $\mathcal{D}$ alors f est identiquement nulle sur $\mathcal{D}$.***

Il est en général commode d'autoriser les fonctions définies sur la sphère à prendre la valeur ∞ : si f est méromorphe en $a \in \mathbf{C}_\infty$ pôle de f (*i.e.*, il existe un entier naturel k tel que $(z-a)^k f(z)$ soit analytique en a) alors on pose $f(a) = \infty$. Donc les pôles de f correspodent aux zéros de $J \circ f$. Une application $f : \mathbf{C}_\infty \to \mathbf{C}_\infty$ est dite méromorphe si elle l'est en tout point. Comme conséquences immédiates :

(i) si f est méromorphe sur $\mathbf{C}_\infty$ alors f est continue sur $\mathbf{C}_\infty$;
(ii) toute fonction constante sur $\mathbf{C}_\infty$, à valeur dans $\mathbf{C}$, est méromorphe ;
(iii) l'ensemble des fonctions méromorphes sur $\mathbf{C}_\infty$ est un corps.

Soit f une fonction analytique non-constante en $a \in \mathbf{C}$ avec $f(a) = c \in \mathbf{C}$, alors il exite un entier naturel $k \geqslant 1$ tel que $f^{(k)}(a) \neq 0$. Le plus petit de ces entiers k s'appelle la multiplicité de l'équation $f(z) = c$ en $z = a$ ou la multiplicité de a. Il vient

$$f(z) = \sum_{n=k}^{\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n$$

au voisinage de a avec $f^{(k)}(a) \neq 0$. Si f est méromorphe en $a \in \mathbf{C}$ pôle de multiplicité d'ordre k en a alors l'équation $f(z) = \infty$ est dite de multiplicité k. Et dans ce cas on a

$$f(z) = \sum_{n=-k}^{\infty} a_n (z-a)^n$$

près de a avec $a_{-k} \neq 0$; $\sum_{n=-k}^{-1} a_n(z-a)^n$ s'appelle la partie principale de f en a. De manière analogue lorsque $a = \infty$ on dira que $f(\infty) = c$ est de multiplicité k si $f \circ J(0) = c$ est de mulitplicité k. Un point a sera dit point simple de f si la multiplicité de $f(z) = f(a)$ est 1 , et point multiple sinon.

Corollaire. — *Une fonction méromorphe non-constante de $\mathbf{C}_\infty$ dans lui même prend n'importe quelle valeur de $\mathbf{C}_\infty$ au plus un nombre fini de fois.*

La description des fonctions méromorphes sur $\mathbf{C}_\infty$ est assez simple comme en témoigne ce lemme, conséquence du théorème de Liouville.

Lemme. — *Les fonctions constantes sont les seules fonctions holomorphes sur la sphère de Riemann.*

Théorème. — ***Deux fonctions méromorphes sur $\mathbf{C}_\infty$ ayant mêmes parties principales en ces pôles diffèrent d'une constante additive.***

Il en existe, naturellement, une version multiplicative.

Théorème. — ***Deux fonctions méromorphes sur $\mathbf{C}_\infty$ ayant mêmes zéros, mêmes pôles avec les mêmes ordres de multiplicité diffèrent d'une constante multiplicative.***

Une *fonction rationnelle* sur $\mathbf{C}$ est une fonction de la forme $f = p/q$ où p et q sont des polynômes, avec q différent du polynôme nul. Dans ce cas f est parfaitement définie sur $\mathbf{C} \setminus q^{-1}(0)$. Lorsque $q(z) = 0$ ou $z = \infty$, on pose $f(z) = \lim_{z' \to z} f(z')$. Ce qui étend f en une fonction définie sur et à valeurs dans $\mathbf{C}_\infty$. Les fonctions rationnelles forment un corps $\mathbf{C}(X)$ que l'on peut voir comme extention algébrique de $\mathbf{C}$ grâce à l'injection

$$\begin{aligned} \mathbf{C} &\rightarrowtail \mathbf{C}(z) \\ a &\mapsto f_a : z \mapsto a \end{aligned}$$

Le théorème fondamental de l'Algèbre assure que toute fonction rationnelle peut être mise sous la forme

$$f(z) = c\frac{(z-\alpha_1)^{m_1}\cdots(z-\alpha_r)^{m_r}}{(z-\beta_1)^{n_1}\cdots(z-\beta_s)^{n_s}}$$

où $\alpha_1, \ldots, \alpha_r$ sont distincts des $\beta_1, \ldots, \beta_s$. Les $\alpha_1 \ldots, \alpha_r$ sont les zéros de f d'ordre $m_1, \ldots, m_r$ et les $\beta_1, \ldots, \beta_s$ les pôles de f d'ordre $n_1, \ldots, n_s$. Le point ∞ est un zéro ou un pôle de f si $(m_1 + \cdots + m_r) - (n_1 + \cdots + n_s)$ est strictement négatif ou strictement positif. Par exemple la fonction $f(z) = (z-1)/(z^2+4)$ admet $1, \infty$ comme zéros d'ordres 1 et $\pm 2i$ comme pôles d'ordre 1. Il est remarquable que cette définition algébrique des fonctions rationnelles soit équivalente à une condition analytique.

Théorème. — ***Une fonction de $\mathbf{C}_\infty$ dans elle-même est rationnelle si et seulement si elle est méromorphe.***

Ce théorème est une manifestation des liens profonds du mariage algèbre–topologie sur la sphère S^2. Si p/q est une représentation irréductible de f (p et q premiers entre eux), on définit le degré de f comme étant le maximum du degré de p et du degré de q. Le théorème fondamental se généralise aussitôt.

Théorème. — ***Si $f : \mathbf{C}_\infty \to \mathbf{C}_\infty$ est méromorphe de degré $d > 0$ alors f prend toute valeur $c \in \mathbf{C}_\infty$ exactement d fois, les ordres de multiplicité étant comptés.***

Les transformations de Moebius

Structure du groupe

On appelle automorphisme de la sphère de Riemann, toute bijection méromorphe $T : \mathbf{C}_\infty \to \mathbf{C}_\infty$. L'ensemble des automorphismes de $\mathbf{C}_\infty$ sera noté $\mathrm{Aut}(\mathbf{C}_\infty)$. Les théorèmes de la section précédente permettent de préciser la forme des automorphismes de $\mathbf{C}_\infty$.

Théorème. — ***Les automorphismes de $\mathbf{C}_\infty$ sont les homographies***

$$T(z) = \frac{az+b}{cz+d} \qquad (a, b, c, d \in \mathbf{C},\ ad - bc \neq 0).$$

En effet, on sait que les applications méromorphes de la sphère $\mathbf{C}_\infty$ sont les fonctions rationnelles, et puisque l'on requiert des bijections il s'ensuit que ces fonctions rationnelles sont nécessairement de degré 1, donc des homographies.

Les applications de la forme

$$T(z) = \frac{az+b}{cz+d}$$

sont connues sous le nom de transformations de Moebius. Elles forment un groupe, et de part leur définition le fait suivant est immédiat.

Corollaire. — $\mathrm{Aut}(\mathbf{C}_\infty)$ *est un groupe d'homéomorphismes de* $\mathbf{C}_\infty$*.*

Il y a une approche beaucoup plus conceptuelle des transformations de Moebius qui consiste à les regarder comme une action de groupe

$$\theta : \mathrm{GL}_2(\mathbf{C}) \to \mathrm{Aut}(\mathbf{C}_\infty)$$

qui à toute matrice

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

associe la transformation

$$T(z) = \frac{az+b}{cz+d}.$$

Le théorème précédent affirme que θ est un épimorphisme ; d'autre part il est clair que son noyau est réduit à $K = \mathrm{Ker}\,\theta = \{\lambda I,\ \lambda \in \mathbf{C}^*\}$. Ceci fournit l'isomorphisme

$$\mathrm{Aut}(\mathbf{C}_\infty) \cong \mathrm{GL}_2(\mathbf{C})/K = \mathrm{PGL}_2(\mathbf{C}).$$

L'épimorphisme $\det : \mathrm{GL}_2(\mathbf{C}) \twoheadrightarrow \mathbf{C}^*$ de noyau $\mathrm{SL}_2(\mathbf{C})$ donne lieu à l'isomorphisme

$$\mathrm{GL}_2(\mathbf{C})/\mathrm{SL}_2(\mathbf{C}) \cong \mathbf{C}^*.$$

Puisque tout nombre complexe admettant au moins une racine carrée, il vient que tout tableau $N \in \mathrm{GL}_2(\mathbf{C})$ peut s'écrire sous la forme λM où λ est une racine carrée de $\det N$ et M est un élément de $\mathrm{SL}_2(\mathbf{C})$; et comme $\theta(N) = \theta(M)$, il vient que tout automorphisme de $\mathbf{C}_\infty$ est de la forme

$$T(z) = \frac{az+b}{cz+d}; \qquad ad - bc = 1,$$

en d'autres termes $\mathrm{SL}_2(\mathbf{C}) \overset{\theta}{\twoheadrightarrow} \mathrm{Aut}(\mathbf{C}_\infty)$. Donc $\mathrm{PGL}_2(\mathbf{C})$ coincide avec $\mathrm{PSL}_2(\mathbf{C})$ image de $\mathrm{SL}_2(\mathbf{C})$ par projectification.

Théorème. — $\mathrm{Aut}(\mathbf{C}_\infty) \cong \mathrm{PGL}_2(\mathbf{C}) = \mathrm{PSL}_2(\mathbf{C})$.

Nous identifierons donc $\mathrm{Aut}(\mathbf{C}_\infty)$ avec $\mathrm{PGL}_2(\mathbf{C})$. Il est intéressant de considérer certaines transformations de Moebius assez simples :

(i) les rotations d'angle θ autour de l'axe passant par 0 et ∞ dans la sphère $\mathbf{C}_\infty$: $R_\theta(z) = e^{\mathrm{i}\theta} z$;
(ii) le demi-tour dans $\mathbf{C}_\infty$ autour de l'axe passant par -1 et 1 : $J(z) = 1/z$;
(iii) les similitudes $S_r(z) = rz$ ($r \in \mathbf{R}$, $r > 0$) qui fixent 0 et le point ∞ ;
(iv) les extensions des translations du plan $T_t(z) = z + t$, ($t \in \mathbf{C}$) qui fixe le point ∞.

En réalité ces transformations suffisent à engendrer le groupe des transformations de Moebius : en effet si $c = 0$ alors $T(z) = (az+b)/d$ avec a et d non nuls et en posant $a/d = re^{\mathrm{i}\theta}$ et $b/d = t$ on a $T(z) = re^{\mathrm{i}\theta} + t$ ou $T = T_t \circ S_r \circ R_\theta$; si c est non nul alors

$$\begin{aligned} T(z) &= \frac{a}{c} - \frac{1}{c(cz+d)} \\ &= (T_t \circ J)(-c^2 z - cd) \end{aligned}$$

et l'on est ramené au cas précédent.

Le corps $\mathbf{C}$ admet deux automorphismes continus (l'identité et la conjugaison), il peut être commode de considérer les transformations obtenues en composant la conjugaison par un automorphisme de $\mathbf{C}_\infty$: ces transformations s'appellent les anti-automorphismes de $\mathbf{C}_\infty$. La composition de deux anti-automorphismes est un automorphisme et la composition d'un automorphisme et d'un anti-automorphisme est un anti-automorphisme. Ainsi l'ensemble des automorphisme et des anti-automorphismes de $\mathbf{C}_\infty$ est un groupe noté $\overline{\mathrm{Aut}}(\mathbf{C}_\infty) = \overline{\mathrm{PGL}_2}(\mathbf{C})$. Les automorphismes conservent les angles alors que les anti-automorphismes les renversent.

Cercles sur la sphère de Riemann

Un cercle dans la sphère $S^2 \subset \mathbf{R}^3$ est l'intersection d'un plan Π avec la sphère S^2. Toujours dans le souci de transférer les propriétés algébrico-topologiques de S^2 à $\mathbf{C}_\infty$, on définit un cercle de la sphère de Riemann comme étant l'image stéréographique d'un cercle de S^2. Si donc $C = S^2 \cap \Pi$ avec Π défini par :

$$\alpha x_1 + \beta x_2 + \gamma x_3 = \delta \qquad (\alpha, \beta, \gamma, \delta \in \mathbf{R}),$$

alors on voit après projection stéréographique que C est défini par

$$2\alpha x + 2\beta y + \gamma(|z|^2 - 1) = \delta(|z|^2 + 1), \qquad z = x + \mathrm{i}y.$$

Cette équation peut se mettre sous la forme

$$az\bar{z} + \bar{b}z + b\bar{z} + c = 0 \qquad a, c \in \mathbf{R},\ b \in \mathbf{C}.$$

Ceci définit un cercle du plan à condition que $S^2 \cap \Pi \neq \varnothing$ *i.e.,* $\alpha^2 + \beta^2 + \gamma^2 > \delta^2$, ce qui en termes de a, b, et c se traduit par $|b|^2 > ac$. Réciproquement, on peut s'assurer que si cette condition est vérifiée alors l'équation ci-dessus permet de définir un cercle sur $\mathbf{C}_\infty$. Si $a \neq 0$ alors on obtient un vrai cercle dans le plan $\mathbf{C}$; sinon on obtient une droite : ce cas correspond aux cercles de $\mathbf{C}_\infty$ passant par le point ∞ ou de manière équivalente aux cercles de S^2 contenant le pôle nord $\mathrm{N}(0,0,1)$. En conclusion les cercles de $\mathbf{C}_\infty$ sont de deux types : les cercles du plan $\mathbf{C}$ au sens usuel, et les droites auquel on a adjoint le point ∞. Le comportement des automorphismes de $\mathbf{C}_\infty$ vis-à-vis des cercles de $\mathbf{C}_\infty$ est assez sympathique.

Théorème. — ***Le groupe des automorphismes*** $\mathrm{PGL}_2(\mathbf{C})$ ***de*** $\mathbf{C}_\infty$ ***préserve l'ensemble des cercles de*** $\mathbf{C}_\infty$.

En effet il n'est pas dur de voir que les rotations R_θ, le demi-tour J, les similitudes S_r et les translations T_t envoient les cercles de $\mathbf{C}_\infty$ sur les cercles de $\mathbf{C}_\infty$ (géométriquement ou par un calcul immédiat), or ces transformations engendrent $\mathrm{PGL}_2(\mathbf{C})$ d'où l'assertion.

Le cercle en long, en large et à travers

Transitivité du groupe $\mathrm{PGL}_2(\mathbf{C})$ et birapport

On dit qu'une action d'un groupe G sur un ensemble Ω est transitive si pour tous a et β de Ω il existe $g \in G$ qui amène de α à β : $g(\alpha) = \beta$. Plus généralement on dit que G agit k-transitivement sur Ω si chaque fois que $(\alpha_1, \ldots, \alpha_k)$ et $(\beta_1, \ldots, \beta_k)$ sont des k-uplets d'éléments distincts de Ω on peut trouver une transformation $g \in G$ telle que $g(\alpha_s) = \beta_s$ pout tout $s = 1, 2, \ldots, k$. Il est clair que la k-transitivité implique la $(k-1)$-transitivité pour tout $k \geqslant 2$ et que la 1-transitivité est la transitivité usuelle.

Théorème. — ***Si (z_1, z_2, z_3) et (w_1, w_2, w_3) sont des triplets de points distincts de $\mathbf{C}_\infty$, alors il existe une unique transformation $T \in \mathrm{PGL}_2(\mathbf{C})$ telle que $T(z_j) = w_j$, $j = 1, 2, 3$.***

Démonstration : Il suffit, pour cela, de montrer que si z_1, z_2 et z_3 sont trois points distincts de $\mathbf{C}_\infty$ il existe un unique automorphisme de $\mathbf{C}_\infty$ qui les envoie sur 0, 1, ∞. Supposons dans un premier temps que les z_j soient tous différents de ∞, soit

$$T(z) = \frac{(z - z_1)(z_2 - z_3)}{(z_1 - z_2)(z_3 - z)}.$$

Alors T envoie bien z_1, z_2, z_3 respectivement sur 0, 1, ∞, et T est une homographie non-dégénérée donc $T \in \mathrm{PGL}_2(\mathbf{C})$. Si maintenant l'un des z_j est ∞ il suffit de prendre la limite du rapport précédent : si $z_1 = \infty$ alors $T(z) = -(z_2 - z_3)/(z_3 - z)$; si $z_2 = \infty$ alors $T(z) = -(z - z_1)/(z_3 - z)$; enfin si $z_3 = \infty$ alors $T(z) = -(z - z_1)/(z_1 - z_2)$. Dans chaque cas T est bien un élément de $\mathrm{PGL}_2(\mathbf{C})$ et envoie z_1, z_2, z_3 sur $0, 1, \infty$. Pour voir l'unicité d'une telle transformation il suffit de remarquer que si U est une autre transformation de Moebius ayant les mêmes effets sur z_1, z_2 et z_3 alors UT^{-1} fixe les trois points $0, 1, \infty$. Posant $UT^{-1}(z) = (az + b)/(cz + d)$ et résolvant les équations $T(z) = z$ pour $z = 0, 1, \infty$ on trouve l'identité et donc $U = T$. Ceci achève la démonstration. □

À la lumière de ce théorème on peut se poser la question de savoir quels sont les éléments de $\mathrm{PGL}_2(\mathbf{C})$ qui laissent globalement invariante une partie Δ de $\mathbf{C}_\infty$ composée de 3 points. L'ensemble de telles transformations est un sous-groupe,

$$S(\Delta) = \{T \in \mathrm{PGL}_2(\mathbf{C}) \mid T(\Delta) = \Delta\} \leqslant \mathrm{PGL}_2(\mathbf{C}).$$

Si $\Theta = \{0, 1, \infty\}$ alors $S(\Delta) = U^{-1}S(\Theta)U$ où $U \in \mathrm{PGL}_2(\mathbf{C})$ est choisie telle que $U(\Delta) = \Theta$. Ainsi $S(\Delta)$ est isomorphe à $S(\Theta)$, il suffit donc de déterminer $G(\Theta)$. D'après le théorème qui précède, il existe un unique élément $U \in \mathrm{PGL}_2(\mathbf{C})$ induisant une permutation τ sur Θ ; cette transformation sera notée $T = T_\tau$. Ainsi $T_\tau \mapsto \tau$ est un isomorphisme de $S(\Theta)$ sur le groupe des permutations de Θ, en d'autres termes $S(\Theta) \cong S_3$. On peut facilement vérifier que les transfomations suivantes fixent Θ :

$$T(z) = z, 1 - z, \frac{1}{z}, \frac{z}{1 - z}, \frac{1}{1 - z}, \frac{z - 1}{z}.$$

Elles sont donc éléments de $S(\Theta)$ et correspondent aux permutations

$$\tau = (0)(1)(\infty),\ (0\infty)(1),\ (0)(1\infty),\ (01\infty),\ (0\infty1).$$

Corollaire. — *Tout automorphisme de $\mathbf{C}_\infty$ autre que l'identité admet au plus deux points fixes distincts.*

Comme conséquence de ce corollaire : l'action de $\mathrm{PGL}_2(\mathbf{C})$ est 3-transitive mais pas 4-transitive sur $\mathbf{C}_\infty$. On peut néanmoins chercher les conditions sous lesquelles deux tétra-uplets sont équivalents sous l'action de $\mathrm{PGL}_2(\mathbf{C})$. Pour ce faire on introduit une notion assez utile : le *birapport*. Si (z_0, z_1, z_2, z_3) est un 4-uplets de points distincts de $\mathbf{C}_\infty$, alors on définit le birapport $\lambda = (z_0, z_1; z_2, z_3)$ comme étant la valeur en z_0 de l'unique élément de $\mathrm{PGL}_2(\mathbf{C})$ qui envoie z_1, z_2, z_3 sur $0, 1, \infty$. Ainsi

$$\lambda = \frac{(z_0 - z_1)(z_2 - z_3)}{(z_1 - z_2)(z_3 - z_0)}$$

avec la convention habituelle de prendre la limite du rapport si l'un des points considérés est ∞.

Théorème. — ***Soient (z_0, z_1, z_2, z_3) et (w_0, w_1, w_2, w_3) deux tétra-uplets de points distincts de $\mathbf{C}_\infty$. Pour qu'il existe une transformation de Moebius $T \in \mathrm{PGL}_2(\mathbf{C})$ vérifiant $T(z_j) = w_j$,($j = 0, 1, 2, 3$), il faut et il suffit que $(z_0, z_1; z_2, z_3) = (w_0, w_1; w_2, w_3)$.***

Démonstration : Supposons que l'on ait : $T(z_j) = w_j$ $(j = 0, 1, 2, 3)$. Soit U l'unique élément de $\mathrm{PGL}_2(\mathbf{C})$ envoyant w_1, w_2, w_3 sur $0, 1, \infty$ tel que $U(z_0) = (w_0, w_1; w_2, w_3)$. Alors UT est l'unique élément de $\mathrm{PGL}_2(\mathbf{C})$ qui envoie z_1, z_2, z_3 sur $0, 1, \infty$ et

$$(z_0, z_1; z_2, z_3) = UT(z_0) = U(w_0) = (w_0, w_1; w_2, w_3).$$

Réciproquement si $(z_0, z_1; z_2, z_3) = \lambda = (w_0, w_1; w_2, w_3)$ alors il existe $U, V \in \mathrm{PGL}_2(\mathbf{C})$ avec $U(w_j) = V(z_j) = \lambda, 0, 1, \infty$ pour $j = 0, 1, 2, 3$. Donc $U^{-1}V(z_j) = w_j$ donc $T = U^{-1}V$ convient. □

Birapports et cercles

Trois points distincts de S^2 déterminent de manière unique un plan Π de $\mathbf{R}^3$ donc par projection un cercle $C = \pi(S^2 \cap \Pi)$ dans $\mathbf{C}_\infty$. La 3-transitivité de $\mathrm{PGL}_2(\mathbf{C})$ sur $\mathbf{C}_\infty$ implique :

Théorème. — $\mathrm{PGL}_2(\mathbf{C})$ ***agit transitivement sur l'ensemble des cercles de la sphère de Riemann $\mathbf{C}_\infty$.***

Soient z_1, z_2, z_3 trois points distincts de $\mathbf{C}_\infty$ alors le birapport $\lambda = (z, z_1; z_2, z_3)$ est défini pour tout z différent de z_j $(j = 1, 2, 3)$; on peut étendre son dommaine de définition à $\mathbf{C}_\infty$ tout entier en prenant la limite lorsque $z = z_j$:

$$\lambda = (z_j, z_1; z_2, z_3) = \lim_{z \to z_j} (z, z_1; z_2, z_3).$$

Ainsi le birapport prend également les valeurs $0, 1, \infty$. Le théorème suivant donne une caractérisation simple des cercles de $\mathbf{C}_\infty$.

Théorème. — ***Le cercle** C **de** $\mathbf{C}_\infty$ **passant par les trois points distincts** z_1, z_2, z_3 **est exactement l'ensemble des points** z **de** $\mathbf{C}_\infty$ **pour lesquels le birapport** $(z, z_1; z_2, z_3)$ **est dans** $\mathbf{R} \cup \{\infty\}$.*

Démonstration : Soit $T \in \mathrm{PGL}_2(\mathbf{C})$ tel que $T(z_j) = 0, 1, \infty$ pour $j = 1, 2, 3$; alors $T(z) = (z, z_1; z_2, z_3)$; $z \in C$ si et seulement si $(z, z_1; z_2, z_3) \in T(C)$ mais $T(C)$ est le cercle passant par $0, 1, \infty$ donc $T(C) = \mathbf{R} \cup \{\infty\}$. Ceci achève la preuve. $\square$

Ce théroème, traduit en termes moins prétentieux, dit que les quatres points z, z_1, z_2, z_3 sont cocycliques si et seulement si les angles définis par les veteurs $z - z_1$ et $z - z_3$ d'une part et les vecteurs $z_2 - z_1$ et $z_2 - z_3$ d'autre part diffèrent d'un multiple de π : fait qui nous est familier depuis les classes de première–terminale.

Cercle et inversion

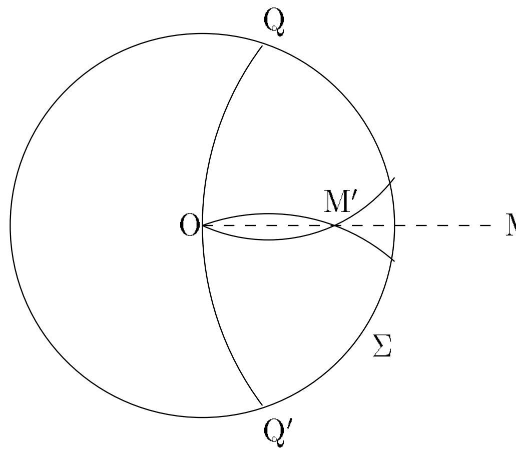
Soit C le cercle de $\mathbf{C}_\infty$ défini par l'équation

$$az\bar{z} + \bar{b}z + b\bar{z} + c = 0 \quad a, c \in \mathbf{R}, b \in \mathbf{C}, |b|^2 > ac.$$

Si $a \neq 0$ alors C est un cercle de $\mathbf{C}$ au sens usuel et l'on peut définir une transformation I_C appelée *inversion* ou *réflection* à travers le cercle C comme suit : soient p et r le centre et le rayon du cercle C , alors pour tout $z \in C$ il existe un unique $w \in C$ sur la droite passant par p et z tel que

$$\overline{pz} \cdot \overline{pw} = r^2,$$

où $\overline{pz}$ désigne la mesure algébrique du segment pz. On pose $I_C(z) = w$ appelé le *conjugué* ou l'*inverse* de z à travers C. On constate que $w \to \infty$ lorsque $z \to p$, ce qui permet d'étendre I_C en une transformation de $\mathbf{C}_\infty$ en définissant $I_C(p) = \infty$ et $I_C(\infty) = p$. Ainsi I_C est une involution de $\mathbf{C}_\infty$ et les seuls points fixes de I_C sont les points du cercle C.



Construction de l'inverse d'un point
à travers le cercle Σ.

Un calcul routinier montre que

$$\begin{aligned} w &= I_C(z) \\ &= p + \frac{r^2}{\bar{z} - \bar{p}} \\ &= -\frac{b\bar{z} + c}{a\bar{z} + \bar{b}} \qquad \text{avec } p = -\frac{b}{a},\ r^2 = \frac{b\bar{b} - ac}{a^2}. \quad (*) \end{aligned}$$

Cette équation est encore valable pour $z = p, \infty$, et donc pour tout $z \in \mathbf{C}_\infty$, ce qui montre que I_C est un anti-automorphisme de $\mathbf{C}_\infty$, *i.e.*, $I_C \in \overline{\mathrm{PGL}_2}(\mathbf{C})$.

Si $a = 0$ alors $C \setminus \{\infty\}$ est une droite euclidienne d'équation

$$\bar{b}z + b\bar{z} + c = 0$$

et l'on utilise (*) pour définir la transformation

$$w = I_C(z) = -\frac{b\bar{z} + c}{\bar{b}}$$

de $\mathbf{C}_\infty$. Il est clair que I_C est dans ce cas la réflection euclidienne à travers la droite $C \setminus \{\infty\}$. En particulier si $C = \mathbf{R} \cup \{\infty\}$ alors I_C n'est autre chose que la conjugaison usuelle.

En conclusion la transformation définie par (*) est une inversion à travers C si C est un cercle de $\mathbf{C}$ et une réflection euclidienne à travers $C \setminus \{\infty\}$ si c'est une droite de $\mathbf{C}$. On sait que si C est un cercle de $\mathbf{C}_\infty$ alors pour tout $T \in \mathrm{PGL}_2(\mathbf{C})$, $T(C)$ est un cercle C' de $\mathbf{C}_\infty$, le lemme suivant précise le comportement des inversions dans ce cas :

Lemme. — $I_{C'} = T I_C T^{-1}$.

Démonstration : Si $z \in C'$ alors $I_{C'}(z) = z$; de plus puisque $T^{-1}(z) \in C$, on a $I_C T^{-1}(z) = T^{-1}(z)$. Donc si $S = TI_CT^{-1}I_{C'}$ alors $S(z) = z$ pour tout $z \in C'$, donc C' est invariant par S automorphisme de $\mathbf{C}_\infty$ (la composée de deux anti-automorphisme est un automorphisme), *i.e.*, $S \in \mathrm{PGL}_2(\mathbf{C})$. Comme S laisse invariant le cercle C', il fixe au moins trois points de $\mathbf{C}_\infty$, donc S est l'identité, d'où le résultat. $\square$

On déduit de ce lemme que tout élément T de $\mathrm{PGL}_2(\mathbf{C})$ envoie les paires de points conjugués par rapport à C sur des paires de points conjugués par rapport à C'.

Théorème. — ***Soient*** $T \in \mathrm{PGL}_2(\mathbf{C})$ ***et*** C, $C' = T(C)$ ***deux cercles de*** $\mathbf{C}_\infty$. ***Alors si*** $w = I_C(z)$ ***alors*** $T(w) = I_{C'}(T(z))$.

Démonstration : Si $w = I_C(z)$ alors $I_{C'}(T(z)) = TI_CT^{-1}T(z) = TI_C(z) = T(w)$. $\square$

Pour clôturer ce paragraphe, nous allons déterminer les stabilisateurs d'un cercle et d'un disque dans $\mathbf{C}_\infty$. Plus généralement lorsque X est une partie de $\mathbf{C}_\infty$, l'ensemble des éléments de $\mathrm{PGL}_2(\mathbf{C})$ qui laissent globalement invariante X est un sous groupe de $\mathrm{PGL}_2(\mathbf{C})$ appelé sous-groupe stabilisateur de X, que nous noterons $S(X)$. Nous avons déjà considéré le cas où X est un triplet ou un quadruplet. Avant d'aller plus loin, un peu de vocabulaire. On appelle *disque de* $\mathbf{C}_\infty$ tout domaine $\mathbf{C}_\infty$ de frontière un cercle de $\mathbf{C}_\infty$: un disque ou un demi-plan ouvert de $\mathbf{C}$, ou une partie de la forme $E \cup \{\infty\}$, avec E complémentaire d'un disque fermé de $\mathbf{C}$. Grâce à la transitivité de $\mathrm{PGL}_2(\mathbf{C})$ sur l'ensemble des cercle de $\mathbf{C}_\infty$, il suffit de chercher le stabilisateur du cercle $\widehat{\mathbf{R}} = \mathbf{R} \cup \{\infty\}$, les autres lui étant isomorphes par conjugaison par un élément de $\mathrm{PGL}_2(\mathbf{C})$, *i.e.*, pour tout cerle C de $\mathbf{C}_\infty$, il existe $T \in \mathrm{PGL}_2(\mathbf{C})$ tel que $T(\widehat{\mathbf{R}}) = C$, et $S(C) = T^{-1}S(\widehat{\mathbf{R}})T$. Puisque la transformation T est un homéomorphisme, il applique chacun des deux disques bordés par $\widehat{\mathbf{R}}$ sur l'un des disques $\mathcal{U} = \{z \in \mathbf{C},\ \mathrm{Im}(z) > 0\}$ et $\mathcal{L} = \{z \in \mathbf{C},\ \mathrm{Im}(z) < 0\}$. Quitte à considérer une composition par le demi-tour $J : z \mapsto 1/z$, qui échange ces deux disques, tout disque de $\mathbf{C}_\infty$ peut être envoyé par une transformation de Moebius sur le demi-plan supérieur $\mathcal{U} = \{z \in \mathbf{C},\ \mathrm{Im}(z) > 0\}$. Nous somme ainsi ramenés à déterminer $S(\widehat{\mathbf{R}})$ et $S(\mathcal{U})$.

Théorème. — ***Les stabilisateurs recherchés sont***

(i) $S(\widehat{\mathbf{R}}) = \mathrm{PGL}_2(\mathbf{R})$ *;*
(ii) $S(\mathcal{U}) = \mathrm{PSL}_2(\mathbf{R})$.

Démonstration :

(i) L'inversion à travers le cercle $\widehat{\mathbf{R}}$ n'est autre chose que la conjugaison complexe. D'après un théorème précédent on a :

$$\forall z \in \mathbf{C}_\infty \quad \forall T \in \mathrm{PGL}_2(\mathbf{C}) \quad T(\bar{z}) = \overline{T(z)}.$$

D'où l'on conclut que les coefficients a, b, c et d des éléments de $S(\widehat{\mathbf{R}})$, sont réels : $S(\widehat{\mathbf{R}}) \leqslant \mathrm{PGL}_2(\widehat{\mathbf{R}})$. L'autre inclusion est triviale.

(ii) L'inclusion $S(\mathcal{U}) \leqslant \mathrm{PGL}_2(\widehat{\mathbf{R}})$ est évidente car tout homéomorphisme de $\mathcal{U}$ fixe le bord. Soit $T \in \mathrm{PGL}_2(\widehat{\mathbf{R}})$,

$$T(z) = \frac{az+b}{cz+d} \quad a, b, c, d \in \mathbf{R} \quad ad - bc = \pm 1,$$

$$T(z) = \frac{ac\,|z|^2 + adz + bc\bar{z} + bd}{|cz+d|^2}$$

donc

$$\mathrm{Im}\, T(z) = \frac{ad - bc}{|cz+d|^2}\, \mathrm{Im}\, z.$$

On en conclut que $ad - bc = 1$. Ceci établit l'égalité annoncée. $\square$

Nous suspendons pour le moment l'étude des propriétés algébriques de $\mathrm{PGL}_2(\mathbf{C})$ qui sera reprise plus loin. Tournons-nous quelques instants vers ses propriétés analytiques.

Applications conformes

Soient $\mathcal{M}_1$ et $\mathcal{M}_2$ deux surfaces (munies de métriques). Une application $f : \mathcal{M}_1 \to \mathcal{M}_2$ est dite conforme si elle préserve les angles : si γ_1 et γ_2 sont deux courbes tracées sur $\mathcal{M}_1$ et $\mathcal{M}_2$ se rencontrant en P, formant un angle θ, alors $f(\gamma_1)$ et $f(\gamma_2)$ se rencontrent en $f(\mathrm{P})$ et forment le même angle θ en ce point. L'apllication f sera dite une isométrie si elle conserve les distances ; remarquer qu'une isométrie est conforme car les angles peuvent s'exprimer à l'aide des distances. Qu'en est-il des applications que nous avons rencontrées jusqu'à présent ?

Théorème. — ***La projection stéréographique*** $\pi^{-1} : \mathbf{C} \to S^2 \setminus \{\mathrm{N}\}$ ***est conforme.***

Démonstration : Puisque les angles sont définis par les tangentes aux courbes, il suffit de démontrer le théorème pour les droites de $\mathbf{C}$. Soient donc D_1 et D_2 deux droites concourantes faisant un angle θ en leur point d'intersection P. Alors les plans Π_j, $(j = 0, 1)$

définis par D_j et le pôle nord N déterminent des cercles C_j sur S^2. Il est clair que C_j est l'image stéréographique $\pi^{-1}(D_j \cup \{\infty\})$ du cercle $D_j \cup \{\infty\} \in \mathbf{C}_\infty$. En particulier $C_1 \cap C2 = \{\mathrm{N}, \pi^{-1}(\mathrm{P})\}$. Les droites T_1 et T_2 intersections des plans Π_1 et Π_2 avec le plan tangent à S^2 en N sont parallèles aux droites $D_j = \mathbf{C} \cap \Pi_j$, $(j = 1, 2)$, donc elles forment un angle θ en N (le même qu'en $\pi^{-1}(\mathrm{P})$). En remarquant que les droites T_j sont tangentes aux cercles C_j, il s'ensuit que l'angle entre C_1 et C_2 est θ. Ceci achève la preuve. □

Comme corollaire immédiat :

Corollaire. — *La projection stéréographique* $\pi : S^2 \setminus \{\mathrm{N}\} \to \mathbf{C}$ *est conforme.*

Démonstration : Si les deux courbes γ_1 et γ_2 se rencontrent en un point Q autre que N, sous un angle θ, alors leurs tangentes T_j font de même. On considère de nouveua les plans Π_j définis par T_j et N. Ces plans déterminent sur la sphère S^2 deux cercles C_j $(j = 1, 2)$ passant par N et Q, ces plans déterminent aussi des droites $D_j = \mathbf{C} \cap \Pi_j$ passant par $\mathrm{P} = \pi(\mathrm{Q})$. Il est clair que l'angle entre les cercles vaut θ, en raisonnant comme précédemment on prouve que les droites D_1 et D_2 se coupent sous l'angle θ en P. Ceci montre le caractère conforme de π. □

On peut définir l'angle au point ∞ entre deux courbes dans ls plan $\mathbf{C}$ comme étant l'angle au point N entre les courbes $\pi^{-1}(g_1)$ et $\pi^{-1}(\gamma_2)$; il s'ensuit que les projections stéréographisques $\pi : S^2 \to \mathbf{C}_\infty$ et $\pi^{-1}\mathbf{C}_\infty \to S^2$ sont conformes. À l'aide du demi-tour $J : z \mapsto 1/z$ on voit qu'une application sur $\mathbf{C}_\infty$ est conforme en ∞ si et seulement si $f \circ J$ l'est en 0. Lorsque l'on choisit un sens d'orientation sur les surfaces considérées, il est possible de parler d'application conforme positive ou négative, selon qu'elle conserve ou renverse l'orientation.

La conformalité des projections stéréographiques implique qu'une application $f : \mathbf{C}_\infty \to \mathbf{C}_\infty$ est conforme positive (ou négative) si et seulement si $\pi^{-1} f \pi : S^2 \to S^2$ est conforme positive (ou négative).

Théorème. — ***Tout automorphisme (respectivement anti-automorphisme) de*** $\mathbf{C}_\infty$ ***est conforme positive (respectivement négative)***

Il existe une version « réciproque » assez forte de ce théorème.

Théorème. — ***Toute application conforme positive (respectivement négative) de*** $\mathbf{C}_\infty$ ***dans lui-même est un automorphisme (respectivement anti-automorphisme) de*** $\mathbf{C}_\infty$***.***

Pour terminer cet article (assez incomplet sur certains points) nous allons montrer une autre qualité algébrique du groupe $\mathrm{PGL}_2(\mathbf{C})$

$\mathrm{PGL}_2(\mathbf{C})$ en tant que groupe de Galois

Nous avons déjà signalé que l'on pouvait regarder le corps des fractions rationnelles $\mathbf{C}(X)$ à coefficients complexes comme une extension algébrique du corps $\mathbf{C}$. Notre but dans cette partie est de préciser le groupe de Galois Γ, *i.e* l'ensemble des automorphismes de l'extension $\mathbf{C}(X)$ qui fixent $\mathbf{C}$.

On note $X : \mathbf{C}_\infty \to \mathbf{C}_\infty$, l'application identique de $\mathbf{C}_\infty$ regardée comme fonction rationnelle, et aussi comme l'indéterminée de $\mathbf{C}(X)$. Soit $\gamma \in \Gamma, g = \gamma(X)$ l'image de l'indéterminée X. Pour toute fraction rationnelle $f = \sum a_k X^k / \sum b_k X^k$, on a :

$$\begin{aligned}\gamma(f) &= \frac{\gamma(\sum a_k X^k)}{\gamma(\sum b_k X^k)} \\ &= \frac{\sum a_k \gamma(X)^k}{\sum b_k \gamma(X)^k} \\ &= \frac{\sum a_k g^k}{\sum b_k g^k}\end{aligned}$$

Ainsi $\gamma(f) = f \circ g$: l'action de γ se réduit à une composition à droite par $g = \gamma(X)$. En utilsant la surjecivité de γ et l'injectivité de X, il n'est pas dur de voir que $g = \gamma(X)$ est de degré 1, donc élément de $\mathrm{PGL}_2(\mathbf{C})$, en particulier inversible. On définit une application $\Theta : \Gamma \to$, qui à tout automorphisme $\gamma \in \Gamma$ associe l'inverse de $\gamma(X)$. Soient γ_1, $\gamma_2 \in \Gamma$ et $g_k = \gamma_k(X)$, $k = 1, 2$. On a

$$\begin{aligned}\gamma_1 \cdot \gamma_2(f) &= \gamma_1(f \circ g_2) \\ &= f \circ (g_2 \circ g_1)\end{aligned}$$

Ainsi

$$\begin{aligned}\Theta(\gamma_1 \cdot \gamma_2) &= (g_2 \circ g_1)^{-1} \\ &= g_1^{-1} \circ g_2^{-1} \\ &= \Theta(\gamma_1) \circ \Theta(\gamma_2)\end{aligned}$$

Donc Θ ainsi définie ci-haut est un homomorphisme de groupes.

Théorème. — Θ ***est un isomorphisme entre*** Γ ***et*** $\mathrm{PGL}_2(\mathbf{C})$***.***

Démonstration : Soit $\gamma \in \Gamma$ tel que $\gamma(X)$ soit l'élément neutre de $\mathrm{PGL}_2(\mathbf{C})$; comme l'action de γ sur $\mathbf{C}(X)$ se réduit à une composition à droite par $\gamma(X)$, il s'ensuit que γ est l'identité sur $\mathbf{C}(X)$. Donc Θ est un monomorphisme. Soit $h \in \mathrm{PGL}_2(\mathbf{C})$, alors $h^{-1} \in \mathrm{PGL}_2(\mathbf{C})$ et l'application $\gamma : f \mapsto f \circ h^{-1}$. Il est clair que g est un homomorphisme inversible fixant $\mathbf{C}$, *i.e.*, $g \in \Gamma$. Donc Θ est un épimorphisme. Ceci achève la démonstration. $\square$

Conclusion

A travers cette courte présentation du groupe $\mathrm{PGL}_2(\mathbf{C})$, on a pu entrevoir combien la topologie, l'analyse, l'algèbre sont liées, et plus généralement une manifestation de l'unité profonde des mathématiques. Outre le fait de nous changer de $\mathrm{O}(2)$, le groupe des isometries du plan euclidien, ce groupe est au cœur de récents résultats obtenus en géométrie. Afin de donner une taille raisonnable à l'article, il ne nous a pas été possible d'étudier certaines propriétés plus ou moins fondamentales de $\mathrm{PGL}_2(\mathbf{C})$; de toute façon, il ne s'agit que d'une première rencontre. Nous aurons l'occasion par la suite de nous revoir et nous connaître...

Pour en savoir plus...

[Gre74] Marvin Jay Greenberg, *Euclidean and non-euclidean geometries*, 2nd ed., W. H. Freeman and Company, 1974.

[JS87] Gareth A. Jones and David Singerman, *Complex function, an algebraic and geometric viewpoint*, Cambridge University Press, 1987.

[Ped79] P. Pedoe, *Circles, a mathematical view*, Dover Publications Inc., 1979.

[PK81] Gordon Matthews Paul Kelly, *The non-euclidean, hyperbolic plane*, Universitext, Springer Verlag, 1981.

[Rat94] John G. Ratcliff, *Fondations of hyperbolic manifolds*, Graduate Texts in Mathematics, Springer Verlag, 1994.

Livres

Numerical Solution of Stochastic Differential Equations Through Computer Experiments
P.E. Kloeden, E. Platen, H. Schurz
Springer Verlag, 1994

Le livre s'ouvre sur des rappels de probabilités : variable aléatoire, distribution de probabilité, moments, indépendance, espérance conditionnelle et les possibilités de simulation des principales lois par un ordinateur. Cela revient à inverser la fonction de distribution F_X, tâche souvent malaisée : on a recours à des méthodes *ad hoc*. Par exemple, si U_1 et U_2 sont des variables aléatoires indépendantes uniformément distribuées dans $[0, 1]$,

$$G_1 = \sqrt{-2 \ln U_1} \cos(2\pi U_2)$$
$$G_2 = \sqrt{-2 \ln U_1} \sin(2\pi U_2)$$

sont des gaussiennes standard, indépendantes.

L'un des problèmes de la simulation du hasard et la conception des générateurs de nombres pseudo-aléatoire : les générateurs modulaires (?) et leurs problèmes sont évoqués. On peut ensuite vérifier expérimentalement l'indépendance des variables aléatoires, leur adéquation à la loi qu'il sont sensés simuler, ou des théorèmes, par exemple la loi des grands nombres.

Les suites de variables aléatoires indexées par un intervalle de $\mathbf{R}$ constituent le cœur du livre : ils généralisent les chaînes de Markov. Un processus de Wiener est un tel processus à incréments indépendants et $W(t) - W(s) \sim N(0, t - s)$. On peut voir ça comme une fonction indexée par l'espace Ω des épreuves. Ces fonctions sont continues (presque sûrement), mais pas différentiables. On peut néanmoins les développer en une « série de Fourier » dont les coefficients sont des variables aléatoires.

Une équation différentielle stochastique est de la forme :

$$dX_t = a(t, X_t)dt + b(t, X_t)dW_t,$$

où X est l'inconnue, W est un processus de Wiener et a et b des fonctions. Nous ne chercherons pas à donner un sens à dW_t : transformons cela en une équation intégrale,

$$X_t = X_{t_0} + \int_{t_0}^t a(s, X_s)\, ds + \int_{t_0}^t b(s, X_s)\, dW_s.$$

Il reste à donner un sens à l'intégrale de droite. Notre processus X peut être vu comme une fonction

$$\Omega \longrightarrow \mathscr{C}^0([t_0, t], \mathbf{R}).$$

Fixons donc $\omega \in \Omega$. Il faut donner un sens à

$$\int_{t_0}^t b(s, X_s(\omega))\, dW_s(\omega).$$

On pense à une intégrale de Stieltjes, mais $W(\omega)$ est une fonction continue (presque) jamais à variations bornées. On peut néanmoins considérer

$$\lim_{\Delta \to 0} \sum b(s_k, X_{s_k}(\omega)) \frac{W_{s_{k+1}}(\omega) - W_{s_k}(\omega)}{s_{k+1} - s_k}.$$

Cela revient à découper l'intervalle $[t_0, t]$ en petits morceaux et à prendre la valeur de b à *gauche* de chacun de ces morceaux : c'est l'intégrale d'Ito. On aurait pu prendre le milieu : c'est l'intégrale de Stratonovitch. On peut vérifier que ça converge, que c'est bien une variable aléatoire (*i.e.*, c'est mesurable) et même une *martingale*. Une conséquence surprenante de ce choix de l'intégrale d'Ito est la suivante : lors du calcul de la différentielle de la composée de deux variables aléatoire, des dérivées d'ordre deux interviennent :

$$dg(X_t) = g'(X_t)\, dX_t + \tfrac{1}{2} g''(X_t)\, dX_t^2.$$

On peut généraliser assez simplement les méthodes d'approximation des solutions d'une équation différentielle ordinaire (Newton) au cas stochastique, mais il faut reprendre l'étude de la convergence. On peut chercher à approcher les chemins du precessus (approximation forte) ou l'espérance de fonctionnelles de ce processus (approximation faible). D'autre part, les problèmes d'instabilité numérique resurgissent.

L'ouvrage se clos par quelques applications : visualisation de systèmes dynamiques stochastique et étude de leur stabilité et de la bifurcation stochastique ; problème de filtrage (on ne connait les conditions initiales de notre équation que de manière imprécise) ; intégrales fonctionnelles en physique (Feynmann) ; simulation de phénomènes financiers.

Ce livre est pour ceux qui comprennent les choses en les faisant, ou en les faisant faire à l'ordinateur : il ne se substitue pas à un ouvrage théorique, mais en constitue un agréable compagnon. On pourra lire en parallèle le livre d'Øksendal, *Stochastic Differentoal Equations.* **V.Z.**

Geometry of the Standard Model of Elementary Particles, Andrzej Derdzinski
Springer Verlag, Lecture Notes in Physics, 1992

Le monde physique a toujours servi d'inspiration aux mathématiques. Cette remarque est rendue plus pertinente par l'avènement de la mécanique quantique, de la théorie des particules élémentaires et de la théorie quantique des champs : ces domaines s'appliquent en géométrie, en théorie des nombres, et des raisonnements physiques « heuristiques » permettent de conjecturer des résultats que l'on démontre ensuite proprement.

Mais le monde des physiciens nous est fermé : ils ne parlent pas la même langue. Ils prennent les outils mathématiques du siècle dernier, qui se ramènent toujours aux nombres et aux fonctions à valeurs numériques et tentent de les utiliser pour manipuler des objets mathématiques plus récents : fibrés, connexions, etc.

La plupart des livres de physique sont écrits dans cette langue archaïsante et approximative. J'en ai trouvé un qui échappe à cette règle.

Les particules élémentaires (photons, quarks, électrons) peuvent être décrites par un fibré vectoriel complexe sur l'*espace-temps*, muni d'une structure géométrique supplémentaire, que l'on interprète comme l'équation vérifiée par les sections correspondant à un état physique.

Certaines opérations sur ces fibrés ont une interprétation physique : le conjugué complexe d'un fibré correspond à l'antiparticule ; une somme directe de fibrés correspond à une superposition de particules, *i.e.*, une particule qui est tantôt d'un type, tantôt d'un autre ; le produit tensoriel (plus exactement, un de ses sous-fibrés) correspond à un mélange de particules, par exemple un neutron est composé de trois quarks.

Cette interprétation en termes de fibrés permet de commencer une classification de particules élémentaires. Ainsi, si le mélange de n particules identiques est décrit par $\mathrm{Sym}^n\,\eta \subset \eta^{\otimes n}$, on dit que c'est un *boson*, dans le cas de $\mathrm{Alt}^n\,\eta$, c'est un *fermion*. Il pourrait y avoir d'autres particules (*anyons*).

Il s'agissait jusqu'à présent de particules libres, *i.e.*, qui n'interagissent pas. Le cas le plus simple de particule en interaction est celui de l'électromagnétisme, régit par les équations de Maxwell qui peuvent se traduire en termes d'un fibré en droites λ et de connexions, décrivant l'état des transporteurs d'interaction. Une particule de charge kq, interagissant, est alors décrite par $\lambda^k \otimes \eta$.

Comme ces équations sont $U(1)$-invariantes : λ est en fait un $U(1)$-fibré. Les équations de Yang–Mills généralisent cela à des G-fibrés.

Les phénomènes de brisure de symétrie correspondent à une réduction de ce groupe G à un sous-groupe : par exemple la transformation d'eau en glace correspond au remplacement de $O(3)$ par un groupe fini.

On peut continuer ainsi : l'interaction forte est décrite par un $SU(3)$-fibré et l'interaction faible par un $U(2)$-fibré. C'est le *modèle standard.*

On peut ensuite tenter de regrouper les trois interactions (électromagnétique, faible et forte) : ce sont les Grandes Théories Unifiées (GUTs). Mais on ne dispose pas pour l'instant de modèle satisfaisant.

Ce livre très concis aborde en termes (presque toujours) mathématiquement corrects, et sans formalisme excessif, la théorie classique des particules élémentaires jusqu'au modèle standard – il ne traite pas la théorie quantique des champs. La Grande Unification est succinctement évoquée et d'autres théories (supersymétrie, cordes) sont passées sous silence.
V.Z.

A Primer of Algebraic D-modules
S.C. Coutinho
Cambridge University Press, 1995

Ce livre constitue une introduction à la théorie des D-modules algébriques sans le formalisme un peu lourd des faisceaux et des catégories dérivées : des méthodes algébriques se révèlent fructueuses pour résoudre des problèmes analytiques — c'est de l'« analyse algébrique ».

Un D-module est un module sur l'algèbre de Weyl : $A_n = k[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$, qui est une sous-algèbre de $\mathrm{End}_k[x_1, \ldots, x_n]$. On peut aussi la définir par générateurs et relations :

$$[x_i, x_j] = [\partial_i, \partial_j] = 0, \quad [\partial_i, x_j] = \delta_{ij}.$$

C'est un anneau intègre, simple (sans idéal bilatère non trivial). On peut voir que $(x_i^n \partial_j^m)$ est une base de l'espace vectoriel sous-jacent.

A_n est l'anneau des opérateurs différentiels de $k[x_1, \ldots, x_n]$; on peut généraliser cette construction à un anneau quelconque.

$k[x_1, \ldots, x_n]$ ou $\mathscr{H}(U)$ (fonctions holomorphes sur un ouvert U de $\mathbf{C}^n$) sont des modules sur A_n. On peut définir la dimension d'un module M de type fini sur A_n comme le degré du polynome de Hilbert de son gradué par une filtration compatible avec la filtration de A_n par le degré. C'est indépendant du choix d'une telle filtration. On peut interpréter géométriquement cette notion : c'est la dimension de la variété algébrique définie par l'idéal $\operatorname{Rad}\operatorname{Ann}_{k[z_1,\ldots,z_{2n}]}\operatorname{Gr}M$ qui est elle aussi indépendante de la filtration sur M.

La dimension d'un module est en fait comprise entre n et $2n$. Un module est dit *holonome* s'il est de dimension n. De tels modules se comportent de manière beaucoup plus simple : cette propriété est par exemple préservée par image directe et réciproque (dont nous ne détaillons pas la construction).

Donnons maintenant quelques exemples et applications. Si une fonction polynomiale $F : k^n \longrightarrow K^n$ possède une réciproque polynomiale, alors $\det J(F)$ est inversible en tout point. Réciproquement, on peut se demander si la condition $\det J(F) = 1$ suffit à assurer l'existence d'un inverse. En fait, si tout endomorphisme de A_n est un automorphisme, c'est vrai.

Considérons un système différentiel

$$P_1(F) = \cdots = P_m(f) = 0 \qquad (*)$$

où $P_i \in A_n$. On peut lui associer le A_n-module $M = A_n/(P_1, \ldots, P_m)$. L'espace vectoriel des solutions polynomiales de $(*)$ est isomorphe à

$$\operatorname{Hom}_{A_n}(M, k[x_1, \ldots, x_n]).$$

De manière plus générale, si S est l'anneau des fonctions holomorphes, des distributions, des microfonctions ou des hyperfonctions, $\operatorname{Hom}_{A_n}(M, S)$ est isomorphe à l'ensemble des solutions appartenant à la classe de fonctions (généralisées) considérée. Un unique objet, le module associé au système différentiel, permet donc d'appréhender les solutions dans des contextes très divers.

Les D-modules permettent encore d'étudier certains problèmes de stabilité des systèmes dynamiques, ou de trouver des algorithmes pour établir des équations fonctionnelles vérifiées par des fonctions spéciales. **V.Z.**