Pierre COLMEZ

ÉLÉMENTS D'ANALYSE ET D'ALGÈBRE

Pierre COLMEZ
C.M.L.S., École Polytechnique, 91128 Palaiseau Cedex, France.

ÉLÉMENTS D'ANALYSE ET D'ALGÈBRE

Pierre COLMEZ

TABLE DES MATIÈRES

VOCABULAIRE MATHÉMATIQUE

La nécessité de définir précisément les objets avec lesquels ils travaillent s'est imposée graduellement aux mathématiciens confrontés à des contradictions d'ordre presque métaphysique. L'avènement de la théorie des ensembles (à partir des travaux fondateurs de G. Cantor dont le début date des années 1870) et l'axiomatisation croissante des mathématiques ont d'une part fait disparaître un certain nombre d'obstacles psychologiques à la création d'objets nouveaux[(1)], et d'autre part débouché sur la création d'un vocabulaire extrêmement précis, qui a rendu possible l'explosion des mathématiques au cours du XX^{e} siècle.

Ce mouvement a fini par atteindre l'enseignement avec l'introduction des « maths modernes » au collège (et même en grande section de maternelle). Dans les années 70, le programme enseigné dans le secondaire et dans les classes préparatoires reposait sur le slogan : « Dieu créa l'ensemble vide et l'homme fit le reste ». C'était un peu radical, mais avait le mérite de présenter les mathématiques de manière cohérente et de montrer que l'on pouvait créer de nouveaux objets à partir d'objets déjà existants. La présentation en était malheureusement extrêmement dogmatique, et l'impression qu'on en retirait était plutôt que Dieu avait créé l'ensemble vide et la théorie des ensembles, et sur sa lancée, les entiers, les entiers relatifs, les nombres rationnels, puis les groupes, les anneaux, les corps et les espaces vectoriels, puis les nombres réels, ensuite il avait introduit des ε et des δ,

(1) Les nombres complexes ont mis près de deux siècles à être acceptés (et même les nombres négatifs ont eu leurs détracteurs ; un cas extrême est Augustus de Morgan qui continuait à les considérer, au milieu du XIX^{e}-siècle, comme dénués de tout fondement, et a passé une bonne partie de sa vie à essayer de prouver qu'on pouvait fort bien s'en passer), alors que, de nos jours, des objets nettement plus compliqués le sont dès qu'ils ont fait la preuve de leur utilité pour résoudre, ou même formuler proprement, certains problèmes ; c'est par exemple le cas de l'anneau des « nombres complexes p-adiques » construit par J.-M. Fontaine (1982). Les obstacles psychologiques n'ont toutefois pas complètement disparu ; l'apparition d'un objet nouveau ne se fait pas sans heurt, et provoque des conflits parfois brutaux entre les anciens, dont le point de vue « On a fait de très bonnes maths pendant 2000 ans sans avoir besoin de ces horreurs » reflète l'appréhension devant la perspective de devoir étudier un nouveau sujet "incompréhensible", et les modernes qui voient dans le nouvel objet la solution à tous les problèmes...

puis créé la topologie..., et quand il avait enfin été content du résultat, il avait fait don aux hommes d'une théorie immuable et parfaite, à la beauté froide et lisse.

Le dogme a changé vers le milieu des années 90, et on est reparti sur le mode : « Dieu a créé les nombres réels, puis les nombres complexes, et envoyé Gauss sur terre pour expliquer qu'il n'y avait pas besoin de chercher plus loin. ». Tout procédé de construction a été soigneusement banni du programme officiel, et une grande partie du vocabulaire mathématique de base a disparu ou a été vidé de sa substance. C'est fort regrettable car la maîtrise du vocabulaire mathématique demande du temps : il décrit des concepts qui reposent souvent sur d'autres concepts, et il faut voir fonctionner ces concepts pour saisir véritablement le sens des mots. Or ce temps fait cruellement défaut une fois passée la période des classes préparatoires.

Ce chapitre essaie de pallier à ces disparitions ; la plus grande partie de son contenu n'est pas utilisée dans le texte principal[(2)], mais est incluse car elle est susceptible de faire son apparition dans n'importe quel domaine utilisant des mathématiques. Il ne prend pas les mathématiques à leur début[(3)], et le lecteur est supposé avoir déjà des notions même vagues de la plupart des sujets qui suivent. Plutôt qu'un cours organisé, il s'agit d'une espèce de dictionnaire, et comme dans un dictionnaire, il n'est pas rare que certains passages fassent appel à des notions définies ultérieurement.

1. Grammaire élémentaire

Si X est un ensemble, on note |X| son cardinal.

L'expression $A \cong B$ signifie qu'il existe un isomorphisme entre A et B (la notion dépend donc de la structure mise sur A et B), ce qui est nettement moins précis (et donc plus souple) qu'une phrase du genre « u réalise un isomorphisme de A sur B » où un isomorphisme explicite est requis. Par exemple, dire que deux espaces vectoriels de dimension finie sur un corps K sont isomorphes revient juste à dire qu'ils ont la même dimension.

---

(2) Les résultats exposés dans le cours sont en grande partie antérieurs à la mise en valeur des concepts présentés dans ce chapitre, ce qui fait que l'on peut les présenter, en se contorsionnant un peu, sans recourir à ces concepts. D'un autre côté, lire « Les misérables » ou les « Disquisitiones arithmeticae » à la lumière d'une lampe électrique est nettement plus confortable qu'à la lueur d'une chandelle, même si ces œuvres datent d'avant l'invention de l'ampoule électrique et si la chandelle a un charme certain...

(3) Il a été écrit de la manière suivante. J'ai d'abord, pour chaque concept de base, fait une liste des énoncés que j'utilise régulièrement sans me poser de question. C'est plus ou moins ce qui se trouve en gros caractères. J'ai ensuite rajouté les démonstrations (en général en petits caractères). Une exception à ce principe est le traitement de l'algèbre linéaire, où j'ai remplacé les démonstrations vues en classes préparatoires par d'autres, donnant des résultats plus puissants. J'ai aussi rajouté, pour les amateurs, une collection de monstres mathématiques, et quelques résultats plus culturels comme la construction des nombres p-adiques, les théorèmes de Sylow ou la simplicité de A_n.

1.1. L'anneau Z des entiers relatifs

• Si A est un sous groupe de $\mathbf{Z}$ (muni de +), il existe $D \geqslant 0$ unique, tel que $A = D\mathbf{Z}$.

Si $A = \{0\}$, alors $D = 0$. Si $A \neq 0$, alors A contient des éléments > 0 puisque A est stable par $x \mapsto -x$; soit D le plus petit de ces éléments. Une récurrence immédiate montre que A contient nD, pour tout $n \in \mathbf{N}$, et donc aussi pour tout $n \in \mathbf{Z}$ puisque A est stable par $x \mapsto -x$. Autrement dit, $A \supset D\mathbf{Z}$.

Maintenant, soit $a \in A$, et soit $r \in \{0, \ldots, D-1\}$ le reste de la division euclidienne de a par D. Alors $a - r \in D\mathbf{Z} \subset A$, et donc $r = a - (a - r) \in A$. Comme D est par hypothèse le plus petit élément strictement positif de A, cela implique $r = 0$, et donc $a \in D\mathbf{Z}$. On en déduit l'inclusion $A \subset D\mathbf{Z}$ et l'égalité $A = D\mathbf{Z}$ que l'on cherchait à démontrer.

On écrit $a \mid b$ (pour a divise b) pour signifier que b est un multiple de a, et $a \nmid b$ pour signifier le contraire. Si $a, b \in \mathbf{Z}$, on définit le *plus grand diviseur commun* $\mathrm{pgcd}(a, b)$ de a et b comme étant 0 si $a = b = 0$, et comme étant le plus grand entier $d > 0$ divisant à la fois a et b, si $a \neq 0$ ou $b \neq 0$. On dit que a et b sont *premiers entre eux*, si $\mathrm{pgcd}(a, b) = 1$.

Un élément p de $\mathbf{N}$ est *premier*, si $p \neq 1$ et si les seuls diviseurs de p sont 1 et p. On note $\mathscr{P} = \{2, 3, 5, \ldots\}$ l'ensemble des nombres premiers. Il est clair que si $p \in \mathscr{P}$, et si $a \in \mathbf{N}$, alors soit $p \mid a$ auquel cas $\mathrm{pgcd}(p, a) = p$, soit $p \nmid a$ auquel cas p est premier à a.

Remarquons que $a\mathbf{Z} + b\mathbf{Z} = \{ax + by,\ x, y \in \mathbf{Z}\}$ est un sous-groupe de $\mathbf{Z}$; et c'est le plus petit sous-groupe de $\mathbf{Z}$ contenant a et b (en effet, un sous-groupe de $\mathbf{Z}$ contenant a et b contient ax et by et donc aussi $ax + by$, pour tous $x, y \in \mathbf{Z}$). On note (a, b), l'élément de $\mathbf{N}$ tel que $a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$; cet élément existe et est unique d'après le point ci-dessus.

• Si $a, b \in \mathbf{Z}$, alors $(a, b) = \mathrm{pgcd}(a, b)$; en particulier, *a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbf{Z}$ tels que* $1 = au + bv$ (théorème de Bézout[4]).

Si $a = b = 0$, le résultat est immédiat. Suposons donc $a \neq 0$ ou $b \neq 0$. Par définition de (a, b), a et b sont des multiples de (a, b), et donc $(a, b) \leqslant \mathrm{pgcd}(a, b)$. Réciproquement, si $d \geqslant 1$ divise a et b, alors d divise $ax + by$, quels que soient $x, y \in \mathbf{Z}$; en particulier, d divise (a, b) et donc $d \leqslant (a, b)$. On en déduit l'inégalité $(a, b) \geqslant \mathrm{pgcd}(a, b)$ qui permet de conclure.

• Si a est premier avec b et c, alors a est premier avec bc ; si a divise bc et si a est premier avec b, alors a divise c (lemme de Gauss).

Si $(a, b) = (a, c) = 1$, il existe u_1, v_1 tels que $au_1 + bv_1 = 1$ et u_2, v_2 tels que $au_2 + cv_2 = 1$. On a donc $1 = (au_1 + bv_1)(au_2 + cv_2) = au + bcv$, avec $u = au_1u_2 + bv_1u_2 + cu_1v_2$ et $v = v_1v_2$, ce qui prouve que $(a, bc) = 1$. On en déduit le premier énoncé.

Si $bc = ad$ et $au + bv = 1$, alors $acu + adv = c$, et donc $a(cu + dv) = c$, ce qui prouve que a divise c ; d'où le second énoncé.

• Si $n \in \mathbf{Z} - \{0\}$, il existe des nombres premiers $p_1, \ldots, p_r$ tels que $n = \mathrm{sign}(n)\, p_1 \cdots p_r$; de plus, les p_i, pour $1 \leqslant i \leqslant r$, sont uniquement déterminés à l'ordre près. En d'autres

[4] Il est en fait dû à C.-G. Bachet de Méziriac (1624) ; Bézout (1730-1783) a démontré l'énoncé analogue dans l'anneau K[T].

termes, n peut se factoriser de manière unique comme produit de facteurs premiers[5] (théorème fondamental de l'arithmétique).

Le cas $n < 0$ se déduit du cas $n > 0$; on peut donc supposer $n > 0$.

L'existence se démontre par récurrence. C'est évident pour $n = 1$, auquel cas, on a $r = 0$ (un produit vide vaut 1 par définition). Maintenant, si $n \geqslant 2$ est premier, alors $n = n$ est une factorisation de n sous la forme voulue. Si $n \geqslant 2$ n'est pas premier, alors $n = ab$, avec $2 \leqslant a \leqslant n-1$ et $2 \leqslant b \leqslant n-1$. On peut donc appliquer l'hypothèse de récurrence à a et b, ce qui permet d'écrire a sous la forme $a = p_1 \cdots p_s$, et b sous la forme $b = p_{s+1} \cdots p_r$, où $p_1, \ldots, p_r$ sont des nombres premiers. On a alors $n = p_1 \cdots p_r$, ce qui prouve que n admet une factorisation sous la forme voulue.

L'unicité se démontre en utilisant le lemme de Gauss. Si $p_1 \cdots p_r = q_1 \cdots q_s$ où les p_i et les q_j sont des nombres premiers, le lemme de Gauss montre que p_r divise l'un des q_j et donc lui est égal. Quitte à permuter les q_j, on peut supposer que $p_r = q_s$, et en divisant les deux membres par $p_r = q_s$, on se ramène à $r-1$ et $s-1$, ce qui permet de conclure par récurrence.

• Il y a une infinité de nombres premiers.

Supposons le contraire, et soient $p_1, \ldots, p_r$ les nombres premiers. Soit $n = (p_1 \cdots p_r) + 1$, et soit p un nombre premier divisant n (il en existe grâce au point précédent). Comme p ne peut pas être un des p_i puisque le reste de la division par p_i est 1, on aboutit à une contradiction qui permet de conclure.

• Si $n \in \mathbf{Z} - \{0\}$, et si p est un nombre premier, on note $v_p(n)$ le nombre de fois que p apparaît dans la décomposition en facteurs premiers de n ; alors $p^{v_p(n)}$ est aussi la plus grande puissance de p divisant n, et $v_p(n)$ est la *valuation p-adique* de n.

On étend cette définition à $n \in \mathbf{Z}$ en posant $v_p(0) = +\infty$. On dispose alors d'un critère de divisibilité assez utile : *a divise b si et seulement si $v_p(a) \leqslant v_p(b)$ pour tout nombre premier p*. En revenant à la définition de $\mathrm{pgcd}(a,b)$, on en déduit la formule $\mathrm{pgcd}(a,b) = \prod_p p^{\inf(v_p(a), v_p(b))}$.

Exercice 1.1. — Si $a, b \in \mathbf{Z}$, on définit le plus petit commun multiple $\mathrm{ppcm}(a,b)$ de a et b comme le plus petit entier $\geqslant 0$, multiple à la fois de a et b.

(i) Montrer que $a\mathbf{Z} \cap b\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$, et que $a\mathbf{Z} \cap b\mathbf{Z} = \mathrm{ppcm}(a,b)\mathbf{Z}$.

(ii) Montrer que $\mathrm{ppcm}(a,b) = \prod_p p^{\sup(v_p(a), v_p(b))}$, si $a \neq 0$ et $b \neq 0$.

Exercice 1.2. — (i) Montrer que $v_p(ab) = v_p(a) + v_p(b)$ et $v_p(a+b) \geqslant \inf(v_p(a), v_p(b))$, pour tous $a, b \in \mathbf{Z}$.

(ii) Montrer que v_p a un unique prolongement à $\mathbf{Q}$ tel que $v_p(xy) = v_p(x) + v_p(y)$, pour tous $x, y \in \mathbf{Q}$, et que l'on a alors $v_p(x+y) \geqslant \inf(v_p(x), v_p(y))$, quels que soient $x, y \in \mathbf{Q}$.

(iii) Montrer que $\sqrt{2}$ est irrationnel.

Exercice 1.3. — (i) Soient $n \geqslant 1$ et p un nombre premier. Montrer que $v_p(n!) = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \cdots$. En déduire que $v_p(n!) = \frac{n - \mathrm{S}_p(n)}{p-1}$, où $\mathrm{S}_p(n)$ est la somme des chiffres de n en base p.

[5] Si n est le produit de deux nombres premiers ayant chacun un millier de chiffres, on peut prouver, avec l'aide d'un ordinateur, que n n'est pas premier, mais il est impossible, à l'heure actuelle, de retrouver les deux nombres premiers qui divisent n. Ceci est à la base de la sécurité du système RSA, datant de 1977, en vigueur pour les transactions sur Internet. C'est aussi une bonne illustration de la différence entre la théorie et la pratique, qui en théorie sont la même chose, mais en pratique...

(ii) Montrer que $[x] - \left[\frac{x}{2}\right] - \left[\frac{x}{3}\right] - \left[\frac{x}{5}\right] + \left[\frac{x}{30}\right]$ est toujours $\geqslant 0$. En déduire que $\frac{(30n)!\,n!}{(15n)!\,(10n)!\,(6n)!}$ est un entier[6], pour tout $n \in \mathbf{N}$.

1.2. Parallélisme entre logique élémentaire et langage ensembliste

• La négation $p \mapsto \overline{p}$ correspond au passage au complémentaire : $\{x,\ \overline{p}(x)\}$ est le complémentaire de $\{x,\ p(x)\}$.

• $\wedge$ ("et") correspond à l'intersection : $\{x,\ p(x) \wedge q(x)\} = \{x,\ p(x)\} \cap \{x,\ q(x)\}$.

• $\vee$ ("ou") correspond à la réunion : $\{x,\ p(x) \vee q(x)\} = \{x,\ p(x)\} \cup \{x,\ q(x)\}$.

• La formule $\overline{p \vee q} = \overline{p} \wedge \overline{q}$ (resp. $\overline{p \wedge q} = \overline{p} \vee \overline{q}$) devient : le complémentaire de la réunion (resp. l'intersection) est l'intersection (resp. la réunion) des complémentaires.

• $\Rightarrow$ correspond à l'inclusion : $p \Rightarrow q$ si et seulement si $\{x,\ p(x)\} \subset \{x,\ q(x)\}$.

• $\forall$ correspond à une intersection : $\{x,\ \forall i \in \mathrm{I}, p_i(x)\} = \cap_{i\in\mathrm{I}}\{x,\ p_i(x)\}$.

• $\exists$ correspond à une réunion : $\{x,\ \exists i \in \mathrm{I}, p_i(x)\} = \cup_{i\in\mathrm{I}}\{x,\ p_i(x)\}$.

Considérons, par exemple, deux espaces métriques X et Y, et une suite de fonctions $(f_n)_{n\in\mathbf{N}}$ de X dans Y. Soit A l'ensemble des $x \in \mathrm{X}$ tels que $f_n(x)$ converge. Alors A peut s'écrire sous la forme :

$$\begin{aligned}\mathrm{A} =& \{x \in \mathrm{X},\ \exists y \in \mathrm{Y},\ \forall j \in \mathbf{N},\ \exists \mathrm{N} \in \mathbf{N},\ \forall n \geqslant \mathrm{N},\ d(f_n(x), y) < 2^{-j}\} \\ =& \cup_{y\in\mathrm{Y}} \cap_{j\in\mathbf{N}} \cup_{\mathrm{N}\in\mathbf{N}} \cap_{n\geqslant\mathrm{N}} f_n^{-1}(\{y' \in \mathrm{Y},\ d(y,y') < 2^{-j}\}).\end{aligned}$$

Si Y est complet, on peut utiliser le critère de Cauchy au lieu de donner un nom à la limite, et on obtient [en notant $f_{n,p} : \mathrm{X} \to \mathrm{Y} \times \mathrm{Y}$ la fonction $x \mapsto (f_n(x), f_p(x))$] :

$$\begin{aligned}\mathrm{A} =& \{x \in \mathrm{X},\ \ \forall j \in \mathbf{N},\ \exists \mathrm{N} \in \mathbf{N}, \forall n, p \geqslant \mathrm{N},\ d(f_n(x), f_p(x)) < 2^{-j}\} \\ =& \cap_{j\in\mathbf{N}} \cup_{\mathrm{N}\in\mathbf{N}} \cap_{n,p\geqslant\mathrm{N}} f_{n,p}^{-1}\big(\{(y,y') \in \mathrm{Y}\times\mathrm{Y},\ d(y,y') < 2^{-j}\}\big).\end{aligned}$$

La seconde formulation a l'avantage de ne faire intervenir que des intersections et réunions indexées par des ensembles dénombrables.

1.3. Ensembles dénombrables

Un ensemble est *dénombrable* s'il est fini ou s'il peut être mis en bijection avec $\mathbf{N}$.

• Un sous-ensemble d'un ensemble dénombrable est dénombrable.

> Il suffit de démontrer qu'un sous-ensemble X de $\mathbf{N}$, qui n'est pas fini, peut être mis en bijection avec $\mathbf{N}$. Si $x \in \mathrm{X}$, soit $\varphi(x) = |\{y \in \mathrm{X},\ y < x\}|$. Si x_0 est le plus petit élément de X, on a $\varphi(x_0) = 0$, ce qui montre que $\varphi(\mathrm{X})$ contient 0. Si $\varphi(x) = n$, et x' est le plus petit élément de X strictement supérieur à x, on a $\varphi(x') = n + 1$, ce qui prouve que φ est surjective. Par ailleurs, φ est injective car strictement croissante (si $x_1 < x_2$, alors $\{y \in \mathrm{X},\ y < x_2\}$ contient $\{y \in \mathrm{X},\ y < x_1\}$ et x_1). Ceci permet de conclure.

[6] Cette observation, couplée avec la formule de Stirling, a permis à P. Tchebychev de montrer, en 1852, que le nombre $\pi(x)$ de nombres premiers $\leqslant x$ vérifie $(0,92 + o(1))\frac{x}{\log x} \leqslant \pi(x) \leqslant (1,05 + o(1))\frac{x}{\log x}$, encadrement que l'on pourra comparer avec le th. des nombres premiers $\pi(x) \sim \frac{x}{\log x}$. En 2005, F. Rodriguez-Villegas a démontré que la série $\sum_{n=0}^{+\infty} \frac{(30n)!\,n!}{(15n)!\,(10n)!\,(6n)!}\mathrm{T}^n$ était algébrique, ce qui signifie qu'il existe un polynôme P à coefficients dans $\mathbf{Q}(\mathrm{T})$ qui l'annule ; il a aussi prouvé que le degré minimal d'un tel polynôme est 483840, ce qui rend son explicitation problématique...

• Si $\varphi : \mathrm{X} \to \mathrm{Y}$ est injective et si Y est dénombrable, alors X est dénombrable ; si $\varphi : \mathrm{X} \to \mathrm{Y}$ est surjective et si X est dénombrable, alors Y est dénombrable.

Si $\varphi : \mathrm{X} \to \mathrm{Y}$ est injective, alors φ réalise une bijection de X sur $\varphi(\mathrm{X})$ qui est dénombrable comme sous-ensemble d'un ensemble dénombrable, et donc X est dénombrable. Si $\varphi : \mathrm{X} \to \mathrm{Y}$ est surjective, on peut choisir, pour tout $y \in \mathrm{Y}$, un antécédent $s(y) \in \mathrm{Y}$ de y par φ. Alors $s : \mathrm{Y} \to \mathrm{X}$ est injective car $s(y_1) = s(y_2)$ implique $y_1 = \varphi(s(y_1)) = \varphi(s(y_2)) = y_2$, et donc Y est dénombrable si X l'est, d'après ce qui précède.

• Un produit fini d'ensembles dénombrables est dénombrable.

Soient $\mathrm{X}_1, \ldots, \mathrm{X}_k$ des ensembles dénombrables, $\mathrm{X} = \mathrm{X}_1 \times \cdots \times \mathrm{X}_k$, et $p_1, \ldots, p_k$ des nombres premiers distincts. Soit $\varphi_i : \mathrm{X}_i \to \mathbf{N}$ injective, pour tout $i \in \{1, \ldots, k\}$. Alors $\varphi : \mathrm{X} \to \mathbf{N}$, définie par $\varphi(x_1, \ldots, x_k) = p_1^{\varphi_1(x_1)} \cdots p_k^{\varphi_k(x_k)}$ est injective d'après le « théorème fondamental de l'arithmétique » (unicité de la factorisation d'un entier naturel non nul en produit de nombres premiers).

• Une réunion dénombrable d'ensembles dénombrables est dénombrable.

Soit $(\mathrm{X}_i)_{i \in \mathrm{I}}$, avec I dénombrable et chacun des X_i aussi. Soient $\varphi_i : \mathrm{X}_i \to \mathbf{N}$, pour $i \in \mathrm{I}$, des applications injectives, et soit $\mathrm{Y} \subset \mathrm{I} \times \mathbf{N}$ l'ensemble des couples $(i, \varphi_i(x))$, pour $i \in \mathrm{I}$ et $x \in \mathrm{X}_i$. Alors Y est dénombrable comme sous-ensemble de l'ensemble dénombrable $\mathrm{I} \times \mathbf{N}$, et l'application $(i, y) \mapsto \varphi_i^{-1}(y)$ de Y dans $\cup_{i \in \mathrm{I}} \mathrm{X}_i$ est surjective, ce qui prouve que $\cup_{i \in \mathrm{I}} \mathrm{X}_i$ est dénombrable.

• $\mathbf{Z}$, $\mathbf{N}^d$, $\mathbf{Z}^d$, si $d \in \mathbf{N}$, et $\mathbf{Q}$ sont dénombrables[7].

L'application $(a, b) \mapsto a - b$ est une surjection de $\mathbf{N} \times \mathbf{N}$ sur $\mathbf{Z}$, et comme $\mathbf{N} \times \mathbf{N}$ est dénombrable, en tant que produit fini d'ensembles dénombrables, il en est de même de $\mathbf{Z}$. Les ensembles $\mathbf{N}^d$, $\mathbf{Z}^d$ sont dénombrables puisque ce sont des produits finis d'ensembles dénombrables. Enfin, $(a, b) \mapsto \frac{a}{b}$ induit une surjection de $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ sur $\mathbf{Q}$ qui, de ce fait est dénombrable, $\mathbf{Z}$ et $\mathbf{Z} - \{0\}$ l'étant.

• $\mathbf{R}$ et l'ensemble $\{0, 1\}^{\mathbf{N}}$ des suites à valeurs dans $\{0, 1\}$ ne sont pas dénombrables.

Supposons que $\{0, 1\}^{\mathbf{N}}$ est dénombrable. Il existe donc une bijection $n \mapsto x_n$ de $\mathbf{N}$ sur $\{0, 1\}^{\mathbf{N}}$. Chaque x_n est une suite $x_n = (x_{n,k})_{k \in \mathbf{N}}$, où $x_{n,k} \in \{0, 1\}$, ce qui permet de considérer la suite $y = (y_k)_{k \in \mathbf{N}}$, où $y_k = 1 - x_{k,k}$. Par construction, la suite y a sa n-ième valeur distincte de celle de x_n, pour tout n, et on a donc $y \neq x_n$, quel que soit $n \in \mathbf{N}$, ce qui est en contradiction avec l'hypothèse selon laquelle $n \mapsto x_n$ est surjective ; c'est donc que $\{0, 1\}^{\mathbf{N}}$ n'est pas dénombrable. Cet argument est *l'argument diagonal* de Cantor (1891).

Pour démontrer que $\mathbf{R}$ n'est pas dénombrable, il suffit de constater que si X désigne le sous-ensemble de $[0, 1[$ des nombres dont le développement décimal ne comportent que des 0 et des 1, alors X est en bijection avec $\{0, 1\}^{\mathbf{N}}$, et donc n'est pas dénombrable. Il en est a fortiori de même de $\mathbf{R}$, qui contient X.

[7] Ces résultats, la non dénombrabilité de $\mathbf{R}$ et la dénombrabilité de l'ensemble des nombres algébriques sont le fruit d'un échange de lettres entre G. Cantor et R. Dedekind datant de la fin 1873. Cantor prouvera en 1877 que $[0, 1]$ et $[0, 1] \times [0, 1]$ peuvent être mis en bijection ; comme il l'écrit à Dedekind : « Je le vois, mais je ne le crois pas ».

Exercice 1.4. — Montrer que l'ensemble $\mathscr{P}(\mathbf{N})$ des parties de $\mathbf{N}$ n'est pas dénombrable, mais que l'ensemble des parties finies de $\mathbf{N}$ est dénombrable.

Exercice 1.5. — On rappelle que $x \in \mathbf{C}$ est *algébrique* s'il existe $\mathrm{P} \in \mathbf{Q}[\mathrm{X}]$ non nul tel que $\mathrm{P}(x) = 0$, et que $x \in \mathbf{C}$ est *transcendant* s'il n'est pas algébrique. Montrer que l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques est dénombrable. En déduire qu'il existe des nombres transcendants.

Exercice 1.6. — Soit $(\mathrm{B}_j)_{j\in\mathrm{I}}$ une famille de disques ouverts non vides de $\mathbf{C}$. Montrer que si les B_j sont deux à deux disjoints, alors I est dénombrable.

Exercice 1.7. — Soit $f : \mathbf{R} \to \mathbf{R}$ une fonction croissante.

(i) Montrer que f admet une limite à droite et une limite à gauche en tout point et que, si $x_0 \in \mathbf{R}$, alors $f(x_0^+) = \inf_{x>x_0} f(x)$ et $f(x_0^-) = \sup_{x<x_0} f(x)$; en déduire que $f(x_0^-) \leqslant f(x_0) \leqslant f(x_0^+)$. A quelle condition f est-elle continue en x_0 ?

(ii) Montrer que, si $x_0 < x_1$, alors $f(x_0^+) \leqslant f(x_1^-)$.

(iii) Montrer que l'ensemble D des points où f est discontinue est dénombrable.

Exercice 1.8. — Soient X un sous-ensemble dénombrable de $\mathbf{R}$, dense (i.e. $]a, b[\cap \mathrm{X} \neq \emptyset$, pour tous $a < b$), et $n \mapsto x_n$ une bijection de $\mathbf{N}$ sur X. On définit, par récurrence, une suite $n \mapsto \varphi(n)$, en posant $\varphi(0) = 0$, $\varphi(1) = 1$ et en prenant pour $\varphi(n)$ le plus petit entier $i \geqslant \varphi(n-1)$ tel que x_i soit entre $x_{\varphi(n-1)}$ et $x_{\varphi(n-2)}$. Montrer que la suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ a une limite et que cette limite n'appartient pas à X. En déduire que $\mathbf{R}$ n'est pas dénombrable.

Exercice 1.9. — (difficile) Un « huit » est la réunion de deux cercles dans le plan, de même rayon (non nul), tangents en un point. Montrer que l'on peut mettre dans le plan au plus un nombre dénombrable de huit deux à deux disjoints.

Exercice 1.10. — (difficile) Un « tripode » est la figure formée de trois segments $[\mathrm{G}, \mathrm{A}]$, $[\mathrm{G}, \mathrm{B}]$ et $[\mathrm{G}, \mathrm{C}]$, où $\mathrm{A}, \mathrm{B}, \mathrm{C}$ sont les sommets d'un triangle équilatéral (non réduit à un point) et G est le centre de gravité du triangle. Montrer que l'on peut mettre dans le plan au plus un nombre dénombrable de tripodes deux à deux disjoints.

2. Produits, sommes et quotients

2.1. Produits et sommes

2.1.1. Produits et sommes directes de groupes commutatifs

Si $(\mathrm{A}_i)_{i\in\mathrm{I}}$ est une famille de groupes (de lois notées multiplicativement), on munit leur produit $\prod_{i\in\mathrm{I}} \mathrm{A}_i$ d'une structure de groupe, en faisant le produit composante par composante [i.e en posant $(x_i)_{i\in\mathrm{I}}(y_i)_{i\in\mathrm{I}} = (x_i y_i)_{i\in\mathrm{I}}$]. L'élément neutre est alors $(e_i)_{i\in\mathrm{I}}$, si e_i désigne l'élément neutre de A_i, et l'inverse de $(x_i)_{i\in\mathrm{I}}$ est $(x_i^{-1})_{i\in\mathrm{I}}$. On dispose, pour tout i, d'une surjection naturelle $p_i : \prod_{i\in\mathrm{I}} \mathrm{A}_i \to \mathrm{A}_i$ envoyant $(x_i)_{i\in\mathrm{I}}$ sur x_i, qui est un morphisme de groupes de manière évidente.

• Le produit vérifie la *propriété universelle* suivante : si B est un groupe, et si $f_i : \mathrm{B} \to \mathrm{A}_i$ est un morphisme de groupes pour tout $i \in \mathrm{I}$, il existe un unique morphisme de groupes $f : \mathrm{B} \to \prod_{i\in\mathrm{I}} \mathrm{A}_i$ tel que $p_i \circ f = f_i$, quel que soit $i \in \mathrm{I}$.

On doit poser $f(x) = (f_i(x))_{i\in \mathrm{I}}$. Il est alors évident que f est un morphisme de groupes, et que l'on a $p_i \circ f = f_i$, quel que soit $i \in \mathrm{I}$.

Si $(\mathrm{A}_i)_{i\in \mathrm{I}}$ est une famille de groupes commutatifs (de loi notée additivement), on définit leur *somme directe* $\oplus_{i\in \mathrm{I}} \mathrm{A}_i$ comme le sous-ensemble du produit $\prod_{i\in \mathrm{I}} \mathrm{A}_i$ des $(x_i)_{i\in \mathrm{I}}$ vérifiant $x_i = 0$ pour presque tout i (i.e. à l'exception d'un nombre fini de i). On dispose alors, pour tout i, d'une injection naturelle $\iota_i : \mathrm{A}_i \to \mathrm{A}$, envoyant $a \in \mathrm{A}_i$ sur $(x_i)_{i\in \mathrm{I}}$, avec $x_i = a$ et $x_j = 0$, si $j \neq i$.

• Si I est fini, la somme directe est égale au produit, mais pas si I est infini[8].

• La somme directe vérifie la *propriété universelle* suivante : si B est un groupe commutatif, et si $f_i : \mathrm{A}_i \to \mathrm{B}$ est un morphisme de groupes pour tout $i \in \mathrm{I}$, il existe un unique morphisme de groupes $f : \oplus_{i\in \mathrm{I}} \mathrm{A}_i \to \mathrm{B}$ tel que $f \circ \iota_i = f_i$, quel que soit $i \in \mathrm{I}$.

On doit poser $f((x_i)_{i\in \mathrm{I}}) = \sum_{i\in \mathrm{I}} f_i(x_i)$, ce qui a un sens car la somme est en fait finie. Il est alors évident que f est un morphisme de groupes, et que l'on a $f \circ \iota_i = f_i$, quel que soit $i \in \mathrm{I}$.

• Si A est un groupe commutatif, et si $(\mathrm{A}_i)_{i\in \mathrm{I}}$ est une famille de sous-groupes de A, on dispose d'un morphisme de groupes naturel de $\oplus_{i\in \mathrm{I}} \mathrm{A}_i$ dans A, induit par l'identité sur A_i, pour tout i. On note $\sum_{i\in \mathrm{I}} \mathrm{A}_i$ l'image de ce morphisme ; c'est le sous-groupe de A engendré par les A_i. On dit que les A_i sont *en somme directe*, si l'application naturelle de $\oplus_{i\in \mathrm{I}} \mathrm{A}_i$ dans A est un isomorphisme. De manière plus concrète, les A_i sont en somme directe, si tout élément x de A peut s'écrire de manière unique sous la forme $x = \sum_{i\in \mathrm{I}} x_i$, avec $x_i \in \mathrm{A}_i$ pour tout i, et $x_i = 0$ pour presque tout i.

• Si B et C sont deux sous-groupes d'un groupe commutatif A, alors B et C sont en somme directe, si et seulement si $\mathrm{B} \cap \mathrm{C} = \{0\}$ et tout élement de A est somme d'un élément de B et d'un élément de C.

2.1.2. Le cas des espaces vectoriels

Soit K un corps (sous-entendu commutatif). Un K-espace vectoriel est en particulier un groupe commutatif, et tout ce que l'on a dit à l'alinéa précédent s'applique. On dispose en plus d'une action de K, définie par $\lambda\,(x_i)_{i\in \mathrm{I}} = (\lambda\, x_i)_{i\in \mathrm{I}}$, si $\lambda \in \mathrm{K}$, sur le produit et la somme directe, ce qui en fait des K-espaces vectoriels. Si $(\mathrm{E}_i)_{i\in \mathrm{I}}$ est une famille de K-espaces vectoriels, ces objets vérifient alors les propriétés universelles suivantes.

• Si F est un K-espace vectoriel, et si $f_i : \mathrm{F} \to \mathrm{E}_i$ est une application linéaire pour tout $i \in \mathrm{I}$, il existe une unique application linéaire $f : \mathrm{F} \to \prod_{i\in \mathrm{I}} \mathrm{E}_i$ telle que $p_i \circ f = f_i$, quel que soit $i \in \mathrm{I}$.

• Si F est un K-espace vectoriel, et si $f_i : \mathrm{E}_i \to \mathrm{F}$ est une application linéaire pour tout $i \in \mathrm{I}$, il existe une unique application linéaire $f : \oplus_{i\in \mathrm{I}} \mathrm{E}_i \to \mathrm{F}$ telle que $f \circ \iota_i = f_i$, quel que soit $i \in \mathrm{I}$.

[8] Le lecteur désireux de comprendre plus en profondeur la différence entre les notions de produit et de somme est invité à se munir d'une loupe et à consulter l'alinéa 2.1.3.

• Si I est fini, les espaces vectoriels $\oplus_{i\in \mathrm{I}} \mathrm{E}_i$ et $\prod_{i\in \mathrm{I}} \mathrm{E}_i$ sont isomorphes, et les E_i sont en somme directe dans $\prod_{i\in \mathrm{I}} \mathrm{E}_i$.

• Les E_i n'ont pas de raison d'être distincts : par exemple, si $\mathrm{K} = \mathbf{C}$, et si $\mathrm{E}_1 = \mathrm{E}_2 = \mathbf{C}$, alors $\mathrm{E}_1 \oplus \mathrm{E}_2 = \mathbf{C}^2$, et $\iota_1(\mathrm{E}_1)$ (resp. $\iota_2(\mathrm{E}_2)$) est la droite engendrée par $\iota_1(1) = (1, 0)$ (resp. $\iota_2(1) = (0, 1)$) ; autrement dit, $\mathbf{C} \oplus \mathbf{C}$ est égal à $\mathbf{C}^2$, muni de sa base canonique.

2.1.3. Produit et somme dans une catégorie

On définit la notion de *catégorie* pour mettre sous un même chapeau les objets ayant les mêmes propriétés. Le lecteur connaît déjà, sans en avoir forcément conscience, un certain nombre de ces catégories (celle des ensembles, celle des groupes ou celle des espaces vectoriels sur $\mathbf{R}$ ou $\mathbf{C}$ par exemple ; il y en a beaucoup d'autres comme celle des espaces topologiques, des espaces de Banach...).

Une catégorie C est une collection d'objets (les objets de la catégorie), et de flèches entre ces objets (les morphismes de la catégorie) : si X et Y sont deux objets de C, on note $\mathrm{Hom}_{\mathrm{C}}(\mathrm{X}, \mathrm{Y})$ les morphismes de X vers Y dans la catégorie C. On impose que l'identité id_{X} soit un morphisme de X dans X, et que l'on puisse composer les morphismes : si X, Y et Z sont trois objets de C, on dispose d'une application $(f, g) \mapsto f \circ g$ de $\mathrm{Hom}_{\mathrm{C}}(\mathrm{X}, \mathrm{Y}) \times \mathrm{Hom}_{\mathrm{C}}(\mathrm{Y}, \mathrm{Z}) \to \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}, \mathrm{Z})$ vérifiant les propriétés évidentes :

$$f \circ \mathrm{id}_{\mathrm{X}} = f,\ \mathrm{id}_{\mathrm{Y}} \circ f = f \text{ et } (f \circ g) \circ h = f \circ (g \circ h).$$

Les exemples les plus simples de catégories sont les suivants :

— La catégorie des ensembles ; les morphismes de X dans Y sont les applications Y^{X} de X dans Y.

— La catégorie des groupes ; les morphismes sont les morphismes de groupes.

— La catégorie des groupes commutatifs ; les morphismes sont les morphismes de groupes.

— La catégorie des anneaux commutatifs ; les morphismes sont les morphismes d'anneaux.

— La catégorie des K-espaces vectoriels, K un corps ; les morphismes sont les applications K-linéaires.

— La catégorie des espaces topologiques ; les morphismes sont les applications continues.

— La catégorie des espaces métriques ; les morphismes sont les applications continues.

— La catégorie des $\mathbf{K}$-espaces de Banach, $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$; les morphismes sont les applications $\mathbf{K}$-linéaires continues.

Dans une catégorie, on définit les notions de *produit* et *somme* par les propriétés universelles suivantes (la propriété universelle implique l'unicité d'un tel objet, mais pas son existence qui doit se démontrer cas par cas).

Si C est une catégorie et les $(\mathrm{X}_i)_{i\in \mathrm{I}}$ sont des objets de C, le produit $\mathrm{X} = \prod_{i\in \mathrm{I}} \mathrm{X}_i$ des X_i est un objet de C muni de morphismes $p_i \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}, \mathrm{X}_i)$, pour $i \in \mathrm{I}$, tel que, si Y est n'importe quel objet de C, et si $f_i \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{Y}, \mathrm{X}_i)$, pour tout $i \in \mathrm{I}$, alors il existe $f \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{Y}, \mathrm{X})$ unique, tel que $p_i \circ f = f_i$ pour tout $i \in \mathrm{I}$.

La somme $\mathrm{X} = \coprod_{i\in \mathrm{I}} \mathrm{X}_i$ des X_i est un objet de C muni de morphismes $\iota_i \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}_i, \mathrm{X})$, pour $i \in \mathrm{I}$, tel que, si Y est n'importe quel objet de C, et si $f_i \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}_i, \mathrm{Y})$, pour tout $i \in \mathrm{I}$, alors il existe $f \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}, \mathrm{Y})$ unique, tel que $f \circ \iota_i = f_i$ pour tout $i \in \mathrm{I}$.

Montrons par exemple l'unicité du produit. Si X (resp. X′) muni des $p_i : \mathrm{X} \to \mathrm{X}_i$ (resp. des $p'_i : \mathrm{X}' \to \mathrm{X}_i$) est un produit des X_i, alors en particulier, il existe $f : \mathrm{X}' \to \mathrm{X}$ unique tel que $p_i \circ f = p'_i$ pour tout i, et il existe $g : \mathrm{X} \to \mathrm{X}'$ unique tel que $p'_i \circ g = p_i$ pour tout i. Alors $f \circ g : \mathrm{X} \to \mathrm{X}$ vérifie $p_i \circ (f \circ g) = p_i$ pour tout i, ce qui implique que $f \circ g = \mathrm{id}_{\mathrm{X}}$ puisque id_{X} vérifie la même propriété, et que par hypothèse, il n'y a qu'un seul morphisme de X dans X ayant cette propriété. Pour la même raison, on a $g \circ f = \mathrm{id}_{\mathrm{X}}$, ce qui prouve que X et X′ sont isomorphes (à isomorphisme unique près puisque f et g étaient uniques). Cette démonstration s'étend à tout objet solution d'un problème universel.

On dit qu'une catégorie admet des produits (resp. des sommes), si tout couple (et donc toute famille finie) d'objets de la catégorie admet un produit (resp. une somme). Toutes les catégories ci-dessus admettent des produits, car on peut munir le produit ensembliste de deux objets des structures additionnelles demandées. Elles admettent aussi toutes une somme, mais celle-ci peut prendre des formes assez variées.

— Dans la catégorie des ensembles, la somme d'une famille $(\mathrm{X}_i)_{i\in \mathrm{I}}$ d'ensemble est leur réunion disjointe $\cup_{i\in \mathrm{I}}(\{i\} \times \mathrm{X}_i)$.

— Dans la catégorie des K-espaces vectoriels, ou dans celle des groupes commutatifs, la somme est la somme directe, et la somme d'un nombre fini d'objets est isomorphe à leur produit comme on l'a vu ci-dessus.

— Dans la catégorie des groupes, la somme de deux groupes A et B est leur produit libre $A \star B$: les éléments de $A \star B$ sont les mots finis composés d'éléments de A et B modulo la relation d'équivalence selon laquelle on peut remplacer toute lettre x dans un mot par deux lettres x_1, x_2 appartenant au même groupe si $x_1 x_2 = x$, et réciproquement, on peut remplacer deux lettres consécutives appartenant au même groupe par leur produit. La somme de deux groupes commutatifs n'est donc pas la même dans la catégorie des groupes que dans celle des groupes commutatif. Par exemple, on a $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) = (\mathbf{Z}/6\mathbf{Z})$, alors que $(\mathbf{Z}/2\mathbf{Z}) \star (\mathbf{Z}/3\mathbf{Z})$ est un groupe infini, isomorphe au groupe $\mathbf{PSL}_2(\mathbf{Z})$, quotient de $\mathbf{SL}_2(\mathbf{Z})$ par son centre $\left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right\}$.

2.2. Relations d'équivalence

2.2.1. Relations d'équivalence et partitions

Si E est un ensemble, une *partition* de E est une famille de sous-ensembles non vides de E, deux à deux disjoints, dont la réunion est E.

Par exemple, $\{\mathbf{R}_+^*, \mathbf{R}_-^*, \{0\}\}$ est une partition de $\mathbf{R}$. Si $D \in \mathbf{N} - \{0\}$, les $r + D\mathbf{Z}$, pour $r \in \{0, \ldots, D-1\}$ forment une partition de $\mathbf{Z}$.

Une *relation* R sur E est un sous-ensemble de $E \times E$. Si $(x, y) \in E \times E$, on écrit souvent $x R y$ pour signifier $(x, y) \in R$.

Une relation R sur E est une *relation d'équivalence* si elle est *réflexive* ($x R x$ quel que soit $x \in E$), *symétrique* ($x R y$ implique $y R x$) et *transitive* ($x R y$ et $y R z$ impliquent $x R z$).

Si R est une relation d'équivalence sur E, et si $x \in E$, la *classe d'équivalence de* x est l'ensemble $C_x = \{y \in E,\ y R x\}$. Un sous-ensemble C de E est *une classe d'équivalence* (pour R), s'il existe $x \in E$ tel que $C = C_x$. Si $x, y \in E$, alors $C_x \cap C_y \neq \emptyset$ si et seulement si $x R y$, et on a alors $C_x = C_y$. Les classes d'équivalence forment donc une partition de E.

Réciproquement, si les $(C_i)_{i \in I}$ forment une partition de E, alors la relation R définie par $x R y$ si et seulement si il existe $i \in I$ tel que $\{x, y\} \subset C_i$ est une relation d'équivalence dont les classes d'équivalence sont les C_i. En d'autres termes, il revient au même de munir un ensemble d'une relation d'équivalence ou de faire une partition de cet ensemble.

Par exemple, la partition de $\mathbf{R}$ ci-dessus correspond à la relation d'équivalence « $x \sim y$ si et seulement si x et y ont même signe » ; celle de $\mathbf{Z}$ correspond à la relation d'équivalence « $a \sim b$ si et seulement si a et b ont même reste dans la division euclidienne par D ».

2.2.2. Passage au quotient par une relation d'équivalence. — Si R est une relation d'équivalence sur E, on définit *le quotient* E/R *de* E *par la relation d'équivalence* R comme l'ensemble des classes d'équivalence. On dispose d'une application naturelle de E dans E/R, à savoir l'application qui à x associe sa classe d'équivalence (souvent notée $\overline{x}$) ; cette application est surjective par construction de E/R. Un sous-ensemble S de E est *un système de représentants* de E/R, s'il contient un et un seul élément de chaque classe d'équivalence. Autrement dit, $S \subset E$ est un système de représentants de E/R si et seulement si l'application naturelle de E dans E/R induit une bijection de S sur E/R.

Cette manière de définir de nouveaux objets en passant au quotient par une relation d'équivalence est une des plus universelles qui soit[9]. Pour le petit enfant, le nombre 5 est la classe d'équivalence des ensembles pouvant être mis en bijection avec l'ensemble {un,deux,trois,quatre,cinq} (ce n'est pas une raison pour le lui définir de cette manière...). Pour le commun des mortels, un nombre réel est un nombre avec une infinité de chiffres derrière la virgule, et comme certains nombres ont deux écritures, il faut passer au quotient... Une couleur aussi est définie par un passage au quotient nettement plus délicat que les passages au quotient mathématiques...

En général, on aime bien que E/R hérite des propriétés que pouvait avoir E (i.e. on aime bien que les propriétés de E *passent au quotient*), ce qui impose des contraintes aux relations d'équivalence que l'on peut considérer. Par exemple, une fonction $f : \mathrm{E} \to \mathrm{X}$ passe au quotient si et seulement si on a $f(x) = f(y)$ pour tout couple d'éléments de E vérifiant $x\mathrm{R}y$ (si c'est le cas, on définit $\overline{f} : \mathrm{E/R} \to \mathrm{X}$ par $\overline{f}(z) = f(x)$ pour n'importe quel élément x de E ayant pour image z dans E/R. Si $\pi : \mathrm{E} \to \mathrm{E/R}$ est l'application naturelle, on a $f = \overline{f} \circ \pi$; on dit que f *se factorise à travers* E/R ou que f se factorise à travers π, ce qui est une terminologie assez parlante puisqu'elle signifie que l'équation $f = g \circ \pi$ a une solution $g = \overline{f}$).

2.3. L'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ des entiers relatifs modulo D

Dans tout ce qui suit, D est un entier $\geqslant 1$. On note $\mathrm{D}\mathbf{Z}$ l'ensemble des multiples de D. On définit une relation *de congruence modulo* D sur $\mathbf{Z}$, en disant que a est congru à b modulo D (ou modulo $\mathrm{D}\mathbf{Z}$), ce qui se note $a \equiv b$ [D] ou $a \equiv b \bmod \mathrm{D}$, si $b - a \in \mathrm{D}\mathbf{Z}$.

• La relation de congruence modulo D est une relation d'équivalence sur $\mathbf{Z}$. On note $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ l'ensemble des classes d'équivalence. L'image d'un entier dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est sa *réduction modulo* D.

> Cette relation est reflexive car 0 est un multiple de D, symétrique car si $b-a$ est un multiple de D, il en est de même de $a - b$, et transitive car si $b - a$ et $c - b$ sont des multiples de D, il en est de même $c - a = (c - b) + (b - a)$.

---

[9] L'expérience montre que les premiers passages au quotient que l'on rencontre sont un peu traumatisants, mais on finit par s'y faire... Il fut un temps pas si lointain, où l'on définissait $\mathbf{Z}$ comme le quotient de $\mathbf{N} \times \mathbf{N}$ par la relation d'équivalence $(a, b) \sim (a', b')$ si et seulement si $a + b' = a' + b$, l'idée étant que (a, b) représente l'entier relatif $a - b$. Au bout de 3 semaines, on avait enfin le droit d'écrire $2 - 3 + 5 - 7 = -3$, ce que n'importe qui ayant regardé un thermomètre comprend très bien. Pour en arriver là, il avait fallu passer par $(2, 0) + (0, 3) + (5, 0) + (0, 7) = (7, 10) = (0, 3)$, puis par $(+2) + (-3) + (+5) + (-7) = (-3)$. On achevait de traumatiser les élèves (et leur parents) en définissant, en classe de $4^{\text{ème}}$, un vecteur comme une classe d'équipollence de bipoints (un bipoint (i.e. un couple de points) (A, B) est *équipollent* à (C, D), si (A, B, D, C) est un parallélogramme). Dans une période plus récente, les aléas de la conjoncture ayant provoqué un tarissement des vocations de professeurs de mathématiques, on s'est retrouvé avec une pénurie que l'on a traitée en diminuant l'horaire de mathématiques dans l'enseignement, et on en a profité pour jeter allègrement à la poubelle toutes ces horribles mathématiques modernes...

• Un système naturel de représentants de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dans $\mathbf{Z}$ est l'ensemble $\{0, 1, \ldots, \mathrm{D}-1\}$; en particulier, $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est de cardinal D.

Si $a, b \in \{0, 1, \ldots, \mathrm{D}-1\}$ sont distincts, et si $b > a$, alors $1 \leqslant b - a \leqslant \mathrm{D}-1$. En particulier $b - a$ n'est pas un multiple de D, ce qui prouve que b et a sont dans des classes distinctes modulo D, et donc que l'application naturelle de $\{0, 1, \ldots, \mathrm{D}-1\}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est injective. Par ailleurs, si $a \in \mathbf{Z}$ est quelconque, et si $r \in \{0, 1, \ldots, \mathrm{D}-1\}$ est le reste de la division de a par D, alors $a - r$ est un multiple de D et a est dans la même classe que r modulo D ; l'application naturelle de $\{0, 1, \ldots, \mathrm{D}-1\}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est donc surjective.

• L'addition et la multiplication sur $\mathbf{Z}$ passent au quotient, et $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ muni des lois d'addition et multiplication ainsi définies est un anneau commutatif[10].

Si $x - x'$ et $y - y'$ sont divisibles par D, alors $(x + y) - (x' + y') = (x - x') + (y - y')$ et $xy - x'y' = x(y - y') + y'(x - x')$ sont divisibles par D, ce qui prouve que le résultat modulo D de l'addition et la multiplication de deux entiers ne dépend que de leurs réductions modulo D ; en d'autres termes, l'addition et la multiplication passent au quotient. Par ailleurs, les identités à verifier pour prouver que $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est un anneau sont déjà vraies dans l'anneau $\mathbf{Z}$; elles le sont donc, a fortiori, dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

• $a \in \mathbf{Z}$ est inversible (pour la multiplication) dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ si et seulement si a est premier à D. On note $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$ l'ensemble des éléments inversibles ; c'est un groupe dont le cardinal est traditionnellement noté $\varphi(\mathrm{D})$, et la fonction φ est la *fonction indicatrice d'Euler*.

Si a est premier à D, il existe, d'après le théorème de Bézout, $u, v \in \mathbf{Z}$ tels que $au + \mathrm{D}v = 1$, ce qui prouve que a est inversible dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, d'inverse u. Réciproquement, si $ab = 1$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, cela signifie que $ab - 1$ est divisible par D, et donc qu'il existe $v \in \mathbf{Z}$ tel que $ab + \mathrm{D}v = 1$; d'après le théorème de Bézout, cela implique que a et D sont premiers entre eux, ce qui permet de conclure.

• D est premier si et seulement si $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est un corps.

L'anneau $\{0\}$ n'est pas un corps (si K est corps, $\mathrm{K} - \{0\}$ est un groupe pour la multiplication et donc est non vide) et 1 n'est pas un nombre premier ; on peut donc supposer $\mathrm{D} \geqslant 2$.

Si $\mathrm{D} \geqslant 2$ n'est pas premier, on peut le factoriser sous la forme $\mathrm{D} = ab$, avec $a \in \{2, \ldots, \mathrm{D}-1\}$ et $b \in \{2, \ldots, \mathrm{D}-1\}$. Donc a et b ne sont pas nuls dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ alors que $ab = \mathrm{D} = 0$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$; l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ admet donc des diviseurs de 0 et n'est pas un corps.

Si D est premier, et si a n'est pas divisible par D, alors a est premier à D et donc inversible dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ d'après le point précédent. Ceci permet de conclure.

Un nombre premier a tendance à être noté p, et si on veut insister sur le fait que $\mathbf{Z}/p\mathbf{Z}$ est un corps, on le note $\mathbf{F}_p$. Par exemple, on parlera d'espaces vectoriels sur $\mathbf{F}_2$ au lieu

[10] La manière qui est probablement la plus efficace pour penser à l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est de le voir comme étant l'anneau $\mathbf{Z}$ auquel on a rajouté la relation $\mathrm{D} = 0$; on fait donc les additions et les multiplications comme si on était dans $\mathbf{Z}$, mais on se permet d'enlever le multiple de D que l'on veut au résultat. Par exemple, dans $\mathbf{Z}/21\mathbf{Z}$, on a $6 \times 14 = 4 \times 21 = 0$ et $4 \times 16 = 1 + 3 \times 21 = 1$, ce qui montre que 6 et 14 sont des diviseurs de 0, alors que 4 est inversible, d'inverse 16

d'espaces vectoriels sur $\mathbf{Z}/2\mathbf{Z}$ pour parler des objets qui peuplent Internet[11] et dans lesquels vivent les codes correcteurs d'erreurs.

• Tout corps de cardinal p est isomorphe à $\mathbf{F}_p$; autrement dit $\mathbf{F}_p$ est *le corps à p éléments*[12].

Soit K un corps à p élément. On dispose d'un morphisme d'anneaux $f : \mathbf{Z} \to \mathrm{K}$ envoyant 1 sur 1. Ce morphisme d'anneaux est en particulier un morphisme de groupes additifs. Son image est donc un sous-groupe du groupe $(\mathrm{K}, +)$, et son cardinal est un diviseur de $|\mathrm{K}| = p$, d'après le théorème de Lagrange, et comme cette image a au moins deux éléments, à savoir 0 et 1, c'est K tout entier. On en déduit que f induit un isomorphisme de $\mathbf{Z}/\mathrm{Ker}\, f$ sur K, et comme $|\mathrm{K}| = p$, on a $\mathrm{Ker}\, f = p\mathbf{Z}$, et donc $\mathrm{K} \cong \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. Ceci permet de conclure.

• Si D' est un diviseur de D, alors l'application naturelle $\mathbf{Z} \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$ se factorise à travers une application naturelle $(\mathbf{Z}/\mathrm{D}\mathbf{Z}) \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$ qui est un morphisme d'anneaux.

Si D' est un diviseur de D, alors un multiple de D est aussi un multiple de D'. On en déduit que, si $a \equiv b \bmod \mathrm{D}$, alors $a \equiv b \bmod \mathrm{D}$; autrement dit l'application naturelle $\mathbf{Z} \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$ se factorise à travers une application naturelle $(\mathbf{Z}/\mathrm{D}\mathbf{Z}) \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$. On obtient un morphisme d'anneaux car les identités à vérifier sont déjà valables en remontant à $\mathbf{Z}$.

• Si a et b sont premiers entre eux, l'application naturelle $\mathbf{Z}/ab\mathbf{Z} \to (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est un isomorphisme d'anneaux qui induit un isomorphisme de groupes de $(\mathbf{Z}/ab\mathbf{Z})^*$ sur $(\mathbf{Z}/a\mathbf{Z})^* \times (\mathbf{Z}/b\mathbf{Z})^*$ (théorème des restes chinois).

L'application naturelle $\mathbf{Z}/ab\mathbf{Z} \to (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est un morphisme d'anneaux d'après le point précédent. Il est injectif car, si $x \in \mathbf{Z}$ a une réduction modulo ab qui est dans le noyau, c'est que x est divisible par a et par b, et donc par ab puisqu'on a supposé a et b premiers entre eux ; autrement dit, le noyau est réduit à 0. Comme les deux ensembles considérés ont même cardinal ab, une application injective est aussi bijective, ce qui montre que $\mathbf{Z}/ab\mathbf{Z} \to (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est un isomorphisme. On conclut en remarquant que si A et B sont deux anneaux, alors $(\mathrm{A} \times \mathrm{B})^* = \mathrm{A}^* \times \mathrm{B}^*$.

En fait, on peut décrire explicitement l'isomorphisme inverse. Comme a et b sont premiers entre eux, il existe $u, v \in \mathbf{Z}$ tels que $1 = au + bv$. Si $(x, y) \in (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$, et si $\tilde{x}, \tilde{y} \in \mathbf{Z}$ ont pour image x et y dans $\mathbf{Z}/a\mathbf{Z}$ et $\mathbf{Z}/b\mathbf{Z}$ respectivement, alors l'image de $bv\tilde{x} + au\tilde{y}$ dans $\mathbf{Z}/ab\mathbf{Z}$ ne dépend pas des choix de $\tilde{x}$ et $\tilde{y}$ et s'envoie sur (x, y) dans $(\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$, comme le montre un petit calcul immédiat. On remarque que $x \mapsto bv\tilde{x}$ induit un isomorphisme de

[11] Internet aime beaucoup $\mathbf{Z}/\mathrm{D}\mathbf{Z}$. Non content de faire voyager des milliards de $\mathbf{F}_2$-espaces vectoriels, Internet est très gourmand de grands nombres premiers, par exemple pour le système RSA de sécurité à clé publique (1977). Ce système et la fabrication de grands nombres premiers reposent sur l'arithmétique dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ qui s'avère être nettement plus subtile que ce que l'on pourrait attendre d'un objet aussi petit.

[12] Plus généralement, si q est une puissance d'un nombre premier, il y a, à isomorphisme près, un unique corps à q élément, et ce corps est noté $\mathbf{F}_q$. On a beaucoup fantasmé ces dernières années autour du corps $\mathbf{F}_1$ « à 1 élément » dont on voit la trace dans plusieurs phénomènes sans comprendre quel genre d'objet cela pourrait bien être (pas l'anneau $\{0\}$ en tout cas). Certains y voient la clef d'une démonstration de l'hypothèse de Riemann.

$\mathbf{Z}/a\mathbf{Z}$ sur le sous-groupe $b\mathbf{Z}/ab\mathbf{Z}$ de $\mathbf{Z}/ab\mathbf{Z}$ et que $y \mapsto au\tilde{y}$ induit un isomorphisme de $\mathbf{Z}/b\mathbf{Z}$ sur le sous-groupe $a\mathbf{Z}/ab\mathbf{Z}$ de $\mathbf{Z}/ab\mathbf{Z}$. On en déduit le résultat suivant :

• Si a et b sont premiers entre eux, alors $\mathbf{Z}/ab\mathbf{Z}$ est la somme directe de ses sous-groupes $b\mathbf{Z}/ab\mathbf{Z}$ et $a\mathbf{Z}/ab\mathbf{Z}$; de plus, on a des isomorphismes de groupes additifs $b\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/a\mathbf{Z}$ et $a\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/b\mathbf{Z}$, et donc $\mathbf{Z}/ab\mathbf{Z}$ est isomorphe à $(\mathbf{Z}/a\mathbf{Z}) \oplus (\mathbf{Z}/b\mathbf{Z})$, comme groupe additif.

Exercice 2.1. — Montrer que si $a \neq 0$ et $b \neq 0$ ne sont pas premiers entre eux, les groupes additifs $\mathbf{Z}/ab\mathbf{Z}$ et $(\mathbf{Z}/a\mathbf{Z}) \oplus (\mathbf{Z}/b\mathbf{Z})$ ne sont pas isomorphes.

Exercice 2.2. — Résoudre les équations $4x + 3 = 0$, $14x + 2 = 0$ et $14x + 7 = 0$ dans $\mathbf{Z}/21\mathbf{Z}$.

Exercice 2.3. — Résoudre l'équation $x^2 + x + 1 = 0$ dans $\mathbf{Z}/91\mathbf{Z}$. (Comme 91 est relativement petit[13], on peut tester chaque élément de $\mathbf{Z}/91\mathbf{Z}$ et voir lesquels conviennent, mais c'est un peu fastidieux...)

Exercice 2.4. — (i) Soit $p \in \mathscr{P}$. Montrer que si $p \neq 3$, et si l'équation $x^2 + x + 1 = 0$ a une solution dans $\mathbf{F}_p$, alors elle en a deux.

(ii) (difficile) Montrer qu'il existe une infinité de nombres premiers p tels que l'équation $x^2 + x + 1 = 0$ ait deux solutions dans $\mathbf{F}_p$.

(iii) En déduire que quel que soit $\mathrm{M} > 0$, il existe $\mathrm{D} \in \mathbf{N}$ tel que $x^2 + x + 1 = 0$ ait plus de M solutions dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

Exercice 2.5. — Montrer que si $p \in \mathscr{P}$, alors $\mathbf{Z}/p^n\mathbf{Z}$ a $p^n - p^{n-1}$ éléments inversibles. En déduire que, si $\mathrm{D} \geqslant 2$, alors $\varphi(\mathrm{D}) = \mathrm{D} \cdot \prod_{p|\mathrm{D}}(1 - \frac{1}{p})$, où φ est la fonction indicatrice d'Euler.

2.4. Quotients d'espaces vectoriels

Soit E un espace vectoriel sur un corps K, soit R une relation d'équivalence sur E, et soit $\mathrm{F} \subset \mathrm{E}$ la classe d'équivalence de 0. Pour que la structure d'espace vectoriel de E passe au quotient, on doit en particulier avoir $\lambda x \in \mathrm{F}$ si $\lambda \in \mathrm{K}$ et $x \in \mathrm{F}$ (puisque $\lambda 0 = 0$ dans E/R) et $x + y \in \mathrm{F}$ si $x, y \in \mathrm{F}$ (puisque $0 + 0 = 0$ dans E/R) ; en d'autres termes, F

[13] Essayer de résoudre de la même manière l'équation $x^2 = 5$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, avec $\mathrm{D} = 2^{2802} - 2^{521} - 2^{2281} + 1$ est voué à l'échec, même avec l'aide d'un ordinateur. Par contre, en partant de $\mathrm{D} = (2^{521} - 1)(2^{2281} - 1)$, si on sait que $p_1 = 2^{521} - 1$ et $p_2 = 2^{2281} - 1$ sont premiers (ce sont des *nombres premiers de Mersenne* découverts par Robinson en 1952), alors on peut sans trop d'effort calculer le nombre de solutions de l'équation et, avec l'aide d'un ordinateur et d'algorithmes astucieux, calculer explicitement ces solutions. Le calcul du nombre de solutions repose sur la *loi de réciprocité quadratique* conjecturée par Euler en 1783 et démontrée par Gauss en 1801. Si p est un nombre premier, et si $a \in \mathbf{Z}$ n'est pas divisible par p, on pose $(\frac{a}{p}) = 1$, si a est un carré modulo p (i.e. si l'équation $x^2 = a$ a des solutions dans $\mathbf{F}_p$) et $(\frac{a}{p}) = -1$ si a n'est pas un carré modulo p (si l'équation $x^2 = a$ n'a pas de solutions dans $\mathbf{F}_p$). La loi de réciprocité quadratique s'énonce alors ainsi : *si p et q sont deux nombres premiers impairs distincts, alors* $(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}(\frac{p}{q})$. On applique ce qui précède à $p = p_1$ et $q = 5$. Comme $p_1 = 2^{521} - 1 = 2^{4 \cdot 130 + 1} - 1 = 2 \cdot (2^4)^{130} - 1 = 2 - 1 = 1$ dans $\mathbf{F}_5$, on a $(\frac{p_1}{5}) = 1$ et donc $(\frac{5}{p_1}) = 1$, d'après la loi de réciprocité quadratique. On en déduit que l'équation $x^2 = 5$ a deux solutions dans $\mathbf{F}_{p_1}$. Pour la même raison, elle en a aussi 2 dans $\mathbf{F}_{p_2}$ et donc 4 dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

doit être un sous-espace vectoriel de E. De plus, comme $a + 0 = a$ dans E/R, les classes d'équivalence doivent être de la forme $a + \mathrm{F}$.

Réciproquement, si F est un sous-espace vectoriel de E, la relation $\sim_{\mathrm{F}}$, définie sur E par $x \sim_{\mathrm{F}} y$ si et seulement si $x - y \in \mathrm{F}$, est une relation d'équivalence. Le quotient E/ $\sim_{\mathrm{F}}$ est traditionnellement noté E/F. Comme « $x - y \in \mathrm{F}$ »⇒ « $\lambda x - \lambda y \in \mathrm{F}$ » , et comme « $x - y \in \mathrm{F}$ et $x' - y' \in \mathrm{F}$ »⇒« $(x + x') - (y + y') \in \mathrm{F}$ », la structure d'espace vectoriel sur E passe au quotient.

Si $\mathrm{F}' \subset \mathrm{E}$ est un sous-espace vectoriel supplémentaire de F, les classes d'équivalence pour $\sim_{\mathrm{F}}$ sont les $a + \mathrm{F}$, pour $a \in \mathrm{F}'$, et l'application naturelle $\mathrm{F}' \to \mathrm{E/F}$ est un isomorphisme d'espaces vectoriels. En d'autres termes, *dans le cas des espaces vectoriels*, un quotient est toujours isomorphe à un sous-objet, mais il est très souvent nocif de remplacer, dans les raisonnements, un quotient par un sous-objet qui lui est isomorphe. Par exemple, si F est un sous-espace vectoriel d'un espace vectoriel E, le dual F^* de F (i.e. l'ensemble des formes linéaires de F dans K) est naturellement un quotient du dual E^* de E (on peut restreindre à F une forme linéaire sur E, et F^* est le quotient de E^* par le sous-espace des formes linéaires identiquement nulles sur F), et n'est pas, en général, un sous-espace de E^*, de manière naturelle.

• L'espace E/F vérifie la propriété universelle suivante : si $u : \mathrm{E} \to \mathrm{E}'$ est une application K-linéaire, et si $\operatorname{Ker} u$ contient F, alors u *se factorise à travers* E/F (i.e. il existe une unique application linéaire $\overline{u} : \mathrm{E/F} \to \mathrm{E}'$, telle que $u = \overline{u} \circ \pi$, où $\pi : \mathrm{E} \to \mathrm{E/F}$ est la projection canonique).

• Si $u : \mathrm{E} \to \mathrm{E}'$ est une application linéaire, alors u se factorise à travers $\mathrm{E}/\operatorname{Ker} u$, et l'application induite $\overline{u} : \mathrm{E}/\operatorname{Ker} u \to \operatorname{Im} u$ est un isomorphisme d'espaces vectoriels.

2.5. Anneaux quotients

Soit A un anneau commutatif (un anneau a toujours un élément unité 1), soit R une relation d'équivalence sur A, et soit $\mathrm{I} \subset \mathrm{E}$ la classe d'équivalence de 0. Pour que la structure d'anneau de A passe au quotient, on doit en particulier avoir $\lambda x \in \mathrm{I}$ si $\lambda \in \mathrm{A}$ et $x \in \mathrm{I}$ (puisque $\lambda 0 = 0$ dans A/R) et $x + y \in \mathrm{I}$ si $x, y \in \mathrm{I}$ (puisque $0 + 0 = 0$ dans A/R) ; un sous-ensemble de A vérifiant ces deux propriétés est un *idéal* de A. De plus, comme $a + 0 = a$ dans A/R, les classes d'équivalence doivent être de la forme $a + \mathrm{I}$.

Réciproquement, si I est un idéal de A, la relation $\sim_{\mathrm{I}}$, définie sur E par $x \sim_{\mathrm{I}} y$ si et seulement si $x - y \in \mathrm{I}$, est une relation d'équivalence. Le quotient A/ $\sim_{\mathrm{I}}$ est traditionnellement noté A/I. Comme « $x - y \in \mathrm{I}$ et $x' - y' \in \mathrm{I}$ »⇒« $(x + x') - (y + y') \in \mathrm{I}$ », et comme « $x - y \in \mathrm{I}$ et $x' - y' \in \mathrm{I}$ »⇒« $xx' - yy' = x(y - y') + y'(x - x') \in \mathrm{I}$ », la structure d'anneau sur A passe au quotient.

Contrairement à ce qui se passe dans le cas des espaces vectoriels, l'anneau A/I n'est pas, en général, isomorphe à un sous-anneau de A. Par exemple $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ n'est pas isomorphe à un sous-anneau de $\mathbf{Z}$, ni même à un sous-groupe additif.

• L'anneau A/I vérifie la propriété universelle suivante : si $f : \mathrm{A} \to \mathrm{A}'$ est un morphisme d'anneaux, et si $\operatorname{Ker} f$ contient I, alors f se factorise à travers A/I (i.e. il existe un unique morphisme d'anneaux $\overline{f} : \mathrm{A/I} \to \mathrm{A}'$, tel que $f = \overline{f} \circ \pi$, où $\pi : \mathrm{A} \to \mathrm{A/I}$ est la projection canonique).

• Si $f : \mathrm{A} \to \mathrm{A}'$ est un morphisme d'anneaux, alors $\mathrm{Ker}\, f$ est un idéal de A, f se factorise à travers $\mathrm{A}/\mathrm{Ker}\, f$ et l'application induite $\overline{f} : \mathrm{A}/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ est un isomorphisme d'anneaux.

Le lecteur connaît déjà beaucoup d'anneaux définis de cette manière. Par exemple :

– le corps des nombres complexes[14] $\mathbf{C} = \mathbf{R}[\mathrm{X}]/(\mathrm{X}^2+1)$ (prendre le quotient de $\mathbf{R}[\mathrm{X}]$ par l'idéal[15] (X^2+1) revient à rajouter à $\mathbf{R}$ un élément X vérifiant $\mathrm{X}^2+1=0$, et donc X devient une racine carrée de -1 dans le quotient) ;

– l'anneau $\mathbf{Z}[\mathrm{X}]/(10\mathrm{X}-1)$ des nombres décimaux (prendre le quotient de $\mathbf{Z}[\mathrm{X}]$ par $(10\mathrm{X}-1)$ revient à rajouter à $\mathbf{Z}$ un élément X vérifiant $10\mathrm{X}=1$, et $a_n\mathrm{X}^n+\cdots+a_0 \in \mathbf{Z}[\mathrm{X}]$ devient le nombre décimal $\frac{a_n}{10^n}+\cdots+\frac{a_1}{10}+a_0$) ;

– le corps $\mathbf{F}_p$, quotient de $\mathbf{Z}$ par l'idéal $p\mathbf{Z}$ (p étant un nombre premier) ;

– l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ quotient de $\mathbf{Z}$ par l'idéal $\mathrm{D}\mathbf{Z}$ (D entier quelconque).

On en rencontre beaucoup d'autres, par exemple les anneaux suivants.

– $\mathbf{Z}[\mathrm{X}]/(\mathrm{X}^2+1)$, anneau des *entiers de Gauss* ; en envoyant X sur i ou $-i$, cet anneau s'identifie au sous-anneau des $\{a+ib,\ a,b\in\mathbf{Z}\}$ de $\mathbf{C}$.

– $\mathbf{Z}[\mathrm{X}]/(\mathrm{X}^3-2)$. Il s'identifie à un sous-anneau de $\mathbf{C}$ de trois manières différentes : on peut envoyer X sur $\sqrt[3]{2}$, ou sur $e^{2i\pi/3}\sqrt[3]{2}$ ou sur $e^{4i\pi/3}\sqrt[3]{2}$. Dans le premier cas, l'image est un sous-anneau de $\mathbf{R}$, dans les autres cas, elle n'est pas incluse dans $\mathbf{R}$.

– L'anneau $\mathrm{K}[\varepsilon]/(\varepsilon^2)$ des *nombres duaux*, où K est un corps ; ε est alors l'analogue algébrique d'un infiniment petit [16].

– L'anneau $\mathbf{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{DY}^2-(\mathrm{X}^3-\mathrm{X}))$ des fonctions rationnelles sur la courbe algébrique $\mathrm{C_D}$ d'équation $\mathrm{DY}^2=\mathrm{X}^3-\mathrm{X}$ dans $\mathbf{C}^2$ (si $f\in\mathbf{C}[\mathrm{X},\mathrm{Y}]$, la restriction de f à $\mathrm{C_D}$ ne dépend que de l'image de f modulo l'idéal engendré par $\mathrm{P}(\mathrm{X},\mathrm{Y})=\mathrm{DY}^2-(\mathrm{X}^3-\mathrm{X})$, puisque P est identiquement nul sur $\mathrm{C_D}$).

Exercice 2.6. — Montrer que, si D' est un diviseur de D, alors $\mathbf{Z}/\mathrm{D}'\mathbf{Z}$ est le quotient de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ par l'idéal engendré par D'.

2.6. Groupes quotients

2.6.1. Groupe opérant sur un ensemble. — Soit G un groupe d'élément neutre 1, et soit X un ensemble. On dit que G *opère à gauche* sur X ou que l'on a une *action à gauche de* G *sur* X si on dispose d'une application $(g,x)\mapsto g\cdot x$ de $\mathrm{G}\times\mathrm{X}$ dans X telle que $1\cdot x=x$, quel que soit $x\in\mathrm{X}$, et $g\cdot(g'\cdot x)=gg'\cdot x$, quels que soient $g,g'\in\mathrm{G}$ et $x\in\mathrm{X}$. On remarquera que si $g\in\mathrm{G}$, alors $x\mapsto\sigma_g(x)=g\cdot x$ est une bijection de X dans X, la bijection réciproque étant $x\mapsto\sigma_{g^{-1}}(x)=g^{-1}\cdot x$, et que l'on a $\sigma_{gg'}=\sigma_g\circ\sigma_{g'}$, quels que soient $g,g'\in\mathrm{G}$. Définir

[14] Cette définition de $\mathbf{C}$ est due à Cauchy (1847).

[15] De manière générale, si A est un anneau, et si a est un élément de A, on note souvent (a) l'idéal de A engendré par A ; on a donc $(a)=a\mathrm{A}$.

[16] On peut difficilement faire plus petit puisque $\varepsilon\neq 0$, alors que $\varepsilon^2=0$; si $\mathrm{P}\in\mathrm{K}[\mathrm{X}]$ est un polynôme, on a $\mathrm{P}(\mathrm{X}+\varepsilon)=\mathrm{P}(\mathrm{X})+\mathrm{P}'(\mathrm{X})\varepsilon$ dans $\mathrm{K}[\varepsilon]/(\varepsilon^2)$, comme le montre la formule de Taylor pour les polynômes. Peut-on rêver de développements limités plus sympathiques ?

une action de G sur X revient donc à se donner un morphisme de G dans le groupe des *permutations* de X (i.e. les bijections de X dans X) muni de la composition.

On dit que G *opère à droite* sur X si on a une application $(g,x) \mapsto x \star g$ de $\mathrm{G} \times \mathrm{X}$ dans X telle que $x \star 1 = x$, quel que soit $x \in \mathrm{X}$, et $(x \star g) \star g' = x \star gg'$, quels que soient $g, g' \in \mathrm{G}$ et $x \in \mathrm{X}$. On peut toujours transformer une action à gauche en action à droite (et vice-versa), en posant $x \star g = g^{-1} \cdot x$.

Par exemple, si K est un corps commutatif, le groupe $\mathbf{GL}_n(\mathrm{K})$ opère naturellement (à gauche) sur beaucoup d'objets :
— par définition, il opère sur l'espace vectoriel K^n ;
— comme l'action est linéaire, elle transforme une droite vectorielle en droite vectorielle et donc $\mathbf{GL}_n(\mathrm{K})$ opère sur l'ensemble $\mathbf{P}^{n-1}(\mathrm{K})$ des droites vectorielles de K^n (*espace projectif* de dimension $n-1$ sur K) ;
— il opère sur l'ensemble $\mathbf{M}_n(\mathrm{K})$ des matrices $n \times n$ à coefficients dans K, par multiplication à gauche (i.e. $\mathrm{A} \cdot \mathrm{M} = \mathrm{AM}$), par multiplication à droite (i.e. $\mathrm{A} \cdot \mathrm{M} = \mathrm{MA}^{-1}$) et par similitude (i.e. $\mathrm{A} \cdot \mathrm{M} = \mathrm{AMA}^{-1}$, ce qui correspond à un changement de base).
— Il opère sur les ensembles des matrices symétriques et antisymétriques par $\mathrm{A} \cdot \mathrm{M} = \mathrm{AM}\,{}^t\mathrm{A}$,
— Le groupe $\mathbf{GL}_n(\mathbf{C})$ opère sur l'ensemble des matrices auto-adjointes (i.e. vérifiant ${}^t\mathrm{M} = \overline{\mathrm{M}}$) par $\mathrm{A} \cdot \mathrm{M} = \mathrm{AMA}^*$, avec $\mathrm{A}^* = {}^t\overline{\mathrm{A}}$.

Exercice 2.7. — Soit K un corps commutatif. On rajoute à K un élément ∞, et on étend l'arithmétique de K en posant $\frac{a}{0} = \infty$, si $a \neq 0$ (on ne donne pas de sens à $\frac{0}{0}$), et $\frac{a\infty+b}{c\infty+d} = \frac{a}{c}$, si $a \neq 0$ ou $c \neq 0$.

(i) Montrer que l'application qui à $v = (x,y) \in \mathrm{K}^2 - \{(0,0)\}$ associe $\lambda(v) = \frac{x}{y} \in \mathrm{K} \cup \{\infty\}$ induit une bijection de la droite projective $\mathbf{P}^1(\mathrm{K})$, ensemble des droites vectorielles de K^2, sur $\mathrm{K} \cup \{\infty\}$.

(ii) Montrer que l'action de $\mathbf{GL}_2(\mathrm{K})$ sur $\mathrm{K} \cup \{\infty\}$ qui s'en déduit est donnée par $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d}$.

Si G opère (à gauche ou à droite) sur X, et si $x \in \mathrm{X}$, un *translaté* de x est un point de X dans l'image de $\mathrm{G} \times \{x\}$, et *l'orbite* O_x de x est l'ensemble des translatés de X (i.e. l'image de $\mathrm{G} \times \{x\}$ dans X). Une *orbite* pour l'action de G est un sous-ensemble O de X de la forme O_x pour un certain $x \in \mathrm{X}$.

• La relation $\sim_{\mathrm{G}}$ définie sur X par « $x \sim_{\mathrm{G}} y$ si et seulement si il existe $g \in \mathrm{G}$ tel que $y = g \cdot x$ (si l'action est à gauche) ou $y = x \star g$ (si l'action est à droite) » est une relation d'équivalence sur X dont les classes d'équivalence sont les orbites.

On peut se contenter de traiter le cas d'une action à gauche. On a $x = 1 \cdot x$, et donc $\sim_{\mathrm{G}}$ est reflexive. Si $y = g \cdot x$, alors $x = g^{-1} \cdot y$, et donc $\sim_{\mathrm{G}}$ est symétrique. Enfin, si $y = g \cdot x$ et $z = h \cdot y$, alors $z = hg \cdot x$, et donc $\sim_{\mathrm{G}}$ est transitive. Cela prouve que $\sim_{\mathrm{G}}$ est une relation d'équivalence sur X. La classe d'équivalence de x est O_x par définition de O_x, ce qui prouve que les classes d'équivalence sont les orbites.

L'espace quotient $\mathrm{X}/\sim_{\mathrm{G}}$, ensemble des orbites, est traditionnellement noté $\mathrm{G}\backslash\mathrm{X}$ si l'action est à gauche, et X/G si l'action est à droite. Un système de représentants de $\mathrm{G}\backslash\mathrm{X}$ ou X/G dans X est parfois appelé un *domaine fondamental*.

• Si $x \in \mathrm{X}$, l'ensemble G_x des $g \in \mathrm{G}$ fixant x (i.e. $g \cdot x = x$) est un sous-groupe de G, appelé *stabilisateur* de x.

Comme $1 \cdot x = x$, on a $1 \in \mathrm{G}_x$. Si $g \cdot x = x$, alors $x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, et donc G_x est stable par passage à l'inverse. Enfin, si $g \cdot x = x$ et $h \cdot x$, alors $gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, ce qui prouve que G_x est stable par la loi de groupe de G, et donc est un sous-groupe de G.

On fabrique des tas de groupes intéressants en considérant les stabilisateurs d'éléments d'ensembles munis d'actions de groupes.
— Si M est une matrice symétrique, le stabilisateur de M dans $\mathbf{GL}_n(\mathrm{K})$ pour l'action $\mathrm{A} \cdot \mathrm{M} = \mathrm{AM}\,{}^t\mathrm{A}$ est le *groupe orthogonal* associé à M ; si $\mathrm{M} = \mathrm{I}_n$, ce groupe est noté $\mathbf{O}_n(\mathrm{K})$. Si $\mathrm{K} = \mathbf{R}$, si $p + q = n$, et si M est la matrice diagonale avec p fois 1 et q fois -1 sur la diagonale, le groupe obtenu est noté $\mathbf{O}(p, q)$; en particulier $\mathbf{O}(n) = \mathbf{O}_n(\mathbf{R})$.
— Si M est une matrice antisymétrique, le stabilisateur de M dans $\mathbf{GL}_n(\mathrm{K})$ pour l'action $\mathrm{A} \cdot \mathrm{M} = \mathrm{AM}\,{}^t\mathrm{A}$ est le *groupe symplectique* associé à M ; si $n = 2m$ est pair, et si M est la matrice par bloc $\left(\begin{smallmatrix} 0 & \mathrm{I}_m \\ -\mathrm{I}_m & 0 \end{smallmatrix}\right)$, ce groupe est noté $\mathbf{Sp}_n(\mathrm{K})$.
— Le stabilisateur de I_n pour l'action $\mathrm{A} \cdot \mathrm{M} = \mathrm{AMA}^*$ de $\mathbf{GL}_n(\mathbf{C})$ est le *groupe unitaire* $\mathbf{U}(n)$.

Exercice 2.8. — Montrer que, si $y = g \cdot x$, alors $\mathrm{G}_y = g\mathrm{G}_x g^{-1} = \{gxg^{-1},\ x \in \mathrm{G}_x\}$. En déduire que, si G est fini, le cardinal du stabilisateur est constant dans chaque orbite.

Exercice 2.9. — (i) Montrer que le groupe D_4 des isométries du carré de sommets $\mathrm{A} = (1, 1)$, $\mathrm{B} = (-1, 1)$, $\mathrm{C} = (-1, -1)$ et $\mathrm{D} = (1, -1)$ est un groupe d'ordre 8, et expliciter ses éléments.

(ii) Soit $\mathrm{O} = (0, 0)$, et soit $\mathrm{S} = \{\mathrm{O}, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}\}$. Montrer que S est stable sous l'action de D_4, et déterminer les orbites sous l'action de D_4, ainsi que le stabilisateur d'un des éléments de chaque orbite.

(iii) Soit T l'ensemble des paires d'éléments distincts de S. Déterminer les orbites de T sous l'action de D_4, ainsi que le stabilisateur d'un élément de chaque orbite.

(iv) Quel lien y a-t-il entre le cardinal d'une orbite et celui du stabilisateur dans tous les cas ci-dessus ?

2.6.2. Classes de conjugaison

• Si G est un groupe, alors $(g, x) \mapsto g \cdot x = gxg^{-1}$ est une action (à gauche) de G sur lui-même.

Si $g, h, x \in \mathrm{G}$, alors $gh \cdot x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g \cdot (hxh^{-1}) = g \cdot (h \cdot x)$.

L'action de G sur lui-même ainsi définie est l'action *par conjugaison*. L'orbite de $x \in \mathrm{G}$ est alors la *classe de conjugaison de* x, les éléments de la classe de conjugaison de x sont dits *conjugués à* x (et donc x et y *sont conjugués* dans G s'il existe $h \in \mathrm{G}$ tel que $y = hxh^{-1}$), et l'ensemble $\mathrm{Conj}(\mathrm{G})$ des orbites est *l'ensemble des classes de conjugaison de* G. Le stabilisateur Z_x de x pour cette action est appelé le *centralisateur* de x ; c'est l'ensemble des $g \in \mathrm{G}$ qui commutent à x.

• G est commutatif si et seulement si les classes de conjugaison sont réduites à un élément.

La classe de conjugaison de $x \in \mathrm{G}$ est l'ensemble des gxg^{-1}, pour $g \in \mathrm{G}$. Comme elle contient x, elle est réduite à un élément si et seulement si $gxg^{-1} = x$, quel que soit $g \in \mathrm{G}$, et donc si et seulement si x commute à tous les éléments de G. Ceci permet de conclure.

• Le *centre* Z de G est l'ensemble des $x \in \mathrm{G}$ commutant à tout élément de G ; c'est aussi l'ensemble des $x \in \mathrm{G}$ dont la classe de conjugaison est réduite à un point, et c'est un sous-groupe de G.

Si $xg = gx$ et $yg = gy$ quel que soit $g \in \mathrm{G}$, alors $xyg = xgy = gxy$, ce qui montre que xy commute à tous les éléments de G et donc que Z est stable par la loi de groupe. De même, si $xg = gx$ quel que soit $g \in \mathrm{G}$, alors $gx^{-1} = x^{-1}xgx^{-1} = x^{-1}gxx^{-1} = x^{-1}g$, ce qui prouve que Z est stable par passage à l'inverse. Comme il contient l'élément neutre ; c'est un sous-groupe de G. Le reste ayant été démontré ci-dessus, cela permet de conclure.

Exercice 2.10. — (i) Soient X un ensemble et G un groupe opérant sur X. Si $g \in \mathrm{G}$, on note X_g l'ensemble $\{x \in \mathrm{X},\ g \cdot x = x\}$ des points fixes de g.

(a) Si $g, h \in \mathrm{G}$, quel lien y a-t-il entre les points fixes de g et ceux de hgh^{-1} ?

(b) Montrer que si X est fini et si g, g' sont conjugués dans G, alors ils ont le même nombre de points fixes.

(ii) Soient V un espace vectoriel sur un corps K et G un groupe. On dit que G *opère linéairement* sur V si G opère sur V et si $v \mapsto g \cdot v$ est une application linéaire de V dans V, pour tout $g \in \mathrm{G}$ (on dit alors que V est une *représentation* de G).

(a) Montrer que, si c'est le cas et si $g \in \mathrm{G}$, l'ensemble des points fixes de g est un sous-espace espace vectoriel de V.

(b) Montrer que, si V est de dimension finie et si g, g' sont conjugués dans G, alors leurs points fixes sont des espaces vectoriels de même dimension.

2.6.3. Quotients de groupes. — Si G est un groupe, et si H est un sous-groupe de G, on peut utiliser la multiplication dans G pour faire agir H sur G à gauche ($h \cdot x = hx$) et à droite ($x \star h = xh$). Une classe à gauche est alors de la forme $\mathrm{H}x = \{hx,\ h \in \mathrm{H}\}$, pour $x \in \mathrm{G}$, et une classe à droite, de la forme $x\mathrm{H} = \{xh,\ h \in \mathrm{H}\}$, pour $x \in \mathrm{G}$. Les quotients H\G (à gauche) et G/H (à droite) de G par H ne sont, en général, pas des groupes, mais la multiplication dans G les munit d'actions de G (à droite pour H\G et à gauche pour G/H). Réciproquement, si R est une relation d'équivalence sur G telle que la multiplication dans G induise une action à gauche (resp. à droite) de G sur G/R, et si H est la classe d'équivalence de e, alors H est un sous-groupe de G et G/R = G/H (resp. G/R = H\G).

• Si G opère (à gauche) sur un ensemble X, si $x \in \mathrm{X}$, et si G_x est le stabilisateur de x dans G, alors $g \mapsto g \cdot x$ induit un isomorphisme de G/G_x sur l'orbite O_x de x (c'est un isomorphisme de G-*ensembles*, i.e. d'ensembles munis d'une action de G).

Commençons par remarquer que, si g_1, g_2 ont même image dans G/G_x, alors il existe $h \in \mathrm{G}_x$ tel que $g_2 = g_1 h$, ce qui implique que $g_2 \cdot x = (g_1 h) \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x$; l'application $g \mapsto g \cdot x$ passe donc au quotient et nous définit une application $\iota : \mathrm{G}/\mathrm{G}_x \to \mathrm{O}_x$ qui est surjective par définition de O_x. Maintenant, si $g_1 \cdot x = g_2 \cdot x$, alors $g_2^{-1} g_1 \cdot x = x$ et donc $g_2^{-1} g_1 \in \mathrm{G}_x$; on en déduit que $g_1 \in g_2 \mathrm{G}_x$ et donc que g_1 et g_2 ont même image dans G/G_x, ce qui prouve que ι est injective et donc bijective. Enfin, si $h \in \mathrm{G}$ et $g \in \mathrm{G}/\mathrm{G}_x$, alors $h \cdot \iota(g) = h \cdot (g \cdot x) = hg \cdot x = \iota(hg)$, ce qui prouve que ι commute à l'action de G et donc est un morphisme de G-ensembles.

• La classe de conjugaison de x est isomorphe à G/Z_x, où Z_x est le centralisateur de x.

C'est un cas particulier du point précédent.

Pour que la structure de groupe de G passe au quotient G/H, il faut et il suffit que, quels que soient $x, x' \in \mathrm{G}$ et $h, h' \in \mathrm{H}$, on puisse trouver $h'' \in \mathrm{H}$ tel que $xhx'h' = xx'h''$.

Comme $h''(h')^{-1} = (x')^{-1}hx'$, on voit que la condition précédente est équivalente à ce que H soit laissé stable par la conjugaison $h \mapsto ghg^{-1}$, quel que soit $g \in \mathrm{G}$. Si tel est le cas on dit que H est *distingué* (*normal* en "franglais") dans G.

Un *groupe simple* est un groupe dont les seuls sous-groupes distingués sont $\{1\}$ et le groupe lui-même.

• Le groupe G/H vérifie la propriété universelle suivante : si $f : \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, et si $\mathrm{Ker}\, f$ contient H, alors f se factorise à travers G/H (i.e. il existe un unique morphisme de groupes $\overline{f} : \mathrm{G/H} \to \mathrm{G}'$, tel que $f = \overline{f} \circ \pi$, où $\pi : \mathrm{G} \to \mathrm{G/H}$ est la projection canonique).

• Si $u : \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, alors $\mathrm{Ker}\, u$ est distingué dans G et u se factorise à travers $\mathrm{G/Ker}\, u$ et induit un isomorphisme de groupes de $\mathrm{G/Ker}\, u$ sur $\mathrm{Im}\, u$. Si G est simple, alors u est soit injectif soit trivial ($u(g) = 1$, quel que soit $g \in \mathrm{G}$).

3. Groupes finis

3.1. Généralités sur les groupes

Un *groupe* G est un ensemble non vide, muni d'une loi $(g, h) \to gh$ de $\mathrm{G} \times \mathrm{G} \to \mathrm{G}$ qui est *associative* (i.e $(g_1g_2)g_3 = g_1(g_2g_3)$, quels que soient $g_1, g_2, g_3 \in \mathrm{G}$), possède un *élément neutre* (i.e. il existe $e \in \mathrm{G}$ tel que $eg = ge = g$, pour tout $g \in \mathrm{G}$), et telle que tout élément g admet un *inverse* (i.e. il existe $g^{-1} \in \mathrm{G}$ tel que $gg^{-1} = g^{-1}g = e$).

Un groupe G est *commutatif* ou *abélien* si $gh = hg$ quels que soient $g, h \in \mathrm{G}$. La loi de groupe d'un groupe commutatif est souvent notée $+$, auquel cas l'élément neutre est noté 0 et l'inverse de $x \in \mathrm{G}$ est noté $-x$ et appelé *l'opposé* de x. Une loi notée $+$ ou $\oplus$ ou $\boxplus$ est implicitement commutative, à moins que l'auteur n'ait vraiment décidé de rendre son texte illisible. Si la loi de groupe est notée multiplicativement, l'élément neutre de G est en général noté 1 au lieu de e ; s'il s'agit d'un groupe de bijections d'un ensemble X, l'élément neutre est l'identité de X, et est souvent noté id.

Si G est un groupe d'élément neutre 1, si $x \in \mathrm{G}$, on définit x^n, pour $n \in \mathbf{Z}$, en posant $x^0 = 1$, et $x^{n+1} = x^n x$, si $n \in \mathbf{N}$, et $x^n = (x^{-1})^{-n}$, si $n \leqslant 0$. Si G est commutatif et si la loi est notée $+$, l'élément x^n est noté nx, et on a $0x = 0$ et $(-1)x = -x$. On vérifie facilement que si $n \in \mathbf{Z}$, alors $x^{n+1} = x^n x$ et $x^{n-1} = x^n x^{-1}$, ce qui permet de montrer, par récurrence sur m, que $x^{m+n} = x^m x^n$ quels que soient $m, n \in \mathbf{N}$. Autrement dit, $n \mapsto x^n$ *est un morphisme de groupes de* $\mathbf{Z}$ *dans* G.

Si x et y commutent, on a $(xy)^n = x^n y^n$, mais s'ils ne commutent pas, c'est en général faux (et si $n = 2$ ou si $n = -1$, cela n'est vrai que si x et y commutent).

Un *sous-groupe* H d'un groupe G est une partie de H qui contient l'élément neutre, est stable par la loi de groupe ($h_1, h_2 \in \mathrm{H} \Rightarrow h_1h_2 \in \mathrm{H}$) et par passage à l'inverse ($h \in \mathrm{H} \Rightarrow h^{-1} \in \mathrm{H}$) ; c'est donc un groupe pour la loi induite par celle de G.

Si les $(\mathrm{H}_i)_{i\in\mathrm{I}}$ sont des sous-groupes d'un groupe G, alors $\cap_{i\in\mathrm{I}}\mathrm{H}_i$ est un sous-groupe de G. Ceci permet de définir le *sous-groupe* $\langle\mathrm{X}\rangle$ *de* G *engendré* par une partie X de G comme étant l'intersection de tous les sous-groupes de G qui la contiennent. Par exemple, si $x \in \mathrm{G}$, le sous-groupe $\langle x\rangle$ engendré par x est l'ensemble des x^n, pour $n \in \mathbf{Z}$.

En effet, d'une part un sous-groupe qui contient x contient x^n, pour $n \in \mathbf{N}$, comme le montre une récurrence immédiate, et comme il contient x^{-1}, il contient aussi x^n, pour $n \leqslant 0$; d'autre part, l'ensemble des x^n, pour $n \in \mathbf{Z}$, est un groupe qui contient x, puisque c'est l'image de $\mathbf{Z}$ par le morphisme $x \mapsto x^n$.

3.2. Groupes cycliques

3.2.1. Structure des groupes cycliques, ordre d'un élément

Un groupe est *cyclique* s'il peut être engendré par un seul élément. Autrement dit, G est cyclique, s'il existe $x \in \mathrm{G}$ tel que le morphisme $x \mapsto x^n$ de $\mathbf{Z}$ dans G soit surjectif. Si G est cyclique, un *générateur* de G est un élément x de G tel que le morphisme $x \mapsto x^n$ de $\mathbf{Z}$ dans G soit surjectif.

• Le groupe $\mathbf{Z}$ est cyclique, et il admet deux générateurs 1 et -1. Si $\mathrm{D} \geqslant 1$, le groupe $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est cyclique et les générateurs de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ sont les éléments de $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$, c'est-à-dire les (réductions modulo D des) entiers premiers à D.

L'énoncé concernant $\mathbf{Z}$ est immédiat. Il est aussi immédiat que $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est cyclique et que 1 en est un générateur. Maintenant, si $a \in \mathbf{Z}/\mathrm{D}\mathbf{Z}$ en est un générateur, alors il existe en particulier $b \in \mathbf{Z}$ tel que $ba = 1$, ce qui fait que la réduction modulo D de b est un inverse de a, et donc que a est inversible. Réciproquement, si a est inversible, alors $n \mapsto na$ est bijectif de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ et donc $n \mapsto na$ est surjectif de $\mathbf{Z}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, ce qui prouve que a est un générateur de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

• Le groupe $\boldsymbol{\mu}_\mathrm{D}$ des racines D-ièmes de l'unité dans $\mathbf{C}$ est cyclique, engendré par $e^{2i\pi/\mathrm{D}}$, et $n \mapsto e^{2i\pi\, n/\mathrm{D}}$ induit un isomorphisme de groupes $\mathbf{Z}/\mathrm{D}\mathbf{Z} \cong \boldsymbol{\mu}_\mathrm{D}$. Un générateur de $\boldsymbol{\mu}_\mathrm{D}$ est une *racine primitive* D*-ième de l'unité*, et les racines primitives D-ièmes de l'unité sont, d'après le point précédent, les racines de la forme $e^{2i\pi\, a/\mathrm{D}}$, pour a premier à D.

• Un groupe cyclique infini est isomorphe à $\mathbf{Z}$; un groupe cyclique de cardinal D est isomorphe[(17)] à $\mathbf{Z}/\mathrm{D}\mathbf{Z}$. En particulier, un groupe cyclique est commutatif.

[(17)] Un groupe cyclique est donc un objet parfaitement ennuyeux d'un point de vue théorique. La situation est, en pratique, assez différente : il est très difficile, étant donné un groupe cyclique G de cardinal N très grand ($\sim 10^{100}$), un générateur g de G et $x \in \mathrm{G}$, de déterminer l'élément n de $\mathbf{Z}/\mathrm{N}\mathbf{Z}$ tel que $x = g^n$ (problème du *logarithme discret*), alors que calculer g^n se fait sans problème. Ceci est à la base des signatures électroniques : G, N et g sont publics et on attribue à chaque personne P un code $n(\mathrm{P}) \in \mathbf{Z}/\mathrm{N}\mathbf{Z}$ (tenu secret), à partir duquel P fabrique une signature publique $s(\mathrm{P}) = g^{n(\mathrm{P})}$. Deux personnes P et Q peuvent s'assurer de leur identité mutuelle de la manière suivante : P calcule $s(\mathrm{Q})^{n(\mathrm{P})}$ et Q calcule $s(\mathrm{P})^{n(\mathrm{Q})}$, chacun de son côté ; si les résultats sont les mêmes (à savoir $g^{n(\mathrm{P})n(\mathrm{Q})}$), alors P et Q sont bien P et Q (sinon, cela veut dire que quelqu'un a réussi à retrouver le code de l'un des deux à partir de sa signature publique, ce qui est réputé être impossible). Les groupes cycliques utilisés sont en général construits à partir de courbes elliptiques sur les corps finis.

Soit G un groupe cyclique, et soit x un générateur de G. Alors $f : \mathbf{Z} \to \mathrm{G}$ défini par $f(n) = x^n$ est un morphisme surjectif, et il y a deux cas :
— f est injectif et alors G est isomorphe à $\mathbf{Z}$;
— le noyau de f est non nul et donc de la forme $\mathrm{D}\mathbf{Z}$, avec $\mathrm{D} \geqslant 1$, puisque c'est un sous-groupe de $\mathbf{Z}$; alors f se factorise à travers $\overline{f} : \mathbf{Z}/\mathrm{D}\mathbf{Z} \to \mathrm{G}$, et $\overline{f}$ est surjectif puisque f l'est et injectif puisqu'on a factorisé modulo $\mathrm{Ker}\, f$; autrement dit $\overline{f}$ est un isomorphisme de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ sur G et, en particulier, G et $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ ont même cardinal.

Ceci permet de conclure.

• Si G est un groupe quelconque et $x \in \mathrm{G}$, le sous-groupe $\langle x \rangle$ de G engendré par x est cyclique par définition. On définit *l'ordre de* x comme le cardinal du groupe $\langle x \rangle$. Si x est d'ordre D, le noyau du morphisme $n \to x^n$ de $\mathbf{Z}$ dans G est $\mathrm{D}\mathbf{Z}$ d'après ce qui précède, ce qui fait que *l'ordre de* x *est aussi le plus petit entier* $n > 0$ *tel que* x^n *soit égal à l'élément neutre.*

3.2.2. Sous-groupes des groupes cycliques

• Si $\mathrm{D} \geqslant 1$, l'application $d \mapsto d\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est une bijection de l'ensemble des diviseurs de D sur celui des sous-groupes de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

Si G est un sous-groupe de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, on peut considérer son image inverse dans $\mathbf{Z}$, qui est un sous-groupe de $\mathbf{Z}$ contenant $\mathrm{D}\mathbf{Z}$; on obtient ainsi une bijection de l'ensemble des sous-groupes de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dans celui des sous-groupes de $\mathbf{Z}$ contenant $\mathrm{D}\mathbf{Z}$, la bijection inverse étant $\tilde{\mathrm{G}} \to \tilde{\mathrm{G}}/\mathrm{D}\mathbf{Z}$. Comme un sous-groupe de $\mathbf{Z}$ contenant $\mathrm{D}\mathbf{Z}$ est de la forme $d\mathbf{Z}$, avec d diviseur de D, cela permet de conclure.

• Si G est un groupe cyclique, tous les sous-groupes de G sont cycliques, et si G est de cardinal D, alors G admet exactement un sous-groupe de cardinal D′, pour tout diviseur D′ de D.

Si G est infini, alors G est isomorphe à $\mathbf{Z}$, et tous les sous-groupes non nuls de G sont isomorphes à $\mathbf{Z}$, et donc cycliques.

Si G est fini de cardinal D, alors G est isomorphe à $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, et on sait que les sous-groupes de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ sont de la forme $d\mathbf{Z}/\mathrm{D}\mathbf{Z}$, pour d diviseur de D. Or $n \mapsto dn$ induit une surjection de $\mathbf{Z}$ sur $d\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dont le noyau est $\mathrm{D}'\mathbf{Z}$, où $\mathrm{D}' = \mathrm{D}/d$, ce qui montre que $d\mathbf{Z}/\mathrm{D}\mathbf{Z} \cong \mathbf{Z}/\mathrm{D}'\mathbf{Z}$. Comme $d \mapsto \mathrm{D}' = \mathrm{D}/d$ est une permutation de l'ensemble des diviseurs de D, cela permet de conclure.

3.3. Groupes abéliens finis

Soit $\mathscr{P}$ l'ensemble des nombres premiers. D'après le théorème des restes chinois, si $\mathrm{D} \in \mathbf{N} - \{0\}$, alors $\mathbf{Z}/\mathrm{D}\mathbf{Z} \cong \oplus_{p \in \mathscr{P}} (\mathbf{Z}/p^{v_p(\mathrm{D})}\mathbf{Z})$. La somme ci-dessus est en fait une somme finie car $v_p(\mathrm{D}) = 0$, sauf pour un nombre fini de nombres premiers. Ce résultat se généralise à tous les groupes abéliens finis sous la forme (cf. n° 4.3 du § 4 pour la démonstration).

Théorème 3.1. — (Kronecker, 1867) *Soit* G *un groupe abélien fini et, si* $p \in \mathscr{P}$*, soit* G_p *l'ensemble des éléments de* G *d'ordre une puissance de* p*.*

(i) G_p *est un sous-groupe de* G*, nul pour presque tout* p*, et* $\mathrm{G} = \oplus_{p \in \mathscr{P}} \mathrm{G}_p$*.*

(ii) *Si $p \in \mathscr{P}$, il existe une suite finie d'entiers $a_{p,i} \geqslant 1$, décroissante et uniquement déterminée, telle que l'on ait* $\mathrm{G}_p \cong \oplus_i (\mathbf{Z}/p^{a_{p,i}}\mathbf{Z})$.

Remarque 3.2. — Avec les notations du théorème, on a $|\mathrm{G}| = \prod_p \prod_i p^{a_i}$, et donc $|\mathrm{G}|$ est un multiple de p^{a_i}, pour tous p et i, ce qui prouve que la multiplication par $|\mathrm{G}|$ annule tout élément de G, puisqu'elle annule tous les $\mathbf{Z}/p^{a_{p,i}}\mathbf{Z}$. Autrement dit, dans un groupe commutatif, l'ordre d'un élément divise l'ordre du groupe (cas particulier du théorème de Lagrange).

Exercice 3.3. — Décomposer $(\mathbf{Z}/108\mathbf{Z})^*$ et $(\mathbf{Z}/200\mathbf{Z})^*$ sous la forme ci-dessus.

Exercice 3.4. — (i) Soit K un corps fini commutatif[18]. Montrer que le groupe K^* est cyclique (on pourra considérer le nombre de solutions de l'équation $x^p = 1$, pour p nombre premier divisant $|\mathrm{K}^*|$ et utiliser le th. 3.1).

(ii) Soit $p \neq 2$ un nombre premier. Montrer que x est un carré dans $\mathbf{F}_p^*$ (i.e. $x = y^2$, avec $y \in \mathbf{F}_p^*$) si et seulement si $x^{(p-1)/2} = 1$.

(iii) En déduire que -1 est un carré dans $\mathbf{F}_p^*$ si et seulement si p est de la forme $4n+1$.

(iv) Soit p de la forme $4n+3$. Montrer que l'équation $a^2 + b^2 = p$ n'a pas de solution avec $a, b \in \mathbf{Z}$.

Exercice 3.5. — (i) Soit p un nombre premier. Montrer que, si $x \equiv 1 + p^k a \bmod p^{k+1}$, et si $k \geqslant 1$ ($k \geqslant 2$, si $p = 2$), alors $x^p \equiv 1 + p^{k+1}a \bmod p^{k+2}$. En déduire que $(1+p)^{p^{n-2}} \neq 1$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$, si $p \neq 2$ et $n \geqslant 2$, et que $(1+4)^{p^{n-3}} \neq 1$ dans $(\mathbf{Z}/2^n\mathbf{Z})^*$, si $n \geqslant 3$.

(ii) Soit N le noyau de la réduction modulo p de $(\mathbf{Z}/p^n\mathbf{Z})^*$ dans $\mathbf{F}_p^*$ (dans $(\mathbf{Z}/4\mathbf{Z})^*$, si $p = 2$). Montrer que N est isomorphe à $\mathbf{Z}/p^{n-1}\mathbf{Z}$ (à $\mathbf{Z}/2^{n-2}\mathbf{Z}$, si $p = 2$).

(iii) En utilisant le résultat de l'ex. 3.4, montrer que $(\mathbf{Z}/p^n\mathbf{Z})^* \cong (\mathbf{Z}/(p-1)\mathbf{Z}) \oplus (\mathbf{Z}/p^{n-1}\mathbf{Z})$ en tant que groupe commutatif, si $p \neq 2$ et $n \geqslant 1$.

(iv) Montrer que $(\mathbf{Z}/2^n\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2^{n-2}\mathbf{Z})$, si $n \geqslant 2$.

3.4. Le théorème de Lagrange et ses variantes

Si G est un groupe fini, et si H est un sous-groupe de G, alors $h \mapsto xh$ induit une bijection de H sur xH, ce qui fait que les classes à droite xH ont toutes le même cardinal $|\mathrm{H}|$. Comme G est la réunion disjointe des xH, pour $x \in \mathrm{G}/\mathrm{H}$, on en déduit la formule

$$|\mathrm{G}| = |\mathrm{G}/\mathrm{H}| \cdot |\mathrm{H}|.$$

En particulier, $|\mathrm{H}|$ divise $|\mathrm{G}|$, ce qui se traduit par :

• Si G est un groupe fini, alors le cardinal de tout sous-groupe de G divise celui de G (théorème de Lagrange).

On peut spécialiser cela au sous-groupe engendré par un élément x de G : le cardinal de ce sous-groupe est, par définition, l'ordre de x, ce qui nous donne :

• Dans un groupe fini l'ordre d'un élément divise le cardinal du groupe.

[18] Cette hypothèse est en fait superflue car tout corps fini est commutatif (théorème de Wedderburn).

Finalement, on remarque que |G/H| aussi divise |G|. Si X est un ensemble sur lequel G agit, si O est une orbite, si $x \in \mathrm{O}$, et si H est le stabilisateur de x, on sait que $\mathrm{O} \cong \mathrm{G/H}$. On en déduit que :

• Dans un ensemble sur lequel agit un groupe fini, le cardinal d'une orbite divise le cardinal du groupe et, plus précisément, le produit du cardinal de l'orbite par celui du stabilisateur d'un de ses éléments est égal au cardinal du groupe.

En particulier, en appliquant ceci à l'action de G sur lui-même par conjugaison intérieure, on obtient :

• Dans un groupe fini, le cardinal d'une classe de conjugaison divise le cardinal du groupe.

• Si X est un ensemble fini sur lequel agit un groupe fini G, on peut découper X en orbites pour cette action. Si on choisit un élément par orbite, et si on utilise l'isomorphisme $\mathrm{O}_x \cong \mathrm{G/G}_x$, où G_x est le stabilisateur de x, on obtient la *formule des classes* :

$$|\mathrm{X}| = \sum_{x \in \mathrm{G}\backslash\mathrm{X}} |\mathrm{O}_x| = |\mathrm{G}| \cdot \sum_{x \in \mathrm{G}\backslash\mathrm{X}} \frac{1}{|\mathrm{G}_x|}.$$

Exercice 3.6. — Montrer que tout élément $x \in \mathbf{F}_p^*$ vérifie $x^{p-1} = 1$. En déduire le petit théorème de Fermat[19] (si $n \in \mathbf{Z}$, alors $n^p - n$ est divisible par p).

Exercice 3.7. — (démonstration combinatoire du petit th. de Fermat). Soient $n \geqslant 1$ et X l'ensemble des applications de $\mathbf{Z}/p\mathbf{Z}$ dans $\{1, \ldots, n\}$. Si $g \in \mathbf{Z}/p\mathbf{Z}$ et $\phi \in \mathrm{X}$, on définit $g \cdot \phi$ par $(g \cdot \phi)(x) = \phi(x + g)$, pour tout $x \in \mathbf{Z}/p\mathbf{Z}$ (la loi de groupe de $\mathbf{Z}/p\mathbf{Z}$ est notée additivement).

(i) Vérifier que ceci définit une action de groupe.

(ii) Quels sont les points fixes de cette action ? Combien y en a-t-il ?

(iii) Combien d'éléments a une orbite non réduite à un point ?

(iv) Calculer le nombre de ces orbites, et en déduire le petit théorème de Fermat.

3.5. Le groupe symétrique S_n

3.5.1. Permutations

Si $n \in \mathbf{N} - \{0\}$, on note S_n le groupe des bijections de $\{1, \ldots, n\}$. Comme il y a n manières de choisir l'image de 1, $n-1$ de choisir celle de 2 une fois celle de 1 choisie, etc. le cardinal de S_n est $n(n-1)\cdots 1 = n!$. Par définition, S_n opère sur $\{1, \ldots, n\}$; il opère donc aussi sur toutes sortes d'objets construits à partir de $\{1, \ldots, n\}$ comme l'ensemble des parties de $\{1, \ldots, n\}$ (l'image d'une partie $\{i_1, \ldots, i_p\}$ par σ est $\{\sigma(i_1), \ldots, \sigma(i_p)\}$).

Exercice 3.8. — On fait agir S_n sur l'ensemble des parties de $\{1, \ldots, n\}$ comme ci-dessus.

(i) Si $p \leqslant n$, quelle est l'orbite de $\{1, \ldots, p\}$?

(ii) Quel est le stabilisateur de $\{1, \ldots, p\}$; quel est son cardinal ?

(iii) Retrouver la valeur $\frac{n!}{p!\,(n-p)!}$ pour le nombre de parties à p éléments d'un ensemble à n éléments.

[19] Énoncé dans une lettre à Frenicle du 18 octobre 1640.

Un élément de S_n est une *permutation*. Si $\sigma \in \mathrm{S}_n$, on définit le *support* de σ comme l'ensemble des $i \in \{1, \ldots, n\}$ tels que $\sigma(i) \neq i$. Il est plus ou moins évident que *deux permutations de supports disjoints permutent entre elles*.

On peut représenter une permutation σ de S_n sous la forme d'une matrice à 2 lignes et n colonnes en mettant les nombres de 1 à n sur la première ligne et leurs images par σ juste en-dessous. Cette représentation est très commode pour faire le produit de deux permutations (en n'oubliant pas que c'est la matrice de droite qui agit en premier). Par exemple, si σ et τ sont les permutations de S_6 définies par $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 5$, $\sigma(4) = 6$, $\sigma(5) = 1$ et $\sigma(6) = 3$, et $\tau(1) = 4$, $\tau(2) = 2$, $\tau(3) = 1$, $\tau(4) = 6$, $\tau(5) = 5$ et $\tau(6) = 3$, alors

$$\sigma = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 2&4&5&6&1&3 \end{smallmatrix}\right), \quad \tau = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 4&2&1&6&5&3 \end{smallmatrix}\right) \quad \text{et} \quad \sigma\tau = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 2&4&5&6&1&3 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 4&2&1&6&5&3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 6&4&2&3&1&5 \end{smallmatrix}\right).$$

Une permutation $\sigma \in \mathrm{S}_n$ est un *k-cycle* s'il existe $i_1, \ldots, i_k$ distincts, tels que

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots,\ \sigma(i_k) = i_1, \quad \text{et } \sigma(j) = j, \text{ si } j \notin \{i_1, \ldots, i_k\}.$$

On note $(i_1, i_2, \ldots, i_k)$ le k-cycle défini ci-dessus ; son support est l'ensemble $\{i_1, \ldots, i_k\}$; il est d'ordre k. On remarquera que le k-cycle $(i_1, i_2, \ldots, i_k)$ est aussi égal au k-cycle $(i_a, i_{a+1}, \ldots, i_{a+k-1})$, si on écrit les indices modulo k, et a est n'importe quel élément de $\mathbf{Z}/k\mathbf{Z}$. Pour rétablir une unicité de l'écriture, il suffit d'imposer que i_1 soit le plus petit élément de $\{i_1, \ldots, i_k\}$. Il est commode d'étendre la notation ci-dessus aux « cycles de longueur 1 » (qui sont tous égaux à l'identité...).

- Si σ est un k-cycle, alors $\sigma^k = \mathrm{id}$.
- Une permutation peut s'écrire comme un produit de cycles de supports disjoints.

  Si σ est une permutation, on fabrique une partition de $\{1, \ldots, n\}$ en prenant les orbites $\mathrm{O}_1, \ldots, \mathrm{O}_s$ sous l'action de σ (i.e. sous l'action du sous-groupe cyclique de S_n engendré par σ). Si O_i est une de ces orbites, de cardinal k_i, on peut considérer le cycle $c_i = (a, \sigma(a), \ldots, \sigma^{k_i-1}(a))$, où a est le plus petit élément de O_i ; c'est un cycle de longueur k_i et de support O_i, et σ est le produit des c_i, pour $i \in \{1, \ldots, s\}$.

Comme des cycles ayant des supports deux à deux disjoints commutent entre eux, on peut faire le produit dans n'importe quel ordre dans la décomposition d'une permutation en cycles de supports disjoints. Par exemple, soit $\sigma \in \mathrm{S}_6$ la permutation définie par : $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 5$, $\sigma(4) = 6$, $\sigma(5) = 1$ et $\sigma(6) = 4$. Alors on a $\sigma = (1, 3, 5)(4, 6)(2) = (4, 6)(2)(1, 3, 5)$... Très souvent on omet les cycles de longueur 1 de la décomposition ; on écrit donc plutôt la permutation précédente sous la forme $\sigma = (1, 3, 5)(4, 6)$ ou $\sigma = (4, 6)(1, 3, 5)$.

- Tout élément de S_n est conjugué à un unique élément de la forme

$$(1, \ldots, \ell_1)(\ell_1 + 1, \ldots, \ell_1 + \ell_2) \cdots (\ell_1 + \cdots + \ell_{s-1} + 1, \ldots, \ell_1 + \cdots + \ell_{s-1} + \ell_s),$$

où $(\ell_1, \dots, \ell_s)$ est une *partition* de n, c'est-à-dire une suite décroissante d'entiers $\geqslant 1$ dont la somme est n. Les classes de conjugaison de S_n sont donc en bijection naturelle avec les partitions de n.

Soit $\sigma \in \mathrm{S}_n$. La conjugaison $\sigma \mapsto \alpha\sigma\alpha^{-1}$ par un élément α de S_n transforme un k-cycle $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$, en le k-cycle $\alpha(i_1) \mapsto \alpha(i_2) \mapsto \cdots \mapsto \alpha(i_k) \mapsto \alpha(i_1)$. On en déduit en particulier que les longueurs des cycles apparaissant dans les décompositions de deux permutations conjuguées sont les mêmes, ce qui implique l'unicité d'un conjugué de la forme voulue, les ℓ_j étant les longueurs des cycles apparaissant dans la décomposition de σ rangées dans l'ordre décroissant. Écrivons donc σ comme un produit de cycles $\tau_1 \dots \tau_s$ à supports disjoints. Soit ℓ_j la longueur de τ_j. On a $\ell_1 + \cdots + \ell_s = n$, et quitte à permuter les τ_j, on peut supposer que $\ell_1 \geqslant \ell_2 \cdots \geqslant \ell_s$. On peut alors écrire τ_j sous la forme $\tau_j = (i_{\ell_1+\cdots+\ell_{j-1}+1}, \dots, i_{\ell_1+\cdots+\ell_{j-1}+\ell_j})$, et $k \mapsto i_k$ nous définit une permutation α de $\{1, \dots, n\}$, car les supports des τ_j forment une partition de $\{1, \dots, n\}$. Alors $\alpha^{-1}\sigma\alpha$ est un conjugué de σ de la forme voulue, ce qui permet de conclure.

• Un 2-cycle est appelé une *transposition*, et S_n est engendré par les transpositions ; plus précisément, tout élément de S_n est produit de moins de $n-1$ transpositions.

La démonstration se fait par récurrence sur n. Pour $n = 1$ (et $n = 2$), le résultat est immédiat. Si $n \geqslant 2$, et si $\sigma \in \mathrm{S}_n$ vérifie $\sigma(n) \neq n$, alors $\tau = (\sigma(n), n)$ est une transposition et $\tau\sigma$ fixe n, et donc peut être vu comme un élément de S_{n-1}. D'après l'hypothèse de récurrence, $\tau\sigma$ est un produit de moins de $n-2$ transpositions à support dans $\{1, \dots, n-1\}$, et donc $\sigma = \tau(\tau\sigma)$ est un produit de moins de $n-1$ transpositions. On en déduit le résultat, le cas $\sigma(n) = n$ se traitant directement.

Exercice 3.9. — Calculer $(1,2)(2,3)(3,4)(4,5)$ dans S_5.

Exercice 3.10. — Montrer que S_n est engendré par les transpositions $(1,2), (2,3), \dots, (n-1, n)$.

Exercice 3.11. — Soit $\sigma \in \mathrm{S}_n$ dont la décomposition en cycles disjoints est $\tau_1 \cdots \tau_s$, chaque τ_i étant de longueur ℓ_i. Quel est l'ordre de σ ?

Exercice 3.12. — (i) Combien y a-t-il de cycles de longueur k dans S_n.

(ii) Montrer que le nombre moyen de cycles dans la décomposition d'un éléments de S_n tend vers l'infini avec n. (On pourra commencer par se demander dans combien de permutations un cycle donné apparaît.)

Exercice 3.13. — (difficile mais très surprenant) Le DGAE voulant tester le niveau de compréhension des X a décidé de les mettre à l'épreuve. Pour ce faire, il réunit les 500 membres de la promotion dans l'amphi Poincaré et leur tient ce langage : « J'ai disposé dans l'amphi Arago vos 500 noms dans des casiers numérotés de 1 à 500, à raison d'un par casier. Je vais vous appeler un par un, et demander à chacun d'entre vous d'ouvrir des casiers un par un à la recherche de son nom puis de les refermer sans changer le contenu et de regagner sa chambre sans possibilité de communiquer quoi que ce soit à ses camarades restés dans l'amphi Poincaré. Si tout le monde trouve son nom dans les 250 premiers casiers qu'il a ouverts, vous pouvez partir en vacances. Si l'un d'entre vous ne trouve pas son nom, on recommence le jour suivant (et je change le contenu des casiers bien évidemment). Voilà, vous avez deux heures pour concevoir une stratégie. » Désespoir des X qui se rendent compte que chacun a une chance sur deux de tomber sur son nom, et qu'au total ils ont une chance sur 2^{500} de partir en vacances au bout d'un jour, et donc qu'ils ne partiront pas en vacances. Pourtant au bout d'un certain temps, l'un de nos X déclare :

« pas de panique, avec un peu de discipline, on a 9 chances sur 10 de partir en vacances avant la fin de la semaine ». Saurez-vous retrouver son raisonnement ?

3.5.2. Signature d'une permutation

Si $\sigma \in \mathrm{S}_n$, on définit la *signature* $\mathrm{sign}(\sigma)$ de σ par la formule

$$\mathrm{sign}(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

• $\mathrm{sign} : \mathrm{S}_n \to \{\pm 1\}$ est un morphisme de groupes.

Si $\sigma, \tau \in \mathrm{S}_n$, on a

$$\mathrm{sign}(\sigma\tau) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} = \Big(\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \Big) \Big(\prod_{1 \leqslant i < j \leqslant n} \frac{\tau(i) - \tau(j)}{i - j} \Big).$$

Le second terme est égal à $\mathrm{sign}(\tau)$, et le premier à $\mathrm{sign}(\sigma)$ car on a $\frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}$, ce qui permet d'écrire le produit sous la forme $\prod_{1 \leqslant \tau(i) < \tau(j) \leqslant n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} = \mathrm{sign}(\sigma)$.

• Si τ est un k-cycle, alors $\mathrm{sign}(\tau) = (-1)^{k-1}$.

On a $\mathrm{sign}(\alpha\sigma\alpha^{-1}) = \mathrm{sign}(\alpha)\mathrm{sign}(\sigma)\mathrm{sign}(\alpha)^{-1} = \mathrm{sign}(\sigma)$, ce qui prouve que la signature est invariante par conjugaison et donc que tous les k-cycles ont même signature. Cela permet de prendre $\tau = (n-1, n)$ pour calculer la signature d'une transposition. On a alors

$$\begin{aligned} \mathrm{sign}(\tau) =& \Big(\prod_{1 \leqslant i < j \leqslant n-2} \frac{\tau(i) - \tau(j)}{i - j} \Big) \Big(\prod_{i \leqslant n-2} \frac{\tau(i) - \tau(n-1)}{i - (n-1)} \Big) \Big(\prod_{i \leqslant n-2} \frac{\tau(i) - \tau(n)}{i - n} \Big) \cdot \frac{\tau(n-1) - \tau(n)}{(n-1) - n} \\ =& \Big(\prod_{i \leqslant n-2} \frac{i - n}{i - (n-1)} \Big) \Big(\prod_{i \leqslant n-2} \frac{i - (n-1)}{i - n} \Big) \cdot (-1) = -1, \end{aligned}$$

ce qui prouve le résultat pour une transposition. Maintenant, le k-cycle $\sigma_k = (i_1, \ldots, i_k)$ est le produit des transpositions $(i_1, i_2) \cdots (i_{k-1}, i_k)$, et comme il y a $k-1$ transpositions dans ce produit, on a $\mathrm{sign}(\sigma_k) = (-1)^{k-1}$, ce qu'on cherchait à démontrer.

Exercice 3.14. — Montrer que $\mathrm{sign}(\sigma) = (-1)^{n - \omega(\sigma)}$, où $\omega(\sigma)$ est le nombre d'orbites de σ.

Exercice 3.15. — Si $\sigma \in \mathrm{S}_n$, on note u_σ l'endomorphisme de $\mathbf{C}^n$ envoyant un élément e_i de la base canonique de $\mathbf{C}^n$ sur $e_{\sigma(i)}$.

(i) Montrer que $\sigma \mapsto u_\sigma$ est un morphisme de groupes de S_n dans $\mathbf{GL}_n(\mathbf{C})$.

(ii) Montrer que si τ est une transposition, alors u_τ est une symétrie par rapport à un hyperplan que l'on déterminera. Que vaut $\det u_\tau$?

(iii) En déduire que $\det u_\sigma = \mathrm{sign}(\sigma)$ pour tout $\sigma \in \mathrm{S}_n$.

3.5.3. Groupe alterné

On définit le *groupe alterné* A_n comme le noyau de la signature. Comme la signature est surjective sur $\{\pm 1\}$, on a $|\mathrm{A}_n| = \frac{1}{2}|\mathrm{S}_n| = \frac{n!}{2}$. Un k-cycle est dans A_n, si et seulement si k est impair.

• A_n est engendré par les 3-cycles.

Cela se démontre par récurrence sur n. Le résultat est évident (et vide) si $n \leqslant 2$. Soit $n \geqslant 3$, et soit $\sigma \in \mathrm{A}_n$. Si $\sigma(n) \neq n$, on peut choisir un 3-cycle $(n, \sigma(n), c)$, où $c \notin \{n, \sigma(n)\}$, et alors $\tau^{-1}\sigma$ fixe n et peut être écrit comme un produit de 3-cycles à support dans $\{1, \ldots, n-1\}$ d'après l'hypothèse de récurrence ; donc $\sigma = \tau(\tau^{-1}\sigma)$ peut être écrit comme un produit de 3-cycles. On en déduit le résultat, le cas $\sigma(n) = n$ se traitant directement.

• Si $n \geqslant 5$, tous les 3-cycles sont conjugués dans A_n.

Il suffit de prouver qu'ils sont tous conjugués à $\sigma_0 = (1, 2, 3)$. Soit σ un 3-cycle. Comme les 3-cycles sont tous conjugués dans S_n, il existe $\alpha \in \mathrm{S}_n$ tel que $\sigma = \alpha\sigma_0\alpha^{-1}$. Si $\alpha \in \mathrm{A}_n$, on a gagné. Sinon, $\tau = (4, 5)$ commute avec σ_0 puisque leurs supports sont disjoints, et $\beta = \alpha\tau \in \mathrm{A}_n$ vérifie $\beta\sigma_0\beta^{-1} = \alpha\tau\sigma_0\tau^{-1}\alpha^{-1} = \alpha\sigma_0\alpha^{-1} = \sigma$, ce qui montre que σ est conjugué à σ_0 dans A_n.

• Le groupe A_5 est un groupe simple.

Soit H un sous-groupe distingué de A_5 non réduit à l'identité. On veut prouver que $\mathrm{H} = \mathrm{A}_5$ et il suffit de prouver que H contient un 3-cycle, car ceci implique qu'il contient tous les 3-cycles puisque ceux-ci sont conjugués dans A_5, et donc $\mathrm{H} = \mathrm{A}_5$ puisque les 3-cycles engendrent A_5.

Soit donc $\sigma \in \mathrm{H} - \{1\}$. Il y a trois possibilités : σ est un 3-cycle et il n'y a rien à faire, ou σ est un 5-cycle ou c'est le produit de 2 tranpositions de supports disjoints.

• Si σ est le 5-cycle (a, b, c, d, e), soit $\tau = (a, b, c)$. Alors H contient $\tau^{-1}\sigma^{-1}\tau$ puisqu'il est distingué et donc aussi $h = \sigma\tau^{-1}\sigma^{-1}\tau$. Or τ^{-1} est le 3-cycle (c, b, a) et $\sigma\tau^{-1}\sigma^{-1}$ est le 3-cycle $(\sigma(c), \sigma(b), \sigma(a)) = (d, c, b)$. Donc $h = (d, c, b)(a, b, c)$ laisse fixe e et $a \mapsto b \mapsto d$, $b \mapsto c \mapsto b$, $c \mapsto a \mapsto a$, et $d \mapsto d \mapsto c$; c'est donc le 3-cycle (a, d, c).

• Si $\sigma = \sigma_1\sigma_2$, avec $\sigma_1 = (a, b)$, $\sigma_2 = (c, d)$, et a, b, c, d distincts deux à deux, et si $\tau = (c, d, e)$, où $e \notin \{a, b, c, d\}$, alors H contient $h = \sigma\tau^{-1}\sigma^{-1}\tau$. Or σ_1 commute à σ_2 et τ, donc $h = \sigma_2\tau^{-1}\sigma_2^{-1}\tau$. Maintenant, $\tau^{-1}\sigma_2^{-1}\tau$ est la transposition $(\tau^{-1}(c), \tau^{-1}(d)) = (e, c)$ et donc $h = (c, d)(e, c) = (c, e, d)$ est un 3-cycle.

• Si $n \geqslant 5$, le groupe A_n est un groupe simple[(20)].

Soit $n \geqslant 5$, soit H un sous-groupe distingué de A_n, et soient $\sigma \neq \mathrm{id}$ un élément de H et $\tau = (a, b, c)$ un 3-cycle. Alors H contient $h = \tau\sigma\tau^{-1}\sigma^{-1}$ qui est le produit des 3-cycles τ et $\sigma\tau^{-1}\sigma^{-1} = (\sigma(c), \sigma(b), \sigma(a))$. Soit alors $b = \sigma(a)$, et soit $c \notin \{a, \sigma(a), \sigma^2(a)\}$, non fixé par σ si jamais σ échange a et $\sigma(a)$ (un tel c existe toujours, sinon σ serait une transposition, ce qui est impossible puisque $\sigma \in \mathrm{A}_n$). La condition mise sur c fait que $h \neq \mathrm{id}$, et celle mise sur b implique que le support de h est inclus dans $\{a, \sigma(a), \sigma^2(a), c, \sigma(c)\}$ et donc comporte au plus 5 éléments. Soit X de cardinal 5 contenant le support de h, et soit $\mathrm{Perm(X)}$ le groupe des permutations de X. Alors $\mathrm{H} \cap \mathrm{Perm(X)}$ est un sous-groupe distingué de $\mathrm{Perm(X)}$, et donc contient un 3-cycle d'après l'étude du cas $n = 5$. On en déduit que $\mathrm{H} = \mathrm{A}_n$ comme-ci-dessus puisque A_n est engendré par les 3-cycles qui sont tous conjugués dans A_n.

Exercice 3.16. — (i) Montrer que si G est un groupe fini abélien, et si d divise $|\mathrm{G}|$, alors G a un sous-groupe de cardinal d. (On pourra utiliser le théorème de structure.)

(ii) Montrer que si $f : \mathrm{S}_5 \to \mathrm{S}_3$ est un morphisme de groupes, alors $\mathrm{Im}(f)$ a 1 ou 2 éléments.

(iii) Montrer que S_5 n'a pas de sous-groupe d'ordre 40.

[(20)] Ce résultat, conjugué avec la théorie de Galois, explique que l'on ne puisse pas trouver de formule générale donnant les racines d'une équation de degré n, si $n \geqslant 5$.

3.6. Les théorèmes de Sylow

Cauchy a démontré (cf. ex. 3.18) que, si G est un groupe fini d'ordre (*l'ordre d'un groupe* est, par définition, son cardinal) divisible par p, alors G contient un élément d'ordre p (et donc un sous-groupe (cyclique) d'ordre p). D'un autre côté, l'ordre d'un sous-groupe divisant l'ordre du groupe (théorème de Lagrange), tout sous-p-groupe (un *p-groupe* est un groupe dont l'ordre est une puissance de p) de G d'ordre p^a vérifie $a \leqslant v_p(|\mathrm{G}|)$. Un *$p$-Sylow* de G est un sous-groupe d'ordre $p^{v_p(|\mathrm{G}|)}$. (Dans le cas $v_p(|\mathrm{G}|) = 0$, un tel sous-groupe est donc réduit à l'élément neutre.)

• Si G est un groupe commutatif d'ordre divisible par p, alors G contient un sous-groupe cyclique d'ordre p.

Si $x \in \mathrm{G}$, soit n_x l'ordre de x. Par définition cela signifie que le morphisme de groupes de $\mathbf{Z}$ dans G envoyant $a \in \mathbf{Z}$ sur x^a admet pour noyau $n_x\mathbf{Z}$, et donc induit un isomorphisme de $\mathbf{Z}/n_x\mathbf{Z}$ sur le sous-groupe de G engendré par x. Soit alors $\mathrm{X} \subset \mathrm{G}$ engendrant G (on peut prendre $\mathrm{X} = \mathrm{G}$ par exemple). Comme G est commutatif, l'application $\oplus_{x\in\mathrm{X}}(\mathbf{Z}/n_x\mathbf{Z}) \to \mathrm{G}$, envoyant $(a_x)_{x\in\mathrm{X}}$ sur $\prod_{x\in\mathrm{X}} x^{a_x}$ est un morphisme de groupes, et comme X engendre G, ce morphisme est surjectif. L'ordre de G est donc un diviseur de $\prod_{x\in\mathrm{X}} n_x$. Comme p divise $|\mathrm{G}|$, cela implique que p divise un des n_x, et alors $y = x^{n_x/p}$ est d'ordre p et le sous-groupe de G engendré par y est d'ordre p. Ceci permet de conclure.

Théorème 3.17. — (Sylow, 1872) *Si* G *est un groupe fini, l'ensemble des p-Sylow de* G *est non vide. De plus :*

(i) *Tous les p-Sylow de* G *sont conjugués.*

(ii) *Si* Q *est un sous-p-groupe de* G*, alors il existe un p-Sylow de* G *contenant* Q *; en particulier, tout élément d'ordre p est contenu dans un p-Sylow de* G*.*

La démonstration se fait par récurrence sur $|\mathrm{G}|$, le cas $|\mathrm{G}| = 1$ étant évident (et vide). Soit Z le centre de G, et soit $k = v_p(|\mathrm{G}|)$.

• Si p divise l'ordre de Z, alors Z contient, d'après le point précédent, un sous-groupe cyclique C d'ordre p. On peut appliquer l'hypothèse de récurrence à $\mathrm{H} = \mathrm{G}/\mathrm{C}$ qui est d'ordre mp^{k-1}. Si $\mathrm{P_H}$ est un p-Sylow de H, l'image inverse de $\mathrm{P_H}$ dans G est un sous-groupe d'ordre $|\mathrm{P_H}| \cdot |\mathrm{C}| = p^{k-1}p = p^k$; c'est donc un p-Sylow de G.

• Si p ne divise pas $|\mathrm{Z}|$, on fait agir G par conjugaison intérieure ($g \cdot x = gxg^{-1}$) sur G. Par définition du centre, les orbites (qui ne sont autres que les classes de conjugaison de G) ne comportant qu'un seul élément pour cette action, sont exactement les $\{c\}$, pour $c \in \mathrm{Z}$. Comme $|\mathrm{Z}|$ est premier à p et comme $|\mathrm{G}|$ est divisible par p, il y a une orbite O, non réduite à un élément, de cardinal premier à p. Si $x \in \mathrm{O}$, et si H est l'ensemble des éléments de G commutant à x, on a $\mathrm{O} = \mathrm{G}/\mathrm{H}$. On en déduit que $|\mathrm{H}| = \frac{|\mathrm{G}|}{|\mathrm{O}|}$. Comme $v_p(|\mathrm{O}|) = 0$, on a $v_p(|\mathrm{H}|) = v_p(|\mathrm{G}|) = k$, et comme $|\mathrm{O}| > 1$, on a $|\mathrm{H}| < |\mathrm{G}|$. L'hypothèse de récurrence montre que H contient un sous-groupe d'ordre p^k, et donc que G aussi.

Maintenant, si P est un p-Sylow de G, et si Q est un sous-p-groupe de G, on peut faire agir Q sur G/P par translation à gauche. Comme G/P est de cardinal premier à p, puisque P est un p-Sylow, au moins une des orbites O a un cardinal premier à p. Mais O est de la forme Q/H, où H est un sous-groupe de Q, et comme Q est un p-groupe, on a $|\mathrm{Q}/\mathrm{H}|$ premier

à p si et seulement si $\mathrm{H} = \mathrm{Q}$. Il existe donc $x \in \mathrm{G/P}$ fixe par Q tout entier. En prenant un représentant $\tilde{x}$ de x dans G, cela se traduit par $\mathrm{Q}\tilde{x}\mathrm{P} \subset \tilde{x}\mathrm{P}$, ou encore par $\mathrm{Q} \subset \tilde{x}\mathrm{P}\tilde{x}^{-1}$.

Si Q est un p-Sylow, on en déduit que $\mathrm{Q} = \tilde{x}\mathrm{P}\tilde{x}^{-1}$ pour des raisons de cardinal, ce qui démontre le (i). Si Q est un sous-p-groupe quelconque, cela montre que Q est contenu dans un sous-groupe d'ordre p^k, c'est-à-dire dans un p-Sylow. Ceci démontre le (ii) et permet de conclure.

Exercice 3.18. — Soient p un nombre premier et G un groupe fini de cardinal divisible par p. On fait agir $\mathbf{Z}/p\mathbf{Z}$ sur G^p par $i \cdot (x_0, \ldots, x_{p-1}) = (x_i, x_{i+1}, \ldots, x_{i-1})$ (i.e. on décale les indices de i, en identifiant $\mathbf{Z}/p\mathbf{Z}$ et $\{0, \ldots, p-1\}$). Soit X le sous-ensemble de G^p des $(x_0, \ldots, x_{p-1})$ vérifiant $x_0 \cdots x_{p-1} = 1$.

(i) Montrer que X est stable par $\mathbf{Z}/p\mathbf{Z}$. Quels sont les points fixes de cette action ?

(ii) Montrer que $|\mathrm{X}|$ est divisible par p ; en déduire que G admet des éléments d'ordre p.

4. Algèbre linéaire

Dans le n° 4.1, on rappelle (et complète) sans démonstration les résultats vus en classe préparatoire concernant la réduction des endomorphismes (diagonalisation, mise sous forme de Jordan...). Au n° 4.2, on explique comment on peut retrouver ces résultats en utilisant le théorème de structure des modules de torsion sur les anneaux principaux démontré au n° 4.3. L'intérêt de cette nouvelle approche est de ne rien supposer sur le corps K, alors que l'approche vue en classe préparatoire impose plus ou moins à K d'être algébriquement clos (ce qui, il faut le reconnaître, est le cas de $\mathbf{C}$, mais est loin d'être celui de $\mathbf{F}_2$).

4.1. Généralités

Soit K un corps commutatif, et soit V un K-espace vectoriel *de dimension finie*.

4.1.1. Endomorphismes

On note End(V) l'ensemble des *endomorphismes* de V, c'est-à-dire, l'ensemble des applications $u : \mathrm{V} \to \mathrm{V}$ qui sont linéaires. Muni de l'addition $(u_1 + u_2)(v) = u_1(v) + u_2(v)$, et de la composition des endomorphismes, End(V) est un anneau non commutatif (sauf en dimension 1), possédant un élément unité (que nous noterons 1) en la personne de l'application identité $\mathrm{id} : \mathrm{V} \to \mathrm{V}$. L'*homothétie de rapport* λ est l'application $v \mapsto \lambda v$. On la note simplement λ, ce qui est compatible avec le fait que l'identité (que l'on a notée 1) peut aussi être vue comme l'homothétie de rapport 1.

4.1.2. Le théorème de Cayley-Hamilton

Si $u \in \mathrm{End(V)}$, on note $\det(u) \in \mathrm{K}$ son déterminant. On a $\det(u_1\, u_2) = \det(u_1)\, \det(u_2)$, si $u_1, u_2 \in \mathrm{End(V)}$. On note $\mathrm{Car}_u(\mathrm{X})$ le *polynôme caractéristique* $\mathrm{Car}_u(\mathrm{X}) = \det(\mathrm{X} - u)$ de u. Si V est de dimension d, c'est un polynôme de degré d, dont le développement est donné par

$$\mathrm{Car}_u(\mathrm{X}) = \mathrm{X}^d - \mathrm{Tr}(u)\mathrm{X}^{d-1} + \cdots + (-1)^d \det(u),$$

où $\mathrm{Tr}(u)$ est, par définition, la *trace* de u. On a $\mathrm{Tr}(u_1 u_2) = \mathrm{Tr}(u_2 u_1)$, si $u_1, u_2 \in \mathrm{End(V)}$.

L'ensemble des $P \in K[X]$ tels que $P(u) = 0$ est un idéal de $K[X]$, non nul car $\mathrm{End}(V)$ est de dimension $(\dim V)^2$ et donc $1, u, \ldots, u^{(\dim V)^2}$ forment une famille liée. On note Min_u le générateur unitaire de cet idéal. C'est le *polynôme minimal* de u et, d'après le théorème de Cayley-Hamilton (1858), Car_u annule u ; autrement dit, Car_u est un multiple de Min_u.

4.1.3. Automorphismes

Si $u \in \mathrm{End}(V)$, le noyau et l'image de u, définis par

$$\mathrm{Ker}(u) = \{v \in V,\ u(v) = 0\} \text{ et } \mathrm{Im}(u) = \{v \in V,\ \exists v' \in V,\ u(v') = v\},$$

sont des sous-espaces vectoriels de V, et on a les équivalences :

$$\det u \neq 0 \Leftrightarrow \mathrm{Ker}(u) = 0 \Leftrightarrow u \text{ injectif} \Leftrightarrow u \text{ bijectif} \Leftrightarrow u \text{ surjectif} \Leftrightarrow \mathrm{Im}(u) = V.$$

Un *automorphisme* de V est un élément de $\mathrm{End}(V)$ vérifiant les conditions ci-dessus. On note $\mathrm{GL}(V) \subset \mathrm{End}(V)$ l'ensemble des automorphismes de V ; c'est le groupe des éléments inversibles de l'anneau $\mathrm{End}(V)$.

4.1.4. Matrices

Si V est de dimension d, et si on choisit une base $e_1, \ldots, e_d$ de V, on peut associer à tout élément u de $\mathrm{End}(V)$ sa matrice dans la base $e_1, \ldots, e_d$. C'est l'élément $(a_{i,j})_{1 \leqslant i,j \leqslant d}$ de $\mathbf{M}_d(K)$ défini par $u(e_j) = \sum_{i=1}^d a_{i,j} e_i$. La trace de u est alors la somme $\sum_{i=1}^d a_{i,i}$ des coefficients diagonaux de la matrice de u ; cette somme ne dépend donc pas du choix de la base. Le groupe $\mathrm{GL}(V)$ s'identifie au groupe $\mathbf{GL}_d(K)$ des matrices $d \times d$ inversibles (ce qui équivaut à ce que le déterminant soit non nul) à coefficients dans K.

Si $f_1, \ldots, f_d$ est une autre base de V, si P est la matrice dont les colonnes sont $f_1, \ldots, f_d$ exprimés dans la base $e_1, \ldots, e_d$, les matrices M et M′ de u dans les bases $e_1, \ldots, e_d$ et $f_1, \ldots, f_d$ sont reliées par la formule $M' = P^{-1}MP$.

4.1.5. Espaces propres, espaces caractéristiques

Soit $u \in \mathrm{End}(V)$. On dit que $\lambda \in K$ est une *valeur propre* de u, si $u - \lambda$ n'est pas inversible, ce qui équivaut à $\mathrm{Ker}(u - \lambda) \neq 0$, et donc à l'existence de $v \in V$, non nul, tel que $u(v) = \lambda v$; un tel v est un *vecteur propre* de u pour la valeur propre λ. Le *spectre* $\mathrm{Spec}(u)$ de u est l'ensemble des valeurs propres de u. C'est aussi l'ensemble des racines du polynôme caractéristique $\mathrm{Car}_u(X) = \det(X - u)$ de u.

Si $\lambda \in \mathrm{Spec}(u)$, le noyau de $\mathrm{Ker}(u - \lambda)$ est l'*espace propre* associé à la valeur propre λ. On dit que u est *diagonalisable*, si $V = \oplus_{\lambda \in \mathrm{Spec}(u)} \mathrm{Ker}(u - \lambda)$. Ceci équivaut à l'existence d'une base $(e_i)_{i \in I}$ de V (constituée de vecteurs propres) dans laquelle la matrice de u est une *matrice diagonale* (i.e. $a_{i,j} = 0$ si $i \neq j$). Le polynôme minimal de u est alors le produit des $(X - \lambda)$, pour $\lambda \in \mathrm{Spec}(u)$; en particulier, tous ses zéros sont dans K et ces zéros sont simples. Réciproquement, *s'il existe* $P \in K[X]$*, dont tous les zéros sont simples et appartiennent à* K*, avec* $P(u) = 0$*, alors* u *est diagonalisable.*

Si $\lambda \in \mathrm{Spec}(u)$, la suite des $\mathrm{Ker}\,(u-\lambda)^k$ est croissante, et donc stationnaire (i.e. constante à partir d'un certain rang). On note e_λ le plus petit k tel que $\mathrm{Ker}\,(u-\lambda)^{k'} = \mathrm{Ker}\,(u-\lambda)^k$,

quel que soit $k' \geqslant k$. Alors $\mathrm{Ker}\,(u-\lambda)^{e_\lambda}$ est le *sous-espace caractéristique* associé à λ. Si K est algébriquement clos, V est la somme directe $\oplus_{\lambda\in\mathrm{Spec}(u)}\mathrm{V}_\lambda$ de ses sous-espaces caractéristiques. On note d_λ la dimension de V_λ ; c'est la *multiplicité* de la valeur propre λ, et c'est aussi la multiplicité de λ en tant que racine de Car_u.

4.1.6. Mise sous forme de Jordan

Un *bloc de Jordan* $\mathrm{J}_{\lambda,r}$ d'ordre r pour λ est une matrice $r\times r$ avec des λ sur la diagonale, des 1 juste au-dessus de la diagonale et des 0 partout ailleurs. Les polynômes minimal et caractéristique de $\mathrm{J}_{\lambda,r}$ sont tous deux égaux à $(\mathrm{X}-\lambda)^r$. Une matrice est *sous forme de Jordan* si elle est diagonale par blocs, et si chacun des blocs est un bloc de Jordan (on ne demande pas aux blocs d'être de la même taille, ni d'être associés au même λ).

On peut trouver une base de V_λ dans laquelle la matrice de u est sous forme de Jordan. La taille des blocs $r_{\lambda,1}\geqslant r_{\lambda,2}\geqslant\cdots\geqslant r_{\lambda,k_\lambda}$ est alors indépendante du choix de la base, et on a $r_{\lambda,1}=e_\lambda$ et $\sum_{j=1}^{k_\lambda} r_{\lambda,j}=d_\lambda\geqslant e_\lambda$. En juxtaposant les bases des V_λ, pour $\lambda\in\mathrm{Spec}(u)$, cela permet, si Car_u a toutes ses racines dans K (ce qui est automatique si K est algébriquement clos), de mettre la matrice de u sur V sous forme de Jordan. On en déduit que les polynômes minimal Min_u et caractéristique Car_u de u sont donnés par

$$\mathrm{Min}_u(\mathrm{X})=\prod_{\lambda\in\mathrm{Spec}(u)}(\mathrm{X}-\lambda)^{e_\lambda}\quad\text{et}\quad\mathrm{Car}_u(\mathrm{X})=\prod_{\lambda\in\mathrm{Spec}(u)}(\mathrm{X}-\lambda)^{d_\lambda}.$$

On déduit aussi de l'existence de la forme de Jordan que $\mathrm{Tr}(u)$ (resp. $\det(u)$) est la somme (resp. le produit) des valeurs propres de u, comptées avec multiplicité.

4.2. Modules de torsion sur K[T] et réduction des endomorphismes

4.2.1. Anneaux et modules. — Si A est un anneau (avec élément unité 1), un A-*module* M est un groupe commutatif pour une loi $+$, muni d'une action $(a,x)\mapsto ax$ de A, vérifiant :

$$0\,x=0,\quad 1\,x=x,\quad a(x+y)=ax+ay,\quad (a+b)x=ax+bx,\quad (ab)x=a(bx),$$

quels que soient $x,y\in\mathrm{M}$ et $a,b\in\mathrm{A}$.

• Si A est un corps commutatif, on retombe sur la définition d'un espace vectoriel, et il y a de grandes similarités entre la théorie des modules sur un anneau commutatif et celle des espaces vectoriels sur un corps commutatif.

• Tout groupe commutatif est naturellement un $\mathbf{Z}$-module, en définissant nx par récurrence sur n, par $0x=0$, $(n+1)x=nx+x$ si $n\in\mathbf{N}$, et $nx=-((-n)x)$, si $n\leqslant 0$. (Montrer que ceci définit bien une action de $\mathbf{Z}$ est un exercice fastidieux qui n'est pas sans rappeler la démonstration du fait que $\mathbf{Z}$ est un anneau en partant des axiomes de Peano.)

• Si A est commutatif, un sous-A-module de A n'est autre qu'un idéal de A.

• Si K est un corps commutatif, et si V est un K-espace vectoriel, alors V est un module sur l'anneau End(V) (non commutatif si $\dim\mathrm{V}\geqslant 2$).

• Si $(M_i)_{i\in I}$ est une famille de A-modules, les groupes commutatifs $\oplus_{i\in I}M_i$ et $\prod_{i\in I}M_i$ sont naturellement munis d'une action de A (comme dans le cas des espaces vectoriels), et sont donc des A-modules.

• Si $M' \subset M$ sont deux A-modules, le groupe commutatif quotient M/M' est muni d'une action de A et donc est un A-module.

• Un *morphisme* $u : M_1 \to M_2$ *de* A*-modules* est un morphisme de groupes additifs commutant à l'action de A (i.e. $u(ax) = a\,u(x)$, si $x \in M_1$ et $a \in A$) ; si A est un corps commutatif, on retombe sur la définition d'une application linéaire entre espaces vectoriels.

• Si $u : M_1 \to M_2$ est un morphisme de A-modules, alors $\mathrm{Ker}\,u$ et $\mathrm{Im}\,u$ sont des A-modules, et u induit un isomorphisme de A-modules de $M_1/\mathrm{Ker}\,u$ sur $\mathrm{Im}\,u$.

Si M est un A-module et si les M_i, pour $i \in I$, sont des sous-A-modules de M, alors l'intersection des M_i est un A-module. Ceci permet de définir le *sous-*A*-module engendré* par une famille $(e_j)_{j\in J}$ d'éléments de M, comme l'intersection de tous les sous-A-modules de M contenant les e_j. Comme dans le cas des espaces vectoriels, ce module est l'ensemble des combinaisons linéaires finies, à coefficients dans A, en les e_j.

Un A-module M est *de type fini* si on peut trouver un ensemble fini $e_1, \ldots, e_d$ d'éléments de M tels que l'application $(a_1, \ldots, a_d) \mapsto a_1e_1 + \cdots + a_de_d$ soit une surjection de A^d sur M ; autrement dit, M est de type fini s'il admet une famille génératrice finie. Une différence essentielle avec le cas des espaces vectoriels sur un corps est qu'un A-module ne possède pas, en général, de base sur A.

Un A-module M est *de torsion* si, pour tout $x \in M$, on peut trouver $a \in A - \{0\}$, tel que $ax = 0$. Un A-module de torsion non nul est un exemple de module ne possédant pas de base puisque toute famille ayant plus d'un élément est liée. Si A est commutatif, un exemple typique de A-module de torsion est un module de la forme A/I, où I est un idéal de A distinct de $\{0\}$ et A ; par exemple, $\mathbf{Z}/D\mathbf{Z}$ est un $\mathbf{Z}$-module de torsion, si $D \geqslant 2$.

4.2.2. Structure des modules de torsion sur K[T]. — Soit K un corps commutatif. Comme le montre la discussion suivant le th 4.2 ci-dessous, un K-espace vectoriel de dimension finie muni d'un endomorphisme K-linéaire u est la même chose qu'un K[T]-module de torsion et de type fini. Ce changement de point de vue est particulièrement intéressant à cause du théorème de structure (th. 4.2) ci-dessous, que le lecteur pourra comparer avec le théorème de structure (th. 3.1) pour les groupes finis abéliens (nous démontrons les deux simultanément au n° 4.3).

Un polynôme $P \in K[T]$ est dit *irréductible* s'il est de degré $\geqslant 1$ et si on ne peut pas le factoriser sous la forme $P = Q_1Q_2$, avec $Q_1, Q_2 \in K[T]$ et $\deg Q_1 \geqslant 1$, $\deg Q_2 \geqslant 1$. Un corps K est algébriquement clos si et seulement si les polynômes irréductibles de K[T] sont de degré 1 ; les polynômes irréductibles de $\mathbf{R}[T]$ sont de degré 1 ou 2, ceux de $\mathbf{Q}[T]$

ou de $\mathbf{F}_p[\mathrm{T}]$ ont des degrés arbitraires. On note $\mathscr{P}_{\mathrm{K[T]}}$ l'ensemble des polynômes unitaires irréductibles de degré $\geqslant 1$.

Si $\mathrm{Q} \in \mathrm{K[T]}$, on note $\mathrm{K[T]/Q}$ (au lieu de $\mathrm{K[T]/QK[T]}$ ou $\mathrm{K[T]/(Q)}$) le quotient de K[T] par l'idéal engendré par Q.

Exercice 4.1. — Montrer que si $\mathrm{Q} \in \mathscr{P}_{\mathrm{K[T]}}$, alors $\mathrm{K[T]/Q}$ est un corps.

Théorème 4.2. — *Soit* M *un* K[T]*-module de torsion et de type fini. Si* $\mathrm{P} \in \mathscr{P}_{\mathrm{K[T]}}$*, soit* $\mathrm{M_P}$ *l'ensemble des* $x \in \mathrm{M}$ *tués par une puissance de* P.

(i) $\mathrm{M_P}$ *est un sous-*K[T]*-module de* M*, nul sauf pour un nombre fini de* $\mathrm{P} \in \mathscr{P}_{\mathrm{K[T]}}$*, et* $\mathrm{M} = \oplus_{\mathrm{P} \in \mathscr{P}_{\mathrm{K[T]}}} \mathrm{M_P}$.

(ii) *Il existe* $r_{\mathrm{P}} \in \mathbf{N}$ *et une unique famille décroissante d'entiers* $a_{\mathrm{P},i} \geqslant 1$*, tels que* $\mathrm{M_P} = \oplus_{1 \leqslant i \leqslant r_{\mathrm{P}}} \mathrm{K[T]/P}^{a_{\mathrm{P},i}}$.

4.2.3. Exemples. — Soit M un K[T]-module de torsion et de type fini, et soient $e_1, \ldots, e_d$ engendrant M. Par définition, cela veut dire que $(x_1, \ldots, x_d) \mapsto x_1 e_1 + \cdots + x_d e_d$, de $(\mathrm{K[T]})^d$ dans M, est surjective. Par ailleurs, si $\mathrm{P}_i \in \mathrm{K[T]} - \{0\}$, pour $i \in \{1, \ldots, d\}$, vérifie $\mathrm{P}_i e_i = 0$ (de tels P_i existent puisque M est de torsion), alors le noyau de l'application précédente contient $(\mathrm{P}_1) \times \cdots \times (\mathrm{P}_d)$, et donc M est un quotient de $\mathrm{K[T]/P}_1 \times \cdots \times \mathrm{K[T]/P}_d$, qui est un K-espace vectoriel de dimension finie $\deg \mathrm{P}_1 \cdots \deg \mathrm{P}_d$. On en déduit que M est un K-espace vectoriel de dimension finie. De plus, la multiplication par T sur M est K-linéaire, ce qui munit M d'un élément privilégié u_{M} de $\mathrm{End(M)}$.

Réciproquement, si V est un K-espace vectoriel de dimension finie, et si u est un endomorphisme de V, alors $\mathrm{P} \mapsto \mathrm{P}(u)$ induit un morphisme d'anneaux de K[T] dans End(V). Comme V est un End(V)-module, cela muni V d'une action de K[T] (où $\mathrm{P} \in \mathrm{K[T]}$ agit par $\mathrm{P}(u) \in \mathrm{End(V)}$), ce qui permet de voir V comme un K[T]-module ; par construction, on a $u_{\mathrm{V}} = u$. De plus, le K[T]-module V est de torsion car $\mathrm{Min}_u \in \mathrm{K[T]}$ tue tous les éléments de V puisque, par définition, Min_u agit par $\mathrm{Min}_u(u)$ sur V, et que $\mathrm{Min}_u(u) = 0$.

Exemple 4.3. — (Modules cycliques) Soit $\mathrm{Q} = \mathrm{T}^d + a_{d-1}\mathrm{T}^{d-1} + \cdots + a_0 \in \mathrm{K[T]}$, avec $d \geqslant 1$, et soit $\mathrm{M} = \mathrm{K[T]/Q}$. Alors la matrice de u_{M} dans la base $1, \mathrm{T}, \ldots, \mathrm{T}^{d-1}$ est

$$\mathrm{A_Q} = \begin{pmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ddots & \vdots & -a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \ldots & 1 & -a_{d-1} \end{pmatrix}$$

et les polynômes minimal et caractéristique de u_{M} sont tous deux égaux à Q.

Par construction Q(T) est la multiplication par 0 sur M, et donc $\mathrm{Q}(u_{\mathrm{M}}) = 0$, ce qui implique que le polynôme minimal de u_{M} divise Q. Par ailleurs, si $\mathrm{P}(u_{\mathrm{M}}) = 0$, alors en particulier, $\mathrm{P}(u_{\mathrm{M}}) \cdot 1 = \mathrm{P(T)}$ est nul dans $\mathrm{M} = \mathrm{K[T]/Q}$, et donc P est un multiple de Q. Ceci prouve que le polynôme minimal de u_{M} est bien Q.

Le polynôme caractéristique de u_{M}, qui n'est autre que le déterminant de $\mathrm{X} - u_{\mathrm{M}}$, peut se calculer en développant par rapport à la dernière colonne. Le coefficient de $\mathrm{X} + a_{d-1}$ est le déterminant d'une matrice $(d-1)\times(d-1)$, triangulaire inférieure, avec des X sur la diagonale, et donc est égal à X^{d-1}. Si $i \geqslant 2$, le coefficient de a_{d-i} est $(-1)^{i-1}\times$ le déterminant d'une matrice diagonale par blocs, un des blocs de dimension $(d-i)\times(d-i)$ étant triangulaire inférieur avec des X sur la diagonale, et l'autre, de dimension $(i-1)\times(i-1)$, étant triangulaire supérieur avec des -1 sur la diagonale ; il est donc égal à $(-1)^{i-1}\mathrm{X}^{d-i}(-1)^{i-1} = \mathrm{X}^{d-i}$. On en déduit que

$$\det(\mathrm{X} - u_{\mathrm{M}}) = (\mathrm{X} + a_{d-1})\mathrm{X}^{d-1} + a_{d-2}\mathrm{X}^{d-2} + \cdots + a_0 = \mathrm{Q}(\mathrm{X}).$$

Exemple 4.4. — (Modules nilpotents) Soit $\lambda \in \mathrm{K}$, et soit $\mathrm{M} = \mathrm{K}[\mathrm{T}]/(\mathrm{X}-\lambda)^d$. Alors la matrice de u_{M} dans la base $f_1 = (\mathrm{X}-\lambda)^{d-1}, f_2 = (\mathrm{X}-\lambda)^{d-2}, \ldots, f_d = 1$ est un bloc de Jordan $\mathrm{J}_{\lambda,d}$.

On a $\mathrm{X}(\mathrm{X}-\lambda)^{d-i} = (\mathrm{X}-\lambda)^{d-(i-1)} + \lambda(\mathrm{X}-\lambda)^{d-i}$, ce qui se traduit par $u_{\mathrm{M}}(f_i) = f_{i-1} + \lambda f_i$, si $i \neq 1$, et par $u_{\mathrm{M}}(f_1) = \lambda f_1$ car $(\mathrm{X}-\lambda)^d = 0$ dans M.

4.2.4. Application à la réduction des endomorphismes

Corollaire 4.5. — *Si* K *est algébriquement clos, si* V *est un* K*-espace vectoriel de dimension finie, et si* $u \in \mathrm{End}(\mathrm{V})$*, alors il existe une base de* V *dans laquelle la matrice de* u *est sous forme de Jordan.*

Démonstration. — On peut supposer que V est un K[T]-module de torsion et de type fini, et que u est la multiplication par T. Maintenant, comme K est algébriquement clos, $\mathscr{P}_{\mathrm{K[T]}}$ est l'ensemble des $\mathrm{T}-\lambda$, avec $\lambda \in \mathrm{K}$. On déduit du th. 4.2 une décomposition de V sous la forme $\mathrm{V} = \oplus_{i\in\mathrm{I}}\mathrm{K}[\mathrm{T}]/(\mathrm{T}-\lambda_i)^{a_i}$ (dans laquelle plusieurs λ_i peuvent être égaux). On conclut en utilisant le résultat de l'exemple 4.4, selon lequel la matrice de la multiplication par T sur $\mathrm{K}[\mathrm{T}]/(\mathrm{T}-\lambda_i)^{a_i}$ peut se mettre sous forme de Jordan.

Remarque 4.6. — La décomposition de V sous la forme $\oplus_\lambda \mathrm{V}_{\mathrm{T}-\lambda}$ fournie par le (i) du th. 4.2 n'est autre que la décomposition de V comme somme directe de sous-espaces caractéristiques.

Lemme 4.7. — *Soit* $(\mathrm{Q}_i)_{i\in\mathrm{I}}$ *une famille finie d'éléments de* K[T] *de degrés* $\geqslant 1$*. Si* $\mathrm{M} = \oplus_{i\in\mathrm{I}}\mathrm{K}[\mathrm{T}]/\mathrm{Q}_i$*, alors le polynôme minimal de* u_{M} *est le* ppcm *des* Q_i*, pour* $i \in \mathrm{I}$*, et le polynôme caractéristique de* u_{M} *est le produit des* Q_i*, pour* $i \in \mathrm{I}$*.*

Démonstration. — Le polynôme minimal de u_{M} doit en particulier annuler $\mathrm{K}[\mathrm{T}]/\mathrm{Q}_i$ pour tout i ; il doit donc être divisible par Q_i d'après les résultats de l'exemple 4.3, et donc aussi par le ppcm des Q_i. Réciproquement, le ppcm des Q_i est divisible par Q_i ; il annule donc $\mathrm{K}[\mathrm{T}]/\mathrm{Q}_i$ pour tout i et est un multiple du polynôme minimal de u_{M} ; d'où le résultat en ce qui concerne le polynôme minimal de u_{M}.

Pour calculer le polynôme caractéristique de u_{M}, on remarque que chaque $\mathrm{K}[\mathrm{T}]/\mathrm{Q}_i$ est stable par u_{M}, et donc que la matrice de u_{M} est diagonale par blocs, avec un bloc pour chaque i correspondant à l'action de u_{M} sur $\mathrm{K}[\mathrm{T}]/\mathrm{Q}_i$. Comme le polynôme caractéristique

d'une matrice diagonale par blocs est le produit des polynômes caractéristiques des blocs, les résultats de l'exemple 4.3 permettent de conclure.

Corollaire 4.8. — (Cayley-Hamilton) *Si* V *est un* K*-espace vectoriel de dimension finie, et si* $u \in \mathrm{End}(\mathrm{V})$*, le polynôme minimal de* u *divise le polynôme caractéristique de* u*.*

Démonstration. — On peut supposer que V est un K[T]-module de torsion et de type fini, et que u est la multiplication par T. Reprenons les notations du théorème 4.2. Si on note $\mathrm{Spec}(u)$ l'ensemble des $\mathrm{P} \in \mathscr{P}_{\mathrm{K[T]}}$ tels que $\mathrm{V_P} \neq 0$, on déduit du lemme 4.7 que

$$\mathrm{Min}_u(\mathrm{X}) = \prod_{\mathrm{P}\in\mathrm{Spec}(u)} \mathrm{P}^{a_{\mathrm{P},1}}, \quad \text{et} \quad \mathrm{Car}_u(\mathrm{X}) = \prod_{\mathrm{P}\in\mathrm{Spec}(u)} \mathrm{P}^{a_{\mathrm{P},1}+\cdots+a_{\mathrm{P},r_\mathrm{P}}},$$

ce qui permet de conclure.

4.3. Modules de torsion sur les anneaux principaux

4.3.1. Généralités sur les idéaux

Dans tout ce qui suit, les anneaux considérés sont supposés commutatifs. Un anneau A est *intègre* s'il n'est pas réduit à 0 (i.e. si $0 \neq 1$ dans A), et s'il ne possède pas de *diviseur de* 0 (i.e. $xy = 0 \Rightarrow x = 0$ ou $y = 0$). Un idéal I de A est dit *premier* si l'anneau A/I est intègre, ce qui équivaut, en remontant dans A, à « $\mathrm{I} \neq \mathrm{A}$ et $xy \in \mathrm{I} \Rightarrow x \in \mathrm{I}$ ou $y \in \mathrm{I}$ ». En particulier, l'*idéal nul* $\{0\}$ est premier si et seulement si A est intègre.

Lemme 4.9. — *Les conditions suivantes sont équivalentes pour un idéal* I *d'un anneau* A*.*

(i) A/I *est un corps.*

(ii) *Si* $x \in \mathrm{A} - \mathrm{I}$*, alors l'idéal engendré par* I *et* x *contient* 1*.*

(iii) *Les seuls idéaux de* A *contenant* I*, sont* A *et* I*.*

Démonstration. — Si I vérifie (iii) et si $x \notin \mathrm{A}$, alors l'idéal engendré par A et x contient strictement A et donc est égal à A ; en particulier, il contient 1, ce qui démontre l'implication (iii)⇒(ii).

Si I vérifie (ii), et si $x \notin \mathrm{I}$, alors il existe $b \in \mathrm{I}$ et $u \in \mathrm{A}$ tels que $b + ux = 1$. On en déduit que x est inversible dans A/I d'inverse u, et donc que tout élément non nul de A/I est inversible ; autrement dit, A/I est un corps. D'où l'implication (ii)⇒(i).

Finalement, si A/I est un corps, et si J est un idéal de A contenant I, alors J/I est un idéal de A/I, et donc est soit réduit à 0 (ce qui implique $\mathrm{J} = \mathrm{I}$), soit égal à A/I (ce qui implique $\mathrm{J} = \mathrm{A}$). On en déduit l'implication (i)⇒(iii), ce qui permet de conclure.

Un idéal satisfaisant les propriétés du lemme est dit *maximal*. Un corps étant intègre, un idéal maximal est premier, mais la réciproque est fausse. Par exemple, l'idéal (X) de $\mathbf{Z}[\mathrm{X}]$ est premier puisque $\mathbf{Z}[\mathrm{X}]/(\mathrm{X}) = \mathbf{Z}$ est intègre, mais il n'est pas maximal puisque $\mathbf{Z}$ n'est pas un corps.

4.3.2. Anneaux principaux. — Si A est un anneau, un idéal de A est *principal* s'il est engendré par un élément. Un *anneau principal* est un anneau intègre dans lequel tout idéal est principal.

Par exemple, $\mathbf{Z}$ est un anneau principal. En effet, un idéal est en particulier un sous-groupe pour l'addition, et on a vu que tout sous-groupe de $\mathbf{Z}$ est de la forme $\mathrm{D}\mathbf{Z}$, avec $\mathrm{D} \in \mathbf{N}$; c'est donc aussi un idéal principal, et tout idéal de $\mathbf{Z}$ est principal.

De même, K[T] est un anneau principal. En effet, soit I un idéal de K[T] non réduit à 0, et soit $\mathrm{B} \in \mathrm{I} - \{0\}$ de degré minimal. Soit $\mathrm{P} \in \mathrm{I}$, et soit R le reste de la division euclidienne de P par B. Alors

$\mathrm{R} = \mathrm{P} - \mathrm{BQ} \in \mathrm{I}$ puisque $\mathrm{P} \in \mathrm{I}$ et $\mathrm{B} \in \mathrm{I}$, et $\deg \mathrm{R} < \deg \mathrm{B}$ par définition du reste. Ceci implique que $\mathrm{R} = 0$, par construction de B, et donc P est un multiple de B et $\mathrm{I} = (\mathrm{B})$ est principal.

Proposition 4.10. — *Si* A *est un anneau principal, et si* I *est un idéal premier non nul de* A*, alors* A/I *est un corps. Autrement dit, tout idéal premier non nul d'un anneau principal est maximal.*

Démonstration. — Soit J un idéal de A contenant strictement I. Soit a un générateur de J et p un générateur de I. Comme $\mathrm{I} \subset \mathrm{J}$, il existe $b \in \mathrm{A}$ tel que $p = ab$. Comme $\mathrm{J} \neq \mathrm{I}$, on a $a \notin \mathrm{I}$, et comme I est premier, l'égalité $p = ab$ implique que $b \in \mathrm{I}$, et donc qu'il existe $c \in \mathrm{A}$ tel que $b = pc$. On a alors $p(1 - ac) = 0$, et comme A est intègre et $p \neq 0$, cela implique que a est inversible dans A d'inverse c, et donc que $\mathrm{J} = \mathrm{A}$. On en déduit que I est maximal, ce qui permet de conclure.

Lemme 4.11. — *Toute suite croissante d'idéaux de* A *est stationnaire.* (Un anneau vérifiant cette propriété est dit *noethérien*, et donc *un anneau principal est noethérien.*).

Démonstration. — Soit $(\mathrm{I}_n)_{n \in \mathbf{N}}$ une suite croissante d'idéaux de A, et soit $\mathrm{I} = \cup_{n \in \mathbf{N}} \mathrm{I}_n$. Si $a, b \in \mathrm{I}$, il existe $n, m \in \mathbf{N}$ tels que $a \in \mathrm{I}_n$ et $b \in \mathrm{I}_m$, et comme la suite est croissante, a et b appartiennent à $\mathrm{I}_{\sup(n,m)}$, et donc $a + b \in \mathrm{I}_{\sup(n,m)} \subset \mathrm{I}$. Comme I est aussi stable par multiplication par $\lambda \in \mathrm{A}$, cela montre que I est un idéal. Maintenant, I est principal puisqu'on a supposé A principal ; il est donc de la forme (λ), pour un certain $\lambda \in \mathrm{I}$, et il existe $n \in \mathbf{N}$ tel que $\lambda \in \mathrm{I}_n$. On a alors $(\lambda) \subset \mathrm{I}_n \subset \mathrm{I} = (\lambda)$, ce qui montre que $\mathrm{I}_m = \mathrm{I}_n$, quel que soit $m \geqslant n$. Ceci permet de conclure.

Lemme 4.12. — *Tout idéal propre de* A *est contenu dans un idéal maximal.*

Démonstration. — Supposons le contraire. Soit $\mathrm{I} \neq \mathrm{A}$ un idéal de A contenu dans aucun idéal maximal. En particulier, I n'est pas maximal et il existe $\mathrm{I}_1 \neq \mathrm{A}$ contenant strictement I. Alors I_1 n'est contenu dans aucun idéal maximal, sinon un idéal maximal qui contiendrait I_1 contiendrait aussi I, ce qui permet de réitérer le processus, et donc de construire une suite strictement croissante $(\mathrm{I}_n)_{n \in \mathbf{N}}$ d'idéaux de A. Comme ceci est contraire au lemme 4.11, cela permet de conclure.

Lemme 4.13. — *Si* $b \in \mathrm{A} - \{0\}$*, et si* p *est premier et divise* b*, l'idéal* (b/p) *contient strictement* (b)*.*

Démonstration. — Supposons le contraire. Il existe alors $a \in \mathrm{A}$ tel que $b/p = ba$, et donc $b(1 - ap) = 0$. Comme A est intègre, cela implique que p est inversible dans A d'inverse a, ce qui est contraire à l'hypothèse selon laquelle p est premier. Ceci permet de conclure.

On dit que a et b sont *premiers entre eux*, si l'idéal (a, b) de A engendré par a et b est égal à A, ce qui équivaut à l'existence de $u, v \in \mathrm{A}$ tels que $au + bv = 1$ puisque $(a, b) = \{au + bv,\ u, v \in \mathrm{A}\}$, et qu'un idéal de A contenant 1 est égal à A. On écrit souvent $(a, b) = 1$, pour dire que a et b sont premiers entre eux.

Lemme 4.14. — (lemme de Gauss)
(i) *Si* a *est premier avec* b *et* c*, alors* a *est premier avec* bc*.*
(ii) *Si* a *divise* bc *et si* a *est premier avec* b*, alors* a *divise* c*.*

Démonstration. — Si $(a, b) = (a, c) = 1$, il existe u_1, v_1, u_2, v_2 tels que $au_1 + bv_1 = au_2 + cv_2 = 1$. On a donc $1 = (au_1 + bv_1)(au_2 + cv_2) = au + bcv$, avec $u = au_1u_2 + bv_1u_2 + cu_1v_2$ et $v = v_1v_2$, ce qui prouve que $(a, bc) = 1$. On en déduit le premier énoncé.

Si $bc = ad$ et $au + bv = 1$, alors $acu + adv = c$, et donc $a(cu + dv) = c$, ce qui prouve que a divise c ; d'où le second énoncé.

Théorème 4.15. — *Si $a \in \mathrm{A} - \{0\}$, il existe une unité u de* A *et $p_1, \ldots, p_r \in \mathscr{P}_\mathrm{A}$ tels que $a = u\,p_1 \cdots p_r$; de plus, les p_i, pour $1 \leqslant i \leqslant r$, sont uniquement déterminés à l'ordre près. En d'autres termes, a peut se factoriser de manière unique comme produit de facteurs premiers.*

Démonstration. — Commençons par montrer l'existence d'une telle factorisation. Si a est une unité, il n'y a rien à faire puisque $a = a$ est une factorisation sous la forme souhaitée. Si a n'est pas une unité, alors il existe $p_1 \in \mathscr{P}_\mathrm{A}$ divisant a, et on pose $a_1 = a/p_1$, ce qui fait que, d'après le lemme 4.13, l'idéal (a_1) contient strictement (a). En réitérant le processus, on construit une suite d'éléments p_i de $\mathscr{P}_\mathrm{A}$ et une suite d'éléments a_i de A, avec $a_{i+1}p_{i+1} = a_i$. La suite d'idéaux (a_i) est alors strictement croissante, ce qui implique, d'après le lemme 4.11, que le procédé s'arrête. Autrement dit, il existe s tel que a_s soit une unité de A, et $a = a_s p_1 \cdots p_s$ est une factorisation de a sous la forme voulue.

L'unicité se démontre en utilisant le lemme de Gauss. Si $u\,p_1 \cdots p_r = v\,q_1 \cdots q_s$ où les p_i et les q_j sont des nombres premiers et u, v des unités de A, le lemme de Gauss montre que p_r divise l'un des q_j et donc lui est égal. Quitte à permuter les q_j, on peut supposer que $p_r = q_s$, et en divisant les deux membres par $p_r = q_s$ (ce qui est licite car A est intègre), on se ramène à $r - 1$ et $s - 1$, ce qui permet de conclure par récurrence.

On note $v_p(a)$ le nombre de fois que p apparaît dans la factorisation de a en facteurs premiers. Alors $p^{v_p(a)}$ est la plus grande puissance de p divisant a ; on a donc $v_p(ab) = v_p(a) + v_p(b)$ et $v_p(a + b) \geqslant \inf(v_p(a), v_p(b))$.

Si $a_1, \ldots, a_n \in \mathrm{A} - \{0\}$, on définit $\mathrm{pgcd}(a_1, \ldots, a_n)$ par $\mathrm{pgcd}(a_1, \ldots, a_n) = \prod_p p^{\inf_i v_p(a_i)}$, ce qui fait de $\mathrm{pgcd}(a_1, \ldots, a_n)$ le plus grand diviseur commun des a_i (à multiplication près par une unité de A)

Lemme 4.16. — (théorème de Bézout) $\mathrm{pgcd}(a_1, \ldots, a_n)$ *est un générateur de l'idéal $(a_1, \ldots, a_n)$ engendré par les a_i.*

Démonstration. — Commençons par démontrer le résultat pour $n = 2$, et posons $a_1 = a$ et $a_2 = b$. Il est clair que tout élément de (a, b) est un multiple de $\mathrm{pgcd}(a, b)$; il suffit donc de prouver que $d = \mathrm{pgcd}(a, b) \in (a, b)$. Pour cela, écrivons a et b sous la forme $a = udp_1 \cdots p_r$ et $b = vdq_1 \cdots q_s$, où u, v sont des unités de A et $p_1, \ldots, p_r, q_1, \ldots q_s$ des éléments de $\mathscr{P}_\mathrm{A}$. Par définition de d, on a $p_i \neq q_j$ quels que soient i et j, ce qui prouve, d'après le lemme de Gauss, que a/d et b/d sont premiers entre eux. Il existe donc $x, y \in \mathrm{A}$ tels que $(a/d)x + (b/d)y = 1$, et alors $d = ax + by \in (a, b)$, ce que l'on cherchait à démontrer.

Maintenant, comme $\inf_{i \leqslant n} v_p(a_i) = \inf(\inf_{i \leqslant n-1} v_p(a_i), v_p(a_n))$, on a

$$\mathrm{pgcd}(a_1, \ldots, a_n) = \mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n).$$

De même, l'idéal $(a_1, \ldots, a_n)$ est l'idéal engendré par $(a_1, \ldots, a_{n-1})$ et par a_n, ce qui permet de déduire, par récurrence, le cas général du cas $n = 2$.

On dit que les a_i sont *premiers entre eux dans leur ensemble* si $\mathrm{pgcd}(a_1, \ldots, a_n) = 1$, ce qui équivaut (cf. lemme 4.16) à l'existence de $\alpha_1, \ldots, \alpha_n \in \mathrm{A}$ tels que $\alpha_1 a_1 + \cdots + \alpha_n a_n = 1$.

Exercice 4.17. — Soient $\mathrm{A}, \mathrm{B}, \mathrm{C} \in \mathbf{C}[\mathrm{T}]$, non tous constants, premiers entre eux deux à deux, et vérifiant $\mathrm{A} + \mathrm{B} = \mathrm{C}$, et soit $\Delta = \mathrm{AB}' - \mathrm{BA}'$ (on a aussi $\Delta = \mathrm{AC}' - \mathrm{CA}' = \mathrm{CB}' - \mathrm{BC}'$).

(i) Montrer que $\Delta \neq 0$ et $\deg \Delta \leqslant \inf(\deg \mathrm{A} + \deg \mathrm{B}, \deg \mathrm{B} + \deg \mathrm{C}, \deg \mathrm{C} + \deg \mathrm{A}) - 1$.

(ii) Montrer que, si z est un zéro de ABC de multiplicité $m_z \geqslant 1$, alors la multiplicité de z comme zéro de Δ est $m_z - 1$.

(iii) Si $Q \in \mathbf{C}[T]$ est non nul, on note $r(Q)$ le nombre de ses zéros (sans multiplicité[21]). Montrer que[22] $r(ABC) \geqslant \sup(\deg A, \deg B, \deg C) + 1$.

(iv) Montrer que, si $n \geqslant 3$, si A, B, C sont des éléments de $\mathbf{C}[T]$, premiers entre eux deux à deux, et si $A^n + B^n = C^n$, alors A, B et C sont constants (théorème de Fermat pour les polynômes).

Exercice 4.18. — (Tout nombre premier de la forme $4n+1$ est somme de deux carrés (Fermat, 1640)). On aura à utiliser le fait que, si $p \neq 2$ est un nombre premier, l'équation $x^2 + 1$ a une solution dans $\mathbf{F}_p$ si et seulement si p est de la forme $4n+1$ (ex. 3.4).

1) Si $x \in \mathbf{R}$, on peut écrire x de manière unique sous la forme $n+u$, avec $n \in \mathbf{Z}$ et $u \in [\frac{-1}{2}, \frac{1}{2}[$. Ceci permet d'écrire $z = x + iy \in \mathbf{C}$, de manière unique, sous la forme $z = [z] + \{z\}$, où $[z] = n + im$, avec $n, m \in \mathbf{Z}$ et $\{z\} = u + iv$, avec $u, v \in [\frac{-1}{2}, \frac{1}{2}[$.

(i) Vérifier que $K = \{x + iy,\ x, y \in \mathbf{Q}\}$ est un sous-corps de $\mathbf{C}$ et que $A = \{x + iy,\ x, y \in \mathbf{Z}\}$ est un sous-anneau de $\mathbf{C}$ (c'est l'anneau des entiers de Gauss).

(ii) Si $z = x + iy \in K$, soit $N(z) = x^2 + y^2$. Vérifier que $N(z_1 z_2) = N(z_1)N(z_2)$, pour tous $z_1, z_2 \in K$.

(iii) Montrer que u est inversible dans A si et seulement si $N(u) = 1$. En déduire que $A^* = \{1, -1, i, -i\}$.

(iv) Si $a \in A$ et $b \in A - \{0\}$, soit $r = b\{\frac{a}{b}\}$. Montrer que $N(r) < N(b)$. En déduire que l'on peut écrire a sous la forme $a = bc + r$, avec $c, r \in A$ et $N(r) < N(b)$.

(v) Montrer que A est un anneau principal.

2) Notons A^+ l'ensemble des $x + iy \in A$, avec $x > 0$ et $y \geqslant 0$. Tout élément non nul de A peut alors s'écrire de manière unique sous la forme ua, avec $u \in A^*$ et $a \in A^+$. On dit que q est un nombre premier de A si $q \in A^+$ et si l'idéal (q) est premier ; on note $\mathscr{P}_A$ l'ensemble des nombres premiers de A et, comme d'habitude, $\mathscr{P}$ celui des nombres premiers usuels. Comme A est principal, il résulte de la théorie générale que tout élément non nul de A peut se factoriser sous la forme $uq_1 \cdots q_r$, où $u \in A^*$, et $q_1, \cdots, q_r \in \mathscr{P}_A$ sont uniquement déterminés à l'ordre près.

(i) Montrer que, si $q \in \mathscr{P}_A$, alors $\mathbf{Z} \cap (q)$ est un idéal premier de $\mathbf{Z}$. En déduire que q divise un unique $p \in \mathscr{P}$ et que $N(q) = p$ ou $N(q) = p^2$.

(ii) Soit $q \in A^+$. Montrer que $q \in \mathscr{P}_A$ si $N(q) \in \mathscr{P}$.

(iii) Soit $p \in \mathscr{P}$ de la forme $4n+1$. Montrer qu'il existe $a \in A - \{0\}$ tel que $p \mid N(a)$ et $0 < N(a) < p^2$, et que $\mathrm{pgcd}(a, p)$ est premier dans A et divise strictement p.

(iv) Montrer que tout nombre premier de la forme $4n+1$ est somme de deux carrés.

---

[21] Plus généralement, si K est un corps, et si $P \in K[T]$ est non nul, on définirait $r(Q)$ comme le degré du *radical* $\mathrm{rad}(P)$ de P, produit des polynômes unitaires irréductibles divisant P (e.g. si $K = \mathbf{R}$, alors $\mathrm{rad}(X^5(X^2+1)^2(X-2)) = X(X^2+1)(X-2)$).

[22] On dispose d'un dictionnaire heuristique entre $K[T]$ et $\mathbf{Z}$ qui est un guide précieux pour essayer de deviner ce qui peut être vrai en théorie des nombres. Dans ce dictionnaire, $\deg P$ devient $\log|n|$ (voir ci-dessous), et l'énoncé ci-dessus devient (en définissant le *radical* $\mathrm{rad}(n)$ d'un entier n, non nul, comme le produit des nombres premiers divisant n (le radical de $720 = 6!$ est $2 \cdot 3 \cdot 5 = 30$)) : pour tout $\varepsilon > 0$, il existe $C(\varepsilon) > 0$ tel que, si a, b, c sont des entiers, non nuls, premiers entre eux deux à deux, et vérifiant $a + b = c$, alors

$$\sup(\log|a|, \log|b|, \log|c|) \leqslant (1+\varepsilon)\log(\mathrm{rad}(abc)) + C(\varepsilon).$$

Cet énoncé, connu sous le nom de « conjecture *abc* », date de 1985, et ne semble pas sur le point d'être démontré (comme quoi, l'équation $a+b=c$ est plus subtile qu'elle n'en a l'air...). Nous laissons au lecteur le plaisir d'expliciter ce que cet énoncé implique au sujet du théorème de Fermat. Pour justifier l'analogie entre $\deg P$ et $\log|n|$, on peut regarder le cas où K est un corps fini, par exemple $\mathbf{F}_p$: dans ce cas, le cardinal de l'anneau $\mathbf{F}_p[T]/P$ est lié à $\deg P$ par la formule $\log|\mathbf{F}_p[T]/P| = \deg P \cdot \log p$, que l'on peut mettre en parallèle avec la formule $\log|n| = \log|\mathbf{Z}/n\mathbf{Z}|$.

(v) Soit $p \in \mathscr{P}$ impair. Montrer que, si $p \notin \mathscr{P}_{\mathrm{A}}$, il existe $q_p = x + iy \in \mathrm{A}^+$, unique, avec $x > y$, vérifiant $\mathrm{N}(q_p) = p$ et que la factorisation de p est $p = (-i)q_p q_p^*$, où $q_p^* = i\overline{q_p}$.

(vi) Montrer que tout $p \in \mathscr{P}$ de la forme $4n+3$ est premier dans A.

(vii) Montrer que les éléments de $\mathscr{P}_{\mathrm{A}}$ sont $1+i$, les $p \in \mathscr{P}$ de la forme $4n+3$, et les q_p, q_p^*, pour $p \in \mathscr{P}$ de la forme $4n+1$.

4.3.3. Structure des modules de torsion sur un anneau principal. — Les anneaux $\mathbf{Z}$ et $\mathrm{K}[\mathrm{T}]$ sont principaux, ce qui fait que le théorème 4.19 ci-dessous a pour conséquences les th. 3.1 et 4.2.

Soit A un anneau principal, et soit $\mathscr{P}_{\mathrm{A}}$ l'ensemble des idéaux premiers non nuls de A. Choisissons pour tout élément de $\mathscr{P}_{\mathrm{A}}$ un générateur, et identifions $\mathscr{P}_{\mathrm{A}}$ à l'ensemble de ces générateurs. Alors tout élément non nul x de A se factorise, de manière unique, sous la forme $x = u\prod_{p\in\mathscr{P}_{\mathrm{A}}} p^{v_p(x)}$, où u est inversible dans A. De plus, x et y sont premiers entre eux (ce qui signifie que l'idéal de A engendré par x et y contient 1), si et seulement si $\inf(v_p(x), v_p(y)) = 0$ quel que soit $p \in \mathscr{P}_{\mathrm{A}}$, et A/p est un corps quel que soit $p \in \mathscr{P}_{\mathrm{A}}$.

Si M est un A-module, et si $a \in \mathrm{A}$, on note $a\mathrm{M} \subset \mathrm{M}$ l'image du morphisme $x \mapsto ax$ de A-modules. C'est un sous-A-module de M qui est, par construction, tué par a, et donc l'action de A sur $\mathrm{M}/a\mathrm{M}$ se factorise à travers A/a, ce qui fait de $\mathrm{M}/a\mathrm{M}$ un A/a-module. En particulier, si $p \in \mathscr{P}_{\mathrm{A}}$, alors $\mathrm{M}/p\mathrm{M}$ est un espace vectoriel sur le corps A/p.

Théorème 4.19. — *Soit* M *un* A*-module de torsion et de type fini. Si* $p \in \mathscr{P}_{\mathrm{A}}$*, soit* M_p *l'ensemble des* $x \in \mathrm{M}$ *tués par une puissance de* p*.*

(i) M_p *est un sous-*A*-module de* M*, nul sauf pour un nombre fini de* p*, et* $\mathrm{M} = \oplus_{p\in\mathscr{P}_{\mathrm{A}}}\mathrm{M}_p$*.*

(ii) *Si* $r_p = \dim_{\mathrm{A}/p}(\mathrm{M}/p\mathrm{M})$*, alors il existe une unique famille décroissante d'entiers* $a_{p,i} \geqslant 1$*, pour* $1 \leqslant i \leqslant r_p$*, telle que* $\mathrm{M}_p = \oplus_{1\leqslant i\leqslant r_p}\mathrm{A}/p^{a_{p,i}}$*.*

Démonstration. — Si $p^a x = 0$ et $p^b y = 0$, alors $p^{\sup(a,b)}(\lambda x + \mu y) = 0$ quels que soient $\lambda, \mu \in \mathrm{A}$. On en déduit que M_p est un sous-A-module de M.

Soient $x_1, \ldots, x_d$ engendrant M. Si $i \in \{1, \ldots, d\}$, soit $\lambda_i \in \mathrm{A}$ tel que $\lambda_i x_i = 0$, et soit $\lambda = \lambda_1 \cdots \lambda_d$. On a $\lambda x = 0$ quel que soit $x \in \mathrm{M}$. Si $p \in \mathscr{P}_{\mathrm{A}}$ ne divise pas λ, et si $x \in \mathrm{M}_p$ est tué par p^a, alors x est tué par tout élément de l'idéal (λ, p^a) de A engendré par λ et p^a, c'est-à-dire par A, puisque λ et p^a sont premiers entre eux. On a donc $x = 0$, et $\mathrm{M}_p = 0$ si p ne divise pas λ.

Soit $\mathscr{P}_{\mathrm{A}}(\lambda) \subset \mathscr{P}_{\mathrm{A}}$ l'ensemble des diviseurs premiers de λ, et soit $\lambda = \prod_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)} p^{n_p}$ la factorisation de λ en facteurs premiers. Les $\frac{\lambda}{p^{n_p}}$, pour $p \in \mathscr{P}_{\mathrm{A}}(\lambda)$ sont premiers entre eux dans leur ensemble. Il existe donc, d'après le théorème de Bézout, des éléments α_p de A tels que l'on ait $\sum_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)} \alpha_p \frac{\lambda}{p^{n_p}} = 1$. On en déduit que l'on peut décomposer tout élément x de M sous la forme $\sum_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)} x_p$, avec $x_p = \frac{\alpha_p\lambda}{p^{n_p}}x$, et $x_p \in \mathrm{M}_p$ car x_p est tué par p^{n_p}. En résumé, $\mathrm{M} = \sum_{p\in\mathscr{P}} \mathrm{M}_p$.

Enfin, si $x_p \in \mathrm{M}_p$, pour $p \in \mathscr{P}_{\mathrm{A}}(\lambda)$, et si $\sum_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)} x_p = 0$, alors $x_p = -\sum_{\ell\neq p} x_\ell$ est à la fois tué par p^{n_p} et par $p^{-n_p}\lambda$, qui sont premiers entre eux par définition de n_p. On a donc $x_p = 0$ quel que soit p, ce qui termine de démontrer le (i).

Passons à la démonstration du (ii). Commençons par montrer que l'on peut calculer r_p en ne considérant que M_p. Si $\ell \in \mathscr{P}_{\mathrm{A}}$ est distinct de p, la multiplication par p induit une surjection sur M_ℓ : en effet, il existe n tel que $\ell^n\mathrm{M}_\ell = 0$, et comme p et ℓ^n sont premiers entre eux, il existe $a, b \in \mathrm{A}$ tels que $ap + b\ell^n = 1$. Les multiplications par a et p sont inverses l'une de l'autre sur M_ℓ, et donc $\mathrm{M}_\ell/p\mathrm{M}_\ell = 0$. Il en résulte que r_p est aussi la dimension de $\mathrm{M}_p/p\mathrm{M}_p$ sur A/p.

La démonstration du (ii) va se faire en deux étapes. On commence par démontrer, par récurrence sur $r = r_p$ (le cas $r = 0$ étant vide), l'existence d'une décomposition sous la forme voulue, puis on démontre, toujours par récurrence, l'unicité de la famille $a_{p,i}$.

Si $x \in \mathrm{M}_p$, on note $n(x)$ le plus petit $n \in \mathbf{N}$ tel que $p^n x = 0$. Donc $p^{n(x)}x = 0$ et $p^{n(x)-1}x \neq 0$, si $n(x) \geqslant 1$. Soient $e_1 \in \mathrm{M}_p$ réalisant le maximum de $n(x)$, pour $x \in \mathrm{M}_p$ (comme $n(x) \leqslant n_p$, quel que soit $x \in \mathrm{M}_p$, il existe un tel e_1), et $a_1 = n(e_1)$. Soit $\mathrm{N} = \mathrm{M}_p/(\mathrm{A}/p^{a_1})e_1$. Alors $\mathrm{N}/p\mathrm{N}$ est, d'après le lemme 4.20 ci-dessous (utilisé pour $\mathrm{M} = \mathrm{M}_p$, $\mathrm{M}' = p\mathrm{M}_p$ et $\mathrm{M}'' = (\mathrm{A}/p^{a_1})e_1$) le quotient de $\mathrm{M}_p/p\mathrm{M}_p$ par le sous-(A/p)-espace vectoriel engendré par l'image de e_1, et comme cette image est non nulle (sinon, on aurait $e_1 = pf$ et $n(f) = n(e_1) + 1 > n(e_1)$), on en déduit que $\dim_{\mathrm{A}/p}(\mathrm{N}/p\mathrm{N}) = r - 1$, ce qui permet d'appliquer l'hypothèse de récurrence à N. Il existe donc $\overline{e}_2, \dots, \overline{e}_r \in \mathrm{N}$ et $a_2 \geqslant \cdots \geqslant a_r$ tels que $\mathrm{N} = \oplus_{2 \leqslant i \leqslant r}(\mathrm{A}/p^{a_i})\overline{e}_i$.

Soit $e_i' \in \mathrm{M}_p$ un relèvement quelconque de $\overline{e}_i$. On a alors $p^{a_i}e_i' = b_i e_1$, avec $b_i \in \mathrm{A}$, bien défini modulo p^{a_1}. Comme $p^{a_1}e_i' = 0$, on en déduit que $p^{a_1-a_i}b_i \in p^{a_1}\mathrm{A}$, et donc que $b_i \in p^{a_i}\mathrm{A}$. Soit $c_i = p^{-a_i}b_i \in \mathrm{A}$, et soit $e_i = e_i' - c_i e_1$. On a alors $p^{a_i}e_i = 0$. Maintenant, soit $x \in \mathrm{M}_p$, et soit $\overline{x}$ son image dans N. Il existe alors $\lambda_2 \in \mathrm{A}/p^{a_2}, \dots, \lambda_r \in \mathrm{A}/p^{a_r}$, uniques, tels que $\overline{x} = \lambda_2\overline{e}_2 + \cdots + \lambda_r\overline{e}_r$. Comme $p^{a_i}e_i = 0$, l'élément $\lambda_i e_i$ de M_p est bien défini, et $x - \sum_{i=2}^r \lambda_i e_i \in (\mathrm{A}/p^{a_1})e_1$, et donc $\mathrm{M}_p = (\mathrm{A}/p^{a_1})e_1 + \big((\mathrm{A}/p^{a_2})e_2 \oplus \cdots \oplus (\mathrm{A}/p^{a_r})e_r\big)$. De plus, $(\mathrm{A}/p^{a_1})e_1 \cap \big((\mathrm{A}/p^{a_2})e_2 \oplus \cdots \oplus (\mathrm{A}/p^{a_r})e_r\big) = 0$ car un élément de l'intersection a une image nulle dans N, et que $x \mapsto \overline{x}$ induit une bijection de $(\mathrm{A}/p^{a_2})e_2 \oplus \cdots \oplus (\mathrm{A}/p^{a_r})e_r$ sur N. Il en résulte que $\mathrm{M}_p = (\mathrm{A}/p^{a_1})e_1 \oplus (\mathrm{A}/p^{a_2})e_2 \oplus \cdots \oplus (\mathrm{A}/p^{a_r})e_r$. Comme $a_1 \geqslant a_2$, cela fournit une décomposition de M_p sous la forme voulue.

Il reste l'unicité des $a_{p,i}$. Supposons que $\mathrm{M}_p = \oplus_{1 \leqslant i \leqslant r}(\mathrm{A}/p^{a_i})e_i = \oplus_{1 \leqslant j \leqslant s}(\mathrm{A}/p^{b_j})f_j$, avec $a_1 \geqslant a_2 \geqslant \cdots a_r \geqslant 1$ et $b_1 \geqslant b_2 \geqslant \cdots b_s \geqslant 1$. Soit $n(\mathrm{M}_p)$ le maximum des $n(x)$, pour $x \in \mathrm{M}_p$. Alors $n(\mathrm{M}_p) = a_1$ et $n(\mathrm{M}_p) = b_1$, et donc $a_1 = b_1$. Maintenant, on peut écrire e_1 sous la forme $e_1 = \sum_{j=1}^s \lambda_j f_j$, et comme $p^{a_1-1}e_1 \neq 0$, cela implique qu'il existe j tel que $p^{a_1-1}\lambda_j f_j \neq 0$. En particulier, on a $p^{a_1-1}f_j \neq 0$, ce qui prouve que $b_j \geqslant a_1 = b_1$ et donc que $b_j = b_1$. Quitte à permuter les f_j, on peut donc supposer $j = 1$. La propriété $p^{a_1-1}\lambda_1 f_1 \neq 0$ implique alors (car $a_1 = b_1$) que $\lambda_1 \notin p\mathrm{A}$, et donc que λ_1 est premier à p et p^{a_1}, et est inversible dans $\mathrm{A}/p^{a_1}\mathrm{A}$. En notant μ_1 son inverse, cela permet d'écrire f_1 sous la forme $\mu_1 e_1 - \sum_{j=2}^s \mu_1\lambda_j f_j$, ce qui prouve que l'on a aussi $\mathrm{M}_p = (\mathrm{A}/p^{b_1})e_1 \oplus_{2 \leqslant j \leqslant s} (\mathrm{A}/p^{b_j})f_j$. On en déduit que $\mathrm{M}_p/(\mathrm{A}/p^{b_1})e_1 = \oplus_{2 \leqslant i \leqslant r}(\mathrm{A}/p^{a_i})e_i = \oplus_{2 \leqslant j \leqslant s}(\mathrm{A}/p^{b_j})f_j$, et une récurrence immédiate permet d'en conclure que l'on a $a_i = b_i$ quel que soit i (et donc aussi que $r = s$). Ceci termine la démonstration.

Lemme 4.20. — *Soient* M *un* A*-module, et* $\mathrm{M}', \mathrm{M}''$ *deux sous-modules de* M*. Alors :*

(i) $\mathrm{M}' + \mathrm{M}'' = \{x + y,\ x \in \mathrm{M}',\ y \in \mathrm{M}''\}$ *est un sous-module de* M *;*

(ii) *l'image de* M' *dans* M/M'' *est*[23] $\mathrm{M}'/(\mathrm{M}' \cap \mathrm{M}'')$ *et celle de* M'' *dans* M/M' *est* $\mathrm{M}''/(\mathrm{M}' \cap \mathrm{M}'')$ *;*

(iii) *les* A*-modules* $(\mathrm{M}/\mathrm{M}'')/(\mathrm{M}'/(\mathrm{M}' \cap \mathrm{M}''))$ *et* $(\mathrm{M}/\mathrm{M}')/(\mathrm{M}''/(\mathrm{M}' \cap \mathrm{M}''))$ *sont naturellement isomorphes à* $\mathrm{M}/(\mathrm{M}' + \mathrm{M}'')$ *; en particulier, ils sont isomorphes entre eux.*

Démonstration. — Le (i) est immédiat. Maintenant, la composée de l'injection de M' dans M avec la projection de M sur M/M'' fournit un morphisme de A-modules dont le noyau est $\mathrm{M}' \cap \mathrm{M}''$; l'image est donc isomorphe à $\mathrm{M}'/(\mathrm{M}' \cap \mathrm{M}'')$. L'argument étant le même dans l'autre cas, en inversant les rôles de M' et M'', cela démontre le (ii).

Enfin, l'application naturelle de M' dans $(\mathrm{M}' + \mathrm{M}'')/\mathrm{M}''$ est surjective (si $x \in \mathrm{M}'$ et $y \in \mathrm{M}''$, alors l'image de $x + y$ est aussi celle de x), et son noyau est $\mathrm{M}' \cap \mathrm{M}''$. L'image de M' dans M/M'' est donc aussi $(\mathrm{M}' + \mathrm{M}'')/\mathrm{M}''$, ce qui fait que $(\mathrm{M}/\mathrm{M}'')/(\mathrm{M}'/(\mathrm{M}' \cap \mathrm{M}'')) = (\mathrm{M}/\mathrm{M}'')/((\mathrm{M}' + \mathrm{M}'')/\mathrm{M}'') = \mathrm{M}/(\mathrm{M}' + \mathrm{M}'')$ (le noyau de la projection de M sur $\mathrm{M}/(\mathrm{M}' + \mathrm{M}'')$ contient M' et donc cette projection se factorise à travers M/M' ; comme l'application induite est surjective et que son noyau est $(\mathrm{M}' + \mathrm{M}'')/\mathrm{M}''$, cela fournit l'isomorphisme $(\mathrm{M}/\mathrm{M}'')/((\mathrm{M}' + \mathrm{M}'')/\mathrm{M}'') = \mathrm{M}/(\mathrm{M}' + \mathrm{M}'')$ ci-dessus). On en déduit le (iii).

[23] Plus exactement : « est naturellement isomorphe à »

Exercice 4.21. — Soit G un groupe, et soient G', G'' deux sous-groupes distingués de G.
(i) Montrer que $G' \cap G''$ et $G'G'' = \{xy,\ x \in G'\ y \in G''\}$ sont des sous-groupes distingués de G.
(ii) Montrer que $(G/G')/(G''/(G' \cap G''))$ et $(G/G'')/(G'/(G' \cap G''))$ sont isomorphes. (On pourra les comparer à $G/(G'G'')$.)

5. Topologie

Les notions de topologie générale interviennent directement dans toutes les branches des mathématiques, comme on s'en est aperçu graduellement à partir des travaux de Hausdorff (1906). Parmi les espaces topologiques, les espaces métriques (dont les espaces vectoriels normés sont un cas particulier fondamental[24]), définis par Fréchet (1906), forment une catégorie d'objets aux propriétés particulièrement agréables. Les suites y jouent un rôle privilégié permettant souvent de simplifier les démonstrations qui, pour un espace topologique général, utilisent le langage de la théorie des ensembles. Chaque fois que c'est le cas, nous avons doublé la démonstration dans le cas général d'une démonstration propre aux espaces métriques afin de diversifier les approches.

5.1. Espaces topologiques

5.1.1. Ouverts, fermés, voisinages

Si X est un ensemble, une *topologie* $\mathscr{T}$ sur X est un sous-ensemble de l'ensemble des parties de X, contenant X et $\emptyset$, stable par intersection finie et par réunion quelconque. Avec des quantificateurs, cela se traduit par :
- $\emptyset \in \mathscr{T}$ et $X \in \mathscr{T}$;
- si I est un ensemble fini, et si $U_i \in \mathscr{T}$, pour $i \in I$, alors $\cap_{i\in I} U_i \in \mathscr{T}$;
- si I est un ensemble quelconque, et si $U_i \in \mathscr{T}$, pour $i \in I$, alors $\cup_{i\in I} U_i \in \mathscr{T}$.

Si $(X, \mathscr{T})$ est un *espace topologique* (i.e. un ensemble X muni d'une topologie $\mathscr{T}$), les éléments de $\mathscr{T}$ sont *les ouverts*. On dit que $F \subset X$ est *fermé*, si son complémentaire est ouvert. Donc X et $\emptyset$ sont des fermés, et les fermés sont stables par réunion finie et intersection quelconque.

Une *base d'ouverts* pour une topologie $\mathscr{T}$ est un sous-ensemble $\mathscr{B}$ de $\mathscr{T}$ tel que tout élément de $\mathscr{T}$ soit réunion d'éléments de $\mathscr{B}$. Par exemple, dans un espace métrique (voir plus loin), les boules ouvertes forment une base d'ouverts.

Si $(X, \mathscr{T})$ est un espace topologique, et si $x \in X$, un *voisinage* V de x est un sous-ensemble de X contenant un ouvert contenant x. Un ensemble est donc ouvert si et seulement si il est voisinage de chacun de ses points.

[24] Mais il y a quand même des exemples parfaitement naturels de distances qui ne sont pas induites par une norme sur un espace vectoriel ambiant ; par exemple, la distance sur la terre n'est pas induite par une norme sur l'espace (à moins que la terre ne soit redevenue plate...).

Une *base de voisinages* de x est une famille de voisinages de x telle que tout ouvert contenant x contienne un élément de la famille. Par exemple, dans un espace métrique, les boules ouvertes de centre x ou les boules fermées de centre x et de rayon non nul forment une base de voisinages de x.

5.1.2. Exemples

• La *topologie discrète* sur un ensemble X est celle pour laquelle $\mathscr{T} = \mathscr{P}(\mathrm{X})$, ensemble des parties de X. De manière équivalente, X est muni de la topologie discrète si les singletons sont des ouverts (en effet toute partie de X est la réunion des singletons qu'elle contient).

• La *topologie grossière* sur X est la topologie dont les seuls ouverts sont X et $\emptyset$.

• La topologie naturelle sur $\mathbf{R}$ est celle pour laquelle les segments ouverts forment une base d'ouverts.

• Si E est un espace vectoriel sur $\mathbf{R}$ ou $\mathbf{C}$ muni d'une norme $\| \ \|$, la topologie sur E associée à $\| \ \|$ est celle pour laquelle les boules ouvertes forment une base d'ouverts.

• La *topologie de Zariski* sur $\mathbf{C}^n$ est définie de la manière suivante : $\mathrm{F} \subset \mathbf{C}^n$ est un *fermé de Zariski* si et seulement si il existe une famille de polynômes $\mathrm{P}_i \in \mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, pour $i \in \mathrm{I}$, telle que F soit l'ensemble des zéros communs des P_i (i.e. $\mathrm{F} = \cap_{i\in\mathrm{I}}\{z \in \mathbf{C}^n,\ \mathrm{P}_i(z) = 0\}$). Alors $\mathbf{C}^n$ est un fermé de Zariski (en prenant une famille vide), $\emptyset$ est un fermé de Zariski (en prenant $\mathrm{P}_1 = \mathrm{X}_1$ et $\mathrm{P}_2 = \mathrm{X}_1 - 1$), et une intersection quelconque des fermés de Zariski est un fermé de Zariski (si F_j, pour $j \in \mathrm{J}$, est l'ensemble des zéros communs de la famille $(\mathrm{P}_{i,j})_{i\in\mathrm{I}_j}$, alors $\cap_{j\in\mathrm{J}}\mathrm{F}_j$ est l'ensemble des zéros communs de la famille $(\mathrm{P}_{i,j})_{j\in\mathrm{J},\, i\in\mathrm{I}_j}$), ce qui montre qu'en définissant un ouvert de $\mathbf{C}^n$ pour la topologie de Zariski comme le complémentaire d'un fermé de Zariski, on obtient bien une topologie dont les fermés sont les fermés de Zariski.

• On peut munir un ensemble quelconque de la *topologie du filtre des complémentaires des parties finies*, pour laquelle une partie non vide est un ouvert si et seulement si elle a un complémentaire fini.

5.1.3. Comparaison de topologies

Si $\mathscr{T}_1$ et $\mathscr{T}_2$ sont deux topologies sur X, on dit que $\mathscr{T}_1$ est *plus fine* que $\mathscr{T}_2$ si $\mathscr{T}_1$ contient $\mathscr{T}_2$. Le summum de la finesse est donc la discrétion ; à l'opposé, la topologie la moins fine est la topologie grossière. On fera attention au fait que, si on prend deux topologies quelconques, il n'y a aucune raison pour qu'il y en ait une qui soit plus fine que l'autre (cf. ex. 10.2).

5.2. Espaces métriques

Si X est un ensemble, une application $d : \mathrm{X} \times \mathrm{X} \to \mathbf{R}_+$ est une *distance* sur X si elle vérifie les propriétés suivantes :

- $d(x, y) = 0$ si et seulement si $x = y$ (séparation) ;
- $d(x, y) = d(y, x)$ quels que soient $x, y \in \mathrm{X}$;

• $d(x,z) \leqslant d(x,y) + d(y,z)$ quels que soient $x, y, z \in \mathrm{X}$ (inégalité triangulaire).

• Si la distance vérifie l'inégalité $d(x,z) \leqslant \sup(d(x,y), d(y,z))$ plus forte que l'inégalité triangulaire, on dit qu'elle est *ultramétrique* ou *non archimédienne*.

Si $x \in \mathrm{X}$ et $r > 0$, on note $\mathrm{B}(x,r) = \{y \in \mathrm{X},\ d(x,y) \leqslant r\}$ la *boule fermée de centre x et de rayon r*, et $\mathrm{B}(x,r^-) = \{y \in \mathrm{X},\ d(x,y) < r\}$ la *boule ouverte de centre x et de rayon r*.

• Une boule ouverte contient une boule ouverte centrée en chacun de ses points.

L'inégalité triangulaire montre que, si $r > 0$, si $y \in \mathrm{B}(x,r^-)$, et si $s = r - d(x,y)$, alors $\mathrm{B}(y,s^-) \subset \mathrm{B}(x,r^-)$.

• L'ensemble $\mathscr{T}_d$ constitué de $\emptyset$ et des réunions (quelconques) de boules ouvertes est une topologie sur X, et $\mathrm{U} \in \mathscr{T}_d$ si et seulement si, quel que soit $x \in \mathrm{U}$, il existe $r > 0$ tel que $\mathrm{B}(x,r^-) \subset \mathrm{U}$.

Par construction $\mathscr{T}_d$ contient $\emptyset$ et X et est stable par réunion quelconque. Il suffit donc de prouver que $\mathscr{T}_d$ est stable par intersection finie. Soit $\mathrm{U} \in \mathscr{T}_d$ non vide, et soit $x \in \mathrm{U}$. Par définition de $\mathscr{T}_d$, il existe $y \in \mathrm{X}$ et $r > 0$ tels que $\mathrm{B}(y,r^-) \subset \mathrm{U}$ et $x \in \mathrm{B}(y,r^-)$; le point ci-dessus montre qu'il existe $s > 0$ tel que $\mathrm{B}(x,s^-) \subset \mathrm{B}(y,r^-) \subset \mathrm{U}$. La stabilité par intersection finie s'en déduit puisque si $(\mathrm{U}_i)_{i\in\mathrm{I}}$ est une famille finie d'éléments de $\mathscr{T}_d$, et si $x \in \cap_{i\in\mathrm{I}}\mathrm{U}_i$, alors pour tout i, il existe $s_i > 0$ tel que $\mathrm{B}(x,s_i^-) \subset \mathrm{U}_i$, ce qui fait que $\cap_{i\in\mathrm{I}}\mathrm{U}_i$ contient $\mathrm{B}(x,s^-)$, si $s = \inf_{i\in\mathrm{I}} s_i$ (et $s \neq 0$ car I est fini).

On note en général (X, d) au lieu de $(\mathrm{X}, \mathscr{T}_d)$ l'espace topologique ainsi obtenu. Un espace topologique obtenu de cette manière est appelé un *espace métrique*. Par construction, les boules ouvertes forment une base d'ouverts de la topologie.

Deux distances sur X sont *équivalentes* si elles définissent la même topologie.

Un espace topologique $(\mathrm{X}, \mathscr{T})$ est *métrisable* s'il existe une distance d sur X telle que l'on ait $\mathscr{T} = \mathscr{T}_d$.

• Dans un espace métrique, les boules fermées sont des fermés.

Si $x \notin \mathrm{B}(x_0,r)$, et si $s = d(x,x_0) - r$, alors $s > 0$ et le complémentaire de $\mathrm{B}(x_0,r)$ contient $\mathrm{B}(x,s^-)$. On en déduit que ce complémentaire est ouvert et donc que $\mathrm{B}(x_0,r)$ est fermée.

• Si (X, d) est un espace métrique, et si $x \in \mathrm{X}$, les $\mathrm{B}(x,r^-)$ forment une base de voisinages de x ; il en est de même des $\mathrm{B}(x,r)$, pour $r > 0$.

On a vu ci-dessus que si U est un ouvert non vide contenant x, alors U contient une boule ouverte $\mathrm{B}(x,r^-)$, avec $r > 0$, ce qui prouve que les $\mathrm{B}(x,r^-)$ forment une base de voisinages de x. De plus, $\mathrm{B}(x,r^-)$ contient $\mathrm{B}(x,r/2)$ qui contient $\mathrm{B}(x,(r/2)^-)$, ce qui prouve que les $\mathrm{B}(x,r)$ forment aussi une base de voisinages de x.

• Deux distances d_1 et d_2 sur un ensemble X sont équivalentes si et seulement si, pour tout $x \in \mathrm{X}$, toute boule ouverte de centre x pour d_1 contient une boule ouverte de centre x pour d_2 et réciproquement.

La première condition équivaut à ce que l'identité $(\mathrm{X}, d_2) \to (\mathrm{X}, d_1)$ est continue, ainsi que son inverse, et la seconde condition est une traduction de cette bicontinuité utilisant le fait que les boules ouvertes de centre x forment une base de voisinages de x.

Exercice 5.1. — Montrer que, si (X, d) est un espace métrique, et si $x \in \mathrm{X}$, les $\mathrm{B}(x, 2^{-j})$, pour $j \in \mathbf{N}$, forment une base de voisinages de x.

Exercice 5.2. — Soit X un ensemble. Montrer que $d : \mathrm{X} \times \mathrm{X} \to \mathbf{R}_+$, définie par $d(x, y) = 0$ si $x = y$ et $d(x, y) = 1$, si $x \neq y$, est une distance (*la distance triviale*) sur X. Quelle est la topologie associée ?

Exercice 5.3. — Soit $f : \mathbf{R} \to \mathbf{R}$ définie par $f(x) = \frac{x}{1+|x|}$. Montrer que $(x, y) \mapsto d'(x, y) = |f(x) - f(y)|$ est une distance sur $\mathbf{R}$, qui est équivalente à la distance usuelle $d(x, y) = |x - y|$.

5.3. Continuité

Si X et Y sont deux espaces topologiques, si $f : \mathrm{X} \to \mathrm{Y}$ est une application, et si $x \in \mathrm{X}$, on dit que f est *continue en* x, si quel que soit l'ouvert V de Y contenant $f(x)$, il existe un ouvert U de X, contenant x, tel que $f(\mathrm{U}) \subset \mathrm{V}$. De manière équivalente, f est continue en x si, quel que soit le voisinage V de $f(x)$ dans Y, il existe un voisinage U de x tel que $f(\mathrm{U}) \subset \mathrm{V}$. Il suffit de vérifier ceci pour V dans une base de voisinages de $f(x)$.

On dit que $f : \mathrm{X} \to \mathrm{Y}$ est *continue*, si elle est continue en tout point $x \in \mathrm{X}$.

On dit que $f : \mathrm{X} \to \mathrm{Y}$ est un *homéomorphisme* si f est continue bijective, et si sa réciproque $f^{-1} : \mathrm{Y} \to \mathrm{X}$ est continue. On dit que X et Y sont *homéomorphes*[25] s'il existe un homéomorphisme $f : \mathrm{X} \to \mathrm{Y}$.

Si (X, d) est un espace métrique, si $(\mathrm{Y}, \mathscr{T})$ est un espace topologique, et si $x_0 \in \mathrm{X}$, on voit, en revenant à la définition, que $f : \mathrm{X} \to \mathrm{Y}$ est continue en x_0 si et seulement si, pour tout U ouvert de Y contenant $f(x_0)$, il existe $\delta > 0$ tel que $d(x_0, x) < \delta$ implique $f(x) \in \mathrm{U}$. Si Y est aussi métrique, cela se traduit (au choix) par :

- pour tout $\varepsilon > 0$, il existe $\delta = \delta(x, \varepsilon) > 0$ tel que $d_{\mathrm{X}}(x_0, x) < \delta \Rightarrow d_{\mathrm{Y}}(f(x_0), f(x)) < \varepsilon$;
- pour tout $j \in \mathbf{N}$, il existe $\delta = \delta(x, j) > 0$ tel que $d_{\mathrm{X}}(x_0, x) < \delta \Rightarrow d_{\mathrm{Y}}(f(x_0), f(x)) \leqslant 2^{-j}$.

On dit que $f : \mathrm{X} \to \mathrm{Y}$ est *uniformément continue* sur X, si pour tout $\varepsilon > 0$ il existe $\delta = \delta(\varepsilon) > 0$ tel que $d_{\mathrm{X}}(x, x') < \delta$ implique $d_{\mathrm{Y}}(f(x), f(x')) < \varepsilon$. La différence entre la continuité et la continuité uniforme est que δ ne dépend pas de x ; en particulier, une application uniformément continue est continue.

Si $\kappa \in \mathbf{R}_+$, on dit que $f : \mathrm{X} \to \mathrm{Y}$ est *κ-lipschitzienne* (ou *lipschitzienne de rapport κ*), si on a $d_{\mathrm{Y}}(f(x), f(x')) \leqslant \kappa\, d_{\mathrm{X}}(x, x')$, quels que soient $x, x' \in \mathrm{X}$. Une application lipschitzienne est uniformément continue et donc aussi continue.

Exercice 5.4. — Soit (X, d) un espace métrique. Montrer que $d : \mathrm{X} \to \mathbf{R}$ est continue.

- Les conditions suivantes sont équivalentes :
  (i) $f : \mathrm{X} \to \mathrm{Y}$ est continue ;

[25] Montrer que deux espaces topologiques ne sont pas homéomorphes est loin d'être évident en général (le lecteur est invité à essayer de prouver qu'un pneu et un ballon de football ne sont pas homéomorphes) ; la topologie algébrique (Analysis in situ de Poincaré) fournit des tas d'outils permettant de le faire.

(ii) il existe une base d'ouverts $\mathscr{B}$ de Y telle que l'image réciproque par f de tout $U \in \mathscr{B}$ est un ouvert de X ;

(iii) l'image réciproque par f de tout ouvert de Y est un ouvert de X ;

(iv) l'image réciproque par f de tout fermé de Y est un fermé de X.

L'équivalence de (iii) et (iv) vient juste de ce que l'image réciproque du complémentaire est le complémentaire de l'image réciproque (si $A \subset Y$, alors $f^{-1}(Y - A) = X - f^{-1}(A)$).

Si f est continue, si V est un ouvert de Y, et si $y \in V \cap f(X)$, il existe, pour tout $x \in X$ vérifiant $f(x) = y$, un ouvert U_x de X qui contient x et vérifie $f(U_x) \subset V$. Alors $U = \cup_{y \in V \cap f(X)} \big(\cup_{x \in f^{-1}(y)} U_x \big)$ est un ouvert qui contient $\cup_{y \in V \cap f(X)} f^{-1}(y) = f^{-1}(V)$, et qui vérifie $f(U) \subset V$, ce qui prouve que $f^{-1}(V) = U$ et donc que $f^{-1}(V)$ est ouvert. On en déduit l'implication (i)⇒(iii), et comme l'implication (iii)⇒(i) est immédiate (si V est un ouvert contenant $f(x)$, alors $U = f^{-1}(V)$ est un ouvert de X qui contient x et qui vérifie $f(U) \subset V$), cela prouve que les propriétés (i) et (iii) sont équivalentes.

L'implication (iii)⇒(ii) est immédiate. Réciproquement, soit $\mathscr{B}$ une base d'ouverts de Y, et soit V un ouvert de Y. Il existe alors une famille $(V_i)_{i \in V}$ d'éléments de $\mathscr{B}$ telle que $V = \cup_{i \in I} V_i$. On a alors $f^{-1}(V) = \cup_{i \in I} f^{-1}(V_i)$, et si $f^{-1}(V_i)$ est ouvert pour tout i, il en est de même de $f^{-1}(V)$. On en déduit l'équivalence des propriétés (ii) et (iii), ce qui permet de conclure.

• Soient X, Y, Z des espaces topologiques. Si $f : X \to Y$ est continue en x, et si $g : Y \to Z$ est continue en $f(x)$, alors $g \circ f : X \to Z$ est continue en x ; si $f : X \to Y$ et $g : Y \to Z$ sont continues, alors $g \circ f : X \to Z$ est continue.

Soit W un ouvert de Z contenant $g(f(x))$. Comme g est continue en $f(x)$, il existe un ouvert V de Y qui contient $f(x)$ et qui vérifie $g(V) \subset W$, et comme f est continue en x, il existe un ouvert U de X qui contient x et qui vérifie $f(U) \subset V$. Alors $g \circ f(U) \subset W$, ce qui permet de démontrer le premier énoncé ; le second en est une conséquence immédiate

5.4. Sous-espaces, produits, quotients

5.4.1. Topologie induite

Si $(X, \mathscr{T})$ est un espace topologique, et si $Y \subset X$, alors $\mathscr{T}_Y = \{U \cap Y,\ U \in \mathscr{T}\}$ est une topologie sur Y appelée la *topologie induite*. Autrement dit, tout sous-ensemble d'un espace topologique est naturellement un espace topologique.

5.4.2. Topologie produit

Si $(X_i, \mathscr{T}_i)_{i \in I}$ est une famille (éventuellement infinie) d'espaces topologiques, on appelle *topologie produit* sur $X = \prod_{i \in I} X_i$, la topologie la moins fine rendant continues les projections $p_i : X \to X_i$, pour $i \in I$. De manière explicite, une base d'ouverts pour cette topologie est constituée des $\prod_{i \in J} U_i \times \prod_{i \in I - J} X_i$, où J décrit les sous-ensembles *finis* de I, et U_i est, si $i \in J$, un ouvert de X_i.

• Si Y est un espace topologique, alors $f : Y \to \prod_{i \in I} X_i$ est continue si et seulement si $p_i \circ f : Y \to X_i$ est continue, quel que soit $i \in I$.

Comme la composée d'applications continues est continue, si $f : Y \to \prod_{i \in I} X_i$ est continue, alors $p_i \circ f : Y \to X_i$ est continue, quel que soit $i \in I$. Réciproquement, si les $p_i \circ f$, pour $i \in I$, sont continues, et si $U = \prod_{i \in J} U_i \times \prod_{i \in I - J} X_i$, où $J \subset I$ est fini, est un élément de la base

d'ouverts ci-dessus, alors $f^{-1}(\mathrm{U}) = \cap_{i\in \mathrm{J}}(p_i \circ f)^{-1}(\mathrm{U}_i)$ est un ouvert comme intersection finie d'ouverts. Ceci implique que f est continue, ce qui permet de conclure.

• Si $(\mathrm{X}, d_\mathrm{X})$ et $(\mathrm{Y}, d_\mathrm{Y})$ sont deux espaces métriques, alors l'espace topologique $\mathrm{X}\times\mathrm{Y}$ est métrisable, la topologie produit pouvant être définie par la distance $d_{\mathrm{X}\times\mathrm{Y}}((x,y),(x',y')) = \sup(d_\mathrm{X}(x,x'), d_\mathrm{Y}(y,y'))$, ou par toute autre distance équivalente, comme par exemple $\sqrt{d_\mathrm{X}(x,x')^2 + d_\mathrm{Y}(y,y')^2}$.

La distance $d_{\mathrm{X}\times\mathrm{Y}}$ fait qu'une boule de $\mathrm{X}\times\mathrm{Y}$ est le produit d'une boule de X et d'une boule de Y, ce qui prouve que la topologie qu'elle définit est bien la topologie produit.

5.4.3. Topologie quotient

Si X est un espace topologique et $\sim$ est une relation d'équivalence sur X, on définit la *topologie quotient* sur $\mathrm{X}/\sim$ en disant que U est ouvert dans $\mathrm{X}/\sim$ si et seulement si son image inverse dans X est ouverte dans X. C'est la topologie la plus fine rendant continue la surjection canonique $\pi : \mathrm{X} \to \mathrm{X}/\sim$.

• Si Y est un espace topologique, alors $f : \mathrm{X}/\sim \to \mathrm{Y}$ est continue si et seulement si $f\circ\pi : \mathrm{X}\to\mathrm{Y}$ est continue.

$f : \mathrm{X}/\sim \to \mathrm{Y}$ est continue est continue si et seulement si $f^{-1}(\mathrm{U})$ est ouvert pour tout ouvert U de Y, ce qui équivaut, par définition de la topologie quotient, à ce que $\pi^{-1}(f^{-1}(\mathrm{U}))$ est ouvert dans X, pour tout ouvert U de Y, et donc à ce que $f\circ\pi : \mathrm{X}\to\mathrm{Y}$ soit continue.

Exercice 5.5. — Quelle est la topologie quotient sur $\mathbf{R}/\mathbf{Q}$?

Voici quelques espaces que l'on peut construire par des passages au quotient. Le lecteur est invité à s'armer de ciseaux et de colle pour voir à quoi ressemblent les trois premiers espaces, et à chercher sur Internet (par exemple sur le site `http://www.mathcurve.com/surfaces/surfaces.shtml` de R. Ferréol) des images des deux derniers (on ne peut pas les plonger physiquement dans $\mathbf{R}^3$).

— Le *cylindre* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(x,1)$, si $x\in[0,1]$.

— La *bande de Moebius* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(1-x,1)$, si $x\in[0,1]$.

— Le *tore* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(x,1)$, si $x\in[0,1]$ et $(0,y)\sim(1,y)$, si $y\in[0,1]$. C'est aussi le quotient de $\mathbf{R}^2$ par $\mathbf{Z}^2$ ou encore le produit $(\mathbf{R}/\mathbf{Z})^2$ de deux cercles.

— La *bouteille de Klein* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(x,1)$, si $x\in[0,1]$ et $(0,y)\sim(1,1-y)$, si $y\in[0,1]$.

— Le *plan projectif réel* : c'est le quotient de la sphère unité de $\mathbf{R}^3$ par la relation d'équivalence $x\sim -x$; il est homéomorphe au quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(1-x,1)$, si $x\in[0,1]$ et $(0,y)\sim(1,1-y)$, si $y\in[0,1]$.

5.5. Espaces séparés

Une topologie est *séparée* si, quels que soient $x, y\in\mathrm{X}$, avec $x\neq y$, on peut trouver des ouverts U, V de X, avec $x\in\mathrm{U}$, $y\in\mathrm{V}$, et $\mathrm{U}\cap\mathrm{V}=\emptyset$. Par exemple, la topologie discrète est séparée (prendre $\mathrm{U}=\{x\}$ et $\mathrm{V}=\{y\}$), et la topologie grossière est on ne peut moins

séparée (sauf si X a 0 ou 1 élément). Dans un espace séparé, les points sont fermés, mais la réciproque n'est pas vraie[26].

• Un espace métrique est séparé.

Si $x \neq y$, on a $d(x,y) > 0$, et si $r = \frac{1}{2}d(x,y)$, alors $\mathrm{B}(x,r^-) \cap \mathrm{B}(y,r^-) = \emptyset$, d'après l'inégalité triangulaire.

• Si les X_i sont séparés, alors $\mathrm{X} = \prod_{i\in\mathrm{I}} \mathrm{X}_i$ est séparé.

Si $x = (x_i)_{i\in\mathrm{I}}$ et $y = (y_i)_{i\in\mathrm{I}}$ sont deux éléments distincts de X, il existe $j \in \mathrm{I}$ tel que $x_j \neq y_j$, et comme X_j est séparé, il existe des ouverts disjoints U_j et V_j de X_j contenant x_j et y_j respectivement. Alors $\mathrm{U} = \mathrm{U}_j \times \prod_{i\neq j} \mathrm{X}_i$ et $\mathrm{V} = \mathrm{V}_j \times \prod_{i\neq j} \mathrm{X}_i$ sont des ouverts disjoints de X contenant x et y respectivement. On en déduit la séparation de X.

• X est séparé si et seulement si la diagonale $\Delta = \{(x,x),\ x \in \mathrm{X}\}$ est fermée dans $\mathrm{X} \times \mathrm{X}$.

Si X est séparé, alors quels que soient $x, y \in \mathrm{X}$ distincts, il existe des ouverts $\mathrm{U}_{x,y}$, $\mathrm{V}_{x,y}$ disjoints, avec $x \in \mathrm{U}_{x,y}$ et $y \in \mathrm{V}_{x,y}$. La condition « $\mathrm{U}_{x,y}$, $\mathrm{V}_{x,y}$ disjoints » est équivalente à ce que l'ouvert $\mathrm{W}_{x,y} = \mathrm{U}_{x,y} \times \mathrm{V}_{x,y}$ de $\mathrm{X} \times \mathrm{X}$ ne rencontre pas Δ. De plus, $\mathrm{W}_{x,y}$ contient (x,y), ce qui fait que la réunion des $\mathrm{W}_{x,y}$, pour $x \neq y$, est égale à $(\mathrm{X} \times \mathrm{X}) - \Delta$ qui est donc ouvert en tant que réunion d'ouverts. On en déduit que Δ est fermée.

Réciproquement, si Δ est fermée, alors $(\mathrm{X}\times\mathrm{X}) - \Delta$ est ouvert. Par définition de la topologie produit, cela implique que si $(x,y) \in (\mathrm{X} \times \mathrm{X}) - \Delta$ (i.e. si $x \neq y$), alors il existe U, V ouverts de X tels que $\mathrm{U} \times \mathrm{V} \subset (\mathrm{X} \times \mathrm{X}) - \Delta$ et $(x,y) \in \mathrm{U} \times \mathrm{V}$. Alors $x \in \mathrm{U}$, $y \in \mathrm{V}$ et $\mathrm{U} \cap \mathrm{V} = \emptyset$. On en déduit la séparation de X.

Exercice 5.6. — Montrer que, si $f : \mathrm{X} \to \mathrm{Y}$ est injective et continue, et si Y est séparé, alors X est séparé.

Un espace métrique est séparé grâce à la *condition de séparation* « $d(x,y) = 0 \Rightarrow x = y$ ». Si on supprime la condition de séparation, on obtient une *semi-distance* qui permet encore de définir une topologie $\mathscr{T}_d$ dans laquelle un ouvert non vide est une réunion (quelconque) de boules ouvertes. L'espace topologique $(\mathrm{X}, \mathscr{T}_d)$ n'est plus forcément séparé (si $x \neq y$, mais $d(x,y) = 0$, alors tout ouvert de X contenant x contient aussi y). C'est le cas des espaces $\mathscr{L}^1(\mathbf{R}^m)$ et $\mathscr{L}^2(\mathbf{R}^m)$ des fonctions sommables ou de carré sommable par exemple.

On peut fabriquer un espace séparé à partir de (X, d), en identifiant deux points dont la distance est nulle. De manière précise, on définit une relation $\sim$ sur X par $x \sim y$ si et seulement si $d(x,y) = 0$; la relation $\sim$ est une relation d'équivalence grâce à la symétrie de d et à l'inégalité triangulaire. De plus, on a $d(x,y) = d(x',y')$ si $x \sim x'$ et $y \sim y'$, toujours grâce à l'inégalité triangulaire. On en déduit le fait que

[26] Par exemple, dans $\mathbf{C}^n$ muni de la topologie de Zariski, les points sont fermés puisque $z = (z_1, \ldots, z_n)$ est l'ensemble des zéros communs de la famille de polynômes $\mathrm{X}_i - z_i$, pour $i \in \mathrm{I}$, mais la topologie de Zariski est fort peu séparée puisque tout ouvert de Zariski non vide est dense (pour la topologie de Zariski et aussi pour la topologie usuelle de $\mathbf{C}^n$). Il a fallu attendre les travaux de A. Weil (1952) et J-P. Serre (*Géométrie algébrique et géométrie analytique*, connu sous le nom de GAGA, 1956) pour que l'on se rende compte que cette topologie, loin d'être une curiosité pathologique, permet de retrouver, de manière algébrique, la plupart des invariants que l'on peut définir en utilisant la topologie usuelle. Ceci servit de point de départ à la révolution grothendieckienne.

d définit une distance sur l'ensemble $X/\sim$ des classes d'équivalence pour la relation $\sim$, et le séparé de (X, d) est l'ensemble $X/\sim$ muni de la distance induite par d.

Un exemple de cette construction est le passage de $\mathscr{L}^1(\mathbf{R}^m)$ à $L^1(\mathbf{R}^m)$ ou de $\mathscr{L}^2(\mathbf{R}^m)$ à $L^2(\mathbf{R}^m)$ rencontré dans le cours.

5.6. Intérieur, adhérence, densité

Si X est un espace topologique, et $Y \subset X$, alors la réunion $\overset{\circ}{Y}$ de tous les ouverts de X contenus dans Y est un ouvert, et donc est le plus grand ouvert contenu dans Y ; c'est *l'intérieur* de Y. On dit que Y *est d'intérieur vide* si $\overset{\circ}{Y} = \emptyset$.

De même, l'intersection $\overline{Y}$ de tous les fermés de X contenant Y est un fermé appelé *l'adhérence* de Y. On dit que Y est *dense dans* X si $\overline{Y} = X$. De manière équivalente, Y est dense dans X si et seulement si $Y \cap U \neq \emptyset$ quel que soit U ouvert non vide de X, ou encore si et seulement si tout point de X admet au moins un point de Y dans chacun de ses voisinages. Si (X, d) est un espace métrique, cela se traduit encore par : Y est dense dans X si et seulement si, quels que soient $x \in X$ et $\varepsilon > 0$, il existe $y \in Y$ tel que $d(x, y) < \varepsilon$.

• $\mathbf{Q}$ est dense dans $\mathbf{R}$ et $\mathbf{Q}_p$ (par construction).

• Les polynômes sont denses dans l'espace des fonctions continues sur $[0, 1]$ muni de la norme $\|\phi\|_\infty = \sup_{x\in[0,1]} |\phi(x)|$ de la convergence uniforme (théorème de Weierstrass).

• Si X est muni de la topologie grossière, tout point est dense dans X.

• Si Y est dense dans X, si Z est séparé, et si $f, g : X \to Z$ sont continues et coïncident sur Y, alors $f = g$.

> Il suffit de prouver que l'ensemble A des $x \in X$ vérifiant $f(x) = g(x)$ est fermé dans X, puisque A contenant Y, et Y étant dense dans X, cela implique $A = X$. Or A est l'image inverse de la diagonale $\Delta = \{(x, x),\ x \in X\}$ dans $X \times X$ par l'application $x \mapsto (f(x), g(x))$, qui est continue, et l'hypothèse Z séparé est équivalente à ce que Δ soit fermé dans $X \times X$, ce qui fait que A est fermé comme image inverse d'un fermé par une application continue.

Exercice 5.7. — Soit X un espace topologique. Montrer que $Y \subset X$ est d'intérieur vide si et seulement si son complémentaire est dense dans X.

Exercice 5.8. — (i) Montrer que si Y_1 est dense dans X_1 et si Y_2 est dense dans X_1, alors $Y_1 \times Y_2$ est dense dans $X_1 \times X_2$.

(ii) Soit $f : Y \to Z$ une application continue entre espaces métriques. Montrer que si X est dense dans Y, et si la restriction de f à X est une isométrie, alors f est une isométrie.

Exercice 5.9. — (i) Montrer que si U est ouvert, alors l'intérieur de l'adhérence de U contient U, et qu'on n'a pas toujours égalité, mais que l'adhérence de l'intérieur de l'adhérence de U est l'adhérence de U.

(ii) Montrer que, si F est fermé, alors l'adhérence de l'intérieur de F est contenu dans F, et qu'on n'a pas toujours égalité, mais que l'intérieur de l'adhérence de l'intérieur de F est l'intérieur de F.

Exercice 5.10. — Montrer que $A = \{(n, e^n),\ n \in \mathbf{N}\}$ est dense dans $\mathbf{C}^2$ muni de la topologie de Zariski. Est-t-il dense dans $\mathbf{C}^2$ pour la topologie usuelle ?

5.7. Suites dans un espace topologique

5.7.1. Suites, suites extraites

Soit X un espace topologique. Si $(x_n)_{n\in\mathbf{N}}$ est une suite d'élément de X, et si $a \in \mathrm{X}$, on dit que x_n *tend vers* a ou que x_n *a pour limite* a, si pour tout voisinage V de a, il existe $\mathrm{N} \in \mathbf{N}$, tel que $x_n \in \mathrm{V}$, si $n \geqslant \mathrm{N}$. Il suffit bien évidemment de vérifier ceci pour V dans une base de voisinages de a.

Si X est séparé, une suite a au plus une limite comme on le constate aisément en revenant à la définition d'espace séparé. On prendra garde au fait que ce n'est plus forcément le cas, si l'espace n'est pas séparé. On dit qu'une suite est *convergente* si elle a au moins une limite. On réserve la notation $\lim_{n\to+\infty} x_n = a$ au cas où l'espace est séparé et donc la limite est unique.

On obtient une traduction agréable de la notion de suite convergente en introduisant l'espace topologique $\overline{\mathbf{N}} = \mathbf{N} \cup \{+\infty\}$, muni de la topologie pour laquelle les ouverts sont les parties de $\mathbf{N}$ auxquelles on a rajouté les complémentaires dans $\overline{\mathbf{N}}$ des parties finies de $\mathbf{N}$. C'est alors un simple exercice de montrer que $\lim_{n\to+\infty} x_n = a$ si et seulement si la suite x_n se prolonge en une fonction continue de $\overline{\mathbf{N}}$ dans X prenant la valeur a en $+\infty$ (i.e. l'application de $\overline{\mathbf{N}}$ dans X obtenue en envoyant n sur x_n et $+\infty$ sur a est continue).

Une suite $(y_n)_{n\in\mathbf{N}}$ est dite *extraite* de $(x_n)_{n\in\mathbf{N}}$ s'il existe $\varphi : \mathbf{N} \to \mathbf{N}$ tendant vers $+\infty$ quand n tend vers $+\infty$, telle que $y_n = x_{\varphi(n)}$, pour tout $n \in \mathbf{N}$.

• Si a est une limite de $x = (x_n)_{n\in\mathbf{N}}$, alors a est aussi limite de toute suite extraite.

Soit $\varphi : \mathbf{N} \to \mathbf{N}$ tendant vers $+\infty$ quand n tend vers $+\infty$, ce qui se traduit par le fait que φ peut s'étendre par continuité à $\overline{\mathbf{N}}$, en posant $\varphi(+\infty) = +\infty$. Si a est une limite de x, alors x peut aussi s'étendre par continuité à $\overline{\mathbf{N}}$, en posant $x(+\infty) = a$ et donc $x \circ \varphi$ est continue sur $\overline{\mathbf{N}}$, ce qui se traduit par le fait que a est limite de la suite extraite $(x_{\varphi(n)})_{n\in\mathbf{N}}$.

On peut aussi se passer de $\overline{\mathbf{N}}$, et revenir à la définition. Si V est un voisinage de a, alors il existe $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in \mathrm{V}$, pour tout $n \geqslant \mathrm{N}$. Par ailleurs, si $\varphi : \mathbf{N} \to \mathbf{N}$ tend vers $+\infty$ quand n tend vers $+\infty$, il existe $\mathrm{N}' \in \mathbf{N}$ tel que $\varphi(n) \geqslant \mathrm{N}$, si $n \geqslant \mathrm{N}'$. On a donc $x_{\varphi(n)} \in \mathrm{V}$, pour tout $n \geqslant \mathrm{N}'$, ce qui permet de montrer que $(x_{\varphi(n)})_{n\in\mathbf{N}}$ tend vers a.

5.7.2. Suites et continuité

• Si $f : \mathrm{X} \to \mathrm{Y}$ est continue, et si $x = (x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de X admettant a comme limite, alors $(f(x_n))_{n\in\mathbf{N}}$ admet $f(a)$ pour limite.

La suite x se prolonge en une fonction continue de $\overline{\mathbf{N}}$ dans X prenant la valeur a en $+\infty$, et comme f est continue, $f \circ x$ est continue sur $\overline{\mathbf{N}}$, ce qui se traduit par le fait que $f(a)$ est limite de la suite $(f(x_n))_{n\in\mathbf{N}}$.

On peut aussi se passer de $\overline{\mathbf{N}}$, et dire que si V est un voisinage de $f(a)$, alors $f^{-1}(\mathrm{V})$ contient un voisinage U de a puisque f est continue, et qu'il existe $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in \mathrm{U}$, si $n \geqslant \mathrm{N}$, ce qui implique $f(x_n) \in \mathrm{V}$, si $n \geqslant \mathrm{N}$.

• Si X est un espace métrique, alors $f : \mathrm{X} \to \mathrm{Y}$ est continue en x si et seulement si pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X tendant vers x, la suite $(f(x_n))_{n\in\mathbf{N}}$ tend vers $f(x)$.

On a déjà démontré (dans le cas d'espaces topologiques généraux) que si $f : \mathrm{X} \to \mathrm{Y}$ est continue en x, alors pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X tendant vers x, la suite $(f(x_n))_{n\in\mathbf{N}}$ tend vers $f(x)$. Maintenant, si f est non continue en x, il existe un voisinage V de $f(x)$, tel que, pour tout $n \in \mathbf{N}$, il existe $x_n \in \mathrm{B}(x, 2^{-n})$ avec $f(x_n) \notin \mathrm{V}$. Alors $x_n \to x$ dans X, tandis que $f(x_n) \not\to f(x)$. En prenant la contraposée, on en déduit que, si pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X tendant vers x, la suite $(f(x_n))_{n\in\mathbf{N}}$ tend vers $f(x)$, alors f est continue en x. Ceci permet de conclure.

On prendra garde au fait que cette caractérisation de la continuité par les suites n'est pas valable pour un espace topologique général.

Exercice 5.11. — Soit X un espace métrique (ou métrisable).

(i) Soit $\mathrm{Z} \subset \mathrm{X}$. Montrer que $a \in \mathrm{X}$ est dans l'adhérence $\overline{\mathrm{Z}}$ de Z si et seulement si il existe une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de Z, ayant a pour limite.

(ii) Montrer que Z est dense dans X si et seulement si tout point de X est la limite d'une suite d'éléments de Z.

(iii) Montrer que, si Y est un espace métrique, si f, g sont deux applications continues de X dans Y, telles que l'on ait $f(x) = g(x)$, pour tout $x \in \mathrm{Z}$, où Z est dense dans X, alors $f = g$.

6. Compacité

6.1. Espaces compacts

Un espace topologique X est dit *compact* s'il est non vide, séparé, et si de tout recouvrement de X par des ouverts, on peut extraire un sous-recouvrement fini [(27)]. Autrement dit, X (non vide et séparé) est compact si, quelle que soit la famille $(\mathrm{U}_i)_{i\in\mathrm{I}}$ d'ouverts de X telle que $\cup_{i\in\mathrm{I}}\mathrm{U}_i = \mathrm{X}$, il existe $\mathrm{J} \subset \mathrm{I}$ fini tel que $\cup_{i\in\mathrm{J}}\mathrm{U}_i = \mathrm{X}$. En passant aux complémentaires, on voit que la compacité de X (séparé) est équivalente à ce que de toute famille de fermés de X d'intersection vide, on puisse extraire une famille finie d'intersection vide.

• Un ensemble fini, muni de la topologie discrète, est compact.

• L'espace $\overline{\mathbf{N}} = \mathbf{N} \cup \{+\infty\}$, muni de la topologie pour laquelle les ouverts sont les parties de $\mathbf{N}$ et les complémentaires dans $\overline{\mathbf{N}}$ des parties finies de $\mathbf{N}$, est un espace compact.

$\overline{\mathbf{N}}$ est séparé car, si $x \neq y$, alors $x \neq +\infty$ ou $y \neq +\infty$, ce qui fait que l'un des deux singletons $\{x\}$ ou $\{y\}$ est ouvert, ainsi que son complémentaire. Par ailleurs, si les $(\mathrm{U}_i)_{i\in\mathrm{I}}$ forment un recouvrement ouvert de $\overline{\mathbf{N}}$, alors un des U_i contient $+\infty$, et son complémentaire est fini ; on peut donc extraire du recouvrement par les U_i un sous-recouvrement fini.

• Le segment $[0, 1]$ est compact.

Soit $(\mathrm{U}_i)_{i\in\mathrm{I}}$ une famille d'ouverts de $[0, 1]$ formant un recouvrement. Soit A l'ensemble des $a \in [0, 1]$ tels que $[0, a]$ puisse être recouvert par un nombre fini de U_i, et soit M la borne supérieure de A. Par hypothèse, il existe $i(\mathrm{M}) \in \mathrm{I}$ et $\varepsilon > 0$ tels que $]\mathrm{M}-\varepsilon, \mathrm{M}+\varepsilon[\cap[0, 1] \subset \mathrm{U}_{i(\mathrm{M})}$,

[(27)] La notion de compacité a été dégagée en 1894 par Borel (pour des questions de mesure, cf. (ii) de l'ex. 6.1, auquel Borel se référait sous le nom de *théorème fondamental de la théorie de la mesure*) et par Cousin (pour des applications aux fonctions de plusieurs variables complexes).

et par définition de M, il existe $a \in]\mathrm{M}-\varepsilon, \mathrm{M}[$ et $\mathrm{J} \subset \mathrm{I}$ fini, tels que $[0,a] \subset \cup_{i\in \mathrm{J}} \mathrm{U}_i$. Mais alors $[0,b] \subset \cup_{i\in \mathrm{J}\cup\{i(\mathrm{M})\}} \mathrm{U}_i$, quel que soit $b \in [\mathrm{M}, \mathrm{M}+\varepsilon[\cap[0,1]$, et donc $[\mathrm{M}, \mathrm{M}+\varepsilon[\cap[0,1] \subset \mathrm{A}$. Par définition de M, ceci implique $\mathrm{M} = 1$, et permet de conclure.

Exercice 6.1. — (i) Montrer que pour tout $\varepsilon > 0$, il existe une suite de segments ouverts $]a_n, b_n[$ telle que $\sum_{n\in\mathbf{N}}(b_n - a_n) < \varepsilon$ et l'adhérence de $\cup_{n\in\mathbf{N}}]a_n, b_n[$ contienne $[0,1]$.

(ii) Soit $]a_n, b_n[$, pour $n \in \mathbf{N}$, une suite de segments ouverts tels que $[0,1] \subset \cup_{n\in\mathbf{N}}]a_n, b_n[$. Montrer que $\sum_{n\in\mathbf{N}}(b_n - a_n) > 1$. (On pourra admettre que le résultat est vrai pour une famille finie.)

6.2. Compacité et suites

Si X est un espace topologique, et si $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de X, on dit que $a \in \mathrm{X}$ est une *valeur d'adhérence* de la suite $(x_n)_{n\in\mathbf{N}}$, si tout voisinage de a contient une infinité de termes de la suite. Ceci équivaut à ce que a soit dans l'adhérence F_k de $\{x_n,\ n \geqslant k\}$, pour tout $k \in \mathbf{N}$. En particulier, l'ensemble des valeurs d'adhérence d'une suite est un fermé, puisque c'est l'intersection des fermés F_k, pour $k \in \mathbf{N}$.

• Si X est un espace métrique, alors a est une valeur d'adhérence de la suite $(x_n)_{n\in\mathbf{N}}$, si et seulement si on peut extraire une sous-suite de la suite $(x_n)_{n\in\mathbf{N}}$ ayant pour limite a.

Si on peut extraire de $(x_n)_{n\in\mathbf{N}}$, une sous-suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ de limite a, et si V est un voisinage de a, alors $x_{\varphi(n)} \in \mathrm{V}$, pour tout n assez grand, ce qui prouve que a est une valeur d'adhérence de la suite (noter que ce sens n'utilise pas le fait que X est métrique). Réciproquement, si X est métrique, et si a est une valeur d'adhérence de $(x_n)_{n\in\mathbf{N}}$, alors pour tout $n \in \mathbf{N}$, il existe une infinité de termes de la suite dans $\mathrm{B}(a, 2^{-n})$, et donc on peut choisir $\varphi(n) \geqslant n$ tel que $x_\varphi(n) \in \mathrm{B}(a, 2^{-n})$. La suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ est alors extraite de la suite $(x_n)_{n\in\mathbf{N}}$ et converge vers a. Ceci permet de conclure.

• Dans un compact, toute suite admet une valeur d'adhérence ; dans un compact métrique, on peut extraire de toute suite une sous-suite convergente.

Soit X un compact, et soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de X. Soit F_n, si $n \in \mathbf{N}$ l'adhérence de l'ensemble $\{x_{n+p},\ p \in \mathbf{N}\}$; l'intersection des F_n est, par définition ou presque, l'ensemble des valeurs d'adhérence de la suite $(x_n)_{n\in\mathbf{N}}$. Comme l'intersection d'un nombre fini de F_n est toujours non vide puisqu'elle contient les x_n, pour n assez grand, la compacité de X assure que l'intersection des fermés F_n, pour $n \in \mathbf{N}$, est non vide, ce qui permet de conclure.

Exercice 6.2. — (i) Montrer que dans un compact, une suite ayant une seule valeur d'adhérence a une limite.

(ii) Donner un exemple de suite à valeurs dans $\mathbf{R}$ ayant une seule valeur d'adhérence mais ne convergeant pas.

• Un espace métrique est compact si et seulement si toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X admet une valeur d'adhérence[(28)] (théorème de Borel-Lebesgue).

[(28)] Cette caractérisation est parfois prise comme définition des espaces compacts. Elle est effectivement d'un maniement plus facile que la caractérisation en termes de recouvrements ouverts si on cherche à vérifier qu'un espace (métrique) est compact. Par contre, si on veut utiliser la compacité d'un espace pour en tirer des conséquences, c'est en général la caractérisation par les recouvrements ouverts qui est la plus naturelle et la plus puissante.

On sait déjà que dans un compact (même non métrique), toute suite admet une valeur d'adhérence ; montrons la réciproque dans le cas d'un espace métrique. Soit $(U_i)_{i\in I}$ un recouvrement ouvert de X. Alors, quel que soit $x \in X$, il existe $k(x) \geqslant 0$ et $i \in I$, tels que $B(x, r(x)^-) \subset U_i$, où $r(x) = 2^{-k(x)}$. On cherche à prouver qu'on peut extraire du recouvrement par les U_i un recouvrement fini, et il suffit de prouver qu'on peut en faire autant du recouvrement par les $B(x, r(x)^-)$.

Pour cela, construisons par récurrence une suite x_n d'éléments de X vérifiant :

- $x_n \in Y_n$, où Y_n est le fermé complémentaire de $\cup_{j\leqslant n-1} B(x_j, r(x_j)^-)$,
- $k(x_n) \leqslant k(y)$, quel que soit $y \in Y_n$.

Si la construction s'arrête, c'est que les $B(x_j, r(x_j)^-)$, pour $j \leqslant n-1$ recouvrent X, ce que l'on veut. Sinon, la suite $(x_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence y_0, et on a $y_0 \in Y_n$, quel que soit $n \in \mathbf{N}$, car Y_n est fermé et $x_{n+p} \in Y_n$, quel que soit $p \in \mathbf{N}$. Par construction de la suite $(x_n)_{n\in\mathbf{N}}$, on a $d(x_n, x_{n+p}) \geqslant 2^{-k(x_n)}$, quels que soient $n, p \in \mathbf{N}$. Comme on peut extraire une sous-suite de Cauchy de la suite $(x_n)_{n\in\mathbf{N}}$, on en déduit que $k(x_n) \to +\infty$. En particulier, il existe n tel que $k(x_n) \geqslant k(y_0) + 1$, en contradiction avec la construction de x_n (puisque $y_0 \in Y_n$). Ceci permet de conclure.

Exercice 6.3. — Montrer que $[0, 1]$ est compact en passant par les suites.

6.3. Propriétés de base des compacts

Les énoncés qui suivent sont d'un usage constant.

6.3.1. Compacts d'un espace topologique

- Si X est compact, alors $Y \subset X$ est compact, si et seulement si Y est fermé.

Supposons Y fermé. Soit $(U_i)_{i\in I}$ un recouvrement[29] ouvert de Y. Par définition, il existe, pour tout $i \in I$, un ouvert V_i de X tel que $U_i = V_i \cap Y$, et comme $U = X - Y$ est ouvert, les V_i, pour $i \in I$, et U forment un recouvrement ouvert de X. Comme X est supposé compact, il existe $J \subset I$ fini, tel que $X \subset U \cup \left(\cup_{i\in J} V_i\right)$, et les U_i, pour $i \in J$ forment un recouvrement ouvert de Y extrait du recouvrement initial. On en déduit la compacité de Y.

Réciproquement, supposons $Y \subset X$ compact. Soit $a \notin Y$. Comme X est séparé, pour tout $y \in Y$, il existe des ouverts U_y, V_y tels que $y \in U_y$, $a \in V_y$ et $U_y \cap V_y = \emptyset$. Les U_y, pour $y \in Y$, forment un recouvrement ouvert de Y ; il existe donc $J \subset Y$ fini tel que $Y \subset \cup_{y\in J} U_y$. Mais alors $V = \cap_{y\in J} V_y$ est un ouvert de X contenant a et ne rencontrant pas Y, ce qui prouve que a n'appartient pas à l'adhérence $\overline{Y}$ de Y. On a donc $\overline{Y} \subset Y$, ce qui prouve que Y est fermé.

- Si X_1 et X_2 sont compacts, alors $X_1 \times X_2$ est compact.

[29] Si X est un espace métrique, on peut passer par les suites. Comme X est compact, une suite $(y_n)_{n\in\mathbf{N}}$ d'éléments de Y a une valeur d'adhérence dans X, et si Y est fermé, cette valeur d'adhérence est dans Y, ce qui prouve que Y est compact. Réciproquement, si Y est compact, si a est dans l'adhérence de Y, il existe une suite $(y_n)_{n\in\mathbf{N}}$ d'éléments de Y ayant pour limite a dans X, et sa seule valeur d'adhérence dans X est alors a. Comme Y est supposé compact, cette suite admet une valeur d'adhérence dans Y, et comme sa seule valeur d'adhérence dans X est a, cela implique $a \in Y$. On en déduit que Y est fermé.

Soit $(U_i)_{i\in I}$ une famille d'ouverts de $X_1 \times X_2$ formant un recouvrement[30]. Si $y \in X_2$, soit $I(y)$ l'ensemble des $i \in I$ tels que $U_i \cap (X_1 \times \{y\})$ soit non vide. Si $i \in I(y)$, et si $(a, y) \in U_i$, il existe $V_{i,y,a}$ ouvert de X_1 contenant a et $W_{i,y,a}$ ouvert de X_2 contenant y tels que $U_i \supset V_{i,y,a} \times W_{i,y,a}$. Les U_i, pour i dans I, formant un recouvrement de $X_1 \times X_2$, les $V_{i,y,a}$, pour $i \in I(y)$ et $(a, y) \in U_i$, forment un recouvrement de X_1. Comme X_1 est compact, il existe un ensemble fini $J(y)$ de couples (i, a), avec $i \in I(y)$ et $(a, y) \in U_i$ tels que $X_1 = \cup_{(i,a)\in J(y)} V_{i,y,a}$. Soit alors $W_y = \cap_{(i,a)\in J(y)} W_{i,y,a}$. C'est un ouvert de X_2 contenant y, et U_i contient $V_{i,y,a} \times W_y$, quel que soit $(i, a) \in J(y)$. Comme X_2 est compact, on peut trouver Y fini tel que $X_2 = \cup_{y\in Y} W_y$, et alors

$$\cup_{y\in Y} \cup_{(i,a)\in J(y)} U_i \supset \cup_{y\in Y} \big(\cup_{(i,a)\in J(y)} V_{i,y,a} \times W_y \big) = \cup_{y\in Y} (X_1 \times W_y) = X_1 \times X_2,$$

ce qui montre que l'on peut extraire du recouvrement par les U_i un sous-recouvrement fini.

• L'image d'un compact X par une application continue $f : X \to Y$, où Y est séparé, est un compact.

Soit $(U_i)_{i\in I}$ un recouvrement[31] ouvert de $f(X)$. Par définition, si $i \in I$, il existe U'_i ouvert de Y tel que $U_i = U'_i \cap f(X)$, et comme f est continue, $V_i = f^{-1}(U'_i)$ est ouvert dans X, et $(V_i)_{i\in I}$ est donc un recouvrement ouvert de X. Comme X est compact, il existe $J \subset I$ fini tels que les V_i, pour $i \in J$, recouvrent X, et les U_i, pour $i \in J$, forment alors un recouvrement ouvert fini de $f(X)$ extrait du recouvrement initial. On en déduit la compacité de $f(X)$.

• Si X est compact, et si $f : X \to Y$ est bijective continue avec Y séparé, alors f est un homéomorphisme.

Notons $g : Y \to X$ l'application réciproque de f de telle sorte que si $F \subset X$, alors on a $g^{-1}(F) = \{y \in Y \, \exists x \in F,\, g(y) = x\} = \{y \in Y \, , \exists x \in F,\, y = f(g(y)) = f(x)\} = f(F)$. On veut prouver que $g^{-1}(F)$ est fermé dans Y si F l'est dans X. Or $g^{-1}(F) = f(F)$, et comme F est compact puisque fermé dans un compact, et que Y est séparé, $f(F)$ est compact et donc fermé. Ceci permet de conclure.

6.3.2. Compacts d'un espace métrique

• Si E est un espace métrique, un compact X de E est fermé dans E et borné, mais la réciproque est en générale fausse.

On a déjà vu qu'un compact est toujours fermé. Par ailleurs, si X est compact, et si $x_0 \in X$, alors $x \mapsto d(x_0, x)$ est continue sur X et donc est bornée puisque toute fonction continue à

[30]Si X_1 et X_2 sont des espaces métriques, on peut raisonner en termes de suites. Soit $(x_n, y_n)_{n\in\mathbf{N}}$ une suite d'éléments de $X_1 \times X_2$. Comme X_1 est compact, on peut extraire de la suite $(x_n)_{n\in\mathbf{N}}$ une sous-suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ ayant une limite a dans X_1. Comme X_2 est compact, on peut extraire de la suite $(y_{\varphi(n)})_{n\in\mathbf{N}}$ une sous-suite $(y_{\psi(n)})_{n\in\mathbf{N}}$ ayant une limite b dans X_2, et alors $(x_{\psi(n)}, y_{\psi(n)})_{n\in\mathbf{N}}$ admet (a, b) comme limite dans $X_1 \times X_2$ puisque $(x_{\psi(n)})_{n\in\mathbf{N}}$ est extraite de $(x_{\varphi(n)})_{n\in\mathbf{N}}$, et donc tend vers a dans X_1. Autrement dit la suite $(x_n, y_n)_{n\in\mathbf{N}}$ admet une valeur d'adhérence.

[31]Si X et Y sont des espaces métriques, on peut raisonner en termes de suites. Soit $(y_n)_{n\in\mathbf{N}}$ une suite d'éléments de $f(Y)$, et, si $n \in \mathbf{N}$, soit $x_n \in X$ tel que $y_n = f(x_n)$. Comme X est compact, la suite $(x_n)_{n\in\mathbf{N}}$ admet une valeur d'adhérence $a \in X$, et comme f est continue, $f(a)$ est une valeur d'adhérence de la suite $(y_n)_{n\in\mathbf{N}}$. On en déduit la compacité de $f(X)$.

valeurs réelles sur un compact est bornée. Autrement dit, il existe $M \in \mathbf{R}_+$ tel que $X \subset B(x_0, M)$, et X est borné.

Soit E le segment $[-1, 1[$ de $\mathbf{R}$ muni de la distance induite par la valeur absolue sur $\mathbf{R}$; c'est un espace métrique parfaitement respectable. Alors $X = [0, 1[$ est fermé dans E puisque c'est l'intersection de E avec le fermé $\mathbf{R}_+$ de $\mathbf{R}$, et il est borné. Il n'est pas compact car on ne peut pas extraire de recouvrement fini du recouvrement de X par les ouverts $U_n = X \cap]\frac{-1}{2}, 1 - \frac{1}{n}[$.

• Si X est compact, et $f : X \to \mathbf{R}$ est continue, alors f atteint son maximum et son minimum.

Comme X est compact et f continue, cela implique que $f(X)$ est compact, et donc admet des borne inférieure et supérieure finies car $f(X)$ est borné, et les contient car il est fermé.

• Si E est un espace vectoriel *de dimension finie* sur $\mathbf{R}$ ou $\mathbf{C}$, alors les compacts de E sont les fermés bornés.

Par définition de la norme $\| \ \|_\infty$ sur $\mathbf{R}^n$, un borné de $\mathbf{R}^n$ est inclus dans $[-M, M]^n$, si M est assez grand. Or $[-M, M]$ est compact, puisque c'est l'image de $[0, 1]$ par l'application continue $x \mapsto (2x - 1)M$, et donc $[-M, M]^n$ est compact comme produit de compacts. Comme un fermé d'un compact est compact, on en déduit qu'un fermé borné de $(\mathbf{R}^n, \| \ \|_\infty)$ est compact. Le résultat dans le cas d'un $\mathbf{R}$ ou $\mathbf{C}$-espace vectoriel de dimension finie quelconque s'en déduit si on sait que deux normes sur un $\mathbf{R}$-espace vectoriel de dimension finie sont équivalentes (cf. n° 10.3), et donc que les fermés bornés sont les mêmes, quelle que soit la norme.

• Une fonction continue sur un compact d'un espace métrique est uniformément continue (théorème de[32] Heine, 1872).

$f : X \to Y$, où X et Y sont des espaces métriques, est *uniformément continue* si

$$\forall \varepsilon > 0, \ \exists \delta > 0, \text{ tel que } d_X(x, x') < \delta \Rightarrow d_Y(y, y') < \varepsilon.$$

Supposons X compact. Soit $\varepsilon > 0$. Comme f est continue, pour tout $x \in X$, il existe $\delta_x > 0$ tel que $d_X(x, x') < 2\delta_x \Rightarrow d_Y(f(x), f(x')) < \frac{\varepsilon}{2}$. Les $B_X(x, \delta_x)$ forment un recouvrement[33] ouvert de X ; on peut donc en extraire un recouvrement fini $X \subset_{x \in J} B_X(x, \delta_x)$, où $J \subset X$ est fini. Alors, par construction, si $x' \in X$, il existe $x \in J$ tel que $d_X(x, x') < \delta_x$. Soit alors $\delta = \inf_{x \in J} \delta_x$. Si $x_1, x_2 \in X$ vérifient $d_X(x_1, x_2) < \delta$, et si $x \in J$ est tel que $d_X(x, x_1) < \delta_x$, alors

[32] Ce théorème a en fait été démontré par Dirichlet en 1854, pour les fonctions continues sur un segment, mais Heine a donné son nom à la continuité uniforme alors que Dirichlet se contentait de démontrer le résultat avec des ε et des δ en vue de justifier l'intégration de Cauchy pour les fonctions continues, ce que Cauchy avait omis de faire en confondant les notions de continuité et continuité uniforme.

[33] Comme on travaille avec des espaces métriques, on peut aussi passer par les suites. Supposons donc que X est compact, que $f : X \to Y$ est continue mais pas uniformément continue. En niant la définition de la continuité uniforme rappelée ci-dessus, on voit qu'il existe $\varepsilon > 0$, tel que, quel que soit $n \in \mathbf{N}$, il existe $(x_n, x'_n) \in X \times X$ tels que $d_X(x_n, x'_n) \leqslant 2^{-n}$ et $d_Y(f(x_n), f(x'_n)) \geqslant \varepsilon$. Comme X est supposé compact, il en est de même de $X \times X$, et la suite $(x_n, x'_n)_{n \in \mathbf{N}}$ admet une valeur d'adhérence (a, b) dans $X \times X$. De plus, comme $d_X(x_n, x'_n) \to 0$, on a $a = b$, et comme f est continue, $(f(a), f(b))$ est une valeur d'ahérence de la suite $(f(x_n), f(x'_n))_{n \in \mathbf{N}}$ dans $Y \times Y$. Comme $f(a) = f(b)$, cela est en contradiction avec le fait que $d_Y(f(x_n), f(x'_n)) \geqslant \varepsilon$, quel que soit $n \in \mathbf{N}$ (en effet, $(y, y') \mapsto d_Y(y, y')$ est continue sur $Y \times Y$, et une valeur d'ahérence (c, c') de la suite $(f(x_n), f(x'_n))_{n \in \mathbf{N}}$ doit donc vérifier $d_Y(c, c') \geqslant \varepsilon > 0$). Ceci permet de conclure.

$d_X(x, x_2) < 2\delta_x$, et donc $d_Y(f(x), f(x_1)) < \frac{\varepsilon}{2}$, $d_Y(f(x), f(x_2)) < \frac{\varepsilon}{2}$ et $d_Y(f(x_2), f(x_1)) < \varepsilon$. Ceci montre que f est uniformément continue.

Exercice 6.4. — Soit $(E, \| \|)$ un espace vectoriel normé de dimension finie. On dit que $f : E \to \mathbf{C}$ tend vers 0 à l'infini, si pour tout $\varepsilon > 0$, il existe $M > 0$, tel que $|f(x)| < \varepsilon$, si $\|x\| \geqslant M$. Montrer que, si $f : E \to \mathbf{C}$ est continue et tend vers 0 à l'infini, alors f est bornée et $|f|$ atteint son maximum.

Exercice 6.5. — Soit (X, d) un espace métrique. Si $F \subset X$, et si $x \in X$, on définit la distance $d(x, F)$ de x à F comme la borne inférieure des $d(x, y)$, pour $y \in F$.

(i) Montrer que $x \mapsto d(x, F)$ est continue et même 1-lipschitzienne sur X.

(ii) Montrer que $d(x, F) = 0$ si et seulement si x est dans l'adhérence $\overline{F}$ de F.

(iii) En déduire que si F_1 et F_2 sont des fermés disjoints, il existe des ouverts disjoints U_1, U_2 avec $F_1 \subset U_1$ et $F_2 \subset U_2$.

(iv) On définit la distance entre F_1 et F_2 par $d(F_1, F_2) = \inf_{x \in F_1,\ y \in F_2} d(x, y)$. Montrer que si F_1 et F_2 sont des compacts disjoints, alors $d(F_1, F_2) > 0$.

(v) Montrer que si $F_1 \cap F_2 = \emptyset$, si F_1 est fermé et si F_2 est compact, alors $d(F_1, F_2) \neq 0$.

(vi) Construire des fermés disjoints de $\mathbf{R}$ ou $\mathbf{R}^2$ dont la distance est nulle.

Exercice 6.6. — Soient X un compact métrique et $f : X \to X$ une application contractante (i.e. vérifiant $d(f(x), f(y)) < d(x, y)$, quels que soient $x \neq y$).

(i) Montrer que f a un unique point fixe x_0.

(ii) Montrer que si $x \in X$, et si $f^n = f \circ \cdots \circ f$ (n fois), alors $f^n(x) \to x_0$.

(iii) Montrer que $f^n \to f$ uniformément sur X.

Exercice 6.7. — (difficile) Soit X un espace métrique. Montrer que si toute fonction continue de X dans $\mathbf{R}$ est bornée, alors X est compact.

6.3.3. Compacité locale

La compacité d'un espace est une propriété très agréable, mais rarement vérifiée. Dans les applications, il suffit souvent que cette propriété soit vraie localement : on dit qu'un espace est *localement compact* si tout point possède une base de voisinages constituée de compacts.

• $\mathbf{R}$, $\mathbf{C}$ et, plus généralement, un espace vectoriel de dimension finie sur $\mathbf{R}$ ou $\mathbf{C}$ sont localement compacts.

• Un espace compact est localement compact.

Soient X un compact et $x \in X$. Comme X est séparé, il existe, pour tout $y \neq x$, des ouverts $U_{x,y}$ et $V_{x,y}$, d'intersection vide, contenant x et y respectivement. Il en résulte que y n'appartient pas à l'adherence $F_{x,y}$ de $U_{x,y}$, et donc que, si V est un ouvert contenant x et si F est son complémentaire, alors $F \cap \left(\cap_{y \in X - \{x\}} F_{x,y} \right) = \emptyset$. Or F est compact, en tant que fermé d'un compact, et $F \cap F_{x,y}$ est fermé dans F pour tout y ; on en déduit l'existence d'un sous-ensemble fini Y de $X - \{x\}$ tel que $F \cap \left(\cap_{y \in Y} F_{x,y} \right) = \emptyset$. Soit $U_V = \cap_{y \in Y} U_{x,y}$; alors U_V est un ouvert de X, en tant qu'intersection finie d'ouverts, qui contient x, et dont l'adhérence F_V est contenue dans V, puisque cette adhérence est contenue dans le fermé $F_{x,y}$, pour tout $y \in Y$. Comme F_V est compact, il résulte de ce qui précède, que tout ouvert V contenant x contient un compact F_V qui, lui-même, contient un ouvert U_V dont x est élément. Ceci prouve que les compacts forment une base de voisinage de x, et permet de conclure.

6.4. La droite réelle achevée

6.4.1. Les espaces topologiques ordonnés $\overline{\mathbf{R}}$ *et* $\overline{\mathbf{R}}_+$

On note $\overline{\mathbf{R}} = \mathbf{R} \cup \{\pm\infty\}$ la *droite réelle achevée*. On étend $\leqslant$ de manière naturelle en une relation d'ordre totale sur $\overline{\mathbf{R}}$, en convenant que $-\infty \leqslant a \leqslant +\infty$, quel que soit $a \in \overline{\mathbf{R}}$. On fait de $\overline{\mathbf{R}}$ un espace topologique, en prenant les $]a, b[$, pour $a < b \in \mathbf{R}$, et les $[-\infty, a[$ et $]a, +\infty]$, pour $a \in \mathbf{R}$, comme base d'ouverts. La topologie induite sur $\mathbf{R}$ est donc la topologie usuelle.

• Une suite de nombres réels x_n tend vers $+\infty$ dans $\overline{\mathbf{R}}$ si et seulement si x_n tend vers $+\infty$ au sens classique. (Idem pour $-\infty$.)

Les $]a, +\infty]$ forment une base de voisinages de $+\infty$, et donc $x_n \to +\infty$ dans $\overline{\mathbf{R}}$ si et seulement si, quel que soit $a \in \mathbf{R}$, il existe $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in]a, +\infty]$, si $n \geqslant \mathrm{N}$.

• L'espace topologique $\overline{\mathbf{R}}$ est isomorphe à $[-1, 1]$ en tant qu'espace ordonné et en tant qu'espace topologique ; en particulier, il est compact et métrisable, et tout sous-ensemble non vide de $\overline{\mathbf{R}}$ admet une bonne inférieure et une borne supérieure.

L'application $x \mapsto f(x)$, avec $f(x) = \frac{x}{1+|x|}$, si $x \in \mathbf{R}$, $f(+\infty) = 1$ et $f(-\infty) = -1$, est un homéomorphisme strictement croissant de $\overline{\mathbf{R}}$ sur $[-1, 1]$, dont l'inverse est g défini par $g(x) = \frac{x}{1-|x|}$, si $x \in \mathbf{R}$, $g(1) = +\infty$, $g(-1) = -\infty$ (nous laissons au lecteur le soin de vérifier que f et g sont bien des applications continues inverses l'une de l'autre).

• Une suite $(x_n)_{n\in\mathbf{N}}$ croissante (resp. décroissante) d'éléments de $\overline{\mathbf{R}}$ converge vers la borne supérieure (resp. inférieure) de $\{x_n,\ n \in \mathbf{N}\}$.

• Si $\mathrm{X} \subset \overline{\mathbf{R}}$ est non vide, alors $\sup \mathrm{X}$ et $\inf \mathrm{X}$ sont dans l'adhérence de X.

En utilisant l'homéomorphisme $f : \overline{\mathbf{R}} \to [-1, 1]$, qui est strictement croissant, on se ramène à démontrer le même énoncé pour $\mathrm{X} \subset [-1, 1]$ ce qui permet de traiter tous les cas de la même manière. Maintenant, si la borne supérieure M de X appartient à X, elle appartient a fortiori à son adhérence. Si M n'appartient pas à X, alors pour tout $n > 0$, il existe $x_n \in \mathrm{X}$ avec $\mathrm{M} - 2^{-n} < x_n < \mathrm{M}$, ce qui prouve que M est limite d'une suite d'éléments de X et donc est dans son adhérence. Ceci permet de conclure.

On note $\overline{\mathbf{R}}_+$ la *demi-droite achevée*. C'est l'ensemble des $x \in \overline{\mathbf{R}}$ vérifiant $x \geqslant 0$. On étend l'addition à $\overline{\mathbf{R}}_+$ de la manière évidente, en posant $x + (+\infty) = +\infty$, si $x \in \overline{\mathbf{R}}_+$.

Comme toute suite croissante d'éléments de $\overline{\mathbf{R}}_+$ admet une limite dans $\overline{\mathbf{R}}_+$, on en déduit que :

• Toute série $\sum_{n\in\mathbf{N}} u_n$ à termes dans $\overline{\mathbf{R}}_+$ converge dans $\overline{\mathbf{R}}_+$. Si les u_n sont dans $\mathbf{R}_+$, alors $\sum_{n\in\mathbf{N}} u_n < +\infty$ si et seulement si la série $\sum_{n\in\mathbf{N}} u_n$ converge au sens usuel.

6.4.2. Limite supérieure, limite inférieure

• Toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\overline{\mathbf{R}}$ admet une plus grande valeur d'adhérence $\limsup x_n$, *limite supérieure* de la suite x_n et une plus petite valeur d'adhérence $\liminf x_n$, *limite inférieure* de la suite x_n. De plus, $(x_n)_{n\in\mathbf{N}}$ converge si et seulement si ses limites supérieure

et inférieure sont égales, et la limite de la suite est alors la valeur commune des limites supérieure et inférieure[34].

La compacité de $\overline{\mathbf{R}}$ implique que l'ensemble des valeurs d'adhérence d'une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\overline{\mathbf{R}}$ est non vide. Comme cet ensemble est fermé, les bornes inférieure et supérieure de cet ensemble sont encore des valeurs d'adhérence ; autrement dit toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\overline{\mathbf{R}}$ admet une plus grande valeur d'adhérence. De plus, comme $\overline{\mathbf{R}}$ est un espace compact métrisable, une suite converge si et seulement si elle a une seule valeur d'adhérence et donc si et seulement si ses limites supérieure et inférieure sont égales. On en déduit le résultat.

• On a aussi $\limsup x_n = \inf\limits_{k\in\mathbf{N}} \big(\sup\limits_{n\geqslant k} x_n\big)$ et $\liminf x_n = \sup\limits_{k\in\mathbf{N}} \big(\inf\limits_{n\geqslant k} x_n\big)$.

Pour éviter d'avoir à traiter séparément les cas où une des limites est infinie, on utilise l'homéomorphisme $f : \overline{\mathbf{R}} \to [-1,1]$ ci-dessus pour se ramener au cas de suites à valeurs dans $[-1,1]$. Soient $a = \limsup x_n$ et $b = \inf_{k\in\mathbf{N}} \big(\sup_{n\geqslant k} x_n\big)$, et soit $\varepsilon > 0$. Comme a est une valeur d'adhérence, il existe pour tout $k \in \mathbf{N}$, un entier $n \geqslant k$ tel que $|x_n - a| < \varepsilon$. On a donc $\sup_{n\geqslant k} x_n \geqslant a - \varepsilon$, pour tout k, et donc $b \geqslant a - \varepsilon$, pour tout $\varepsilon > 0$. On en déduit que $b \geqslant a$. Par ailleurs, comme a est la plus grande valeur d'adhérence, il n'y a qu'un nombre fini de n tels que $x_n \geqslant a + \varepsilon$, et donc $\sup_{n\geqslant k} x_n \leqslant a + \varepsilon$, si k est assez grand, et $b \leqslant a + \varepsilon$, pour tout $\varepsilon > 0$. On en déduit que $b \leqslant a$, ce qui permet de démontrer la première égalité. La seconde se démontre de même en renversant les inégalités.

6.5. L'espace topologique $\mathbf{T} = \mathbf{R}/\mathbf{Z}$

$\mathbf{Z}$ étant un sous-groupe de $\mathbf{R}$ pour l'addition, on peut considérer le quotient $\mathbf{R}/\mathbf{Z}$ qui est un groupe commutatif ; on le munit de la topologie quotient, ce qui en fait un espace topologique.

• Si $\pi : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ est l'application naturelle, l'application $f \mapsto f \circ \pi$ est une bijection de l'ensemble des fonctions sur $\mathbf{R}/\mathbf{Z}$ sur celui des fonctions sur $\mathbf{R}$ vérifiant $f(x+n) = f(x)$ pour tous $x \in \mathbf{R}$ et $n \in \mathbf{Z}$. Autrement dit, une fonction sur $\mathbf{R}/\mathbf{Z}$ est la même chose qu'une fonction périodique de période 1 sur $\mathbf{R}$. Par ailleurs, par définition de la topologie quotient, une fonction f sur $\mathbf{R}/\mathbf{Z}$ est continue si et seulement si $f \circ \pi$ est continue sur $\mathbf{R}$. Autrement dit, l'espace $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ des fonctions continues sur $\mathbf{R}/\mathbf{Z}$ s'identifie naturellement à l'espace des fonctions continues sur $\mathbf{R}$, périodiques de période 1.

• L'application $x \mapsto \exp(2i\pi\, x)$ induit des homéomorphismes de $\mathbf{R}/\mathbf{Z}$ et $[0,1]/(0 \sim 1)$, munis de la topologie quotient, sur le cercle[35] $\mathrm{S}^1 = \{z \in \mathbf{C},\ |z| = 1\}$ muni de la topologie induite par celle de $\mathbf{C}$. En particulier, $\mathbf{R}/\mathbf{Z}$ est un espace compact métrisable.

Notons $\pi : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ l'application naturelle et $f : \mathbf{R} \to \mathrm{S}^1$ l'application $x \mapsto \exp(2i\pi\, x)$. Comme f est périodique de période 1, elle induit une application $\overline{f}$ de $\mathbf{R}/\mathbf{Z}$ dans S^1 qui est bijective de manière évidente, et on a $f = \overline{f} \circ \pi$ par construction. De plus, f est continue de $\mathbf{R}$ dans $\mathbf{C}$, et donc $\overline{f}$ est continue de $\mathbf{R}/\mathbf{Z}$ (muni de la topologie quotient) dans S^1 (muni de la

[34] Ça a l'air un peu tautologique, mais il est très utile de disposer des quantités $\limsup x_n$ et $\liminf x_n$ sans aucune hypothèse sur la suite $(x_n)_{n\in\mathbf{N}}$.

[35] Visuellement, si on prend un segment et qu'on attache ses deux extrémités, on obtient un cercle.

topologie induite par celle de $\mathbf{C}$). Comme f est injective et comme S^1 est séparé car métrique, on en déduit que $\mathbf{R}/\mathbf{Z}$ est séparé (cf. ex. 5.6).

Maintenant, l'application $x \mapsto x$ de $[0,1]$ dans $\mathbf{R}$ est continue, et donc la composée avec π est une application continue de $[0,1]$ dans $\mathbf{R}/\mathbf{Z}$ qui est surjective. Comme la seule relation modulo $\mathbf{Z}$ entre les éléments de $[0,1]$ est $0 \sim 1$, cette application continue induit, par passage au quotient, une injection continue $\iota : [0,1]/(0 \sim 1) \to \mathbf{R}/\mathbf{Z}$, et comme elle est surjective, c'est une bijection continue de $[0,1]/(0 \sim 1)$ sur $\mathbf{R}/\mathbf{Z}$. Comme $\mathbf{R}/\mathbf{Z}$ est séparé, on en déduit, par le même argument que ci-dessus, que $[0,1]/(0 \sim 1)$ est séparé. Comme $[0,1]$ est compact et comme l'application naturelle de $[0,1]$ dans $[0,1]/(0 \sim 1)$ est continue par définition de la topologie quotient, on en déduit, en utilisant les deux derniers points de l'alinéa 6.3.1, que :

- $[0,1]/(0 \sim 1)$ est compact ;
- $\iota : [0,1]/(0 \sim 1) \to \mathbf{R}/\mathbf{Z}$ est un homéomorphisme et $\mathbf{R}/\mathbf{Z}$ est compact ;
- $\overline{f} : \mathbf{R}/\mathbf{Z} \to \mathrm{S}^1$ est un homéomorphisme.

Ceci permet de conclure.

Ces diverses identifications permettent de voir un *lacet* γ dans un espace topologique X comme, au choix :

- une application continue $\gamma : \mathrm{S}^1 \to \mathrm{X}$,
- une application continue $\gamma : \mathbf{R} \to \mathrm{X}$, périodique de période 1,
- une application continue $\gamma : \mathbf{R}/\mathbf{Z} \to \mathrm{X}$,
- une application continue $\gamma : [0,1] \to \mathrm{X}$ vérifiant $\gamma(1) = \gamma(0)$.

C'est cette dernière description qui est utilisée la plupart du temps dans le cours.

7. Connexité

7.1. Ensembles connexes

• Si X est un espace topologique, les propriétés suivantes sont équivalentes :

(i) toute application continue de X dans $\{0,1\}$ (muni de la topologie discrète) est constante ;

(ii) toute application continue de X dans un espace topologique discret Y est constante ;

(iii) X ne peut pas s'écrire comme réunion de deux ouverts non vides disjoints ;

(iv) X ne peut pas s'écrire comme réunion de deux fermés non vides disjoints ;

(v) si $\mathrm{Y} \subset \mathrm{X}$ est à la fois ouvert et fermé, alors $\mathrm{Y} = \emptyset$ ou $\mathrm{Y} = \mathrm{X}$.

L'implication (ii)⇒(i) suit juste de ce que $\{0,1\}$ est un ensemble discret. Réciproquement, si Y est discret, toute application $g : \mathrm{Y} \to \{0,1\}$ est continue ; on en déduit que si X vérifie (i), et $f : \mathrm{X} \to \mathrm{Y}$ est continue, alors toute application composée $g \circ f : \mathrm{X} \to \{0,1\}$ est constante, ce qui implique que f est constante. Les conditions (i) et (ii) sont équivalentes.

Maintenant, si $f : \mathrm{X} \to \{0,1\}$ est continue, alors $\mathrm{U}_1 = f^{-1}(\{0\})$ et $\mathrm{U}_2 = f^{-1}(\{1\})$ sont ouverts puisque $\{0\}$ et $\{1\}$ sont ouverts dans $\{0,1\}$, sont disjoints, et $\mathrm{X} = \mathrm{U}_1 \cup \mathrm{U}_2$. Réciproquement, si U_1 et U_2 sont ouverts, disjoints, et si $\mathrm{X} = \mathrm{U}_1 \cup \mathrm{U}_2$, l'application $f : \mathrm{X} \to \{0,1\}$ définie par $f(x) = 0$, si $x \in \mathrm{U}_1$ et $f(x) = 1$ si $x \in \mathrm{U}_2$ est continue. On en déduit qu'il existe $f : \mathrm{X} \to \{0,1\}$ continue non constante si et seulement si on peut écrire X comme réunion

de deux ouverts non vides disjoints ; d'où l'équivalence de (i) et (iii). L'équivalence des autres propriétés avec (iii) est immédiate.

Un espace topologique X est *connexe* s'il est non vide et vérifie une des (et donc toutes les) propriétés équivalentes précédentes.

• Si X_1 et X_2 sont deux ensembles connexes avec $X_1 \cap X_2 \neq \emptyset$, alors $X_1 \cup X_2$ est connexe.

Soit $f : X_1 \cup X_2 \to \{0,1\}$ continue. Les restrictions de f à X_1 et X_2 sont continues et donc constantes. Comme on a supposé $X_1 \cap X_2 \neq \emptyset$, on peut choisir $y \in X_1 \cap X_2$, et f vaut $f(y)$ sur X_1 et X_2 ; par suite elle est constante sur $X_1 \cup X_2$. On en déduit la connexité de $X_1 \cup X_2$.

Ceci permet, si X est un espace topologique quelconque, et $x \in X$, de définir la *composante connexe* C_x de x dans X comme le plus grand sous-ensemble connexe de X contenant x ; c'est la réunion de tous les connexes de X contenant x. On appelle *composante connexe de* X tout sous-ensemble de la forme C_x, pour $x \in X$. On a $y \in C_x$ si et seulement si $C_y = C_x$, ce qui fait que les composantes connexes de X forment une partition de X, *la partition en composantes connexes*. Un ensemble est *totalement discontinu* si les composantes connexes sont réduites à un point.

• Dans $\mathbf{R}$, les connexes sont les segments (tous les segments, i.e. les $[a,b]$, $[a,b[$, $]a,b]$, $]a,b[$, pour $a, b \in \mathbf{R}$, ainsi que les demi-droites ou $\mathbf{R}$ tout entier obtenus en permettant à a ou b de prendre les valeurs $\pm\infty$).

Si $X \subset \mathbf{R}$ n'est pas un segment, c'est qu'il existe $a \notin X$ et $x_1, x_2 \in X$, avec $x_1 < a$ et $x_2 > a$. Alors $U_1 = X \cap]-\infty, a[$ et $U_2 = X \cap]a, +\infty[$ sont des ouverts de X, qui sont non vides, disjoints, et dont la réunion est X, ce qui prouve que X n'est pas connexe. Autrement dit, si X est connexe, alors X est un segment.

Maintenant, soient $a \leqslant b$, et soit $f : [a,b] \to \{0,1\}$ continue. Quitte à remplacer f par $1-f$, on peut supposer que $f(a) = 0$. Soit $X = \{x \in [a,b],\ f(x) = 1\}$, et soit c la borne inférieure de X, si X n'est pas vide. Par définition de c, il existe une suite d'éléments de X (qui peut être la suite constante c, si $c \in X$) ayant pour limite c, et comme f est continue, on a $f(c) = 1$. En particulier, on a $c \neq a$, et si $x \in [a,c[$, alors $f(x) = 0$, par définition de c. Comme f est continue et comme c est dans l'adhérence de $[a,c[$, cela implique que $f(c) = 0$. D'où une contradiction qui prouve que X est vide et donc que f est constante sur $[a,b]$. On en déduit la connexité du segment $[a,b]$.

Pour prouver la connexité de $[a,b[$, on prend une suite croissante b_n tendant vers b, et on écrit $[a,b[$ comme réunion croissante des segments $[a,b_n]$ qui sont connexes d'après ce qui précède. Comme une réunion de connexes dont l'intersection est non vide est connexe, cela prouve que $[a,b[$ est connexe. Les autres cas se traitant de la même manière, cela permet de conclure.

• L'image d'un ensemble connexe par une application continue est un ensemble connexe.

Si X est connexe, si $f : X \to Y$ est continue, et si $g : f(X) \to \{0,1\}$ est continue, alors $g \circ f : X \to \{0,1\}$ est continue, et donc constante puisque X est connexe. Comme $f : X \to f(X)$ est surjective, cela implique que g est constante. On en déduit la connexité de $f(X)$.

• Soit $f : [a,b] \to \mathbf{R}$ continue. Si $f(a)$ et $f(b)$ sont de signes opposés, alors il existe $x \in [a,b]$ tel que $f(x) = 0$ (théorème des valeurs intermédiaires).

Comme $[a,b]$ est connexe, son image par f l'est aussi et donc est un segment de $\mathbf{R}$, et comme cette image contient des réels négatifs et positifs par hypothèse, elle contient 0.

• Si X et Y sont connexes, alors $X \times Y$ est connexe.

Soit $f : X \times Y \to \{0,1\}$ continue. Si $x \in X$, la restriction de f à $\{x\} \times Y$ est continue et donc constante, et si $y \in Y$, la restriction de f à $X \times \{y\}$ est continue et donc constante. Ceci implique que si $(x_1,y_1),(x_2,y_2) \in X \times Y$, alors $f(x_2,y_2) = f(x_2,y_1) = f(x_1,y_1)$, et donc que f est constante. On en déduit la connexité de $X \times Y$.

• Si X est un espace topologique, et si $Y \subset X$ est connexe, alors l'adhérence de Y dans X est connexe.

Soit $f : \overline{Y} \to \{0,1\}$ continue. Comme Y est connexe, la restriction de f à Y est constante. Soit $a \in \{0,1\}$ l'image de Y. Alors $f^{-1}(a)$ est un fermé de $\overline{Y}$ contenant Y, et donc est égal à $\overline{Y}$ par définition de l'adhérence. Autrement dit, f est constante. On en déduit la connexité de $\overline{Y}$.

• Les composantes connexes d'un espace topologique sont fermées.

7.2. Connexité par arcs

Un espace topologique X est dit *connexe par arcs* si, quels que soient $x, y \in X$, il existe $u : [0,1] \to X$ continue, avec $u(0) = x$ et $u(1) = y$ (i.e. si on peut joindre n'importe quelle paire d'éléments de X par un chemin continu). Si X_1 et X_2 sont connexes par arcs, et si $X_1 \cap X_2$ est non vide, alors $X_1 \cup X_2$ est connexe par arcs puisqu'on peut joindre n'importe quel point de $X_1 \cup X_2$ a un point de l'intersection par un chemin continu, et donc n'importe quel couple de points de $X_1 \cup X_2$. Ceci permet, comme ci-dessus, de parler des *composantes connexes par arcs de* X.

• Un espace connexe par arcs est connexe[36], mais il existe des ensembles connexes qui ne sont pas connexes par arcs.

Soit X connexe par arc, et soit $x_0 \in X$. Par hypothèse, il existe, pour tout $x \in X$, une application continue $u : [0,1] \to X$ avec $u(0) = x_0$ et $u(1) = x$. Comme $[0,1]$ est connexe et comme l'image d'un connexe par une application continue est connexe, cela montre que x est dans la composante connexe de x_0. Par suite la composante connexe de x_0 est X tout entier qui, de ce fait, est connexe.

Pour des exemples de connexes non connexes par arcs, voir la rubrique tératologie.

• Un ouvert connexe de $\mathbf{R}^n$ est connexe par arcs.

Soit U un ouvert connexe de $\mathbf{R}^n$, et soient $x_0 \in U$ et X la composante connexe par arcs de x_0. Soit $x \in X$. Comme U est ouvert, il existe $r > 0$ tel que $B(x,r)$ soit incluse dans U. Si $y \in B(x,r)$, le segment $[x,y]$ est inclus dans U, et comme il existe un chemin continu joignant x_0 à x dans U, il suffit de composer ce chemin avec le segment $[x,y]$ pour obtenir un chemin joignant x_0 à y dans U. On en déduit l'appartenance de y à X, et donc l'inclusion de $B(0,r)$ dans X, ce qui prouve que X est ouvert. Maintenant, soit x dans l'adhérence de X dans U, et soit $r > 0$ tel que $B(x,r)$ soit incluse dans U. Par définition de l'adhérence, il existe

[36] C'est le principal intérêt de la connexité par arcs ; la connexité est d'utilisation nettement plus facile.

$y \in \mathrm{X} \cap \mathrm{B}(x,r)$, et comme le segment $[y,x]$ est contenu dans U, on déduit comme ci-dessus que $x \in \mathrm{X}$, ce qui prouve que X est fermé. On a donc prouvé que X est à la fois ouvert et fermé dans U, et comme il est non vide et que U est supposé connexe, cela implique que $\mathrm{X} = \mathrm{U}$. Ceci permet de conclure.

• Un ouvert de $\mathbf{R}^n$ est une réunion dénombrable d'ouverts connexes. Un ouvert de $\mathbf{R}$ est une réunion dénombrable de segments ouverts.

Soit U un ouvert de $\mathbf{R}^n$. Si $x \in \mathrm{U}$, il existe $r > 0$ tel que $\mathrm{B}(x,r) \subset \mathrm{U}$, et comme $\mathrm{B}(x,r)$ est connexe par arcs (et même par segments), la composante connexe de x contient $\mathrm{B}(x,r)$. On en déduit que les composantes connexes de U sont des ouverts. Maintenant, un ouvert de $\mathbf{R}^n$ contient un point dont toutes les coordonnées sont rationnelles, et comme les composantes connexes de U sont disjointes, on obtient une injection de l'ensemble de ces composantes connexes dans $\mathbf{Q}^n$, en choisissant un point à coordonnées rationnelles dans chacune d'entre elles. Comme $\mathbf{Q}^n$ est dénombrable, cela montre que l'ensemble des composantes connexes de U est dénombrable. On en déduit le premier énoncé. Le second en est une conséquence immédiate puisqu'un ouvert connexe de $\mathbf{R}$ est un segment ouvert.

Exercice 7.1. — Montrer que si $n \geqslant 2$, et si U est un ouvert connexe de $\mathbf{R}^n$, alors $\mathrm{U} - \{x\}$ est connexe, quel que soit $x \in \mathrm{U}$.

Exercice 7.2. — (i) Montrer que $\mathbf{R}$ et $\mathbf{R}^2$ ne sont pas homéomorphes ; que $[0,1]$ et $[0,1]^2$ ne sont pas homéomorphes.

(ii) Montrer que $[0,1]$ et le cercle $\mathrm{C} = \{z \in \mathbf{C},\ |z| = 1\}$ ne sont pas homéomorphes.

Exercice 7.3. — Montrer que $[0,1]$ et $]0,1[$ ne sont pas homéomorphes.

Exercice 7.4. — Soit X le sous-ensemble de $\mathbf{R}$ constitué de trois cercles de rayon 1 dont les centres forment les trois sommets d'un triangle équilatéral dont la longueur des côtés est 2 (chacun des cercles est donc tangent aux deux autres). Soit Y formé de trois cercles de rayon 1 centrés en $(0,0)$, $(2,0)$ et $(4,0)$. Montrer que X et Y ne sont pas homéomorphes.

Exercice 7.5. — (difficile)

(i) Soit $(\mathrm{F}_n)_{n\in\mathbf{N}}$ une suite décroissante $(\mathrm{F}_{n+1} \subset \mathrm{F}_n)$ de fermés connexes de $\mathbf{R}^2$, et soit $\mathrm{F} = \cap_{n\in\mathbf{N}}\mathrm{F}_n$.

(a) Donner un exemple où F n'est pas connexe.

(b) Montrer que, si F_0 est compact, alors F est connexe.

(ii) Soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathbf{R}^2$ telle que $d(x_{n+1}, x_n) \to 0$.

(a) Montrer que, si la suite est bornée, l'ensemble de ses valeurs d'adhérence est connexe.

(b) Est-ce forcément le cas si la suite n'est pas bornée ?

Exercice 7.6. — (difficile, sa solution utilise la notion d'espace contractile introduite plus tard dans le cours) Montrer que le cylindre et la bande de Moebius ne sont pas homéomorphes.

8. Complétude

8.1. Suites de Cauchy

Soit (X, d) un espace métrique. Une suite $(x_n)_{n\in\mathbf{N}}$ est *de Cauchy* (ou vérifie le *critère de Cauchy*) si le diamètre de $\{x_k,\ k \geqslant n\}$ tend vers 0 quand $n \to +\infty$, ce qui se traduit, au choix, par :

- quel que soit $\varepsilon > 0$, il existe $\mathrm{N} \in \mathbf{N}$, tel que $d(x_{n+p}, x_n) < \varepsilon$ si $n \geqslant \mathrm{N}$ et $p \in \mathbf{N}$;
- $\lim_{n\to+\infty} \big(\sup_{p\in\mathbf{N}} d(x_{n+p}, x_n)\big) = 0$.

On remarquera qu'une suite de Cauchy est en particulier bornée.

Exercice 8.1. — (i) Montrer que si d est ultramétrique, alors $(x_n)_{n\in\mathbf{N}}$ est de Cauchy si et seulement si $d(x_{n+1}, x_n) \to 0$.

(ii) Construire une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{R}$, vérifiant $d(x_{n+1}, x_n) \to 0$, et qui n'est pas de Cauchy.

- Une suite de Cauchy ayant au moins une valeur d'adhérence a une limite.

  Soit $(x_n)_{n\in\mathbf{N}}$ une suite de Cauchy. Supposons que a en soit une valeur d'adhérence. Comme X est un espace métrique, il existe une suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ extraite de $(x_n)_{n\in\mathbf{N}}$ ayant a pour limite. Soit alors $\varepsilon > 0$. Comme $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, il existe $\mathrm{N}_0 \in \mathbf{N}$ tel que $d(x_{m+p}, x_m) < \varepsilon$, si $m \geqslant \mathrm{N}_0$ et $p \in \mathbf{N}$. Comme $\varphi(n)$ tend vers $+\infty$, il existe $\mathrm{N}_1 \in \mathbf{N}$ tel que $\varphi(n) \geqslant \mathrm{N}_0$, si $n \geqslant \mathrm{N}_1$, et comme $x_{\varphi(n)} \to a$, il existe $\mathrm{N}_2 \geqslant \mathrm{N}_1$ tel que $d(x_{\varphi(n)}, a) < \varepsilon$, si $n \geqslant \mathrm{N}_2$. Alors $d(x_{\varphi(n)+p}, a) < 2\varepsilon$, si $n \geqslant \mathrm{N}_2$ et $p \in \mathbf{N}$, et donc $d(x_m, a) < 2\varepsilon$, si $m \geqslant \varphi(\mathrm{N}_2)$. On en déduit que $x_n \to a$, ce qui permet de conclure.

L'espace (X, d) est *complet* si toute suite de Cauchy admet une valeur d'adhérence ou, ce qui revient au même, une limite. Le critère qui suit permet de ne considérer que des suites convergeant "normalement".

- (X, d) est complet si et seulement si la condition $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$ implique que $(x_n)_{n\in\mathbf{N}}$ a une limite.

  Si $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$, alors $\sup_{p\in\mathbf{N}} d(x_n, x_{n+p}) \leqslant \sum_{k=0}^{+\infty} d(x_{n+k+1}, x_{n+k})$ tend vers 0 quand $n \to +\infty$ puisque majoré par le reste d'une série convergente. On en déduit que la suite $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, et donc converge si (X, d) est complet.

  Réciproquement, si toute suite $(x_n)_{n\in\mathbf{N}}$ telle que $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$ a une limite, et si $(y_n)_{n\in\mathbf{N}}$ est une suite de Cauchy, on peut en extraire une sous-suite $(y_{\varphi(n)})_{n\in\mathbf{N}}$ telle que $\sup_{p\in\mathbf{N}} d(y_{\varphi(n+p)}, y_{\varphi(n)}) \leqslant 2^{-n}$ quel que soit $n \in \mathbf{N}$. Il suffit de définir $\varphi(n)$ comme le N correspondant à $\varepsilon = 2^{-n}$ dans la définition d'une suite de Cauchy. La suite $x_n = y_{\varphi(n)}$ vérifie $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$; elle converge donc, et comme elle est extraite de $(y_n)_{n\in\mathbf{N}}$, cela prouve que $(y_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence et donc une limite puisqu'elle est de Cauchy. On en déduit la complétude de X.

- Si (X, d) est complet, et si Y est fermé dans X, alors (Y, d) est complet.

  Si $(x_n)_{n\in\mathbf{N}}$ est une suite de Cauchy dans Y, alors c'est une suite de Cauchy dans X ; elle a donc une limite dans X qui appartient à Y puisque Y est fermé. D'où la complétude de Y.

- Un espace métrique compact est complet.

  Si $(x_n)_{n\in\mathbf{N}}$ est de Cauchy dans un espace métrique compact X, alors $(x_n)_{n\in\mathbf{N}}$ admet une valeur d'adhérence puisque X est compact, et donc converge d'après le point ci-dessus, ce qui prouve que X est complet.

D'après le point précédent, un espace compact est complet quelle que soit la distance utilisée pour définir la topologie. Ce n'est pas le cas en général : *la complétude est une propriété métrique et pas topologique.*

Exercice 8.2. — (i) Montrer que $d'(x,y) = |f(y) - f(x)|$, avec $f(x) = \frac{x}{1-|x|}$ est une distance sur $]-1,1[$ équivalente à la distance usuelle.

(ii) Montrer que $]-1,1[$ est complet pour d' mais pas pour la distance usuelle.

• $\mathbf{R}$ est complet.

Soit $(x_n)_{n\in\mathbf{N}}$ une suite de Cauchy d'éléments de $\mathbf{R}$. En particulier, la suite est bornée et il existe $\mathrm{M} > 0$ telle que $(x_n)_{n\in\mathbf{N}}$ soit à valeurs dans $[-\mathrm{M},\mathrm{M}]$. Comme $[-\mathrm{M},\mathrm{M}]$ est compact, cela implique que $(x_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence, et donc qu'elle a une limite puisqu'elle est de Cauchy. Ceci permet de conclure.

• Si X et Y sont complets, alors $\mathrm{X}\times\mathrm{Y}$ est complet.

Si $(x_n,y_n)_{n\in\mathbf{N}}$ est une suite de Cauchy dans $\mathrm{X}\times\mathrm{Y}$, alors $(x_n)_{n\in\mathbf{N}}$ est de Cauchy dans X et $(y_n)_{n\in\mathbf{N}}$ est de Cauchy dans Y, et si a et b désignent les limites respectives de $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$, alors $(x_n,y_n)_{n\in\mathbf{N}}$ tend vers (a,b). On en déduit la complétude de $\mathrm{X}\times\mathrm{Y}$.

8.2. Principales propriétés des espaces complets

L'intérêt principal de travailler dans un espace complet est que les problèmes d'existence sont nettement plus faciles. Le théorème du point fixe ci-dessous a de multiples applications à l'existence d'objets (solutions d'équations différentielles, racines de polynômes à coefficients réels, complexes, ou p-adiques, inversion locale de fonctions de classe $\mathscr{C}^1$...). Le lemme de Baire est un autre de ces outils magiques fournissant l'existence d'une infinité de solutions à des problèmes pour lesquels on a du mal à en exhiber une[(37)] ; son utilisation nécessite nettement plus d'astuce que celle du théorème du point fixe.

• Dans un espace complet, une application strictement contractante admet un unique point fixe, et la suite des itérés de tout point tend vers ce point fixe (théorème du point fixe).

Soit (X,d) un espace métrique complet, soit $f:\mathrm{X}\to\mathrm{X}$ une application strictement contractante (i.e. il existe $\alpha<1$ tel que $d(f(x),f(y)) \leqslant \alpha d(x,y)$ quels que soient $x,y\in\mathrm{X}$), et soit $x\in\mathrm{X}$. Définissons par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ en posant $x_0 = x$ et $x_{n+1} = f(x_n)$, si $n\in\mathbf{N}$ (en notant f^n l'application $f\circ\cdots\circ f$ composée n fois, on a aussi $x_n = f^n(x)$). Soit $a = d(x_0,x_1)$. Une récurrence immédiate montre que $d(x_n,x_{n+1}) \leqslant \alpha^n a$ quel que soit $n\in\mathbf{N}$. On a donc, si $p\in\mathbf{N}$, et $n\in\mathbf{N}$

$$d(x_{n+p},x_n) \leqslant d(x_n,x_{n+1}) + \cdots + d(x_{n+p-1},x_{n+p}) \leqslant a(\alpha^n + \cdots + \alpha^{n+p-1}) \leqslant \alpha^n \frac{a}{1-\alpha}.$$

La suite $(x_n)_{n\in\mathbf{N}}$ est donc de Cauchy puisque α^n tend vers 0 quand n tend vers $+\infty$. Notons ℓ sa limite. Une application contractante étant en particulier continue, on a

$$f(\ell) = f(\lim_{n\to+\infty} x_n) = \lim_{n\to+\infty} f(x_n) = \lim_{n\to+\infty} x_{n+1} = \ell,$$

ce qui prouve que ℓ est un point fixe de f. On a donc prouvé que, si x est un point quelconque de X, alors la suite des itérés de x par f tend vers un point fixe de f. Maintenant, si x et y

(37) On tombe alors sur le problème quasi-théologique de savoir si on peut vraiment prétendre avoir démontré qu'un ensemble est non vide si on est incapable d'en produire un élément.

sont deux points fixes de f, on a $d(x,y) = d(f(x),f(y)) \leqslant \alpha d(x,y)$, et donc $d(x,y) = 0$, et $x = y$, ce qui prouve que f a un unique point fixe. Ceci permet de conclure.

• Dans un espace complet, l'intersection d'une suite de fermés emboités, non vides, dont le diamètre tend vers 0, est non vide et réduite à un point (théorème des fermés emboités).

Soit (X, d) un espace métrique complet, et soit $(\mathrm{F}_n)_{n\in\mathbf{N}}$ une suite de fermés emboités (i.e. $\mathrm{F}_{n+1} \subset \mathrm{F}_n$ quel que soit $n \in \mathbf{N}$), non vides, dont le diamètre tend vers 0 (le *diamètre* d'un sous-ensemble Y de X est la borne supérieure de l'ensemble des $d(x,y)$, pour $x, y \in \mathrm{Y}$).

Choisissons pour tout $n \in \mathbf{N}$ un élément x_n de F_n, et notons d_n le diamètre de F_n. Par hypothèse d_n tend vers 0 quand n tend vers $+\infty$. Par ailleurs, x_{n+p} et x_n sont deux éléments de F_n et donc $d(x_{n+p}, x_n) \leqslant d_n$ quels que soient $n, p \in \mathbf{N}$. La suite $(x_n)_{n\in\mathbf{N}}$ est donc de Cauchy. Comme X est supposé complet, cette suite admet une limite x. De plus, si on fixe m, alors $x_n \in \mathrm{F}_n \subset \mathrm{F}_m$, si $n \geqslant m$, et comme F_m est fermé, cela implique que $x \in \mathrm{F}_m$. Ceci étant vrai pour tout $m \in \mathbf{N}$, on a $x \in \mathrm{F} = \cap_{n\in\mathbf{N}}\mathrm{F}_n$, ce qui prouve que F est non vide. Enfin, si x, y sont deux éléments de F, on a $x, y \in \mathrm{F}_n$ pour tout $n \in \mathbf{N}$, et donc $d(x,y) \leqslant d_n$ quel que soit $n \in \mathbf{N}$. On en déduit la nullité de $d(x,y)$, ce qui implique $x = y$, et permet de conclure.

• Dans un espace complet, une intersection dénombrable d'ouverts denses est dense et donc, en particulier, est non vide (lemme de Baire).

Soit (X, d) un espace métrique complet, et soit $(\mathrm{U}_n)_{n\in\mathbf{N}}$ une suite d'ouverts denses de X. Notre but est de prouver que, si $x_0 \in \mathrm{X}$, et si $r_0 > 0$, alors $\mathrm{B}(x_0, r_0^-) \cap (\cap_{n\in\mathbf{N}}\mathrm{U}_n)$ est non vide. Pour cela, nous allons contruire une suite $\mathrm{B}(x_n, r_n)$ de boules fermées vérifiant :

$$0 < r_{n+1} \leqslant \tfrac{r_n}{2} \quad \text{et} \quad \mathrm{B}(x_{n+1}, r_{n+1}) \subset \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-).$$

Supposons $\mathrm{B}(x_n, r_n)$ construite. Comme U_{n+1} est dense dans X, $\mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$ est non vide. Prenons $x_{n+1} \in \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$ quelconque. Comme $\mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$ est un ouvert, il existe $r_{n+1} \in]0, \frac{r_n}{2}]$ tel que $\mathrm{B}(x_{n+1}, 2r_{n+1}^-) \subset \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$, et donc $\mathrm{B}(x_{n+1}, r_{n+1}) \subset \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$, ce qui permet de faire la construction à l'ordre $n+1$.

Maintenant, par construction, les $\mathrm{B}(x_n, r_n)$ forment une suite de fermés emboités (car on a imposé $\mathrm{B}(x_{n+1}, r_{n+1}) \subset \mathrm{B}(x_n, r_n^-)$) dont le diamètre tend vers 0 (car $r_{n+1} \leqslant \frac{r_n}{2}$), et $\mathrm{B}(x_n, r_n) \subset \mathrm{B}(x_0, r_0^-) \cap (\cap_{k\leqslant n}\mathrm{U}_k)$, si $n \geqslant 1$, ce qui implique que $\cap_{n\in\mathbf{N}}\mathrm{B}(x_n, r_n)$, qui est non vide d'après le théorème des fermés emboités, est inclus dans

$$\cap_{n\in\mathbf{N}}(\mathrm{B}(x_0, r_0^-) \cap (\cap_{k\leqslant n}\mathrm{U}_k)) = \mathrm{B}(x_0, r_0^-) \cap (\cap_{n\in\mathbf{N}}\mathrm{U}_n).$$

Ceci permet de conclure.

Le lemme de Baire s'utilise souvent en passant aux complémentaires.

• Dans un espace complet, une réunion dénombrable de fermés d'intérieur vide est d'intérieur vide ; autrement dit, si une réunion dénombrable de fermés est d'intérieur non vide, alors au moins un des fermés est d'intérieur non vide.

Exercice 8.3. — (i) Montrer qu'une intersection dénombrable d'ouverts denses de $\mathbf{R}$ est non dénombrable.

(ii) Peut-on trouver une suite $(f_n)_{n\in\mathbf{N}}$ de fonctions continues sur $\mathbf{R}$ telle que la suite des $f_n(x)$, pour $n \in \mathbf{N}$, soit bornée pour tout x irrationnel et non bornée pour tout x rationnel ?

8.3. Complétion d'un espace métrique

Un espace métrique n'est pas forcément complet, mais il peut se compléter de manière unique. Plus précisément :

• Si (X, d) est un espace métrique, il existe, à isométrie près, un unique espace métrique complet $(\widehat{\mathrm{X}}, d)$, contenant X comme sous-espace dense, qui vérifie la *propriété universelle* suivante : toute application uniformément continue f de X dans un espace métrique Y *complet* se prolonge de manière unique en une application continue de $\widehat{\mathrm{X}}$ dans Y.

Cet espace est le *complété de* X, et un espace complet est son propre complété ; plus généralement, si X est dense dans Y, et si Y est complet, alors Y est le complété de X.

L'unicité suit du résultat plus général (et très utile) suivant appliqué au cas où Y et Z sont deux complétés de X, et f est l'identité sur X, l'application $f : \mathrm{Y} \to \mathrm{Z}$ qu'on en tire est alors une isométrie puisque c'en est une sur X (cf. ex. 5.8).

• Soient $(\mathrm{Y}, d_{\mathrm{Y}})$ et $(\mathrm{Z}, d_{\mathrm{Z}})$ deux espaces complets. Si X est dense dans Y, et si $f : \mathrm{X} \to \mathrm{Z}$ est telle qu'il existe $\rho > 0$, tel que f soit uniformément continue sur $\mathrm{B}_{\mathrm{X}}(x, \rho)$, pour tout $x \in \mathrm{X}$, alors f s'étend de manière unique en une application continue de Y dans Z.

Soit $y \in \mathrm{Y}$, et soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de X tendant vers y quand n tend vers $+\infty$. La suite $(x_n)_{n\in\mathbf{N}}$ est alors de Cauchy, et il existe $n \in \mathbf{N}$ tel que $x_n \in \mathrm{B}_{\mathrm{X}}(x_{n_0}, \rho)$, quel que soit $n \geqslant n_0$. Comme on a supposé que f est uniformément continue sur $\mathrm{B}_{\mathrm{X}}(x_{n_0}, \rho)$, la suite $(f(x_n))_{n\in\mathbf{N}}$ est de Cauchy dans Z, et comme Z est complet, cette suite a une limite, et cette limite ne dépend pas de la suite $(x_n)_{n\in\mathbf{N}}$ de limite y (sinon on pourrait construire une telle suite de telle sorte que que $(f(x_n))_{n\in\mathbf{N}}$ ait deux valeurs d'adhérence). Notons cette limite $f(y)$.

Maintenant, soit $\varepsilon > 0$ et soit $x_0 \in \mathrm{X}$. Comme f est uniformément continue sur $\mathrm{B}_{\mathrm{X}}(x_0, \rho)$, il existe $\delta > 0$ tel que $d_{\mathrm{Z}}(f(x), f(x')) \leqslant \varepsilon$, si $d_{\mathrm{Y}}(x, x') < \delta$ et $x, x' \in \mathrm{B}_{\mathrm{X}}(x_0, \rho)$. Si $y_1, y_2 \in \mathrm{B}_{\mathrm{Y}}(x_0, \rho)$ vérifient $d_{\mathrm{Y}}(y_1, y_2) < \delta$, et si $(x_{1,n})_{n\in\mathbf{N}}$ et $(x_{2,n})_{n\in\mathbf{N}}$ sont des suites d'éléments de X tendant vers y_1 et y_2 respectivement, alors $x_{1,n}, x_{2,n} \in \mathrm{B}_{\mathrm{X}}(x_0, \rho)$ et $d_{\mathrm{Y}}(x_{1,n}, x_{2,n}) < \delta$ si n est assez grand. On a donc $d_{\mathrm{Z}}(f(x_{1,n}), f(x_{2,n})) \leqslant \varepsilon$ pour tout n assez grand, et un passage à la limite montre que $d_{\mathrm{Z}}(f(y_1), f(y_2)) \leqslant \varepsilon$, ce qui prouve que f est uniformément continue sur $\mathrm{B}_{\mathrm{Y}}(x_0, \rho)$. Comme les $\mathrm{B}_{\mathrm{Y}}(x_0, \rho)$, pour $x_0 \in \mathrm{X}$, recouvrent Y, puisque X est dense dans Y, cela permet de conclure.

L'existence se démontre en rajoutant[38] de force les limites des suites de Cauchy.

Pour ce faire, notons Cauchy(X) l'ensemble des suites de Cauchy à valeurs dans X. Si $\hat{x} = (x_n)_{n\in\mathbf{N}}$ et $\hat{y} = (y_n)_{n\in\mathrm{N}}$ sont deux éléments de Cauchy(X), la suite $(d(x_n, y_n))_{n\in\mathbf{N}}$ est de Cauchy dans $\mathbf{R}$ car

$$|d(x_{n+p}, y_{n+p}) - d(x_n, y_n)| = |d(x_{n+p}, y_{n+p}) - d(x_n, y_{n+p}) + d(x_n, y_{n+p}) - d(x_n, y_n)| \leqslant d(x_{n+p}, x_n) + d(y_{n+p}, y_n)$$

d'après l'inégalité triangulaire. Comme $\mathbf{R}$ est complet, cette suite admet une limite que l'on note $\hat{d}(\hat{x}, \hat{y})$. De plus, si $\hat{x} = (x_n)_{n\in\mathbf{N}}, \hat{y} = (y_n)_{n\in\mathbf{N}}, \hat{z} = (z_n)_{n\in\mathbf{N}}$ sont trois éléments de Cauchy(X), un passage à la limite dans l'inégalité triangulaire $d(x_n, z_n) \leqslant d(x_n, y_n) + d(y_n, z_n)$

[38] Beaucoup d'objets mathématiques sont obtenus de cette manière, à commencer par $\mathbf{R}$ qui est le complété de $\mathbf{Q}$ pour la distance usuelle $d(x, y) = |x - y|$, où $|x - y|$ est la valeur absolue de $x - y$, et $\mathbf{Q}_p$ qui est le complété de $\mathbf{Q}$ pour la norme p-adique.

montre que $\hat{d}$ vérifie l'inégalité triangulaire $\hat{d}(\hat{x},\hat{z}) \leqslant \hat{d}(\hat{x},\hat{y}) + \hat{d}(\hat{y},\hat{z})$. De même, $\hat{d}$ vérifie la symétrie $\hat{d}(\hat{x},\hat{y}) = \hat{d}(\hat{y},\hat{x})$, mais elle ne vérifie pas la séparation de la distance (i.e. il n'est pas vrai que $\hat{d}(\hat{x},\hat{y}) = 0$ implique $\hat{x} = \hat{y}$). De fait, il est assez clair que $\hat{d}(\hat{x},\hat{y}) = 0$ équivaut au fait que $\hat{x}$ et $\hat{y}$ ont moralement la même limite. Cela nous conduit à introduire la relation $\sim$ sur Cauchy(X) définie par, $\hat{x} \sim \hat{y}$ si et seulement si $\hat{d}(\hat{x},\hat{y}) = 0$, ce qui fait de $\sim$ une relation d'équivalence, et nous permet de considérer le quotient $\widehat{\mathrm{X}}$ de Cauchy(X) par cette relation d'équivalence (ce qui revient à considérer comme égaux deux éléments $\hat{x},\hat{y}$ de Cauchy(X) vérifiant $\hat{d}(\hat{x},\hat{y}) = 0$).

Il n'y a plus qu'à vérifier que l'objet que l'on a construit est bien celui que l'on voulait.

L'inégalité triangulaire montre que $\hat{d}(\hat{x},\hat{y}) = \hat{d}(\hat{x}',\hat{y}')$ si $\hat{x} \sim \hat{x}'$ et $\hat{y} \sim \hat{y}'$, ce qui montre que $\hat{d}$ passe au quotient, et définit une distance sur $\widehat{\mathrm{X}}$ puisque, par définition de $\widehat{\mathrm{X}}$, la condition $\hat{d}(\hat{x},\hat{y}) = 0$ implique $\hat{x} = \hat{y}$.

On peut identifier $x \in \mathrm{X}$, à la classe dans $\widehat{\mathrm{X}}$ de la suite constante $\iota(x) = (x_n)_{n\in\mathbf{N}}$, avec $x_n = x$ pour tout $n \in \mathbf{N}$. Si $x, y \in \mathrm{X}$, on a $\hat{d}(x,y) = \hat{d}(\iota(x),\iota(y)) = \lim_{n\to+\infty} d(x,y) = d(x,y)$, ce qui montre que $\hat{d}$ induit la distance d sur X. Par ailleurs, si $\hat{x} = (x_n)_{n\in\mathbf{N}}$ est un élément de Cauchy(X), alors $\hat{d}(\hat{x},\iota(x_k)) = \lim_{n\to+\infty} d(x_n,x_k) \leqslant \sup_{n\geqslant k} d(x_n,x_k)$, et comme la suite $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, $\sup_{n\geqslant k} d(x_n,x_k)$ tend vers 0 quand k tend vers $+\infty$. On a donc $\hat{x} = \lim_{k\to+\infty} x_k$ dans $\widehat{\mathrm{X}}$, ce qui prouve que X est dense dans $\widehat{\mathrm{X}}$.

Il reste à prouver que $\widehat{\mathrm{X}}$ est complet. Pour cela soit $(\hat{x}_n)_{n\in\mathbf{N}}$ une suite de Cauchy dans $\widehat{\mathrm{X}}$. Comme X est dense dans $\widehat{\mathrm{X}}$, on peut trouver, quel que soit $n \in \mathbf{N}$, un élément x_n de X tel que $\hat{d}(\hat{x}_n,x_n) \leqslant 2^{-n}$. Soit $\hat{x} = (x_n)_{n\in\mathbf{N}}$. On a

$$d(x_n,x_{n+p}) = \hat{d}(x_n,x_{n+p}) \leqslant \hat{d}(x_n,\hat{x}_n) + \hat{d}(\hat{x}_n,\hat{x}_{n+p}) + \hat{d}(\hat{x}_{n+p},x_{n+p}) \leqslant 2^{1-n} + \hat{d}(\hat{x}_n,\hat{x}_{n+p}),$$

et comme la suite $(\hat{x}_n)_{n\in\mathbf{N}}$ est de Cauchy, on en déduit que $\hat{x} \in$ Cauchy(X). De plus,

$$\hat{d}(\hat{x}_n,\hat{x}) \leqslant \hat{d}(\hat{x}_n,x_n) + \hat{d}(x_n,\hat{x}) \leqslant 2^{-n} + \lim_{m\to+\infty} d(x_n,x_m) \leqslant 2^{-n} + \sup_{p\in\mathbf{N}} d(x_n,x_{n+p}),$$

et comme $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, $\sup_{p\in\mathbf{N}} d(x_n,x_{n+p}) \to 0$. Autrement dit, $\hat{x}_n \to \hat{x}$ dans $\widehat{\mathrm{X}}$. On en déduit la complétude de $\widehat{\mathrm{X}}$.

9. Convergence de fonctions

9.1. Convergence simple

Si X et Y sont deux espaces topologiques, une suite de fonctions $f_n : \mathrm{X} \to \mathrm{Y}$ *converge simplement vers* f si, pour tout $x \in \mathrm{X}$, la suite $f_n(x)$ a pour limite $f(x)$ dans Y. Si c'est le cas, on dit que f est la *limite simple* de la suite f_n.

Il est, en pratique, largement inutile de savoir quelle topologie se cache derrière la convergence simple. Cette topologie n'a rien de mystérieux : c'est la topologie produit sur l'espace des fonctions Y^{X} de X dans Y. En effet, les conditions suivantes sont équivalentes :

- $f_n(x) \to f(x)$, pour tout $x \in \mathrm{X}$;
- $(f_n(x))_{x\in\mathrm{I}} \to (f(x))_{x\in\mathrm{I}}$ pour tout $\mathrm{I} \subset \mathrm{X}$ fini ;
- pour tout $\mathrm{I} \subset \mathrm{X}$ fini, et tout ouvert de Y^{I} de la forme $\mathrm{U} = \prod_{x\in\mathrm{I}} \mathrm{U}_x$ qui contient $(f(x))_{x\in\mathrm{I}}$, il existe $\mathrm{N} \in \mathbf{N}$, tel que $(f_n(x))_{x\in\mathrm{I}} \in \mathrm{U}$, si $n \geqslant \mathrm{N}$;
- pour tout $\mathrm{I} \subset \mathrm{X}$ fini, et tout ouvert de Y^{X} de la forme $\mathrm{U} = \left(\prod_{x\in\mathrm{I}} \mathrm{U}_x\right) \times \left(\prod_{x\notin\mathrm{I}} \mathrm{Y}\right)$ qui contient $(f(x))_{x\in\mathrm{X}}$, il existe $\mathrm{N} \in \mathbf{N}$, tel que $(f_n(x))_{x\in\mathrm{X}} \in \mathrm{U}$, si $n \geqslant \mathrm{N}$;

• $f_n \to f$ dans Y^{X}.

D'après l'exercice ci-dessous, les fonctions continues sont denses dans l'ensemble des fonctions de $\mathbf{R}$ dans $\mathbf{C}$ pour la topologie produit sur l'espace $\mathbf{C}^{\mathbf{R}}$ des fonctions de $\mathbf{R}$ dans $\mathbf{C}$. Or, Baire a montré qu'une limite simple de fonctions continues de $\mathbf{R}$ dans $\mathbf{C}$ est continue en au moins un point. Donc il existe des éléments de $\mathbf{C}^{\mathbf{R}}$ qui ne sont pas limite simple d'une suite de fonctions continues, ce qui n'est possible que si la topologie ci-dessus sur $\mathbf{C}^{\mathbf{R}}$ n'est pas définissable par une distance. Cela explique qu'il existe des fonctions qui sont limites simples de limites simples de fonctions continues, mais qui ne sont pas limites simples de fonctions continues.

Exercice 9.1. — Montrer que l'ensemble des fonctions continues de $\mathbf{R}$ dans $\mathbf{C}$ est dense dans $\mathbf{C}^{\mathbf{R}}$ (muni de la topologie produit).

9.2. Convergence uniforme

Soient X un ensemble et Y un espace métrique (par exemple $\mathrm{Y} = \mathbf{C}$). Soient f et f_n, pour $n \in \mathbf{N}$, des fonctions de X dans Y. On dit que f_n *converge uniformément* vers f sur X ou que f est la *limite uniforme* des f_n, si $\lim_{n\to+\infty} \big(\sup_{x\in\mathrm{X}} d_{\mathrm{Y}}(f(x), f_n(x))\big) = 0$. Ceci peut se réécrire sous la forme : pour tout $\varepsilon > 0$, il existe $\mathrm{N} = \mathrm{N}(\varepsilon)$ tel que $d_{\mathrm{Y}}(f(x), f_n(x)) < \varepsilon$, pour tous $n \geqslant \mathrm{N}$ et $x \in \mathrm{X}$.

La différence avec la convergence simple est que $\mathrm{N}(\varepsilon)$ est le même pour tout $x \in \mathrm{X}$; en particulier, la convergence uniforme implique la convergence simple.

• Si X est un espace topologique, si $f_n \to f$ uniformément sur X, et si f_n est continue en x_0, pour tout $n \in \mathbf{N}$, alors f est continue en x_0. Si les f_n sont continues sur X, il en est de même de f.

Soit $\varepsilon > 0$, et soit $n \in \mathbf{N}$ tel que $\sup_{x\in\mathrm{X}} d_{\mathrm{Y}}(f(x), f_n(x)) < \varepsilon$. Comme f_n est continue en x_0, il existe V ouvert de X contenant x_0 tel que $d_{\mathrm{Y}}(f_n(x), f_n(x_0)) < \varepsilon$, pour tout $x \in \mathrm{V}$. On a alors

$$d_{\mathrm{Y}}(f(x), f(x_0)) \leqslant d_{\mathrm{Y}}(f(x), f_n(x)) + d_{\mathrm{Y}}(f_n(x), f_n(x_0)) + d_{\mathrm{Y}}(f_n(x_0), f(x_0)) < 3\varepsilon,$$

pour tout $x \in \mathrm{V}$. On en déduit la continuité de f en x_0. Le second énoncé en étant une conséquence immédiate, cela permet de conclure.

Exercice 9.2. — Soient $u = (u_k)_{k\in\mathbf{N}}$ et $u^{(n)} = (u_k^{(n)})_{k\in\mathbf{N}}$, pour $n \in \mathbf{N}$, des suites à valeurs dans $\mathbf{C}$. On suppose que $u^{(n)} \to u$ uniformément sur $\mathbf{N}$ et que $\lim_{k\to+\infty} u_k^{(n)} = 0$, pour tout n. Montrer que $\lim_{k\to+\infty} u_k = 0$.

Si X est un ensemble et si Y est un espace métrique, une suite de fonctions $f_n : \mathrm{X} \to \mathrm{Y}$ vérifie le *critère de Cauchy uniforme* sur X si $\lim\limits_{n\to+\infty} \big(\sup\limits_{x\in\mathrm{X},\, p\in\mathbf{N}} d_{\mathrm{Y}}(f_n(x), f_{n+p}(x))\big) = 0$.

• Si X est un espace topologique, si Y est un espace métrique complet, et si $(f_n)_{n\in\mathbf{N}}$ est une suite de fonctions continues de X dans Y vérifiant le critère de Cauchy uniforme, alors $(f_n)_{n\in\mathbf{N}}$ a une limite simple f qui est continue, et f_n converge uniformément vers f sur X.

Si $x \in \mathrm{X}$, la suite $(f_n(x))_{n\in\mathbf{N}}$ est de Cauchy, et donc admet admet une limite $f(x)$, puisque Y est complet. Soit $\delta_n = \sup_{p\in\mathbf{N}} d_{\mathrm{Y}}(f_{n+p}(x), f_n(x))$; par hypothèse, on a $\delta_n \to 0$. Un passage à la limite montre que $d_{\mathrm{Y}}(f(x), f_n(x)) \leqslant \delta_n$, pour tout x, et comme $\delta_n \to 0$, cela prouve

que $f_n \to f$ uniformément sur X, ce qui permet de conclure puisqu'une limite uniforme de fonctions continues est continue.

Exercice 9.3. — Soit $(\mathrm{E}, \| \ \|)$ un espace vectoriel normé (sur $\mathbf{R}$ ou $\mathbf{C}$). On dit que $f : \mathrm{E} \to \mathbf{C}$ *tend vers* ℓ *à l'infini*, si pour tout $\varepsilon > 0$, il existe $\mathrm{M} > 0$ tel que $|f(x) - \ell| < \varepsilon$ pour tout x vérifiant $\|x\| > \mathrm{M}$. Soient f et f_n, pour $n \in \mathbf{N}$, des fonctions de E dans $\mathbf{C}$. On suppose que $f_n \to f$ uniformément sur E, et que f_n tend vers ℓ_n à l'infini. Montrer que $(\ell_n)_{n\in\mathbf{N}}$ a une limite $\ell \in \mathbf{C}$, et que f tend vers ℓ à l'infini.

10. Espaces vectoriels normés

10.1. Normes et applications linéaires continues

Si E est un espace vectoriel sur $\mathbf{K}$, avec $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$, une *norme* $\| \ \|$ sur E est une application $x \mapsto \|x\|$ de E dans $\mathbf{R}_+$ vérifiant les propriétés suivantes :

(i) $\|x\| = 0$ si et seulement si $x = 0$;

(ii) $\|\lambda x\| = |\lambda| \cdot \|x\|$, si $x \in \mathrm{E}$ et $\lambda \in \mathbf{K}$;

(iii) $\|x + y\| \leqslant \|x\| + \|y\|$, si $x, y \in \mathrm{E}$.

Si $\| \ \|$ est une norme sur E, alors $d : \mathrm{E} \times \mathrm{E} \to \mathbf{R}_+$ définie par $d(x, y) = \|x - y\|$ est une distance sur E, ce qui permet de voir un espace vectoriel normé $(\mathrm{E}, \| \ \|)$ comme un cas particulier d'espace métrique.

• Si $(\mathrm{E}, \| \ \|_{\mathrm{E}})$ et $(\mathrm{F}, \| \ \|_{\mathrm{F}})$ sont deux espaces vectoriels normés, et si $u : \mathrm{E} \to \mathrm{F}$ est une application *linéaire*, les conditions suivantes sont équivalentes :

(i) u est continue ;

(ii) u est uniformément continue ;

(iii) il existe $\mathrm{M} \in \mathbf{R}_+$ tel que $\|u(x)\|_{\mathrm{F}} \leqslant \mathrm{M} \cdot \|x\|_{\mathrm{E}}$, quel que soit $x \in \mathrm{E}$.

Si u est continue, l'image inverse de la boule unité ouverte de F contient un voisinage de 0 dans E, et donc une boule ouverte $\mathrm{B}(0, r^-)$, avec $r > 0$. Autrement dit, $\|x\|_{\mathrm{E}} < r$ implique $\|u(x)\|_{\mathrm{F}} < 1$, et donc, quel que soit $x \in \mathrm{E} - \{0\}$,

$$\|u(x)\|_{\mathrm{F}} = \frac{\|x\|_{\mathrm{E}}}{r} \cdot \| \frac{r}{\|x\|_{\mathrm{E}}} u(x)\|_{\mathrm{F}} \leqslant \frac{\|x\|_{\mathrm{E}}}{r}.$$

On en déduit l'implication (i)⇒(iii) (avec $\mathrm{M} = \frac{1}{r}$). Maintenant, si $\|u(x)\|_{\mathrm{F}} \leqslant \mathrm{M} \cdot \|x\|_{\mathrm{E}}$, quel que soit $x \in \mathrm{E}$, alors u est lipschitzienne de rapport M, et donc uniformément continue. On en déduit l'implication (iii)⇒(ii), et comme l'implication (ii)⇒(i) est une évidence, cela permet de conclure.

• Si $(\mathrm{E}, \| \ \|_{\mathrm{E}})$ et $(\mathrm{F}, \| \ \|_{\mathrm{F}})$ sont deux espaces vectoriels normés avec F complet, et si $u : \mathrm{E} \to \mathrm{F}$ est linéaire continue, alors u se prolonge, par continuité, en une application linéaire continue du complété $\widehat{\mathrm{E}}$ de E dans F.

C'est une conséquence de la propriété universelle vérifiée par $\widehat{\mathrm{E}}$.

10.2. La norme d'un opérateur

Si $(\mathrm{E}, \| \ \|_{\mathrm{E}})$ et $(\mathrm{F}, \| \ \|_{\mathrm{F}})$ sont deux espaces vectoriels normés, et si $u : \mathrm{E} \to \mathrm{F}$ est une application linéaire continue, la *norme d'opérateur* $\|u\|$ de u est la borne supérieure de l'ensemble des $\|x\|_{\mathrm{E}}^{-1}\|u(x)\|_{\mathrm{F}}$, pour $x \in \mathrm{E} - \{0\}$. On a donc $\|u(x)\|_{\mathrm{F}} \leqslant \|u\| \cdot \|x\|_{\mathrm{E}}$, quel que soit $x \in \mathrm{E}$, et $\|u\|$ est le plus petit réel ayant cette propriété.

• La norme d'opérateur est une norme sur l'espace vectoriel $\mathrm{Hom}(\mathrm{E}, \mathrm{F})$ des applications linéaires continues de E dans F.

Si $\|u\| = 0$, alors $u(x) = 0$, pour tout x, et donc $u = 0$. Si $u \in \mathrm{End}(\mathrm{E}, \mathrm{F})$ et $\lambda \in \mathbf{K}$, alors

$$\|\lambda\, u\| = \sup_{x \in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|\lambda u(x)\|_{\mathrm{F}} = \sup_{x \in \mathrm{E}-\{0\}} |\lambda| \cdot \|x\|_{\mathrm{E}}^{-1}\|u(x)\|_{\mathrm{F}} = |\lambda| \sup_{x \in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|u(x)\|_{\mathrm{F}} = |\lambda| \cdot \|u\|.$$

Si $u, v \in \mathrm{End}(\mathrm{E}, \mathrm{F})$, alors

$$\begin{aligned}\|u + v\| = \sup_{x \in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|u(x)+v(x)\|_{\mathrm{F}} &\leqslant \sup_{x \in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}(\|u(x)\|_{\mathrm{F}} + \|v(x)\|_{\mathrm{F}}) \\ &\leqslant \big(\sup_{x \in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|u(x)\|_{\mathrm{F}}\big) + \big(\sup_{x \in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|v(x)\|_{\mathrm{F}}\big) = \|u\| + \|v\|.\end{aligned}$$

Ceci permet de conclure.

• La norme d'opérateur est une norme d'algèbre sur l'anneau $\mathrm{End}(\mathrm{E})$ des endomorphismes linéaires continus de E.

Compte-tenu du point précédent, il ne reste plus que l'inégalité $\|u \circ v\| \leqslant \|u\| \cdot \|v\|$ à vérifier. Or $\|u \circ v(x)\|_{\mathrm{E}} \leqslant \|u\| \cdot \|v(x)\|_{\mathrm{E}} \leqslant \|u\| \cdot \|v\| \cdot \|x\|_{\mathrm{E}}$, pour tout $x \in \mathrm{E}$, par définition de $\|u\|$ et $\|v\|$. On en déduit l'inégalité cherchée.

10.3. Normes équivalentes

Deux normes $\| \ \|_1$ et $\| \ \|_2$ sur E sont *équivalentes*, si l'application identité de $(\mathrm{E}, \| \ \|_1)$ dans $(\mathrm{E}, \| \ \|_2)$ est un homéomorphisme (i.e. est continue ainsi que son inverse). D'après l'alinéa précédent, cela équivaut à l'existence de $\mathrm{C} > 0$ tel que $\mathrm{C}^{-1}\|x\|_1 \leqslant \|x\|_2 \leqslant \mathrm{C}\|x\|_1$, quel que soit $x \in \mathrm{E}$.

• Soit E un espace vectoriel de dimension finie sur $\mathbf{K}$. Alors toutes les normes sur E sont équivalentes et E est complet pour n'importe laquelle d'entre elles.

Soit $(e_1, \ldots, e_n)$ une base de E sur $\mathbf{K}$. Comme $\mathbf{K}$ est complet, il suffit de prouver que toute norme sur E est équivalente à la norme $\| \ \|_\infty$ définie par

$$\|x_1e_1 + \cdots + x_ne_n\|_\infty = \sup(|x_1|, \ldots, |x_n|),$$

ce qui se fait par récurrence sur la dimension de E. Si cette dimension est 1, il n'y a rien à faire. Sinon, soit $\| \ \|$ une norme sur E. On déduit de l'inégalité triangulaire que

$$\|x_1e_1 + \cdots + x_ne_n\| \leqslant (\|e_1\| + \cdots + \|e_n\|)\sup(|x_1|, \ldots, |x_n|),$$

d'où l'une des deux inégalités à vérifier. Pour démontrer l'autre, raisonnons par l'absurde. Supposons qu'il existe une suite $x_1^{(k)}e_1 + \cdots + x_n^{(k)}e_n$ qui tende vers 0 pour la norme $\| \ \|$ mais pas pour la norme $\| \ \|_\infty$. Il existe alors $\mathrm{C} > 0$, $i \in \{1, \ldots, n\}$ et une sous-suite infinie telle que l'on ait $|x_i^{(k)}| \geqslant \mathrm{C}$, et donc la suite de terme général $v_k = \frac{x_1^{(k)}}{x_i^{(k)}}e_1 + \cdots + \frac{x_n^{(k)}}{x_i^{(k)}}e_n$ tend encore vers 0 pour $\| \ \|$. On en déduit que e_i est dans l'adhérence de $\mathrm{W} = \mathrm{Vect}(e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n)$, qui

est complet d'après l'hypothèse de récurrence, ce qui implique $e_i \in W$ et est absurde puisque les e_i forment une base de E.

• L'énoncé précédent devient *totalement faux en dimension infinie* : les normes sur un espace E de dimension infinie ne sont pas toutes équivalentes[39], et E peut être complet pour certaines d'entre elles, mais il y en a "beaucoup plus" pour lesquelles ce n'est pas le cas.

Exercice 10.1. — Soit $E = \mathscr{C}([0,1])$ l'espace des fonctions continues de $[0,1]$ dans $\mathbf{C}$.

(i) Montrer que, si $\phi \in E$, alors $\|\phi\|_\infty = \sup_{x\in[0,1]} |\phi(x)|$ est fini et que $\| \ \|_\infty$ est une norme sur E pour laquelle E est complet.

(ii) Montrer que $\| \ \|_1$ définie par $\|\phi\|_1 = \int_0^1 |\phi(t)|\, dt$ est une norme sur E pour laquelle E n'est pas complet.

(iii) Les normes $\| \ \|_\infty$ et $\| \ \|_1$ sont-elles équivalentes ?

Exercice 10.2. — (i) Montrer que, si $\mathscr{T}_1$ et $\mathscr{T}_2$ sont des topologies sur X, alors $\mathscr{T}_1$ est plus fine que $\mathscr{T}_2$ si et seulement si $\mathrm{id} : (X, \mathscr{T}_1) \to (X, \mathscr{T}_2)$ est continue.

(ii) Soit $\mathscr{T}_1$ la topologie sur l'espace $\mathscr{C}_c(\mathbf{R})$ des fonctions continues à support compact définie par la norme $\| \ \|_1$ et $\mathscr{T}_\infty$ celle définie par la norme $\| \ \|_\infty$. Montrer qu'aucune des deux topologies $\mathscr{T}_1$ et $\mathscr{T}_\infty$ n'est plus fine que l'autre.

10.4. La boule unité d'un espace vectoriel normé

• Si E est de dimension finie, la boule unité fermée est compacte.

Par définition, la boule unité fermée est bornée, et comme elle est fermée, et que l'on est en dimension finie, elle est compacte.

• Soit E un espace vectoriel normé. Si la boule unité fermée $B(0,1)$ est compacte, alors E est de dimension finie (théorème de Riesz, 1918).

Si $B(0,1)$ est compacte, on peut extraire un recouvrement fini du recouvrement de $B(0,1)$ par les $B(x, (\frac{1}{2})^-)$, pour $x \in B(0,1)$. Autrement dit, on peut trouver un sous-ensemble fini $\{e_i,\ i \in I\}$ d'éléments de E tels que $B(0,1) \subset \cup_{i\in I} B(e_i, \frac{1}{2})$. Nous allons montrer que le sous-espace E′ engendré par les $(e_i)_{i\in I}$ est égal à E, ce qui permettra de conclure. Comme E′ est fermé, puisque complet, car de dimension finie (n° 10.3), il suffit de montrer que E′ est dense dans E. Soit donc $x \in E$, et soient $a \in \mathbf{Z}$ et $y \in E'$ tels que $\|x - y\| \leqslant 2^{-a}$ (un tel couple existe : il suffit de prendre $y = 0$ et a assez petit pour que $\|x\| \leqslant 2^{-a}$). On a $2^a(x-y) \in B(0,1)$ et, par définition de la famille $(e_i)_{i\in I}$, il existe $i \in I$ tel que $\|2^a(x-y) - e_i\| \leqslant \frac{1}{2}$. Mais alors $y' = y + 2^{-a}e_i \in E'$ et $\|x - y'\| \leqslant 2^{-a-1}$. Ceci permet de construire, par récurrence, une suite $(y_n)_{n\in\mathbf{N}}$ d'éléments de E′ vérifiant $\|x - y_n\| \leqslant 2^{-n-a}$, ce qui prouve que x est dans l'adhérence de E′, et permet de conclure.

[39] Un des problèmes de base en analyse fonctionnelle est précisément de choisir la bonne norme en fonction du problème à résoudre.

10.5. Applications bilinéaires continues

Si $(\mathrm{E}_1, \| \ \|_1)$ et $(\mathrm{E}_2, \| \ \|_2)$ sont deux espaces vectoriels normés, l'espace topologique $\mathrm{E}_1 \times \mathrm{E}_2$ est aussi un espace vectoriel normé, la topologie produit étant celle associée à la norme $\|(x_1, x_2)\| = \sup(\|x_1\|_1, \|x_2\|_2)$ ou à toute autre norme équivalente comme par exemple $\|(x_1, x_2)\| = (\|x_1\|_1^2 + \|x_2\|_2^2)^{1/2}$.

• Soient $(\mathrm{E}_1, \| \ \|_1)$, $(\mathrm{E}_2, \| \ \|_2)$ et $(\mathrm{F}, \| \ \|_\mathrm{F})$ des espaces vectoriels normés, et $b : \mathrm{E}_1 \times \mathrm{E}_2 \to \mathrm{F}$ une application *bilinéaire*. Alors :

(i) b est continue si et seulement si il existe $\mathrm{C} > 0$ tel que $\|b(x_1, x_2)\|_\mathrm{F} \leqslant \mathrm{C} \cdot \|x_1\|_1 \cdot \|x_2\|_2$ quels que soient $x_1 \in \mathrm{E}_1$ et $x_2 \in \mathrm{E}_2$;

(ii) si F est complet et b continue, alors b s'étend par continuité en une application bilinéaire du complété $\widehat{\mathrm{E}}_1 \times \widehat{\mathrm{E}}_2$ de $\mathrm{E}_1 \times \mathrm{E}_2$ dans F.

Si b est continue, il existe $r_1, r_2 > 0$ tels que $b^{-1}(\mathrm{B}_\mathrm{F}(0, 1^-))$ contienne $\mathrm{B}_{\mathrm{E}_1}(0, r_1^-) \times \mathrm{B}_{\mathrm{E}_2}(0, r_2^-)$. Autrement dit, $\|b(x_1, x_2)\|_\mathrm{F} < 1$ si $\|x_1\|_1 < r_1$ et $\|x_2\|_2 < r_2$. Par bilinéarité, cela implique que

$$\|b(x_1, x_2)\|_\mathrm{F} = \frac{\|x_1\|_1 \cdot \|x_2\|_2}{r_1 r_2} \Big\| b\Big(\frac{r_1}{\|x_1\|_1} x_1, \frac{r_2}{\|x_2\|_2} x_2\Big) \Big\|_\mathrm{F} \leqslant \frac{\|x_1\|_1 \cdot \|x_2\|_2}{r_1 r_2}.$$

Réciproquement, s'il existe $\mathrm{C} > 0$ tel que $\|b(x_1, x_2)\|_\mathrm{F} \leqslant \mathrm{C} \cdot \|x_1\|_1 \cdot \|x_2\|_2$, quels que soient $x_1 \in \mathrm{E}_1$ et $x_2 \in \mathrm{E}_2$, alors

$$\|b(x_1 + h_1, x_2 + h_2) - b(x_1, x_2)\|_\mathrm{F} \leqslant \mathrm{C}(\|x_1\|_1 \cdot \|h_2\|_2 + \|h_1\|_1 \cdot \|x_2\|_2 + \|h_1\|_1 \cdot \|h_2\|_2),$$

ce qui prouve que b est lipschitzienne de rapport $\mathrm{C} \cdot (\|x_1\|_1 + \|x_2\|_2 + 1)$ sur $\mathrm{B}_{\mathrm{E}_1}(x_1, 1^-) \times \mathrm{B}_{\mathrm{E}_2}(x_2, 1^-)$. Ceci prouve que b est continue (et donc termine la démonstration du (i)), et permet de déduire le (ii) du deuxième point du n° 8.3.

10.6. Espaces préhilbertiens

Soit E un espace vectoriel sur $\mathbf{K}$.

• Un *produit scalaire* $(x, y) \mapsto \langle x, y\rangle$ sur E est une application de $\mathrm{E} \times \mathrm{E}$ dans $\mathbf{K}$ qui est :

– *sesquilinéaire*, i.e. linéaire par rapport à y (i.e. $\langle x, y_1 + y_2\rangle = \langle x, y_1\rangle + \langle x, y_2\rangle$ et $\langle x, \lambda y\rangle = \lambda\langle x, y\rangle$, si $\lambda \in \mathbf{K}$, $x, y, y_1, y_2 \in \mathrm{E}$), et semi-linéaire[(40)] par rapport à x (i.e. $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$ et $\langle \lambda x, y\rangle = \overline{\lambda}\langle x, y\rangle$, si $\lambda \in \mathbf{K}$, $x, y, x_1, x_2 \in \mathrm{E}$) ;

– *symétrique*, i.e. $\langle y, x\rangle = \overline{\langle x, y\rangle}$, quels que soient $x, y \in \mathrm{E}$;

– *définie positive*, i.e $\langle x, x\rangle \geqslant 0$, si $x \in \mathrm{E}$, et $\langle x, x\rangle = 0$, si et seulement si $x = 0$.

• Un *espace préhilbertien* est un espace vectoriel muni d'un produit scalaire. Si E est préhilbertien, on définit $\| \ \| : \mathrm{E} \to \mathbf{R}$ en posant $\|x\| = \langle x, x\rangle^{1/2}$. Alors $\| \ \|$ est une norme, et on a $|\langle x, y\rangle| \leqslant \|x\| \cdot \|y\|$ pour tous $x, y \in \mathrm{E}$ (*inégalite de Cauchy-Schwarz*) : l'application $\mathbf{R}$-bilinéaire $(x, y) \mapsto \langle x, y\rangle$, de $\mathrm{E} \times \mathrm{E}$ dans $\mathbf{K}$, est continue.

$\|x + ty\|^2 = \|x\|^2 + 2t\,\mathrm{Re}(\langle x, y\rangle) + t^2\|y\|^2$ est toujours $\geqslant 0$, pour $t \in \mathbf{R}$; son discriminant est donc $\leqslant 0$, ce qui se traduit par $|\mathrm{Re}(\langle x, y\rangle)| \leqslant \|x\| \cdot \|y\|$ pour tous $x, y \in \mathrm{E}$. Choisissons alors $\theta \in \mathbf{R}$ tel que $e^{-i\theta}\langle x, y\rangle \in \mathbf{R}_+$. En utilisant la majoration précédente pour $e^{i\theta}x$ et y au lieu de

(40) Si $\mathbf{K} = \mathbf{R}$, on a $\overline{x} = x$, et donc la sesquilinérarité n'est autre que la bilinéarité.

x et y, on obtient $|\langle x,y\rangle| = \mathrm{Re}(\langle e^{i\theta}x,y\rangle) \leqslant \|e^{i\theta}x\|\cdot\|y\| = \|x\|\cdot\|y\|$, ce qui prouve l'inégalité de Cauchy-Schwarz. L'inégalité triangulaire s'en déduit car

$$\|x+y\|^2 = \|x\|^2 + 2\mathrm{Re}(\langle x,y\rangle) + \|y\|^2 \leqslant \|x\|^2 + 2\|x\|\cdot\|y\| + \|y\|^2 = (\|x\|+\|y\|)^2.$$

L'identité $\|\lambda\, x\| = |\lambda|\,\|x\|$ étant immédiate, $\|\ \|$ est une norme, ce qui permet de conclure.

• On dit que $x, y \in \mathrm{E}$ sont *orthogonaux* si $\langle x,y\rangle = 0$. Si x et y sont orthogonaux, ils vérifient la *relation de Pythagore*[41] $\|x+y\|^2 = \|x\|^2 + \|y\|^2$. Dans le cas général, ils vérifient *l'identité de la médiane* $\|x\|^2 + \|y\|^2 = 2\big\|\frac{x+y}{2}\big\|^2 + \frac{1}{2}\|x-y\|^2$, qui se démontre sans problème en développant le membre de droite.

• Si F est un sous-espace vectoriel de E, et si $x \in \mathrm{E}$, il existe au plus un élément $p_{\mathrm{F}}(x)$ de F, appelé (s'il existe) *projection orthogonale de x sur* F, tel que $x - p_{\mathrm{F}}(x)$ soit orthogonal à F tout entier. De plus, on a $p_{\mathrm{F}}(x) = x$, si $x \in \mathrm{F}$, et p_{F} est linéaire et 1-lipschitzien sur son ensemble de définition.

Si $y_1, y_2 \in \mathrm{F}$ sont tels que $x-y_1$ et $x-y_2$ sont orthogonaux à F tout entier, alors $y_1 - y_2 = (x-y_1)-(x-y_2)$ est orthogonal à F, et comme $y_1 - y_2 \in \mathrm{F}$, on a $\langle y_1-y_2, y_1-y_2\rangle = 0$, ce qui implique $y_1 = y_2$. On en déduit l'unicité de p_{F}. La linéarité de p_{F} et la formule $p_{\mathrm{F}}(x) = x$, si $x \in \mathrm{F}$, en sont des conséquences immédiates. Enfin, $x - p_{\mathrm{F}}(x)$ et $p_{\mathrm{F}}(x)$ étant orthogonaux, on a $\|p_{\mathrm{F}}(x)\|^2 = \|x\|^2 - \|x - p_{\mathrm{F}}(x)\|^2$, et donc $\|p_{\mathrm{F}}(x)\| \leqslant \|x\|$. Ceci permet de conclure.

• Une famille $(e_i)_{i\in\mathrm{I}}$ d'éléments de E est dite *orthonormale*, si $\|e_i\| = 1$ pour tout i, et si e_i et e_j sont orthogonaux si $i \neq j$. On a alors $\|\sum_{i\in\mathrm{J}} x_i e_i\|^2 = \sum_{i\in\mathrm{J}} |x_i|^2$, pour toute famille *finie* $(x_i)_{i\in\mathrm{J}}$ de nombres complexes.

• Si F est un sous-espace de dimension finie de E muni d'une base orthonormale $(e_1,\dots,e_d)$, alors p_{F} est partout définie, et $p_{\mathrm{F}}(x) = \sum_{i=1}^{d}\langle e_i,x\rangle\, e_i$. En particulier, si $x \in \mathrm{F}$, ses coordonnées dans la base $(e_1,\dots,e_d)$ sont les $\langle e_i,x\rangle$, et $\|x\|^2 = \sum_{i=1}^{d}|\langle e_i,x\rangle|^2$.

Soit $y = \sum_{i=1}^{d}\langle e_i,x\rangle\, e_i$. Alors $\langle e_j, x-y\rangle = \langle e_j,x\rangle - \sum_{i=1}^{d}\langle e_i,x\rangle\langle e_j,e_i\rangle = 0$, pour tout j. On en déduit que $x-y$ est orthogonal à chacun des e_j, et donc à F tout entier par linéarité. De plus, $y \in \mathrm{F}$ par construction, et donc $y = p_{\mathrm{F}}(x)$. On en déduit le résultat.

• Le *procédé d'orthonormalisation de Schmidt*, décrit ci-dessous, permet, si $(f_i)_{i\in\mathrm{I}}$ est une famille libre d'éléments de E, avec I dénombrable, de fabriquer une base orthonormale de l'espace F engendré par les f_i.

On se ramène, en numérotant les éléments de I, au cas où I est un intervalle de $\mathbf{N}$ contenant 0. On note F_n le sous-espace de F engendré par les f_i, pour $i \leqslant n$. On construit par récurrence une famille orthonormale e_i d'éléments de F telle que $(e_0,\dots,e_n)$ soit une base (orthonormale) de F_n, pour tout n. Pour cela, on pose $e_0 = \frac{1}{\|f_0\|}f_0$, et en supposant $e_0,\dots,e_{n-1}$ construits (et donc F_{n-1} muni d'une base orthonormale), on note $g_n = f_n - p_{\mathrm{F}_{n-1}}(f_n)$. On a $g_n \neq 0$ puisque $f_n \notin \mathrm{F}_{n-1}$, la famille des f_j étant supposée libre. On pose $e_n = \frac{1}{\|g_n\|}g_n$. Par construction, g_n (et donc aussi e_n) est orthogonal à chacun des e_i, pour $i \leqslant n-1$, et comme $\|e_n\| = 1$, cela permet de faire marcher la récurrence.

[41] Si $\mathbf{K} = \mathbf{R}$, la relation de Pythagore entraîne l'orthogonalité (« théorème » de Pythagore, pauvre Pythagore...) ; ce n'est plus le cas si $\mathbf{K} = \mathbf{C}$.

• Tout sous-espace de dimension finie de E possède une base orthonormale.

Il suffit d'appliquer le procédé d'orthonormalisation de Schmidt à une base quelconque.

11. Tératologie

Ce § rassemble un certain nombre de monstres mathématiques.

11.1. Fonctions continues dérivables nulle part

Jusqu'au début du XIX$^{\text{e}}$ siècle (au moins), il était évident pour tout le monde qu'une fonction continue de $\mathbf{R}$ dans $\mathbf{R}$ était dérivable, et même somme de sa série de Taylor, sauf en des points isolés. C'est malheureusement loin d'être le cas puisque Weierstrass (1875) a construit une fonction continue dérivable nulle part, et Banach a montré que l'ensemble de ces fonctions était dense dans celui des fonctions continues.

Soit $\mathrm{E} = \mathscr{C}^0([0,1], \| \ \|_\infty)$. Nous allons construire un sous-ensemble X, dense dans E, constitué de fonctions dérivables nulle part. Pour ce faire, fixons $a \in]\frac{1}{2}, 1[$. Si $n \in \mathbf{N}$, et si $k \in \{0, 1, \dots, 2^n - 1\}$, soit

$$\mathrm{U}_{n,k} = \big\{\phi \in \mathrm{E},\ \big|\phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)\big| > a^n\big\}.$$

• $\mathrm{U}_{n,k}$ est un ouvert de E : en effet $\phi \mapsto \big|\phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)\big|$ est continue sur E comme composée de l'application linéaire continue $\phi \mapsto \Lambda_{n,k}(\phi) = \phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)$ (la continuité de $\Lambda_{n,k}$ suit de la majoration $|\Lambda_{n,k}(\phi)| \leqslant 2\|\phi\|_\infty$), et de la valeur absolue.

On en déduit que $\mathrm{U}_n = \cap_{k=0}^{2^n-1} \mathrm{U}_{n,k}$ et $\mathrm{V}_n = \cup_{m \geqslant n} \mathrm{U}_m$ sont des ouverts de E.

• V_n est dense dans E. En effet, soient $\phi \in \mathrm{E}$ et $\varepsilon > 0$. Comme $[0,1]$ est compact, ϕ est uniformément continue, et il existe $n_0 \in \mathbf{N}$ tel que $|\phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)| \leqslant \varepsilon$, quels que soient $n \geqslant n_0$ et $k \in \{0, 1, \dots, 2^n - 1\}$. Soit $m \geqslant \sup(n_0, n)$ tel que $a^m < \varepsilon$, et soit $\psi \in \mathrm{E}$ définie par $\psi(x) = \phi(x) + \varepsilon \sin(2^m \pi x)$. Si $k \in \{0, 1, \dots, 2^m - 1\}$, on a $\|\psi - \phi\|_\infty \leqslant \varepsilon$ et

$$\big|\psi\big(\frac{k+1}{2^m}\big) - \psi\big(\frac{k}{2^m}\big)\big| = \big| \pm 2\varepsilon + \phi\big(\frac{k+1}{2^m}\big) - \phi\big(\frac{k}{2^m}\big)\big| \geqslant 2\varepsilon - \varepsilon > a^m,$$

ce qui prouve que $\psi \in \mathrm{U}_m \subset \mathrm{V}_n$. On en déduit que, pour tout $\phi \in \mathrm{E}$, on peut trouver un élément de V_n dans tout voisinage de ϕ, et donc que V_n est effectivement dense dans E.

Comme E est complet, il résulte du lemme de Baire que $\mathrm{X} = \cap_{n \in \mathbf{N}} \mathrm{V}_n$ est dense dans E, et pour conclure, il suffit donc de prouver que, si $\phi \in \mathrm{X}$, et si $x_0 \in [0,1]$, alors ϕ n'est pas dérivable en x_0. Pour cela, remarquons que $\phi \in \mathrm{X}$ signifie que ϕ appartient à une infinité de U_n, et donc qu'il existe $b : \mathbf{N} \to \mathbf{N}$, tendant vers $+\infty$ en $+\infty$, telle que $|\phi\big(\frac{k+1}{2^{b(n)}}\big) - \phi\big(\frac{k}{2^{b(n)}}\big)| > a^{b(n)}$, pour tout $n \in \mathbf{N}$ et tout $k \in \{0, 1, \dots, 2^{b(n)} - 1\}$. Soient k_n la partie entière de $2^{b(n)} x_0$, et $u_n = \frac{k_n}{2^{b(n)}}$, $v_n = \frac{k_n+1}{2^{b(n)}}$ (si $x_0 = 1$, on pose $u_n = 1 - \frac{1}{2^{b(n)}}$ et $v_n = 1$). Par construction, $u_n \leqslant x_0 \leqslant v_n$ et $v_n - u_n = \frac{1}{2^{b(n)}}$; en particulier, $u_n \to x_0$ et $v_n \to x_0$. Par ailleurs, pour tout $n \in \mathbf{N}$, on a $\big|\frac{\phi(v_n) - \phi(u_n)}{v_n - u_n}\big| > (2a)^{b(n)}$, et comme $2a > 1$, cela montre que $\big|\frac{\phi(v_n) - \phi(u_n)}{v_n - u_n}\big|$ tend vers $+\infty$, et donc que ϕ n'est pas dérivable en x_0 (si elle l'était, on aurait $\frac{\phi(v_n) - \phi(u_n)}{v_n - u_n} \to \phi'(x_0)$). Ceci permet de conclure.

Exercice 11.1. — Adapter la dernière partie de l'argument pour montrer que $\sum_{n \geqslant 1} \frac{\sin(10^n \pi x)}{2^n}$ est continue sur $\mathbf{R}$, mais n'est dérivable nulle part.

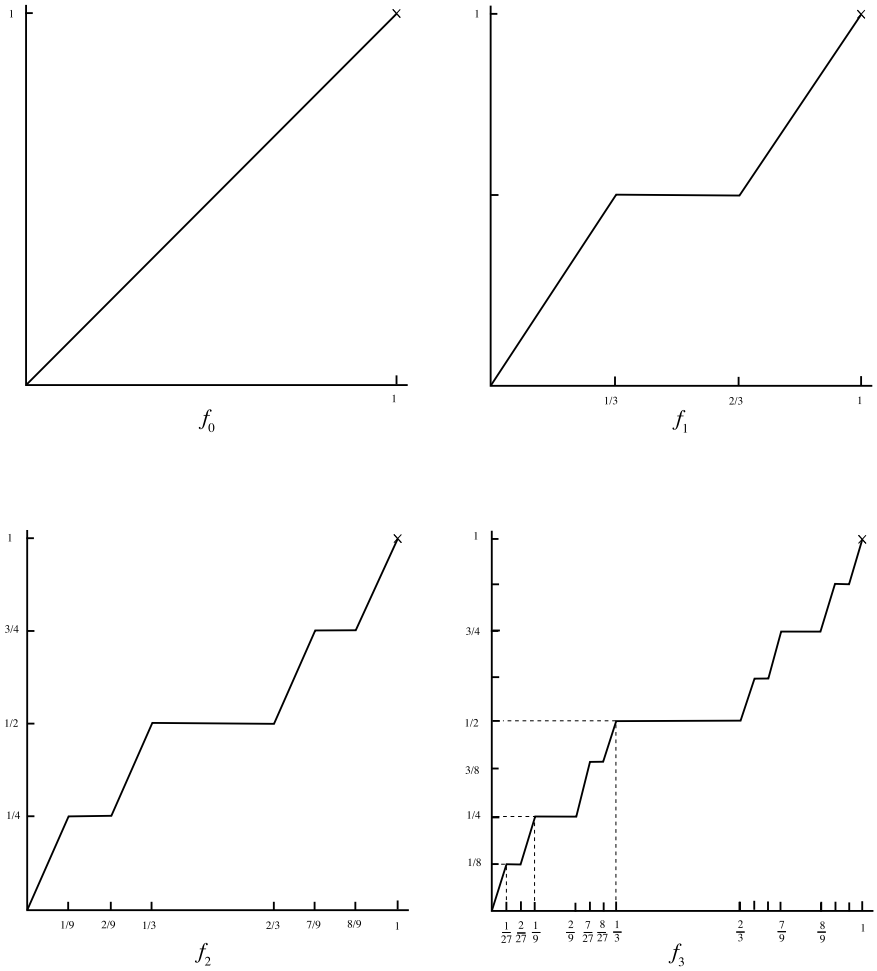

FIG. 1. Graphes de f_0, f_1, f_2 et f_3.

11.2. L'escalier du diable

Il s'agit d'une fonction $f : [0,1] \to \mathbf{R}$, continue, croissante, valant 0 en 0 et 1 en 1, mais qui croît subrepticement : il existe une famille de segments ouverts $]a_n, b_n[$ disjoints, pour $n \in \mathbf{N}$, tels que f soit constante sur chacun des segments $]a_n, b_n[$, et tels que la somme totale $\sum_{n\in\mathbf{N}}(b_n - a_n)$ des longueurs des segments soit égale à 1. La fonction f représente un contrexemple assez frappant à une extension naturelle du théorème fondamental de l'analyse ($\int_a^b f'(t)\,dt = f(b) - f(a)$).

On construit f, par un procédé fractal, comme la limite de $f_n : [0,1] \to [0,1]$, continues, croissantes, affines sur chaque intervalle $\mathrm{I}_{n,i} = [\frac{i}{3^n}, \frac{i+1}{3^n}]$, pour $0 \leqslant i \leqslant 3^n - 1$, construites par récurrence à partir de $f_0(x) = x$ en utilisant la recette suivante : l'image de $\mathrm{I}_{n,i}$ par f_{n+1} est la même que par f_n, mais le graphe de f_{n+1} sur cet intervalle est obtenu en coupant en trois le segment constituant le graphe de f_n, et en introduisant un palier horizontal au milieu.

De manière plus précise, si on note $a_{n,i}$ et $b_{n,i}$ les valeurs de f_n en $\frac{i}{3^n}$ et $\frac{i+1}{3^n}$, alors les fonctions f_n et f_{n+1} sont données par les formules suivantes sur $\mathrm{I}_{n,i}$:

$$f_n(x) = a_{n,i} + (b_{n,i} - a_{n,i})(3^n x - i)$$

$$f_{n+1}(x) = \begin{cases} a_{n,i} + \frac{3}{2}(b_{n,i} - a_{n,i})(3^n x - i) & \text{si } x \in \mathrm{I}_{n+1,3i}, \\ \frac{b_{n,i}+a_{n,i}}{2} & \text{si } x \in \mathrm{I}_{n+1,3i+1}, \\ b_{n,i} + \frac{3}{2}(b_{n,i} - a_{n,i})(3^n x - i - 1) & \text{si } x \in \mathrm{I}_{n+1,3i+2}. \end{cases}$$

En particulier, si f_n est constante sur $\mathrm{I}_{n,i}$, alors $f_{n+1} = f_n$ sur $\mathrm{I}_{n,i}$, et dans le cas général, on a

$$b_{n+1,i} - a_{n+1,i} = \begin{cases} \frac{b_{n,i}-a_{n,i}}{2} & \text{si le chiffre des unités dans l'écriture de } i \text{ en base 3 est 0 ou 2,} \\ 0 & \text{si le chiffre des unités dans l'écriture de } i \text{ en base 3 est un 1.} \end{cases}$$

$$|f_{n+1}(x) - f_n(x)| \leqslant \frac{b_{n,i} - a_{n,i}}{6}, \quad \text{si } x \in \mathrm{I}_{n,i}.$$

Une récurrence immédiate permet d'en déduire que $\|f_{n+1} - f_n\|_\infty \leqslant \frac{1}{6\cdot 2^n}$, et

$$b_{n,i} - a_{n,i} = \begin{cases} \frac{1}{2^n} & \text{si tous les chiffres de l'écriture de } i \text{ en base 3 sont des 0 ou des 2,} \\ 0 & \text{si un des chiffres de l'écriture de } i \text{ en base 3 est un 1.} \end{cases}$$

Comme $\sum_{n\in\mathbf{N}} \frac{1}{6\cdot 2^n} < +\infty$, la série $f_0 + \sum_{n=0}^{+\infty}(f_{n+1} - f_n)$ converge normalement, et sa somme f, qui est aussi la limite de la suite $(f_n)_{n\in\mathbf{N}}$, est continue. Chaque f_n étant croissante, il en est de même de la limite f. Finalement, f est constante sur $\mathrm{I}_{n,i}$, si un des chiffres de i dans le développement en base 3 est un 1. Il y a $3^n - 2^n$ tels i, ce qui fait que la réunion F_n des $\mathrm{I}_{n,i}$, pour i vérifiant la condition précédente, est de longueur totale égale à $1 - \frac{2^n}{3^n}$. Comme f est constante sur (chacun des intervalles composant) F_n, un passage à la limite montre que f est constante sur la réunion des F_n qui est de longueur totale égale à 1. D'un autre côté, on a $f_n(0) = 0$ et $f_n(1) = 1$, pour tout n, et donc $f(0) = 0$ et $f(1) = 1$ par passage à la limite. On a donc bien construit une fonction continue qui croît subrepticement de 0 à 1.

11.3. L'ensemble triadique de Cantor

C'est un fermé K de $\mathbf{R}$ inclus dans $[0,1]$, de mesure nulle, mais quand même assez gros pour qu'il existe une surjection de K sur $[0,1]$. C'est l'ensemble des points de $[0,1]$ en lesquels l'escalier du diable croît.

On construit par récurrence une suite $(\mathrm{K}_n)_{n\in\mathbf{N}}$ de fermés de $[0,1]$, chaque K_n étant la réunion de 2^n segments fermés. On part de $\mathrm{K}_0 = [0,1]$, et si K_n est construit, on obtient K_{n+1} en coupant chacun des segments fermés constituant K_n en 3 segments de même longueur et en enlevant le morceau du milieu (ouvert pour que K_{n+1} soit fermé). On a donc

$$\mathrm{K}_1 = \big[0,1\big] - \big]\frac{1}{3},\frac{2}{3}\big[= \big[0,\frac{1}{3}\big] \cup \big[\frac{2}{3},1\big], \quad \mathrm{K}_2 = \mathrm{K}_1 - \Big(\big]\frac{1}{9},\frac{2}{9}\big[\cup \big]\frac{7}{9},\frac{8}{9}\big[\Big) = \big[0,\frac{1}{9}\big] \cup \big[\frac{2}{9},\frac{3}{9}\big] \cup \big[\frac{6}{9},\frac{7}{9}\big] \cup \big[\frac{8}{9},1\big].$$

On note K l'intersection des K_n ; c'est un fermé de $[0,1]$ comme intersection de fermés. La somme des longueurs des segments constituant K_n est $(\frac{2}{3})^n$ qui tend vers 0 quand $n \to +\infty$, ce qui fait que K est de mesure nulle, puisque $\mathrm{K} \subset \mathrm{K}_n$ pour tout n.

Par ailleurs, K est l'ensemble des $x \in [0,1]$ dont un des développements en base 3 ne comporte que des 0 et des 2 (les seuls nombres ayant deux développements sont ceux de la forme $\frac{k}{3^n}$, avec $k \in \mathbf{Z}$ et $n \in \mathbf{N}$). En effet, les nombres que l'on retire pour passer de K_n à K_{n+1} sont précisément ceux dont tous les développements en base 3 ont un 1 en n-ième position et pas de 1 avant. L'application $(a_n)_{n\geqslant 1} \mapsto \sum_{n=1}^{+\infty} \frac{a_n}{3^n}$ induit donc une bijection de l'ensemble $\{0,2\}^{\mathbf{N}-\{0\}}$ sur K, ce qui nous permet de définir une surjection $f : \mathrm{K} \to [0,1]$, en passant de la base 3 à la base 2, c'est-à-dire en envoyant $\sum_{n=1}^{+\infty} \frac{a_n}{3^n}$ sur $\sum_{n=1}^{+\infty} \frac{b_n}{2^n}$, où $b_n = a_n/2 \in \{0,1\}$.

Exercice 11.2. — (i) Adapter la construction ci-dessus pour construire un fermé de $[0,1]$ d'intérieur vide, mais de mesure non nulle.

(ii) Montrer qu'un tel ensemble est totalement discontinu.

11.4. La courbe de Peano

Il s'agit d'une courbe fractale qui remplit tout le carré, ce qui montre que la notion de dimension est plus problématique que ce qu'on pourrait croire (un probabiliste dirait que pour obtenir une courbe ayant (presque) cette propriété, il suffit de lancer un mouvement brownien qui se chargera de remplir (presque) le plan tout seul).

On construit la courbe de Peano $f : [0,1] \to [0,1]^2$ comme une limite de fonctions f_n, affines par morceaux, construites par récurrence. La fonction f_0 est juste $t \mapsto (t,t)$; son image est donc la diagonale du carré $[0,1]^2$. La fonction f_n est une fonction affine sur chaque intervalle de la forme $\mathrm{I}_{n,i} = [\frac{i}{9^n}, \frac{i+1}{9^n}]$, et le passage de f_{n+1} à f_n se fait en remplaçant chacun des 9^n segments qui constituent l'image de f_n par 9 segments par le procédés indiqués à la figure 2. La figure 3 montre ce que cela donne pour f_2 (les fonctions f_0 et f_1 sont représentées sur la figure 2).

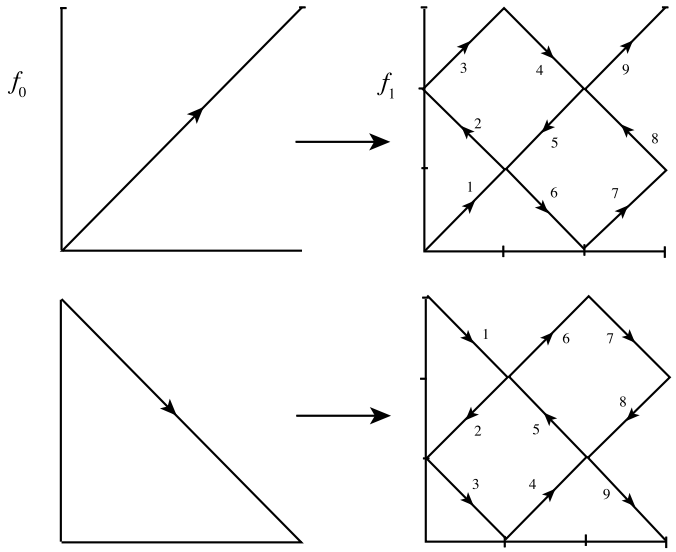

FIG. 2. Procédé d'obtention de f_{n+1} à partir de f_n ; pour un segment allant dans l'autre sens, on renverse juste le sens de parcours.

Par construction, les fonctions f_{n+1} et f_n ont une image incluse dans le même sous-carré de côté de longueur $\frac{1}{3^n}$, sur chacun des segments $\mathrm{I}_{n,i}$, pour $0 \leqslant i \leqslant 9^n - 1$. On a donc $\|f_{n+1} - f_n\|_\infty \leqslant \frac{1}{3^n}$, si on munit $\mathbf{R}^2$ de la norme $\|(x,y)\| = \sup(|x|,|y|)$. On en déduit que f_n converge uniformément sur $[0,1]$, et comme les f_n sont continues, il en est de même de la limite f.

On a $f_{n+1}\big(\frac{i}{9^n}\big) = f_n\big(\frac{i}{9^n}\big)$, si $0 \leqslant i \leqslant 9^n$, et donc $f(\frac{i}{9^n}) = f_n\big(\frac{i}{9^n}\big)$, si $n \in \mathbf{N}$ et $0 \leqslant i \leqslant 9^n$. Or l'image de $\big\{\frac{i}{9^n},\ 0 \leqslant i \leqslant 9^n - 1\big\}$ par f_n est l'ensemble A_n des couples $\big(\frac{a}{3^n}, \frac{b}{3^n}\big)$, avec a, b entiers, $0 \leqslant a, b \leqslant 3^n$, et $a+b$ pair. La réunion des A_n est dense dans $[0,1]^2$, et est contenue dans l'image de f d'après ce qui précède ; l'image de f est donc dense dans $[0,1]^2$. Pour montrer que f remplit tout le carré $[0,1]^2$, il n'y a plus qu'à remarquer que $[0,1]$ étant compact et f continue, $f([0,1])$ est compacte et donc fermée dans $[0,1]^2$, et comme elle est dense, c'est $[0,1]^2$ tout entier !

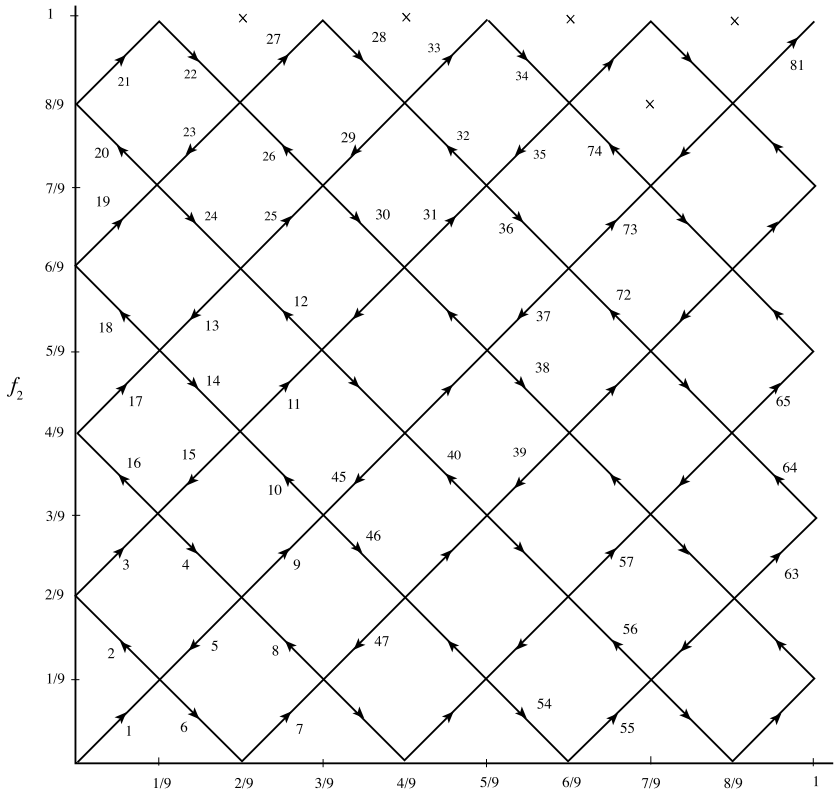

FIG. 3. La fonction f_2 : les nombres apparaissant sur la figure correspondent à l'ordre dans lequel les $9^2 = 81$ segments sont parcourus.

11.5. Ensembles connexes non connexes par arcs

11.5.1. Le graphe de $\sin \frac{1}{x}$

Soit X le graphe de la fonction $x \mapsto \phi(x) = \sin \frac{1}{x}$, pour $x > 0$. L'ensemble X est connexe par arcs, vu que c'est un arc en tant qu'image de $\mathbf{R}_+^*$ par $x \mapsto (x, \phi(x))$ qui est une application continue de $\mathbf{R}_+^*$ dans $\mathbf{R}^2$. Son adhérence $\overline{\mathrm{X}}$ dans X est donc connexe ; nous allons montrer qu'elle n'est pas connexe par arc.

Commençons par montrer que $\overline{\mathrm{X}} = \mathrm{X} \cup \mathrm{I}$, où I est le segment vertical $\mathrm{I} = \{(0, y),\ y \in [-1, 1]\}$.

• Comme $\mathbf{R}^2$ est métrique, un point (a, b) est dans l'adhérence de X, s'il existe une suite $(x_n, y_n)_{n \in \mathbf{N}}$ d'éléments de X convergeant vers (a, b) dans $\mathbf{R}^2$. Or $y_n = \phi(x_n)$ et ϕ est continue sur $\mathbf{R}_+^*$, ce qui fait que, si $a > 0$, on doit avoir $b = \phi(a)$ par continuité. L'intersection de $\overline{\mathrm{X}}$ avec $\mathbf{R}_+^* \times \mathbf{R}$ est donc réduite à X.

• Comme X est contenu dans le fermé $\mathbf{R}_+ \times [-1, 1]$, il en est de même de son adhérence ; on en déduit l'inclusion $\overline{\mathrm{X}} \subset \mathrm{X} \cup \mathrm{I}$.

• Si $b \in [-1, 1]$, alors $(0, b)$ est la limite de $\left(\frac{1}{2n\pi + \arcsin(b)}, b\right) \in \mathrm{X}$, quand $n \to +\infty$, ce qui montre que $(0, b) \in \overline{\mathrm{X}}$, et donc que $\mathrm{I} \subset \overline{\mathrm{X}}$. On en déduit l'égalité $\overline{\mathrm{X}} = \mathrm{X} \cup \mathrm{I}$ que l'on cherchait à établir.

Démontrons, par l'absurde, que $\overline{\mathrm{X}}$ n'est pas connexe par arcs. Supposons donc le contraire ; il existe alors $u : [0, 1] \to \overline{\mathrm{X}}$, continue, telle que $u(0) = (0, 0)$, et $u(1) = (\pi^{-1}, 0)$. Soient $\mathrm{A} = \{t,\ u(t) \in \mathrm{I}\}$ et $a \in [0, 1]$ la borne supérieure de A. Alors $u(a) \in \mathrm{I}$ car I est fermé et u est continue, et $u(t) \notin \mathrm{I}$, si $t > a$. On a donc $u(a) = (0, b)$, et $u(t) = (x(t), y(t))$, avec $x(t) > 0$, si

$t > a$. On peut supposer, sans nuire à la généralité, que $b \neq 1$ (sinon, on remplace 1 par -1 dans ce qui suit). Comme u est continue, il existe $\delta > 0$ tel que $y(t) \neq 1$, si $t \in [a, a+\delta]$. Comme $y(t) = \phi(x(t))$, cela implique que $x(t)$ n'est pas de la forme $\frac{1}{2n\pi+(\pi/2)}$, si $t \in [a, a+\delta]$, Or le seul intervalle de $\mathbf{R}_+$ contenant 0 et ne contenant aucun point de la forme $\frac{1}{2n\pi+(\pi/2)}$, pour $n \in \mathbf{N}$, est $\{0\}$. Comme $t \mapsto x(t)$ est continue sur $[a, a+\delta]$, cela implique $x(t) = 0$, si $t \in [a, a+\delta]$, ce qui est contraire à la définition de a. Ceci permet de conclure.

11.5.2. Le tipi de Cantor

C'est un sous-ensemble T du plan qui défie un peu l'entendement car il est connexe, et il existe $S \in T$ tel que, si on retire S à T, le résultat est totalement discontinu (ce qui signifie, rappelons-le, que les composantes connexes de $T - S$ sont réduites à des points).

Pour construire T, on part de l'ensemble triadique de Cantor K que l'on partitionne en un ensemble K_1 dénombrable et dense[(42)] et son complémentaire K_2.

On identifie K à un sous-ensemble de $\mathbf{R}^2$ par $t \mapsto (t, 0)$, ce qui permet de voir K comme un sous-ensemble du segment horizontal $L = [0,1] \times \{0\}$. On note S le point $(0,1)$, et si $P = (t,0)$, avec $t \in K_1$ (resp. $t \in K_2$), on définit le *rayon* T_P comme l'ensemble des (x,y) appartenant au segment $[P, S[$, avec $y \in \mathbf{Q}$ (resp. $y \notin \mathbf{Q}$). On définit le *tipi de Cantor* T comme la réunion des T_P, pour $P \in K$, auquel on rajoute le *sommet* S de T. Nous allons montrer que T est connexe, mais que T privé de S est totalement discontinu.

Pour montrer que T est connexe, considérons une partition de T en deux ouverts U_1 et U_2, et supposons que $S \in U_1$. Comme U_1 est non vide, il s'agit de montrer que U_2 l'est. Comme il est plus confortable de travailler dans un carré que dans un triangle, on remarque que $(x,y) \mapsto ((1-y)x, y)$ induit un homéomorphisme de $[0,1] \times [0,1[$ sur le triangle de sommets $A = (0,0)$, $B = (1,0)$ et $S = (0,1)$, privé de son sommet S ; l'homéomorphisme réciproque étant $(x,y) \mapsto (\frac{x}{1-y}, y)$. Via cet homéomorphisme, le rayon T_P devient $T'_P = \{P\} \times ([0,1] \cap \mathbf{Q})$, si $P \in K_1$, et $T'_P = \{P\} \times ([0,1] \cap (\mathbf{R} - \mathbf{Q}))$, si $P \in K_2$, et $T - S$ devient la réunion T' de $K_1 \times ([0,1] \cap \mathbf{Q})$, et de $K_2 \times ([0,1] \cap (\mathbf{R} - \mathbf{Q}))$. L'ouvert $U_1 - S$ devient un ouvert U'_1 de T' contenant $([0,1] \times]1-\delta, 1[) \cap T'$, si $\delta > 0$ est assez petit, U_2 devient un ouvert U'_2 de T', et U'_1 et U'_2 forment une partition de T'.

On est alors ramené à prouver que U'_2 est vide. On définit une fonction $h : K \to [0,1]$, par $h(P) = 0$, si $T'_P \cap U'_2 = \emptyset$, et $h(P) = \sup\{y,\ (P,y) \in T'_P \cap U'_2\}$, si $T'_P \cap U'_2 \neq \emptyset$. Comme U'_2 est ouvert, sa vacuité est équivalente à $h = 0$ sur K ; on va donc s'intéresser aux points où $h \neq 0$.

• $h(P) < 1$ pour tout $P \in K$, car $U'_1 \cap U'_2 = \emptyset$ et U'_1 contient $([0,1] \times]1-\delta, 1[) \cap T'$, si $\delta > 0$ est assez petit.

• $h(P) \in \mathbf{Q}$ si $P \in K_2$, car sinon le point $(P, h(P))$ de T'_P appartiendrait à U'_i, pour $i = 1$ ou $i = 2$, et comme U'_i est ouvert, il existerait un segment ouvert $J \subset]0,1[$, contenant $h(P)$, tel que $\{(P,t),\ t \in J\} \cap T'$, soit contenu dans U'_i. Dans les deux cas $i = 1$ et $i = 2$, on obtient une contradiction avec la définition de $h(P)$.

• Si $q \in]0,1[\cap \mathbf{Q}$, et si $P \in K_1$, il existe un ouvert I de K contenant P tel que $h(Q) \neq q$ pour tout $Q \in I$. En effet, le point (P,q) appartient à T'_P par construction, et donc appartient à U'_i, pour $i = 1$ ou $i = 2$. Comme U'_i est ouvert et contient (P,q), il contient un ouvert de la forme $(I \times J) \cap T'$, où I est un ouvert de K contenant P, et J est un ouvert de $]0,1[$, contenant q ; la définition de h montre que l'on a $h(Q) \notin J$, si $Q \in I$.

(42) On peut, par exemple, prendre pour K_1 l'ensemble des éléments de K dont le développement en base 3 est limité, i.e. l'ensemble des nombres de la forme $\sum_{i=1}^{n} \frac{a_i}{3^n}$, avec $n \in \mathbf{N}$, et $a_i \in \{0,2\}$, si $1 \leqslant i \leqslant n$.

Si $q \in]0,1[\cap\mathbf{Q}$, soit F_q l'adhérence de $\{\mathrm{P} \in \mathrm{K},\ h(\mathrm{P}) = q\}$. C'est un fermé de K par construction, et il ne rencontre pas K_1 d'après le point précédent. Il est donc d'intérieur vide puisque K_1 est dense dans K. Comme K est un compact métrique, il est complet, et le lemme de Baire implique que la réunion X de K_1 et des F_q, pour $q \in \mathbf{Q}\cap]0,1[$, est d'intérieur vide, puisque c'est une réunion dénombrable de fermés d'intérieur vide ($\mathbf{Q}\cap]0,1[$ est dénombrable et K_1 est dénombrable et donc est une réunion dénombrable de singletons). L'ensemble $\mathrm{K} - \mathrm{X}$ est donc dense dans K. Or $\mathrm{P} \in \mathrm{K} - \mathrm{X}$ implique $h(\mathrm{P}) = 0$, et donc aussi $\{\mathrm{P}\} \times (]0,1[\cap(\mathbf{R} - \mathbf{Q})) \subset \mathrm{U}'_1$. Donc U'_1 contient $(\mathrm{K} - \mathrm{X}) \times (]0,1[\cap(\mathbf{R} - \mathbf{Q}))$ qui est dense dans T' car il l'est dans $\mathrm{K} \times [0,1[$ qui contient T'. Son complémentaire U'_2 est donc d'intérieur vide, et comme il est ouvert, il est vide. On en déduit la connexité de T.

Il reste à montrer que $\mathrm{T} - \mathrm{S}$ est totalement discontinu, et comme $\mathrm{T} - \mathrm{S}$ est homéomorphe à T', il suffit de prouver que T' l'est. Pour cela considérons deux points distincts (P_1, y_1) et (P_2, y_2) de T'. Si $\mathrm{P}_1 \neq \mathrm{P}_2$, il existe $\mathrm{Q} \notin \mathrm{K}$ dans l'intervalle ouvert d'extrémités P_1 et P_2 puisque K est d'intérieur vide. La droite verticale $\{\mathrm{Q}\} \times \mathbf{R}$ ne rencontre pas T', et les deux demi-plans ouverts qu'elle délimite partitionnent T' en deux ouverts, l'un contenant (P_1, y_1), l'autre (P_2, y_2). On en déduit que (P_2, y_2) n'est pas dans la composante connexe de (P_1, y_1). Une composante connexe de T' est donc incluse dans un rayon T'_P, or un tel ensemble est totalement discontinu puisqu'il est homéomorphe à $\mathbf{Q} \cap [0,1[$ ou à $(\mathbf{R} - \mathbf{Q}) \cap [0,1[$. Les composantes connexes de T' sont donc des points, ce qui permet de conclure.

12. Construction de nombres

Dans ce §, on explique rapidement (sans démonstration) comment construire toutes les quantités usuelles à partir d'un système minimal d'axiomes. Cette problématique n'est apparue que relativement récemment dans l'histoire des mathématiques puisqu'il a fallu attendre 1872 pour que Weierstrass s'aperçoive que les nombres réels n'avaient pas été définis, ce qui aurait pu avoir des conséquences fâcheuses... Une des raisons qui ont poussé les mathématiciens à s'intéresser à ces questions de fondements a été l'apparition de monstres (cf. § précédent) montrant que l'intuition pouvait se révéler fort trompeuse, et de paradoxes menaçant de faire s'écrouler tout l'édifice.

12.1. Entiers naturels

La première présentation axiomatique des entiers remonte à 1888 (Dedekind), simplifiée l'année suivante par Peano. L'ensemble des nombres entiers qui semble être constitué des objets les plus évidents (tout le monde comprend ce que sont $0, 1, 2, \ldots$; le problème est dans le « ... »), ne peut pas être construit ; on est plus ou moins forcé de postuler son existence et d'espérer que le ciel ne va pas nous tomber sur la tête.

• La présentation la plus efficace postule l'existence d'un ensemble $\mathbf{N}$, l'ensemble des entiers naturels, muni d'un élément 0 et d'une application « successeur » $s : \mathbf{N} \to \mathbf{N}$, vérifiant les axiomes (de Peano) suivants :

(A1) l'application s est injective ;

(A2) 0 n'est le successeur d'aucun entier naturel ;

(A3) Si $\mathrm{X} \subset \mathbf{N}$ est tel que $0 \in \mathrm{X}$ et $s(n) \in \mathrm{X}$ pour tout $n \in \mathrm{X}$, alors $\mathrm{X} = \mathbf{N}$ (axiome de récurrence).

On définit alors l'addition et la multiplication par récurrence par $a + 0 = a$ et $a + s(b) = s(a + b)$ (pour l'addition) ; $a\,0 = 0$ et $a\,s(b) = ab + a$ (pour la multiplication). On pose $1 = s(0)$, et on a $s(a) = s(a + 0) = a + s(0) = a + 1$, ce qui permet de supprimer l'application successeur et de la remplacer par $a \mapsto a + 1$. Vérifier, à partir des axiomes de Peano, que l'addition et la multiplication sont

commutatives et que la multiplication est distributive par rapport à l'addition, est un exercice un peu répétitif mais très satisfaisant pour l'esprit.

• On obtient une présentation plus intuitive en partant de l'idée que se fait le petit enfant du nombre 5. On dit qu'un ensemble X est fini s'il ne peut pas être mis en bijection avec $X \cup \{x\}$, si $x \notin X$. On postule l'existence d'un ensemble infini Ω (axiome de l'infini), et on munit l'ensemble des parties de Ω de la relation d'équivalence $\sim$ définie par $X_1 \sim X_2$ s'il existe une bijection de X_1 sur X_2. On définit alors l'ensemble $\mathbf{N}$ des entiers naturels comme l'ensemble des classes d'équivalence de parties finies de Ω pour cette relation d'équivalence. Si X est une partie finie de Ω, on note $|X| \in \mathbf{N}$ sa classe d'équivalence ; c'est un entier naturel que l'on appelle le cardinal de X, et une analyse *a posteriori* de la construction précédente, montre que l'on a défini l'entier n comme la classe d'équivalence de tous les ensembles (inclus dans notre Ω) de cardinal n.

On note 0 le cardinal de l'ensemble vide, 1 celui d'un singleton (i.e. un ensemble X, non vide, tel que $x, y \in X \Rightarrow x = y$)... Si $a, b \in \mathbf{N}$, on choisit $X, Y \subset \Omega$ disjoints, de cardinaux respectifs a et b, et on définit $a+b$ comme le cardinal de $X \cup Y$, et ab comme le cardinal de (tout sous-ensemble de Ω pouvant être mis en bijection avec) $X \times Y$. Il est alors quasi-immédiat que $a+b = b+a$ (car $X \cup Y = Y \cup X$), que $ab = ba$ (car $(x, y) \mapsto (y, x)$ induit une bijection de $X \times Y$ sur $Y \times X$), que $0 \cdot a = a$ pour tout $a \in \mathbf{N}$ (l'ensemble $\emptyset \times X$ est vide quel que soit X), et que $a(b+c) = ab + ac$ (car $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$).

Les choses se compliquent quand on essaie de montrer que $\mathbf{N}$ vérifie l'axiome de récurrence pour l'application successeur $x \mapsto x+1$.

12.2. Entiers relatifs, nombres rationnels

En partant des entiers naturels, on fait les constructions suivantes.

• On construit $\mathbf{Z}$ comme quotient de $\mathbf{N} \times \mathbf{N}$ par la relation d'équivalence $(a, b) \sim (a', b')$ si et seulement si $a + b' = a' + b$, l'idée étant que (a, b) représente l'entier relatif $a - b$. L'application $n \mapsto (n, 0)$ induit une injection de $\mathbf{N}$ dans $\mathbf{Z}$, ce qui permet de voir $\mathbf{N}$ comme un sous-ensemble de $\mathbf{Z}$.

L'addition $(a, b) + (a', b') = (a + a', b + b')$ passe au quotient, et définit une loi qui fait de $\mathbf{Z}$ un groupe commutatif, l'élément neutre étant (la classe de) $(0, 0)$ (ou de (a, a), pour tout $a \in \mathbf{N}$), et l'opposé de (a, b) étant (b, a). L'opposé $-n$ de n est donc représenté par $(0, n)$, et on peut maintenant définir $a - b$, si a et $b \in \mathbf{Z}$, et si $a, b \in \mathbf{N}$, on a $a - b = (a, 0) + (0, b) = (a, b)$, ce que l'on cherchait à obtenir.

La multiplication[43] $(a, b)(a', b') = (aa' + bb', ab' + ba')$ passe au quotient, et $\mathbf{Z}$ muni de l'addition et de la multiplication est un anneau commutatif.

Enfin, on dit que $a \geqslant b$, si $a - b \in \mathbf{N}$, et on obtient de la sorte une relation d'ordre totale sur $\mathbf{Z}$.

• On construit $\mathbf{Q}$ comme quotient de $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ par la relation d'équivalence $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$, l'idée étant que (a, b) représente le nombre rationnel $\frac{a}{b}$. L'application $n \mapsto (n, 1)$ induit une injection de $\mathbf{Z}$ dans $\mathbf{Q}$, ce qui permet de voir $\mathbf{Z}$ comme un sous-ensemble de $\mathbf{Q}$.

L'addition et la multiplication sur $\mathbf{Q}$ sont définies par les formules $(a, b) + (a', b') = (ab' + ba', bb')$ et $(a, b)(a', b') = (aa', bb')$ qui passent au quotient, et $\mathbf{Q}$ muni de l'addition et de la multiplication est un corps commutatif :l'élément neutre pour + est 0, la classe de $(0, b)$, pour tout $b \in \mathbf{N}$, l'opposé de (a, b) est $(-a, b)$, l'élement neutre pour $\times$ est 1, classe de (b, b), pour tout $b \in \mathbf{Z} - \{0\}$, et l'inverse de (a, b), si $(a, b) \neq 0$ (ce qui équivaut à $a \neq 0$) est (b, a). Si $a \in \mathbf{Z}$ et $b \in \mathbf{Z} - \{0\}$, on peut maintenant diviser a par b dans $\mathbf{Q}$, et $b^{-1}a$ est la classe de $(1, b)(a, 1) = (a, b)$, ce que l'on cherchait à obtenir.

Enfin, on dit que q est positif, si q a un représentant (a, b) avec $b \geqslant 0$ et $a \geqslant 0$, et que $q_1 \geqslant q_2$, si $q_1 - q_2$ est positif. On obtient de la sorte une relation d'ordre total sur $\mathbf{Q}$.

---

[43] On rappelle que (a, b) représente $b - a$, et donc que $(aa' + bb', ab' + ba')$ représente $aa' + bb' - ab' - ba' = (a - b)(a' - b')$, ce qui explique comment la formule pour la multiplication a été obtenue.

12.3. Nombres réels, nombres complexes

Pour construire $\mathbf{R}$ à partir de $\mathbf{Q}$, on dispose essentiellement de trois possibilités.

• On peut utiliser les *coupures de Dedekind* (1872), c'est-à-dire l'ensemble des couples (A, B) de parties non vides de $\mathbf{Q}$ tels que $\mathrm{A} \cup \mathrm{B} = \mathbf{Q}$, et tout élément de A est $\leqslant$ à tout élément de B. L'idée étant que si $r \in \mathbf{R}$, alors r correspond à la coupure $(\mathrm{A}_r, \mathrm{B}_r)$ donnée par $\mathrm{A}_r = \{x \in \mathbf{Q},\ x \leqslant r\}$ et $\mathrm{B}_r = \{x \in \mathbf{Q},\ x \geqslant r\}$. Les rationnels s'identifient aux coupures (A, B) telles que $\mathrm{A} \cap \mathrm{B}$ est non vide. Il est alors facile de montrer que l'ensemble $\mathbf{R}$ ainsi construit vérifie la propriété de la borne supérieure (toute partie majorée non vide admet une borne supérieure), puis qu'il est complet.

• On peut aussi, comme G. Cantor (1872), compléter $\mathbf{Q}$ pour la valeur absolue, en rajoutant de force les limites des suites de Cauchy d'éléments de $\mathbf{Q}$. Cela peut se faire, par exemple, de la manière suivante. On considère l'ensemble Cauchy($\mathbf{Q}$) des suites de Cauchy d'éléments de $\mathbf{Q}$ (i.e. l'ensemble des suites $(a_n)_{n\in\mathbf{N}}$, avec $a_n \in \mathbf{Q}$, telles que, pour tout $j \in \mathbf{N}$, il existe $\mathrm{N}_j \in \mathbf{N}$ tel que $|a_p - a_n| < 2^{-j}$, quels que soient $n, p \geqslant \mathrm{N}_j$). Alors Cauchy($\mathbf{Q}$) est un anneau pour l'addition et la multiplication terme à terme dans lequel l'ensemble I des suites tendant vers 0 est un idéal. On définit alors $\mathbf{R}$ comme le quotient de Cauchy($\mathbf{Q}$) par I, ce qui revient (moralement) à identifier deux suites de Cauchy ayant même limite (i.e. dont la différence tend vers 0), et donc « à identifier une suite de Cauchy avec sa limite ». Le résultat $\mathbf{R}$ est un corps[(44)], muni d'une relation d'ordre stricte $<$ totale[(45)], dans lequel $\mathbf{Q}$ (identifié à l'image des suites constantes) est dense[(46)].

• On peut aussi utiliser la construction de « l'homme de la rue » qui part du fait qu'un réel a un développement décimal. Cela conduit à définir $\mathbf{R}$ comme l'ensemble des développements décimaux $a_n \dots a_0, a_{-1}a_{-2}\dots$ avec un nombre fini de chiffres avant la virgule et un nombre infini après, modulo la relation d'équivalence $\sim$, identifiant $a_n \dots a_m 999999\dots$ à $a_n \dots a_{m+1}(a_m + 1)00000\dots$, si $a_m \neq 9$. Nous laissons au lecteur le soin de définir l'addition et la multiplication de deux réels de « l'homme de la rue »...

• Une fois les nombres réels construits, on obtient le corps des nombres complexes $\mathbf{C}$ en rajoutant à $\mathbf{R}$ une racine carrée i de -1, ce qui revient à poser $\mathbf{C} = \mathbf{R}[\mathrm{X}]/(\mathrm{X}^2 + 1)$. Le résultat est un corps complet pour la norme $|z| = \sqrt{x^2 + y^2}$, si $z = x + iy$, et qui est algébriquement clos (résultat connu sous le nom de « théorème fondamental de l'algèbre » bien qu'il n'existe aucune démonstration de ce résultat qui n'utilise pas de technique d'analyse).

12.4. Nombres p-adiques

12.4.1. Le corps $\mathbf{Q}_p$. — La construction de $\mathbf{R}$ de G. Cantor, bien que plus compliquée, est nettement plus souple que celle de R. Dedekind, et se généralise facilement. Il n'a fallu que 25 ans après la construction des nombres réels (qui avait pris quelque deux millénaires...), pour que K. Hensel envisage la construction (1897) des nombres p-adiques, et une petite dizaine d'années pour qu'il leur donne une forme maniable. De nos jours, on procède de la manière suivante.

---

(44) si $(a_n)_{n\in\mathbf{N}}$ est une suite de Cauchy qui ne tend pas vers 0, alors $a_n \neq 0$ si $n \geqslant n_0$, et la suite $(1, \dots, 1, a_{n_0}^{-1}, \dots, a_n^{-1}, \dots)$ est une suite de Cauchy dont l'image dans $\mathbf{R}$ est l'inverse de celle de la suite $(a_n)_{n\in\mathbf{N}}$.

(45) Si $a, b \in \mathbf{R}$, on dit que $a < b$, si $a \neq b$ et si, pour tous représentants $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ de a et b, on a $a_n < b_p$ si n et p sont assez grands ; on constate sans problème que si c'est vrai pour un choix de représentants, alors c'est vrai pour tous.

(46) Cela signifie qu'entre deux éléments de $\mathbf{R}$ on peut toujours trouver un élément de $\mathbf{Q}$. Si $a < b$ sont deux éléments de $\mathbf{R}$, et si $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ sont des représentants de a et b, alors $a_n < b_p$, si $n, p \geqslant n_0$, et $r = \frac{a_{n_0} + b_{n_0}}{2}$ est un élément de $\mathbf{Q}$ vérifiant $a < r < b$.

Soit p un nombre premier. Si $a \in \mathbf{Z} - \{0\}$, on définit la valuation p-adique $v_p(a)$ comme le plus grand entier v tel que p^v divise a. On a $v_p(ab) = v_p(a)+v_p(b)$ si $a, b \in \mathbf{Z}-\{0\}$, ce qui permet d'étendre v_p à $\mathbf{Q}$ en posant $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$, si $a, b \in \mathbf{Z} - \{0\}$, et $v_p(0) = +\infty$. On a alors $v_p(x+y) \geqslant \min(v_p(x), v_p(y))$, si $x, y \in \mathbf{Q}$ car, si x et y sont divisibles par p^v, il en est de même de $x+y$. On en déduit le fait que, si on pose $|x|_p = p^{-v_p(x)}$, alors $|x+y|_p \leqslant \sup(|x|_p, |y|_p)$ et donc que $d_p(x, y) = |x-y|_p$ est une distance sur $\mathbf{Q}$ (la *distance p-adique*), l'inégalité ci-dessus, dite *ultramétrique*, étant plus forte que l'inégalité triangulaire.

On définit $\mathbf{Q}_p$, corps des nombres p-adiques, comme le complété de $\mathbf{Q}$ pour la norme p-adique $|\ |_p$, c'est-à-dire que l'on prend, comme pour définir $\mathbf{R}$, l'anneau des suites de Cauchy (pour la norme $|\ |_p$) d'éléments de $\mathbf{Q}$, et on quotiente par l'idéal des suites tendant vers 0. Si $x \in \mathbf{Q}_p$, et si $(a_n)_{n\in\mathbf{N}}$ est un représentant de x, alors $|a_n|_p$ tend vers une limite dans $\mathbf{R}$ (et même dans $p^{\mathbf{Z}} \cup \{0\}$, car tous ses termes sont dans $p^{\mathbf{Z}} \cup \{0\}$ qui est fermé dans $\mathbf{R}_+$) qui ne dépend que de x, et qu'on note $|x|_p$. Par construction, $|\ |_p$ est une norme ultramétrique sur $\mathbf{Q}_p$, ce qui signifie que $|x|_p = 0$ si et seulement si $x = 0$, que $|xy|_p = |x|_p|y|_p$, quels que soient $x, y \in \mathbf{Q}_p$, et que $|x+y|_p \leqslant \sup(|x|_p, |y|_p)$, et donc $d_p(x, y) = |x-y|_p$ est une distance ultramétrique sur $\mathbf{Q}_p$ pour laquelle $\mathbf{Q}_p$ est complet. On étend v_p à $\mathbf{Q}_p$ par continuité, et on a encore $|x|_p = p^{-v_p(x)}$, si $x \in \mathbf{Q}_p$.

• Dans $\mathbf{Q}_p$, une suite $(x_n)_{n\in\mathbf{N}}$ converge si et seulement si $x_{n+1} - x_n$ tend vers 0 et une série $\sum_{n\in\mathbf{N}} u_n$ converge si et seulement si u_n tend vers 0.

D'après l'inégalité ultramétrique, on a $|x_{n+k} - x_n|_p \leqslant \sup_{0\leqslant i\leqslant k-1} |x_{n+i+1} - x_{x+i}|_p$, ce qui montre que si $|x_{n+1} - x_n|_p$ tend vers 0, alors la suite est de Cauchy. La complétude de $\mathbf{Q}_p$ permet de conclure (l'argument est le même pour une série).

Exercice 12.1. — Montrer que la série $1 + 2 + 4 + 8 + \cdots$ converge vers -1 dans $\mathbf{Q}_2$.

Exercice 12.2. — (i) Montrer que $|x+y|_p = |x|_p$, si $|x|_p > |y|_p$.
(ii) Montrer que $\sum_{n\in\mathbf{N}} u_n \neq 0$, et $\big|\sum_{n\in\mathbf{N}} u_n\big|_p = |u_0|_p$, si $u_n \to 0$, et si $|u_0|_p > |u_n|_p$, pour tout $n \geqslant 1$.

• La topologie de $\mathbf{Q}_p$ possède des propriétés un peu déroutantes au premier abord.
(i) Tout point d'une boule de $\mathbf{Q}_p$ en est « le » centre.
(ii) Deux boules de $\mathbf{Q}_p$ sont soit disjointes soit l'une est contenue dans l'autre (comme des billes de mercure).
(iii) Les boules de $\mathbf{Q}_p$ sont à la fois ouvertes et fermées.
(iv) La topologie de $\mathbf{Q}_p$ est totalement discontinue.

Si $x_1 \in \mathrm{B}(x_0, r)$ et $y \in \mathrm{B}(x_1, r)$, alors $d_p(x_0, y) \leqslant \sup(d_p(x_0, x_1), d_p(x_1, y)) \leqslant r$ (ou $< r$ si on parle de boules ouvertes), et donc $\mathrm{B}(x_1, r) \subset \mathrm{B}(x_0, r)$. L'inclusion dans l'autre sens s'obtient en échangeant les rôles de x_0 et x_1, ce qui permet de démontrer le (i).

D'après le (i), si deux boules ont une intersection non vide, tout élément de l'intersection est le centre des deux boules, ce qui démontre le (ii).

Si B est une boule ouverte de rayon r, le complémentaire de B contient la boule ouverte de rayon r autour de chacun de ses points d'après le (ii), ce qui montre que ce complémentaire est ouvert et donc que B est fermée. Si B est une boule fermée de rayon non nul, alors B est un voisinage de chacun de ses points puisque ceux-ci en sont "le" centre. On en déduit le (iii).

Enfin, si $x \in \mathbf{Q}_p$, si C_x est la composante connexe de x, et si $r > 0$, alors $\mathrm{C}_x \cap \mathrm{B}(x, r)$ est à la fois ouvert et fermé dans C_x, et non vide puisque contenant x. Comme C_x est connexe, cela implique $\mathrm{C}_x \cap \mathrm{B}(x, r) = \mathrm{C}_x$, quel que soit $r > 0$, et donc $\mathrm{C}_x = \{x\}$. On en déduit le (iv).

12.4.2. Construction algébrique de $\mathbf{Q}_p$

L'alinéa précédent a donné une construction analytique de $\mathbf{Q}_p$ comme complété de $\mathbf{Q}$ pour la norme p-adique. Dans cet alinéa, on présente une autre construction de $\mathbf{Q}_p$, à partir des $\mathbf{Z}/p^n\mathbf{Z}$, qui est purement algébrique. L'existence de ces deux points de vue sur les nombres p-adiques offre la possibilité de jongler avec un mélange de techniques d'analyse et d'algèbre, ce qui s'avère précieux pour de nombreuses questions.

• L'ensemble $\mathbf{Z}_p = \{x \in \mathbf{Q}_p,\ |x|_p \leqslant 1\}$ est un sous-anneau fermé de $\mathbf{Q}_p$ qui contient $\mathbf{Z}$.

La multiplicativité de $|\ |_p$ montre que $\mathbf{Z}_p$ est stable par multiplication et l'inégalité ultramétrique montre que $\mathbf{Z}_p$ est stable par addition. C'est donc un sous-anneau de $\mathbf{Q}_p$ qui contient $\mathbf{Z}$ de manière évidente et qui est fermé puisque c'est l'image inverse de $[0,1]$ par l'application $x \mapsto |x|_p$.

• Le sous-groupe $\mathbf{Z}_p^*$ des unités de $\mathbf{Z}_p$ est l'ensemble des $x \in \mathbf{Z}_p$ vérifiant $|x|_p = 1$; c'est aussi $\mathbf{Z}_p - p\mathbf{Z}_p$.

Si $x \in \mathbf{Z}_p - \{0\}$, l'inverse x^{-1} de x dans $\mathbf{Q}_p$ vérifie $|x^{-1}|_p|x|_p = 1$. Comme $|x|_p \leqslant 1$, cet inverse appartient à $\mathbf{Z}_p$ si et seulement si $|x|_p = 1$. Maintenant, pour les mêmes raisons que ci-dessus, l'ensemble des $x \in \mathbf{Z}_p$ vérifiant $|x|_p < 1$ est un idéal de $\mathbf{Z}_p$, et comme $|x|_p < 1$ implique $|x|_p \leqslant p^{-1}$, c'est l'idéal $p\mathbf{Z}_p$. On a donc $\mathbf{Z}_p^* = \mathbf{Z}_p - p\mathbf{Z}_p$.

• L'application naturelle de $\mathbf{Z}/p^n\mathbf{Z}$ dans $\mathbf{Z}_p/p^n\mathbf{Z}_p$ est un isomorphisme.

Si x est un élément de $\mathbf{Z} \cap p^n\mathbf{Z}_p$, on a $v_p(x) \geqslant n$, ce qui signifie que x est divisible par p^n dans $\mathbf{Z}$. On en déduit l'injectivité. Prouvons la surjectivité. Soient $\overline{x} \in \mathbf{Z}_p/p^n\mathbf{Z}_p$ et $x \in \mathbf{Z}_p$ ayant pour image $\overline{x}$ modulo p^n. Comme $\mathbf{Q}$ est dense dans $\mathbf{Q}_p$, il existe $r \in \mathbf{Q}$ vérifiant $v_p(x-r) \geqslant n$; en particulier $v_p(r) \geqslant 0$. Écrivons r sous la forme $\frac{a}{b}$ avec $a, b \in \mathbf{Z}$. Comme $v_p(r) \geqslant 0$, on a $v_p(b) \leqslant v_p(a)$ et quitte à tout diviser par $p^{v_p(b)}$, on peut supposer $v_p(b) = 0$, et donc $(b,p) = 1$, ce qui implique que b est premier à p^n et donc est inversible dans $\mathbf{Z}/p^n\mathbf{Z}$. Soit $\overline{c}$ l'inverse de b dans $\mathbf{Z}/p^n\mathbf{Z}$ et $c \in \mathbf{Z}$ dont la réduction modulo p^n est $\overline{c}$. On a alors $v_p(r - ac) = v_p(a) - v_p(b) + v_p(1-bc) \geqslant n$ et donc $v_p(x - ac) \geqslant n$, ce qui prouve que ac a pour image $\overline{x}$ dans $\mathbf{Z}_p/p^n\mathbf{Z}_p$, et permet de conclure.

• L'application ι, qui à $x \in \mathbf{Z}_p$ associe la suite de ses réductions modulo p^n, est un isomorphisme d'anneaux de $\mathbf{Z}_p$ sur la *limite projective*[47] $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ des $\mathbf{Z}/p^n\mathbf{Z}$.

L'inclusion $p^n\mathbf{Z} \subset p^{n-1}\mathbf{Z}$, induit un morphisme d'anneaux $\pi_n : \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^{n-1}\mathbf{Z}$, surjectif. Si $x \in \mathbf{Z}_p$, la réduction x_n de x modulo p^n peut être vue comme un élément de $\mathbf{Z}/p^n\mathbf{Z}$ d'après le point précédent, et on a $\pi_n(x_n) = x_{n-1}$. Il en résulte que l'application ι est un morphisme d'anneaux de $\mathbf{Z}_p$ dans $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$. Si $x \in \operatorname{Ker}\iota$, on a $x \in p^n\mathbf{Z}_p$ et donc $|x|_p \leqslant p^{-n}$, pour tout $n \in \mathbf{N}$, ce qui implique $x = 0$ et prouve que ι est injectif. Si $(y_n)_{n\in\mathbf{N}} \in \varprojlim \mathbf{Z}/p^n\mathbf{Z}$ et si $\hat{y}_n$ est un relèvement de y_n dans $\mathbf{Z}_p$, alors $\hat{y}_{n+1} - \hat{y}_n \in p^n\mathbf{Z}_p$ puisque $\pi_{n+1}(y_{n+1}) = y_n$; la suite $(\hat{y}_n)_{n\in\mathbf{N}}$ a donc une limite y dans $\mathbf{Z}_p$ et, par construction, $y - \hat{y}_n \in p^n\mathbf{Z}_p$, pour tout $n \in \mathbf{N}$; autrement dit, $\iota(y) = (y_n)_{n\in\mathbf{N}}$, d'où la surjectivité de ι.

[47] Si $(\mathrm{X}_n)_{n\in\mathbf{N}}$ est une suite d'ensembles munis d'applications $\pi_n : \mathrm{X}_n \to \mathrm{X}_{n-1}$, pour $n \geqslant 1$, on définit la *limite projective* $\varprojlim \mathrm{X}_n$ des X_n (relativement aux π_n) comme le sous-ensemble de $\prod_{n\in\mathbf{N}} \mathrm{X}_n$ des suites $(x_n)_{n\in\mathbf{N}}$, avec $x_n \in \mathrm{X}_n$ et $\pi_n(x_n) = x_{n-1}$, si $n \geqslant 1$.

• Le point précédent permet de définir $\mathbf{Z}_p$, algébriquement [48], comme étant $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$, et comme $\mathbf{Q}_p = \mathbf{Z}_p[\frac{1}{p}]$, cela fournit une définition algébrique de $\mathbf{Q}_p$.

12.4.3. Topologie de $\mathbf{Q}_p$

• Tout élément de $\mathbf{Q}_p$ peut s'écrire de manière unique sous la forme $x = \sum_{i=-k}^{+\infty} a_i p^i$, où $a_i \in \{0, \dots, p-1\}$ pour tout i. Il admet donc une unique *écriture en base p*

$$x = \dots a_{n-1} \dots a_0, a_{-1} \dots a_{-k}\,,$$

et on a $|x|_p = p^k$, si $a_{-k} \neq 0$. Une différence avec les nombres réels est qu'il y a une infinité de chiffres avant la virgule et un nombre fini après. Les éléments de $\mathbf{Z}_p$ sont ceux dont l'écriture en base p n'a pas de chiffre après la virgule (du point de vue de l'écriture en base p, ils correspondent au segment $[0, 1]$)

Si $n \in \mathbf{N}$, alors $\{0, \dots, p^n - 1\}$ est un système de représentants de $\mathbf{Z}/p^n\mathbf{Z}$. Soit alors $x \in \mathbf{Q}_p^*$, et soit $k = -v_p(x)$ de telle sorte que $y = p^k x \in \mathbf{Z}_p^*$. Si $n \geqslant -k$, soit $y_n \in \{0, \dots, p^{n+k} - 1\}$ le représentant de l'image de y dans $\mathbf{Z}_p/p^{n+k}\mathbf{Z}_p \cong \mathbf{Z}/p^{n+k}\mathbf{Z}$ (en particulier, $y_{-k} = 0$ et $y_{1-k} \neq 0$, car $y \notin p\mathbf{Z}_p$). Alors $y_{n+1} - y_n$ est divisible par p^{n+k}, ce qui permet de définir $a_n \in \{0, \dots, p-1\}$ par $a_n = p^{-n-k}(y_{n+1} - y_n)$. On a alors $y_n = \sum_{i=0}^{n+k-1} a_{i-k} p^i$; autrement dit, $a_{n-1}a_{n-2} \dots a_{-k}$ est l'écriture de y_n en base p. Par suite, $a_{n-1} \dots a_0, a_{-1} \dots a_{-k}$ est l'écriture de $x_n = p^{-k} y_n$ en base p. Or $y_n - p^k x \in p^{n+k}\mathbf{Z}_p$ par construction, ce qui se traduit par $|y_n - p^k x|_p \leqslant p^{-(n+k)}$, ou encore par $|x_n - x|_p \leqslant p^{-n}$, et montre que $x_n \to x$ dans $\mathbf{Q}_p$. On a donc $x = \sum_{i=-k}^{+\infty} a_i p^i$ (la somme converge puisque son terme général tend vers 0). On en déduit l'existence d'une écriture sous la forme voulue.

Pour démontrer l'unicité, il suffit de constater que si $\sum_{i=-k}^{+\infty} a_i p^i = \sum_{i=-k}^{+\infty} b_i p^i$, alors en multipliant les deux membres par p^k, et en regardant modulo $p\mathbf{Z}_p$, on obtient $a_{-k} - b_{-k} \in p\mathbf{Z}_p$. Comme les a_i et les b_i sont dans un système de représentants modulo $p\mathbf{Z}_p$, cela prouve que $a_{-k} = b_{-k}$. Une récurrence immédiate permet d'en déduire que $a_i = b_i$ pour tout i. Le reste découle de la manière dont les a_i ont été construits ci-dessus.

• $\mathbf{N}$ et $\mathbf{Z}$ sont denses dans $\mathbf{Z}_p$ et $\mathbf{Z}[\frac{1}{p}]$ est dense dans $\mathbf{Q}_p$.

Cela suit de l'existence de l'écriture en base p d'un nombre p-adique (si on coupe cette écriture au n-ième chiffre avant la virgule, on obtient un élément x de $\mathbf{N}$ (resp. $\mathbf{Z}[\frac{1}{p}]$), si on est parti d'un élément de $\mathbf{Z}_p$ (resp. $\mathbf{Q}_p$), et la suite de nombres ainsi obtenue converge vers x).

• $\mathbf{Z}_p$ est compact.

Comme $\mathbf{Z}_p$ est un espace métrique, il suffit de vérifier que toute suite d'éléments de $\mathbf{Z}_p$ admet une sous-suite convergeant dans $\mathbf{Z}_p$. Soit donc $(x_n)_{n\in\mathbf{N}}$ une telle suite, et soit $\sum_{i=0}^{+\infty} a_{n,i} p^i$ l'écriture de x_n en base p. Il existe alors $a_0 \in \{0, \dots, p-1\}$ tel que $a_{n,0} = a_0$ pour une

[48] On dit que $\mathbf{Z}_p$ est le complété de $\mathbf{Z}$ pour la topologie (p)-adique. Cette construction est un cas particulier d'une construction générale permettant d'analytifier beaucoup d'objets algébriques : si A est un anneau et si I est un idéal de A, on peut définir le complété $\widehat{\mathrm{A}}$ de A pour la topologie I-adique (un cas particulier de cette construction est l'anneau K[[T]] des séries entières qui est obtenu à partir de K[T] en complétant pour la topologie (T)-adique ; c'est d'ailleurs par analogie avec cette situation que Hensel a été amené à la construction des nombres p-adiques). De manière précise, si $n \in \mathbf{N}$, on définit l'idéal I^n de A comme l'ensemble des sommes de produits de n éléments de A (on a $\mathrm{I}^0 = \mathrm{A}$ par convention). On a $\mathrm{I}^n \subset \mathrm{I}^{n-1}$ et l'identité de A induit un morphisme (surjectif) d'anneaux $\pi_n : \mathrm{A}/\mathrm{I}^n \to \mathrm{A}/\mathrm{I}^{n-1}$. On définit $\widehat{\mathrm{A}}$ comme la limite projective $\varprojlim \mathrm{A}/\mathrm{I}^n$ des A/I^n (relativement aux morphismes π_n), et on dispose d'une application naturelle $\iota : \mathrm{A} \to \widehat{\mathrm{A}}$ qui n'est pas forcément injective (par exemple, si $\mathrm{I} = \mathrm{A}$, alors $\widehat{\mathrm{A}} = 0$).

infinité de n. Ceci permet d'extraire de la suite $(x_n)_{n\in\mathbf{N}}$ une sous-suite $(x_{\varphi_0(n)})_{n\in\mathbf{N}}$ telle que $a_{\varphi_0(n),0} = a_0$, quel que soit $n \in \mathbf{N}$. Pour la même raison, il existe alors $a_1 \in \{0,\dots,p-1\}$, et une sous-suite $(x_{\varphi_1(n)})_{n\in\mathbf{N}}$, extraite de $(x_{\varphi_0(n)})_{n\in\mathbf{N}}$, telle que $a_{\varphi_1(n),0} = a_1$, quel que soit $n \in \mathbf{N}$. Par récurrence, cela permet de définir $a_k \in \{0,\dots,p-1\}$ et une sous-suite $(x_{\varphi_k(n)})_{n\in\mathbf{N}}$ extraite de $(x_{\varphi_{k-1}(n)})_{n\in\mathbf{N}}$, tels que $a_{\varphi_k(n),i} = a_i$, quels que soient $n \in \mathbf{N}$ et $i \leqslant k$. La suite $(x_{\varphi_n(n)})_{n\in\mathbf{N}}$ est alors extraite (procédé d'*extraction diagonale*) de $(x_n)_{n\in\mathbf{N}}$ et, par construction, on a $a_{\varphi_n(n),i} = a_i$, si $i \leqslant n$, ce qui se traduit par $|x_{\varphi_n(n)} - \sum_{i=0}^{+\infty} a_i p^i|_p \leqslant p^{-n-1}$, et montre que $x_{\varphi_n(n)} \to \sum_{i=0}^{+\infty} a_i p^i$ dans $\mathbf{Z}_p$. Ceci permet de conclure.

• $\mathbf{Q}_p$ est localement compact.

Une boule ouverte $\mathrm{B}(a, r^-)$ de $\mathbf{Q}_p$ est aussi de la forme $a + p^n\mathbf{Z}_p$, où n est le plus grand élément de $\mathbf{Z}$ tel que $p^{-n} < r$. Elle est donc homéomorphe à $\mathbf{Z}_p$, et la compacité de $\mathbf{Z}_p$ permet de conclure.

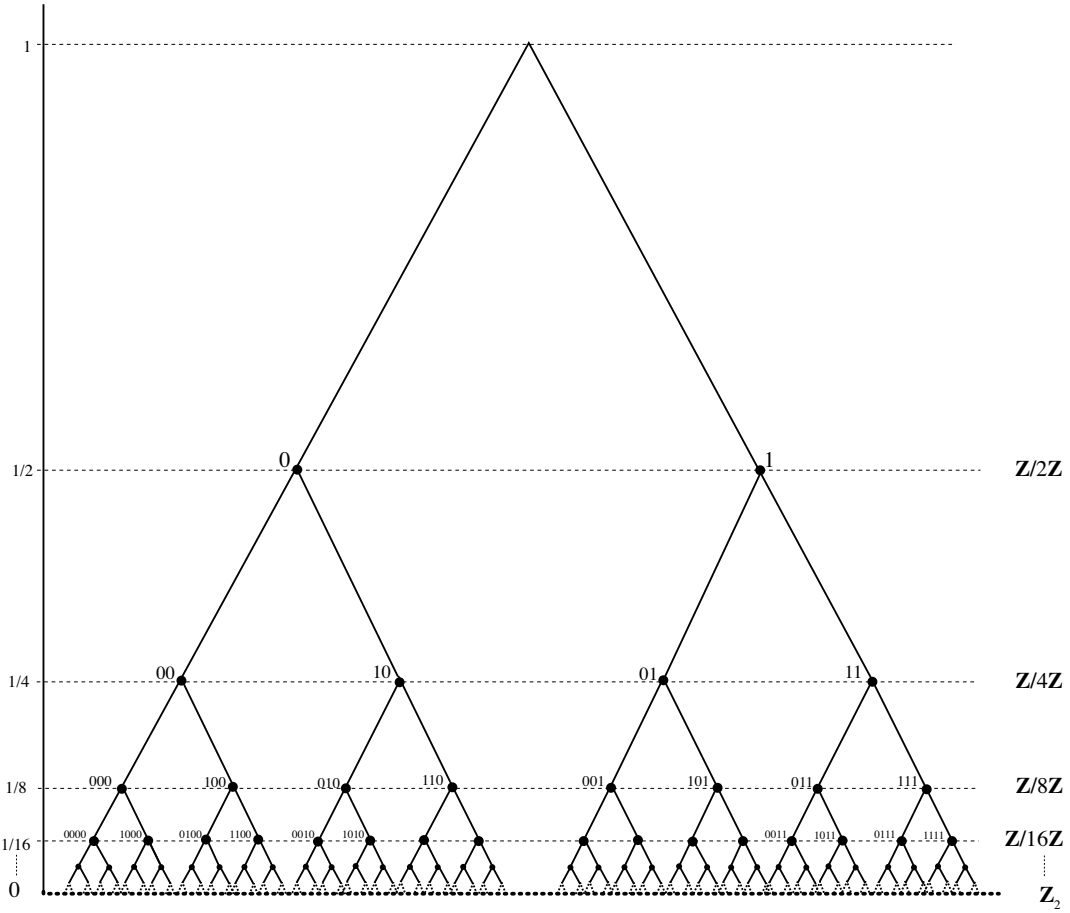

FIG. 4. L'arbre des entiers 2-adiques.

12.4.4. Une description arboricole des nombres p-adiques

La figure 4 ci-dessus fournit une description de $\mathbf{Z}_2$ comme limite (projective) des $\mathbf{Z}/2^n\mathbf{Z}$:

• Les éléments de $\mathbf{Z}_2$ correspondent aux bouts des branches de l'arbre infini (pour obtenir une description analogue de $\mathbf{Z}_p$, il suffit de remplacer l'arbre de la figure par un arbre dans lequel il part, de chacun des noeuds, p branches, numérotées de 0 à $p-1$, au lieu de 2).

• Les ensembles $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, etc. sont identifiés à $\{0,1\}$, $\{0,1,2,3\}$, etc., mais les nombres sont tous écrits en base 2 (si on prend la ligne correspondant à $\mathbf{Z}/8\mathbf{Z}$, ces nombres apparaissent dans l'ordre $0,4,2,6,1,5,3,7$).

• On passe (en montant) de la ligne correspondant à $\mathbf{Z}/2^n\mathbf{Z}$ à celle correspondant à $\mathbf{Z}/2^{n-1}\mathbf{Z}$ en supprimant le premier chiffre du développement en base 2 (celui correspondant à 2^{n-1} dans ce développement), ce qui représente la réduction modulo 2^{n-1} de $\mathbf{Z}/2^n\mathbf{Z}$ dans $\mathbf{Z}/2^{n-1}\mathbf{Z}$.

• Dans l'autre sens, les deux branches partant d'un noeud a de la ligne correspondant à $\mathbf{Z}/2^{n-1}\mathbf{Z}$ aboutissent aux deux classes a et $a+2^{n-1}$ modulo 2^n ; si l'écriture en base 2 de a est $a_{n-2}\dots a_0$, celles de a et $a+2^{n-1}$ sont respectivement $0a_{n-2}\dots a_0$ et $1a_{n-2}\dots a_0$. A la limite, on obtient donc l'écriture en base 2 de l'élément de $\mathbf{Z}_2$ correspondant à la branche infinie de l'arbre.

• La distance entre deux entiers 2-adiques x et y se lit aussi sur l'arbre : c'est la moitié de la hauteur verticale parcourue pour aller de x à y en suivant l'arbre (ou, de manière équivalente, c'est la hauteur du noeud le plus bas appartenant aux branches de x et y). Par exemple, pour aller de 0 à -1, il faut remonter tout en haut, et donc la distance est 1 ; pour aller de $2=\dots00010$ à $\frac{-2}{3}=\dots101010$, il faut passer par le noeud 010 et la distance est $\frac{1}{8}$.

12.4.5. L'anneau des nombres complexes p-adiques

On peut essayer d'imiter la construction de $\mathbf{C}$ à partir de $\mathbf{R}$ pour obtenir des nombres complexes p-adiques. On procède donc de la manière suivante. On commence par rajouter à $\mathbf{Q}_p$ toutes les racines des polynômes à coefficients dans $\mathbf{Q}_p$, et on obtient ainsi un corps $\overline{\mathbf{Q}}_p$ algébriquement clos auquel on étend la norme p-adique $|\ |_p$ (cette étape ne se fait pas toute seule). Une différence avec le cas réel est qu'on est forcé de rajouter une infinité d'éléments et que le résultat n'est pas complet. On complète donc $\overline{\mathbf{Q}}_p$ pour la norme $|\ |_p$, et on obtient un corps $\mathbf{C}_p$ qui est complet et algébriquement clos, et qui est abstraitement isomorphe à $\mathbf{C}$. Le seul problème est que J. Tate (1966) a démontré que $\mathbf{C}_p$ ne contient pas d'analogue raisonnable de $2i\pi$, ce qui est un peu ennuyeux vu le rôle joué par $2i\pi$ dans le monde usuel (cf. la formule de Cauchy par exemple). Le problème a été résolu par J.-M. Fontaine (1982) qui a construit un anneau $\mathbf{B}^+_{\mathrm{dR}}$ (sa construction est assez compliquée...), l'anneau des *nombres complexes p-adiques*, qui contient un $2i\pi$ naturel, et qui est muni d'un morphisme d'anneaux surjectif $\theta : \mathbf{B}^+_{\mathrm{dR}} \to \mathbf{C}_p$ dont le noyau est engendré par le $2i\pi$ de Fontaine (ce qui explique qu'on ne le voit pas dans $\mathbf{C}_p$).

12.4.6. Fragments d'analyse p-adique

L'analyse p-adique a, au moins au début, un petit côté paradisiaque quand on la compare à l'analyse réelle (la vie serait nettement plus agréable si on disposait d'une description de $\mathscr{C}([0,1],\mathbf{R})$ aussi simple que celle de $\mathscr{C}(\mathbf{Z}_p,\mathbf{Q}_p)$ fournie par le théorème de Mahler ci-dessous).

Soit $\mathscr{C}(\mathbf{Z}_p,\mathbf{Q}_p)$ l'ensemble des fonctions continues de $\mathbf{Z}_p$ dans $\mathbf{Q}_p$. Comme $\mathbf{Z}_p$ est compact, une fonction continue sur $\mathbf{Z}_p$ est bornée. Ceci permet de munir $\mathscr{C}(\mathbf{Z}_p,\mathbf{Q}_p)$ de la norme $\|\ \|_\infty$ de la convergence uniforme, définie par $\|f\|_\infty = \sup_{x\in\mathbf{Z}_p}|f(x)|_p$. Une limite uniforme de fonctions continues étant continue, l'espace $\mathscr{C}(\mathbf{Z}_p,\mathbf{Q}_p)$ est complet. Par ailleurs, la norme $\|\ \|_\infty$ vérifie l'inégalité ultramétrique $\|f+g\|_\infty \leqslant \sup(\|f\|_\infty,\|g\|_\infty)$; en effet, on a $|(f+g)(x)|_p \leqslant \sup(|f(x)|_p,|g(x)|_p)$, pour tout $x\in\mathbf{Z}_p$.

Si $n\in\mathbf{N}$, soit $\binom{x}{n}$ le *polynôme binomial*, défini par

$$\binom{x}{n} = \begin{cases} 1 & \text{si } n=0 \\ \dfrac{x(x-1)\dots(x-n+1)}{n!} & \text{si } n\geqslant 1. \end{cases}$$

• $\|\binom{x}{n}\|_\infty = 1$.

On a $\binom{n}{n} = 1$ et donc $\|\binom{x}{n}\|_\infty \geqslant 1$. D'autre part, $\binom{k}{n}$ est le nombre de manières de choisir n objets parmi k et est donc entier. On en déduit que $|\binom{k}{n}|_p \leqslant 1$, pour tout $k \in \mathbf{N}$, et $\mathbf{N}$ étant dense dans $\mathbf{Z}_p$, cela implique que $|\binom{x}{n}|_p \leqslant 1$ quel que soit $x \in \mathbf{Z}_p$; d'où le résultat.

On définit la k-ième *dérivée discrète* $f^{[k]}$ d'une fonction f par récurrence à partir des formules $f^{[0]} = f$ et $f^{[k+1]}(x) = f^{[k]}(x+1) - f^{[k]}(x)$, et le k-ième *coefficient de Mahler* de f par $a_k(f) = f^{[k]}(0)$. On a aussi

$$f^{[k]}(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(x+k-i) \quad \text{et} \quad a_k(f) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(k-i).$$

• Si k est un entier $\geqslant 1$, alors $\binom{p^k}{i}$ est divisible par p, si $1 \leqslant i \leqslant p^k - 1$.

En écrivant de deux manières la dérivée de $(1+\mathrm{X})^{p^k}$, on obtient $i\binom{p^k}{i} = p^k\binom{p^k-1}{i-1}$; on en déduit la divisibilité de $i\binom{p^k}{i}$ par p^k et celle de $\binom{p^k}{i}$ par p, si $1 \leqslant i \leqslant p^k - 1$.

• Si $f \in \mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$, il existe $k \in \mathbf{N}$ tel que $\|f^{[p^k]}\|_\infty \leqslant p^{-1}\|f\|_\infty$.

Comme $\mathbf{Z}_p$ est compact, f est uniformément continue et il existe $k \in \mathbf{N}$ tel que l'on ait $|f(x+p^k) - f(x)|_p \leqslant p^{-1}\|f\|_\infty$, quel que soit $x \in \mathbf{Z}_p$. Maintenant,

$$f^{[p^k]}(x) = f(x+p^k) - f(x) + \Big(\sum_{i=1}^{p^k-1} (-1)^i \binom{p^k}{i} f(x+p^k-i)\Big) + (1+(-1)^{p^k}) f(x).$$

Tous les termes de la somme $\sum_{i=1}^{p^k-1}$ ont, d'après le point précédent, une norme $\leqslant p^{-1}\|f\|_\infty$, et $(1+(-1)^{p^k})f(x)$ est nul si $p \neq 2$ et de norme $\leqslant p^{-1}\|f\|_\infty$ si $p = 2$. Comme on a choisi k de telle sorte que $|f(x+p^k) - f(x)|_p \leqslant p^{-1}\|f\|_\infty$ quel que soit $x \in \mathbf{Z}_p$, l'ultramétricité de $\| \ \|_\infty$ implique que $\|f^{[p^k]}\|_\infty \leqslant p^{-1}\|f\|_\infty$, ce qui permet de conclure.

Théorème 12.3. — (Mahler, 1958) *Si $f \in \mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$, alors*
(i) $\lim_{n\to+\infty} a_n(f) = 0$,
(ii) *f est la somme de la série $\sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$; en particulier, pour tout $x \in \mathbf{Z}_p$, on a $\sum_{n=0}^{+\infty} a_n(f)\binom{x}{n} = f(x)$.*
(iii) $\|f\|_\infty = \sup_{n\in\mathbf{N}} |a_n(f)|_p$.

Une utilisation répétée du point précédent permet de montrer que, si $\varepsilon > 0$ et si $f \in \mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$, il existe $k \in \mathbf{N}$ tel que $\|f^{[p^k]}\|_\infty \leqslant \varepsilon$. Maintenant, si $n \geqslant p^k$, alors $a_n(f)$ est une combinaison linéaire à coefficients entiers des $f^{[p^k]}(i)$, avec $i \in \mathbf{N}$. On en déduit l'inégalité $|a_n(f)| \leqslant \|f^{[p^k]}\|_\infty$ si $n \geqslant p^k$, qui montre que $a_n(f)$ tend vers 0 quand n tend vers $+\infty$; d'où le (i).

Il résulte du (a), de ce que $\|\binom{x}{n}\|_\infty = 1$, et de l'ultramétricité de $\| \ \|_\infty$, que la série $\sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$; notons g sa somme. Comme $\binom{x+1}{n+1} - \binom{x}{n+1} = \binom{x}{n}$, une récurrence immédiate nous fournit la formule $g^{[k]}(x) = \sum_{n=0}^{+\infty} a_{n+k}(f)\binom{x}{n}$, et on a donc $a_k(g) = a_k(f)$, pour tout k. En revenant à la formule donnant $a_k(f)$ en fonction des valeurs de f sur $\mathbf{N}$, on en déduit que $f(k) = g(k)$, pour tout $k \in \mathbf{N}$; comme $\mathbf{N}$ est dense dans $\mathbf{Z}_p$ et f et g sont continues sur $\mathbf{Z}_p$, cela implique $f = g$, ce qui démontre le (ii).

Enfin, $\|f\|_\infty \leqslant \sup_{n\in\mathbf{N}} |a_n(f)|_p$ car $f = \sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ et $\|\binom{x}{n}\|_\infty = 1$, et $|a_n(f)|_p \leqslant \|f\|_\infty$ car $a_n(f)$ est une combinaison linéaire, à coefficients entiers des $\phi(k)$, pour $k \in \mathbf{N}$. On a donc $\|f\|_\infty \geqslant \sup_{n\in\mathbf{N}} |a_n(f)|_p$, ce qui permet de conclure.

Remarque 12.4. — On a démontré en passant que, si $(a_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{Q}_p$ tendant vers 0, alors $\sum_{n=0}^{+\infty} a_n \binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ vers une fonction dont les coefficients de Mahler sont les a_n.

Exercice 12.5. — Si X, Y sont des espaces topologiques, on dit que $f : \mathrm{X} \to \mathrm{Y}$ est *localement constante* si tout $x \in \mathrm{X}$ admet un voisinage sur lequel f est constante.

(i) Montrer que f est localement constante si et seulement si $\{x \in \mathrm{X},\ f(x) = y\}$ est ouvert pour tout $y \in \mathrm{Y}$. En déduire qu'une fonction localement constante est continue.

(ii) Quelles sont les fonctions localement constantes sur $[0, 1]$?

(iii) Montrer que la fonction caractéristique $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ de $a + p^n\mathbf{Z}_p$ est localement constante pour tous $a \in \mathbf{Z}_p$ et $n \in \mathbf{N}$.

(iv) Montrer que, si $\phi : \mathbf{Z}_p \to \mathrm{Y}$ est localement constante, il existe $n \in \mathbf{N}$ tel que ϕ soit constante sur $a + p^n\mathbf{Z}_p$, pour tout $a \in \mathbf{Z}_p$.

(v) Montrer que, si $\mathrm{Y} = \mathbf{R}$ ou $\mathbf{Q}_p$, les fonctions localement constantes de $\mathbf{Z}_p$ dans Y sont denses dans les fonctions continues (munies de la norme de la convergence uniforme).

(vi) Construire une fonction continue surjective de $\mathbf{Z}_p$ sur $[0, 1]$. Quelles sont les fonctions continues de $[0, 1]$ dans $\mathbf{Z}_p$?

Exercice 12.6. — (i) Montrer que $\sum_{n=0}^{+\infty} \binom{1/2}{n} \left(\frac{7}{9}\right)^n$ converge vers $\frac{-4}{3}$ dans $\mathbf{Q}_7$. (On pourra considérer la fonction $x \mapsto \sum_{n=0}^{+\infty} \left(\frac{7}{9}\right)^n \binom{x}{n}$ et ses valeurs aux entiers.)

(ii) Quelle la somme de la série $\sum_{n=0}^{+\infty} \binom{1/2}{n} \left(\frac{7}{9}\right)^n$ dans $\mathbf{R}$?

13. Corrigé des exercices

Exercice 1.1. (i) Si $a = 0$ ou $b = 0$, on a $a\mathbf{Z} \cap b\mathbf{Z} = \{0\}$ et $\mathrm{ppcm}(a, b) = 0$ puisque le seul multiple de 0 est 0. Si $a \neq 0$ et $b \neq 0$, alors $a\mathbf{Z} \cap b\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ comme intersection de deux sous-groupes, qui n'est pas réduit à 0 puisqu'il contient ab. Il existe donc $m \in \mathbf{N}$ tel que $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$. Alors m est un multiple de a (car $a \in m\mathbf{Z}$) et de b (car $b \in m\mathbf{Z}$). Donc $\mathrm{ppcm}(a, b) \mid m$. Réciproquement, si c est un multiple de a et b, alors $c \in a\mathbf{Z}$ et $c \in b\mathbf{Z}$ et donc $c \in m\mathbf{Z}$ et $m \mid c$. En particulier, $m \mid \mathrm{ppcm}(a, b)$, et donc $m = \mathrm{ppcm}(a, b)$, ce qu'il fallait démontrer.

(ii) On a $a \mid c$ (resp. $b \mid c$) si et seulement si $v_p(a) \leqslant v_p(c)$ (resp. $v_p(b) \leqslant v_p(c)$), pour tout $p \in \mathscr{P}$. Donc c est un multiple de a et b si et seulement si $v_p(c) \geqslant \sup(v_p(a), v_p(b))$, pour tout $p \in \mathscr{P}$. Le plus petit entier multiple de a et b est donc $\prod_{p\in\mathscr{P}} p^{\sup(v_p(a),v_p(b))}$, ce qu'il fallait démontrer.

Exercice 1.2. (i) Si $a = 0$ ou $b = 0$, on a $v_p(ab) = v_p(a) + v_p(b)$ car les deux membres valent $+\infty$. Si $a \neq 0$ et $b \neq 0$, on a $a = \mathrm{sign}(a) \prod_{p\in\mathscr{P}} p^{v_p(a)}$, $b = \mathrm{sign}(b) \prod_{p\in\mathscr{P}} p^{v_p(b)}$ et

$$ab = \mathrm{sign}(ab) \prod_{p\in\mathscr{P}} p^{v_p(ab)} = \mathrm{sign}(a)\mathrm{sign}(b) \prod_{p\in\mathscr{P}} p^{v_p(a)+v_p(b)}.$$

On déduit de l'unicité de la décomposition en produit de facteurs premiers que $\mathrm{sign}(ab) = \mathrm{sign}(a)\mathrm{sign}(b)$ et $v_p(ab) = v_p(a) + v_p(b)$, pour tout $p \in \mathscr{P}$.

Maintenant, si $m = \inf(v_p(a), v_p(b))$, alors $p^m \mid a$ et $p^m \mid b$, ce qui implique $p^m \mid a + b$ et donc $v_p(a + b) \geqslant m$, ce qu'on cherchait à démontrer.

(ii) Si $x = \frac{a}{b}$, avec $a \in \mathbf{Z}$ et $b \in \mathbf{Z} - \{0\}$, on doit avoir $v_p(x) = v_p(a) - v_p(b)$, et il faut vérifier que cela ne dépend pas de l'écriture choisie. Or, si $\frac{a'}{b'} = \frac{a}{b}$, on a $ab' = ba'$ et donc $v_p(a) + v_p(b') = v_p(b) + v_p(a')$ et $v_p(a) - v_p(b) = v_p(a') - v_p(b')$, ce qui prouve que $v_p(x)$ est bien défini. De plus, si $y = \frac{c}{d}$, alors $v_p(xy) = v_p(\frac{ac}{bd}) = v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - v_p(b) - v_p(d) = v_p(x) + v_p(y)$. Enfin, si $x, y \in \mathbf{Q}$ et si $c \in \mathbf{N} - \{0\}$ est tel que $cx, cy \in \mathbf{Z}$, on a $v_p(c(x + y)) \geqslant \inf(v_p(cx), v_p(cy))$ et donc

$$v_p(c) + v_p(x + y) \geqslant \inf(v_p(c) + v_p(x), v_p(c) + v_p(y)) = v_p(c) + \inf(v_p(x), v_p(y)),$$

et comme $v_p(c)$ est fini, cela permet de conclure.

(iii) Si $\sqrt{2}$ est rationnel, il existe $x \in \mathbf{Q}$ tel que $x^2 = 2$. On a alors $2v_2(x) = 1$, ce qui est impossible puisque $v_2(x) \in \mathbf{Z}$.

Exercice 1.3. (i) On a $n! = \prod_{k=1}^{n} k$ et donc $v_p(n!) = \sum_{k=1}^{n} v_p(k)$. Or il y a exactement $[\frac{n}{p^i}] - [\frac{n}{p^{i+1}}]$ entiers $\leqslant n$ vérifiant $v_p(k) = i$ (les multiples de p^i privés des multiples de p^{i+1}). On en déduit que $v_p(n!) = \sum_{i=1}^{+\infty} i\big([\frac{n}{p^i}] - [\frac{n}{p^{i+1}}]\big) = \sum_{i=1}^{+\infty} [\frac{n}{p^i}](i - (i-1)) = \sum_{i=1}^{+\infty} [\frac{n}{p^i}]$.

Maintenant, si $n = a_0 + a_1 p + \cdots + a_r p^r$, où $a_i \in \{0, \ldots, p-1\}$, pour tout i, alors $[\frac{n}{p^i}] = a_i + \cdots + a_r p^{r-i}$ et donc

$$\begin{aligned}\sum_{i=1}^{+\infty} [\frac{n}{p^i}] &= \sum_{i=1}^{r} \big(\sum_{s=i}^{r} a_s p^{s-i}\big) = \sum_{s=1}^{r}\sum_{i=1}^{s} a_s p^{s-i} \\ &= \sum_{s=1}^{r} a_s p^{s-1}\big(\frac{1-p^{-s}}{1-p^{-1}}\big) = \sum_{s=1}^{r} a_s\big(\frac{p^s-1}{p-1}\big) = \sum_{s=0}^{r} a_s\big(\frac{p^s-1}{p-1}\big) = \frac{n - \mathrm{S}_p(n)}{p-1}.\end{aligned}$$

(ii) La fonction $x \mapsto [x] - \left[\frac{x}{2}\right] - \left[\frac{x}{3}\right] - \left[\frac{x}{5}\right] + \left[\frac{x}{30}\right]$ prend des valeurs entières. Par ailleurs, elle est aussi égale à $\left\{\frac{x}{2}\right\} + \left\{\frac{x}{3}\right\} + \left\{\frac{x}{5}\right\} - \left\{\frac{x}{30}\right\}$, ce qui montre qu'elle est périodique de période 30 et > -1 sur $[0, 30[$; elle est donc toujours $\geqslant 0$. L'intégralité de $a_n = \frac{(30n)!\, n!}{(15n)!\, (10n)!\, (6n)!}$ s'en déduit en calculant la valuation p-adique de a_n, pour tout p.

Exercice 1.4. L'ensemble $\mathscr{P}(\mathbf{N})$ est en bijection avec $\{0, 1\}^{\mathbf{N}}$ (on associe à $\mathrm{X} \subset \mathbf{N}$ la suite $(x_k)_{k\in\mathbf{N}}$ définie par $x_k = 1$ si $k \in \mathrm{X}$ et $x_k = 0$ si $k \notin \mathrm{X}$) ; il n'est donc pas dénombrable.

L'ensemble des parties finies de $\mathbf{N}$ est la réunion, pour $n \in \mathbf{N}$, de l'ensemble des parties de $\{0, \dots, n\}$; il est donc dénombrable en tant que réunion dénombrable d'ensembles finis.

Exercice 1.5. Si n est fixé, l'ensemble $\mathbf{Q}[\mathrm{X}]^{(n)}$ des polynômes de $\mathbf{Q}[\mathrm{X}]$ de degré n s'injecte dans $\mathbf{Q}^{n+1}$ en envoyant $\mathrm{P} = a_n\mathrm{X}^n + \cdots + a_0$ sur $(a_n, \dots, a_0)$; il est donc dénombrable puisque $\mathbf{Q}$ l'est. On en déduit que $\mathbf{Q}[\mathrm{X}] = \cup_{n\in\mathbf{N}}\mathbf{Q}[\mathrm{X}]^{(n)}$ est dénombrable comme réunion dénombrable d'ensembles dénombrables. Enfin, un polynôme n'ayant qu'un nombre fini de racines dans $\mathbf{C}$, l'ensemble $\overline{\mathbf{Q}}$ est une réunion dénombrable (d'après ce qui précède) d'ensembles finis, et donc est dénombrable.

L'ensemble des nombres transcendants n'est pas dénombrable (sinon $\mathbf{R}$ le serait comme réunion de deux ensembles dénombrables) ; en particulier, il est non vide.

Exercice 1.6. Si on choisit dans chaque disque un point de la forme $a + ib$, avec $a, b \in \mathbf{Q}$, on obtient une injection de I dans $\mathbf{Q}^2$, et comme $\mathbf{Q}^2$ est dénombrable puisque $\mathbf{Q}$ l'est, cela permet de conclure.

Exercice 1.7. (i) Soit $a = \inf_{x>x_0} f(x)$. Par définition de a, on a $f(x) \geqslant a$, si $x > x_0$, et pour tout $\varepsilon > 0$, il existe $x_\varepsilon > x_0$ tel que $f(x_\varepsilon) < a + \varepsilon$. Soit $\delta = x_\varepsilon - x_0$. Comme f est croissante, on a $a \leqslant f(x) < a + \varepsilon$, pour tout $x \in]x_0, x_0 + \delta[$, ce qui prouve que f a une limite à droite $f(x_0^+)$ en x_0, égale à a. La limite à gauche s'étudie exactement de la même manière (ou peut se déduire de ce qu'on vient de faire en étudiant $g(x) = -f(-x)$ en $-x_0$).

Maintenant, comme f est croissante, on a $f(x_0^-) = \sup_{x<x_0} f(x) \leqslant f(x_0) \leqslant \inf_{x>x_0} f(x) = f(x_0^+)$. Comme f admet des limites à gauche et à droite en x_0, elle est continue en x_0 si et seulement si $f(x_0^-) = f(x_0) = f(x_0^+)$, et donc si et seulement si $f(x_0^-) = f(x_0^+)$.

(ii) Comme f est croissante, on a $f(x_0^+) = \inf_{x>x_0} f(x) = \inf_{x_1>x>x_0} f(x) \leqslant \sup_{x_0<x<x_1} f(x) = \sup_{x<x_1} f(x) = f(x_1^-)$.

(iii) Soit $x \in \mathrm{D}$ un point de discontinuité. On a alors $f(x^-) < f(x^+)$, ce qui permet de choisir un élément $r(x) \in \mathbf{Q}$ dans l'intervalle $]f(x^-), f(x^+)[$. Si $x_1 < x_2$ sont deux éléments de D, on a $r(x_1) < f(x_1^+) \leqslant f(x_2^-) < r(x_2)$, ce qui prouve que $x \mapsto r(x)$ est une injection de D dans $\mathbf{Q}$, et $\mathbf{Q}$ étant dénombrable, cela implique que D est dénombrable.

Exercice 1.8. Par construction, la suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ est alternée ; l'intersection des $[x_{\varphi(n)}, x_{\varphi(n+1)}]$ (ou $[x_{\varphi(n+1)}, x_{\varphi(n)}]$) est donc un intervalle $[a, b]$, et il s'agit de prouver qu'il est réduit à un point pour prouver que $(x_{\varphi(n)})_{n\in\mathbf{N}}$ a une limite. Si ce n'est pas le cas, il existe $i \in \mathbf{N}$ tel que $x_i \in [a, b]$, et il existe $n \in \mathbf{N}$ tel que $\varphi(n) < i < \varphi(n+1)$. Alors x_i est entre $x_{\varphi(n)}$ et $x_{\varphi(n-1)}$, ce qui est contraire à la définition de $\varphi(n+1)$. Si la limite de $(x_{\varphi(n)})_{n\in\mathbf{N}}$ appartient à X, alors cette limite est de la forme x_i, et si $\varphi(n) < i < \varphi(n+1)$, on aboutit, comme ci-dessus, à une contradiction avec la définition de $\varphi(n+1)$. La limite n'appartient donc pas à X.

Maintenant, si $\mathbf{R}$ était dénombrable, on pourrait lui appliquer ce qui précède et construire un élément de $\mathbf{R}$ n'appartenant pas à $\mathbf{R}$...

Exercice 1.9. Soit $(\mathrm{H}_i)_{i\in\mathrm{I}}$ une famille de huit dans le plan, deux à deux disjoints. Si H_i est constitué des cercles $\mathrm{C}_{i,1}$ et $\mathrm{C}_{i,2}$, choisissons un point $\mathrm{P}_{i,1}$ (resp. $\mathrm{P}_{i,2}$) à coordonnées rationnelles dans le disque $\mathrm{D}_{i,1}$ (resp. $\mathrm{D}_{i,2}$) délimité par $\mathrm{C}_{i,1}$ (resp. $\mathrm{C}_{i,2}$). On obtient de la sorte une application de I dans $\mathbf{Q}^4$. Soient $i \neq j$ deux éléments de I. Si $\mathrm{P}_{i,1} = \mathrm{P}_{j,1}$, alors l'un des disques $\mathrm{D}_{i,1}$ et $\mathrm{D}_{j,1}$ contient l'autre puisque les cercles $\mathrm{C}_{i,1}$ et $\mathrm{C}_{j,1}$ sont disjoints. Quitte à permuter i et j, on peut supposer que c'est $\mathrm{D}_{i,1}$ qui contient $\mathrm{D}_{j,1}$, mais alors $\mathrm{D}_{i,1}$ contient aussi le point de contact entre $\mathrm{C}_{j,1}$ et $\mathrm{C}_{j,2}$, et donc aussi le cercle $\mathrm{C}_{j,2}$ tout entier puisque $\mathrm{C}_{j,2}$ et $\mathrm{C}_{i,1}$ sont disjoints, et donc aussi le disque $\mathrm{D}_{j,2}$ et le point $\mathrm{P}_{j,2}$. Comme il ne contient pas $\mathrm{P}_{i,2}$ par construction, on en déduit que $i \mapsto (\mathrm{P}_{i,1}, \mathrm{P}_{i,2})$ est injective, et comme $\mathbf{Q}^4$ est dénombrable, il en est de même de I.

Exercice 1.10. L'idée est de prouver que deux tripodes disjoints ne peuvent pas être trop proches. Soient donc Y et Y′ deux tripodes de sommets respectifs $(\mathrm{A}, \mathrm{B}, \mathrm{C})$ et $(\mathrm{A}', \mathrm{B}', \mathrm{C}')$ et de centres de gravité G

et G′. Soit $r = d(\mathrm{G}, \mathrm{A})$. Si $d(\mathrm{A}, \mathrm{A}')$, $d(\mathrm{B}, \mathrm{B}')$ et $d(\mathrm{C}, \mathrm{C}')$ sont toutes trois $< \frac{r}{2}$, on a aussi $d(\mathrm{G}, \mathrm{G}') < \frac{r}{2}$ et un petit dessin montre que suivant le tiers de plan dans lequel se trouve G′, l'un des segments $[\mathrm{G}', \mathrm{A}']$, $[\mathrm{G}', \mathrm{B}']$ ou $[\mathrm{G}', \mathrm{C}']$ rencontre Y. Maintenant, soit $(\mathrm{Y}_i)_{i\in \mathrm{I}}$ une famille de tripodes dans le plan, deux à deux disjoints. Si $i \in \mathrm{I}$, soient $\mathrm{A}_i, \mathrm{B}_i, \mathrm{C}_i$ les sommets de Y_i, G_i le centre de gravité de $(\mathrm{A}_i, \mathrm{B}_i, \mathrm{C}_i)$ et $r_i = d(\mathrm{G}_i, \mathrm{A}_i)$. Choisissons pour tout i un triplet $(\mathrm{P}_{i,1}, \mathrm{P}_{i,2}, \mathrm{P}_{i,3})$ de points à coordonnées rationnelles, avec $d(\mathrm{A}_i, \mathrm{P}_{i,1}) < \frac{r_i}{4}$, $d(\mathrm{B}_i, \mathrm{P}_{i,2}) < \frac{r_i}{4}$ et $d(\mathrm{C}_i, \mathrm{P}_{i,3}) < \frac{r_i}{4}$. Il résulte de la discussion préliminaire que l'on obtient ainsi une injection de I dans $\mathbf{Q}^6$, ce qui prouve que I est dénombrable.

Exercice 2.1. Soit $m = \mathrm{ppcm}(a, b)$. Comme a et b ne sont pas premiers entre eux, on a $m < |ab|$. Or m annule tout élément de $\mathbf{Z}/a\mathbf{Z}$ puisque c'est un multiple de a et tout élément de $\mathbf{Z}/b\mathbf{Z}$ puisque c'est un multiple de b ; on a donc $mx = 0$, pour tout $x \in (\mathbf{Z}/a\mathbf{Z}) \oplus (\mathbf{Z}/b\mathbf{Z})$. Or m n'annule pas 1 dans $\mathbf{Z}/ab\mathbf{Z}$ puisque $m < |ab|$ n'est pas un multiple de ab.

Exercice 2.2. 4 admet 16 comme inverse dans $\mathbf{Z}/21\mathbf{Z}$; l'équation $4x + 3 = 0$ est donc équivalente à $x + 48 = 0$, soit $x = -48 = 3 \times 21 - 48 = 15$.

$14x$ est multiple de 7 dans $\mathbf{Z}/21\mathbf{Z}$, ce que -2 n'est pas. L'équation $14x + 2 = 0$ n'a donc pas de solution dans $\mathbf{Z}/21\mathbf{Z}$.

$14x + 7 = 0$ dans $\mathbf{Z}/21\mathbf{Z}$ équivaut à $7(2x + 1) = 0$ dans $\mathbf{Z}/21\mathbf{Z}$, soit encore à $2x + 1$ multiple de 3 dans $\mathbf{Z}/21\mathbf{Z}$. Les solutions sont donc 1, 4, 7, 10, 13, 16 et 19 modulo 21.

Exercice 2.3. On a $91 = 7 \times 13$ et donc $\mathbf{Z}/91\mathbf{Z} = \mathbf{F}_7 \times \mathbf{F}_{13}$, ce qui nous ramène à trouver les solutions dans les corps $\mathbf{F}_7$ et $\mathbf{F}_{13}$. On remarque que 2 est racine dans $\mathbf{F}_7$, et comme la somme des racines vaut -1, l'autre est $-3 = 4$. De même 3 est racine dans $\mathbf{F}_{13}$, et donc l'autre est $-1 - 3 = -4 = 9$. On est alors confronté au problème de trouver quels sont les éléments de $\mathbf{Z}/91\mathbf{Z}$ correspondant aux couples $(2, 3)$, $(2, 9)$, $(4, 3)$ et $(4, 9)$ de $\mathbf{F}_7 \times \mathbf{F}_{13}$. Pour cela, on remarque que $1 = 2 \times 7 - 13$, et donc que $14 = 2 \times 7$ a pour image 0 dans $\mathbf{F}_7$ et pour image 1 dans $\mathbf{F}_{13}$, alors que -13 a pour image 1 dans $\mathbf{F}_7$ et pour image 0 dans $\mathbf{F}_{13}$. On en déduit, que si $(a, b) \in \mathbf{Z}$, alors $-13a + 14b \in \mathbf{Z}$ ne dépend modulo 91 que des réductions de a et b modulo 7 et 13 respectivement, et l'image de $-13a + 14b$ dans $\mathbf{F}_7 \times \mathbf{F}_{13}$ est (a, b). Les solutions de l'équation $x^2 + x + 1 = 0$ dans $\mathbf{Z}/91\mathbf{Z}$ sont donc $-13 \cdot 2 + 14 \cdot 3 = 16$, $-13 \cdot 2 + 14 \cdot 9 = 100 = 9$, $-13 \cdot 4 + 14 \cdot 3 = -10$ et $-13 \cdot 4 + 14 \cdot 9 = 74 = -17$.

Exercice 2.4. (i) Si a est solution de l'équation $x^2 + x + 1 = 0$, alors $-1 - a$ aussi. Or le système d'équations $x^2 + x + 1 = 0$ et $2x = -1$ est équivalent à $2x = -1$ et $x(x - 1) = 0$. Comme $\mathbf{F}_p$ est un corps, $x(x - 1) = 0$ équivaut à $x = 0$ ou $x = 1$, ce qui est incompatible avec $2x = -1$, sauf si $2 \cdot 1 = -1$, c'est-à-dire si $3 = 0$, et donc si $p = 3$. On en déduit que, si $p \neq 3$, l'équation $x^2 + x + 1 = 0$ a deux solutions dans $\mathbf{F}_p$ si et seulement si elle en a au moins une.

(ii) D'après le (i), si $p \neq 3$, l'équation $x^2 + x + 1 = 0$ a deux solution modulo p, s'il existe $n \in \mathbf{N}$ tel que p divise $n^2 + n + 1$. Supposons, par l'absurde, que l'ensemble des p vérifiant ceci est fini. Cela signifie qu'il existe des nombres premiers $p_1, \cdots, p_k$ tels que pour tout $n \in \mathbf{N}$, il existe $a_1, \ldots, a_k \in \mathbf{N}$ tels que $n^2 + n + 1 = p_1^{a_1} \cdots p_k^{a_k}$. Si $n \leqslant \mathrm{X} - 1$, cela implique que $n^2 + n + 1 \leqslant \mathrm{X}^2$, et donc que chacun des a_i vérifie $a_i \leqslant \frac{\log \mathrm{X}^2}{\log p_i} \leqslant \frac{2}{\log 2} \log \mathrm{X}$; on en déduit que $n^2 + n + 1$ peut prendre au plus $(\frac{2}{\log 2} \log \mathrm{X})^k$ valeurs pour $n \leqslant \mathrm{X} - 1$, ce qui est absurde pour X tendant vers $+\infty$, les valeurs de $n^2 + n + 1$ étant toutes distinctes pour $n \geqslant 0$.

(iii) Il existe un ensemble infini $\{p_1, p_2, \ldots\}$ de nombres premiers tels que l'équation $x^2 + x + 1 = 0$ ait deux solutions dans $\mathbf{F}_p$. Soit $\mathrm{D}_k = p_1 \cdots p_k$. D'après le théorème des restes chinois, $\mathbf{Z}/\mathrm{D}_k\mathbf{Z} = \prod_{i=1}^{k} \mathbf{F}_{p_i}$, et comme l'équation $x^2 + x + 1 = 0$ a deux solutions dans $\mathbf{F}_{p_i}$, pour tout i, elle en a 2^k dans $\mathbf{Z}/\mathrm{D}_k\mathbf{Z}$. Comme 2^k peut être rendu arbitrairement grand, cela permet de conclure.

Exercice 2.5. Les éléments inversibles de $\mathbf{Z}/p^n\mathbf{Z}$ sont en bijection avec les éléments de $\{0, 1, \ldots, p^n - 1\}$ qui sont premiers à p^n. Or être premier à p^n est équivalent à être premier à p d'après le lemme de Gauss

et donc aussi à ne pas être divisible par p, puisque p est premier. Comme il y a p^{n-1} multiples de p dans $\{0, 1, \dots, p^n - 1\}$, on en déduit que $|(\mathbf{Z}/p^n\mathbf{Z})^*| = p^n - p^{n-1}$.

Maintenant, si $\mathrm{D} \geqslant 2$ est quelconque, on peut factoriser D sous la forme $\mathrm{D} = \prod_{p|\mathrm{D}} p^{n_p}$, avec $n_p \geqslant 1$, et le théorème des restes chinois nous dit que l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est isomorphe à $\prod_{p|\mathrm{D}}(\mathbf{Z}/p^{n_p}\mathbf{Z})$. On a donc $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^* = \prod_{p|\mathrm{D}}(\mathbf{Z}/p^{n_p}\mathbf{Z})^*$, ce qui nous donne

$$\varphi(\mathrm{D}) = \prod_{p|\mathrm{D}}(p^{n_p} - p^{n_p-1}) = \mathrm{D}\prod_{p|\mathrm{D}}\big(1 - \frac{1}{p}\big).$$

Exercice 2.7. (i) Si $v_1 = (x_1, y_1)$ et $v_2 = (x_2, y_2)$ engendrent la même droite, il existe $\alpha \in \mathrm{K}^*$ tel que $v_2 = \alpha v_1$, et on a $\lambda(v_2) = \frac{x_2}{y_2} = \frac{\alpha x_1}{\alpha y_1} = \frac{x_1}{y_1} = \lambda(v_1)$, ce qui prouve que $\lambda(v)$ ne dépend que de la droite engendrée par v, et donc que λ induit une application de $\mathbf{P}^1(\mathrm{K})$ dans $\mathrm{K} \cup \{\infty\}$. Cette application est injective car « $\lambda(v_1) = \lambda(v_2)$ » équivaut à « $x_1y_2 = x_2y_1$ », et donc « à v_1 et v_2 colinéaires ». Elle est surjective car $(1, 0)$ s'envoie sur ∞ et $(z, 1)$ sur z, si $z \in \mathrm{K}$. C'est donc une bijection.

(ii) Soit $z \in \mathrm{K} \cup \{\infty\}$, et soit $v = (x, y)$ tel que $\frac{x}{y} = \lambda(v) = z$. Alors, par définition, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \lambda\big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot v\big) = \lambda(ax + by, cx + dy) = \frac{ax+by}{cx+dy} = \frac{az+b}{cz+d}$.

Exercice 2.9. (i) Une isométrie u du carré permute ses sommets et laisse fixe son centre de gravité O. En particulier u est linéaire et est déterminée par l'image de deux points non colinéaires avec O, par exemple A et B. L'image de A doit appartenir à $\{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}\}$, et comme l'angle $\{u(\mathrm{A}), \mathrm{O}, u(\mathrm{B})\}$ doit être un angle droit, cela ne laisse que deux possibilités pour $u(\mathrm{B})$ pour chaque choix de $u(\mathrm{A})$. On en déduit que D_4 a au plus 8 éléments. Comme il contient l'identité id, la symétrie $-\mathrm{id}$ par rapport à O, les rotations ρ^+ et ρ^- de centre O et d'angles respectifs $\frac{\pi}{2}$ et $\frac{-\pi}{2}$, les symétries $\sigma_{\mathrm{A,C}}$ et $\sigma_{\mathrm{C,D}}$ par rapport aux deux diagonales, et les symétries σ_{H} et σ_{V} par rapport aux droites horizontale et verticale, on voit que D_4 a exactement 8 éléments qui sont ceux que nous venons d'énumérer.

(ii) S est de toute évidence stable par D_4, et il y a deux orbites :

• O est fixe par tout élément de D_4 ; son orbite est donc $\{\mathrm{O}\}$ et son stablisateur est D_4 ;

• on passe de A à B, C et D en itérant ρ^+, ce qui montre que l'orbite de A est $\{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}\}$ (elle ne peut contenir O puisque les orbites sont distinctes), et on détermine par inspection que le stabilisateur de A est le groupe à 2 éléments $\{\mathrm{id}, \sigma_{\mathrm{A,C}}\}$.

(iii) Les orbites de T sous l'action de D_4 sont au nombre de 3 :

• l'orbite de $\{\mathrm{O}, \mathrm{A}\}$ consiste en les 4 paires contenant O (on passe de $\{\mathrm{O}, \mathrm{A}\}$ aux autres en itérant ρ^+), et le stabilisateur de $\{\mathrm{O}, \mathrm{A}\}$ est $\{\mathrm{id}, \sigma_{\mathrm{A,C}}\}$;

• l'orbite de $\{\mathrm{A}, \mathrm{B}\}$ consiste en les 4 paires de sommets consécutifs (on passe de $\{\mathrm{A}, \mathrm{B}\}$ aux autres en itérant ρ^+), et le stabilisateur de $\{\mathrm{A}, \mathrm{B}\}$ est $\{\mathrm{id}, \sigma_{\mathrm{V}}\}$;

• l'orbite de $\{\mathrm{A}, \mathrm{C}\}$ consiste en les 2 paires de sommets oppososés $\{\mathrm{A}, \mathrm{C}\}$ et $\{\mathrm{B}, \mathrm{D}\}$, et le stabilisateur de $\{\mathrm{A}, \mathrm{C}\}$ est $\{\mathrm{id}, -\mathrm{id}, \sigma_{\mathrm{A,C}}, \sigma_{\mathrm{B,D}}\}$.

(iv) On remarque que dans tous les cas, le produit du cardinal de l'orbite par celui du stablisateur d'un de ses éléments est $8 = |\mathrm{D}_4|$; il s'agit d'un cas particulier d'un théorème général (si G opère sur X, si $x \in \mathrm{X}$, et si G_x est le stabilisateur de x, alors l'orbite O_x est isomorphe à G/G_x, et donc $|\mathrm{O}_x| = |\mathrm{G}|/|\mathrm{G}_x|$).

Exercice 2.10. (i) Les conditions $g \cdot x = x$ et $hgh^{-1} \cdot (h \cdot x) = h \cdot x$ sont équivalentes. Il en résulte que $x \mapsto h \cdot x$ induit une bijection de X_g sur $\mathrm{X}_{hgh^{-1}}$, ce qui répond au (a). Le (b) s'en déduit puisque si g et g' sont conjugués dans G, il existe h tel que $g' = hgh^{-1}$ et donc $x \mapsto h \cdot x$ induit une bijection de X_g sur $\mathrm{X}_{g'}$ qui, de ce fait, ont le même nombre d'éléments.

(ii) L'ensemble V_g des points fixes de g est l'espace propre associé à la valeur propre 1 ; c'est donc un sous-espace vectoriel de V. Par ailleurs, si $g' = hgh^{-1}$, alors $x \mapsto h \cdot x$ induit une bijection de V_g sur $\mathrm{V}_{g'}$

qui est linéaire puisque G opère linéairement. On en déduit que si l'un des deux espaces est de dimension finie, alors l'autre aussi et les deux dimensions sont les mêmes.

Exercice 3.3. $108 = 2^2 \times 3^3$, et donc $(\mathbf{Z}/108\mathbf{Z})^* \cong (\mathbf{Z}/4\mathbf{Z})^* \oplus (\mathbf{Z}/27\mathbf{Z})^*$. Or $(\mathbf{Z}/4\mathbf{Z})^* = \{\pm 1\}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$, et $(\mathbf{Z}/27\mathbf{Z})^*$ est un groupe de cardinal $\varphi(27) = 2 \cdot 9$ qui est donc isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/9\mathbf{Z})$ ou à $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z})$. Dans le second cas, tout élément de $(\mathbf{Z}/27\mathbf{Z})^*$ vérifierait $x^6 = 1$, or $2^6 = 64 \neq 1$ dans $(\mathbf{Z}/27\mathbf{Z})^*$. On a donc $(\mathbf{Z}/27\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/9\mathbf{Z})$ et $(\mathbf{Z}/108\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/9\mathbf{Z})$.

$200 = 2^3 \cdot 5^2$, et donc $(\mathbf{Z}/200\mathbf{Z})^* \cong (\mathbf{Z}/8\mathbf{Z})^* \oplus (\mathbf{Z}/25\mathbf{Z})^*$. Or $(\mathbf{Z}/8\mathbf{Z})^*$ est un groupe d'ordre 4 dans lequel tout les éléments sont d'ordre 2 (en effet, 1^2, 3^2, 5^2 et 7^2 sont congrus à 1 modulo 8) ; il est donc isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$. Par ailleurs, $\mathbf{Z}/25\mathbf{Z})^*$ est un groupe de cardinal $\varphi(25) = 4 \cdot 5$ qui est donc isomorphe à $(\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ ou à $(\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/5\mathbf{Z})$. Dans le second cas, toute puissance 5-ième serait d'ordre 2, or $2^5 = 32 = 7$ a un carré égal à $49 = -1 \neq 1$, et donc $(\mathbf{Z}/25\mathbf{Z})^* \cong (\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ et $(\mathbf{Z}/200\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$.

La solution ci-dessus est un peu artisanale ; on peut aller plus vite en utilisant les résultats de l'ex. 3.5.

Exercice 3.4. (i) Soit $\oplus_{p \in \mathscr{P}}(\oplus_i(\mathbf{Z}/p^{a_{p,i}}\mathbf{Z}))$ la décomposition de K^* fournie par le th. 3.1. Si K^* n'est pas cyclique, il existe p tel que $a_{p,2} \neq 0$; en effet, sinon on aurait $\mathrm{K}^* \cong \mathbf{Z}/\mathrm{D}\mathbf{Z}$, où $\mathrm{D} = \prod_p p^{a_{p,1}}$, d'après le théorème des restes chinois, et K^* serait cyclique. Mais alors l'équation $x^p = 1$ a au moins p^2 solutions dans K [les éléments de $(p^{a_{p,1}-1}\mathbf{Z}/p^{a_{p,1}}\mathbf{Z}) \oplus (p^{a_{p,2}-1}\mathbf{Z}/p^{a_{p,2}}\mathbf{Z})$], ce qui est impossible dans un corps commutatif.

(ii) Il résulte du (i) que le groupe $\mathbf{F}_p^*$ est isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$ (l'isomorphisme envoie l'élément neutre 1 de $\mathbf{F}_p^*$ sur celui de $\mathbf{Z}/(p-1)\mathbf{Z}$, à savoir 0). Via cet isomorphisme, l'ensemble des carrés devient $2\mathbf{Z}/(p-1)\mathbf{Z}$. Soit alors $x \in \mathbf{Z}/(p-1)\mathbf{Z}$, et soit $\tilde{x} \in \mathbf{Z}$ ayant pour image x modulo $p-1$. On a les équivalences : « $x \in 2\mathbf{Z}/(p-1)\mathbf{Z}$ » $\Leftrightarrow$ « $\tilde{x} \in 2\mathbf{Z}$ » $\Leftrightarrow$ « $\frac{p-1}{2}\tilde{x} \in (p-1)\mathbf{Z}$ » $\Leftrightarrow$ « $\frac{p-1}{2}x = 0$ ». On en déduit le résultat.

(iii) On a $(-1)^{(p-1)/2} = 1$ dans $\mathbf{F}_p^*$ si et seulement si p est de la forme $4n+1$, ce qui permet de conclure en utilisant le (ii).

(iv) Si $a^2 + b^2 = p$ et si $p \mid a$, alors $p \mid b^2 = p - a^2$, et donc $p \mid b$ et $p^2 \mid p$, ce qui est absurde. On en déduit que a et b sont premiers à p, et donc que leurs réductions $\overline{a}$, $\overline{b}$ modulo p appartiennent à $\mathbf{F}_p^*$. Soit $x = \overline{a}^{-1}\overline{b} \in \mathbf{F}_p^*$. En réduisant modulo p la relation $a^2 + b^2 = p$, on obtient $\overline{a}^2(1 + x^2) = 0$, et donc $1 + x^2 = 0$ puisque $\overline{a} \in \mathbf{F}_p^*$. Comme ceci est en contradiction avec le (iii), cela permet de conclure.

Exercice 3.5. (i) On a $(1+p^k a)^p = 1 + p^{k+1}a + \frac{p(p-1)}{2}p^{2k}a^2 + p^{3k}a^3\big(\sum_{i=3}^{p}\binom{p}{i}(p^k a)^{p-i}\big)$. Dans cette somme, tous les termes sauf les deux premiers sont divisibles par p^{k+2}, si $k \geqslant 1$ (ou si $k \geqslant 2$, dans le cas $p = 2$, où $\frac{p(p-1)}{2}$ n'est pas divisible par p). On a donc bien $x \equiv 1 + p^{k+1}a \bmod p^{k+2}$, dans les cas considérés, et une récurrence immédiate montre que $(1+p)^{p^{n-2}} = 1 + p^{n-1} \neq 1$ dans $\mathbf{Z}/p^n\mathbf{Z}$, si $p \neq 2$ et $n \geqslant 2$, et que $(1+4)^{p^{n-3}} = 1 + 2^{n-1} \neq 1$ dans $\mathbf{Z}/2^n\mathbf{Z}$, si $n \geqslant 3$.

(ii) Supposons p impair. Alors N est le sous-groupe image de $1 + p\mathbf{Z}$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$, qui est de cardinal p^{n-1} (car $x \mapsto 1 + px$ induit une bijection de $\mathbf{Z}/p^{n-1}\mathbf{Z}$ sur $1 + p\mathbf{Z}$ modulo $p^n\mathbf{Z}$). Comme $(1+p)^{p^{n-2}} \neq 1$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$, dans la décomposition $\oplus_i(\mathbf{Z}/p^{a_i}\mathbf{Z})$ du groupe N (dont le cardinal est une puissance de p), au moins un des a_i est $\geqslant n-1$, et donc $\mathrm{N} \cong \mathbf{Z}/p^{n-1}\mathbf{Z}$. Le cas $p = 2$ se traite de la même manière.

(iii) La réduction modulo p fournit une surjection $\pi : \mathrm{G} = (\mathbf{Z}/p^n\mathbf{Z})^* \to \mathbf{F}_p^*$, et $\mathbf{F}_p^*$ est un groupe isomorphe à $(\mathbf{Z}/(p-1)\mathbf{Z})$ d'après l'ex. 3.4. Comme $p-1$ et p^{n-1} sont premiers entre eux, il résulte du th. 3.1, que $\mathrm{G}_p = \mathrm{N} \cong \mathbf{Z}/p^{n-1}\mathbf{Z}$ et que G est de la forme $(\mathbf{Z}/p^{n-1}\mathbf{Z}) \oplus \mathrm{G}'$, avec $\mathrm{G}' = \oplus_{\ell \neq p}\mathrm{G}_\ell$. Alors $\mathrm{G}/\mathrm{N} \cong \mathrm{G}'$, et comme $\mathrm{G}/\mathrm{N} \cong \mathbf{F}_p^*$ par définition de N et surjectivité de π, cela permet de conclure.

(iv) Le groupe $(\mathbf{Z}/2^n\mathbf{Z})^*$ est de cardinal $\mathbf{Z}/2^{n-1}\mathbf{Z}$, et contient les sous-groupes N et $\{\pm 1\}$ dont l'intersection est nulle. Ceci implique que N et $\{\pm 1\}$ sont en somme directe, et comme $|\mathrm{N}|\cdot|\{\pm 1\}| = |(\mathbf{Z}/2^n\mathbf{Z})^*|$, cela prouve que $(\mathbf{Z}/2^n\mathbf{Z})^* = \mathrm{N}\oplus\{\pm 1\}$, ce qui permet de conclure puisque $\mathrm{N} \cong \mathbf{Z}/2^{n-2}\mathbf{Z}$ et $\{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$.

Exercice 3.6. Comme $|\mathbf{F}_p^*| = p-1$, on a $x^{p-1} = 1$ pour tout $x \in \mathbf{F}_p^*$ d'après le théorème de Lagrange. On en déduit que $x^p = x$ pour tout $x \in \mathbf{F}_p$, ce qui se traduit, en remontant dans $\mathbf{Z}$, par $p|n^p - n$, pour tout $n \in \mathbf{Z}$.

Exercice 3.7. (i) Si $\phi \in \mathrm{X}$, alors $(g\cdot(h\cdot\phi))(x) = (h\cdot\phi)(x+g) = \phi((x+h)+g) = \phi(x+(g+h)) = ((g+h)\cdot\phi)(x)$, pour tout $x \in \mathbf{Z}_p/p\mathbf{Z}_p$. On en déduit que $g\cdot(h\cdot\phi) = (g+h)\cdot\phi$, pour tout $\phi \in \mathrm{X}$, ce qui prouve que l'on a bien affaire à une action de groupe.

(ii) Les points fixes sont les fonctions constantes : si $g\cdot\phi = \phi$, pour tout $g \in \mathbf{Z}/p\mathbf{Z}$, évaluer en 0 donne $\phi(g) = \phi(0)$, pour tout $g \in \mathbf{Z}/p\mathbf{Z}$. Il y a n telles fonctions.

(iii) Le cardinal d'une orbite divisant celui du groupe, il est égal à p si l'orbite n'est pas réduite à un point.

(iv) Le cardinal de X est n^p et comme il y a n orbites réduites à un point, cela laisse $n^p - n$ éléments qui se répartissent en orbites à p éléments ; il en résulte que $\frac{n^p-n}{p}$ est entier puisque c'est le nombre d'orbites à p éléments.

Exercice 3.8. (i) C'est l'ensemble des parties à p éléments de $\{1,\dots,n\}$.

(ii) Le stabilisateur de $\{1,\dots,p\}$ est l'ensemble des permutations de $\{1,\dots,n\}$ qui permutent les éléments de $\{1,\dots,p\}$ et ceux de $\{p+1,\dots,n\}$; il est donc isomorphe à $\mathrm{S}_p \times \mathrm{S}_{n-p}$ et son cardinal est $p!(n-p)!$.

(iii) Le cardinal d'une orbite est le quotient du cardinal du groupe par celui du stabilisateur d'un de ses éléments (cf. n° 3.4) ; en appliquant ceci à l'orbite de $\{1,\dots,p\}$ sous l'action de S_n, on obtient le fait que le cardinal de l'ensemble des parties à p éléments de $\{1,\dots,n\}$ est $\frac{n!}{p!(n-p)!}$.

Exercice 3.9. On obtient le 5-cycle $(1,2,3,4,5)$.

Exercice 3.10. La démonstration se fait par récurrence sur n. Le résultat est trivial si $n = 2$. Soit $n \geqslant 3$, et soient $\sigma \in \mathrm{S}_n$, et $a = \sigma(n)$. Si $a \neq n$, alors $\sigma' = (n-1,n)\cdots(a,a+1)\sigma$ fixe n, et est dans le sous-groupe engendré par $(1,2),(2,3),\dots,(n-2,n-1)$ d'après l'hypothèse de récurrence. Donc $\sigma = (a,a+1)\cdots(n-1,n)\sigma'$ est dans le sous-groupe engendré par $(1,2),(2,3),\dots,(n-1,n)$. Si $a = n$, alors σ est déjà dans le sous-groupe engendré par $(1,2),(2,3),\dots,(n-2,n-1)$, ce qui prouve que le sous-groupe engendré par $(1,2),(2,3),\dots,(n-1,n)$ est S_n.

Exercice 3.11. Comme les τ_i commutent deux à deux, on a $\sigma^n = \tau_1^n\cdots\tau_s^n$, et comme les τ_i^n sont à supports disjoints, on a $\sigma^n = 1$ si et seulement si $\tau_i^n = 1$ pour tout i. On en déduit que l'ordre de σ est le ppcm des ordres des τ_i, et comme τ_i est d'ordre ℓ_i, l'ordre de σ est le ppcm des ℓ_i.

Exercice 3.12. (i) Choisir un cycle de longueur k revient à choisir les k éléments (n choix pour le premier,..., $n-k+1$ pour le dernier), en tenant compte du fait que les k permutations circulaires des éléments donnent le même cycle ; il y a donc $\frac{1}{k}(n(n-1)\cdots(n-k+1))$ cycles de longueur k.

(ii) Soit $\tau = (i_1,\dots,i_k)$ un cycle de longueur k. Alors τ apparaît dans la décomposition de σ si et seulement si la restriction de σ à $\{i_1,\dots,i_k\}$ est τ, et σ peut permuter les autres éléments comme il veut, et donc τ apparaît dans la décomposition de $(n-k)!$ permutations.

Maintenant, le nombre total de cycles apparaissant dans les permutations de S_n est aussi la somme pour chaque cycle du nombre de permutations dans lequel il apparaît. Ce nombre total est donc, d'après ce qui précède, égal à $\sum_{k=1}^n \frac{1}{k}(n(n-1)\dots(n-k+1))\cdot(n-k)! = n!(1+\frac{1}{2}+\cdots+\frac{1}{n})$, et le nombre moyen de cycles est $1+\frac{1}{2}+\cdots+\frac{1}{n}$ qui tend bien vers $+\infty$.

Exercice 3.14. Si $\tau_1 \dots \tau_r$ est la décomposition de σ en cycles (en incluant les cycles de longueur 1), et si τ_i est de longueur ℓ_i, alors $\omega(\sigma) = r$, $\sum_{i=1}^{r} \ell_i = n$ et

$$\operatorname{sign}(\sigma) = \prod_{i=1}^{r} \operatorname{sign}(\tau_i) = \prod_{i=1}^{r} (-1)^{\ell_i - 1} = (-1)^{n-r} = (-1)^{n-\omega(\sigma)}.$$

Exercice 3.15. (i) On a $u_{\sigma\tau}(e_i) = e_{\sigma\tau(i)} = e_{\sigma(\tau(i))} = u_\sigma(e_{\tau(i)}) = u_\sigma(u_\tau(e_i))$, ce qui prouve que les endomorphisme $u_{\sigma\tau}$ et $u_\sigma u_\tau$ coïncident sur la base canonique, et donc sont égaux. De plus, l'image de la base canonique est une base (vu que c'est la base canonique à l'ordre près) ; u_σ est donc élément de $\mathbf{GL}_n(\mathbf{C})$ et $\sigma \mapsto u_\sigma$ est un morphisme de groupes de S_n dans $\mathbf{GL}_n(\mathbf{C})$.

(ii) Si τ est la transposition (i, j), alors u_τ est la symétrie par rapport à l'hyperplan engendré par $\frac{e_i+e_j}{2}$ et les e_ℓ, pour $\ell \notin \{i, j\}$, de direction la droite engendrée par $\frac{e_i-e_j}{2}$. Ceci implique que u_τ a $n-1$ valeurs propres égales à 1 et une égale à -1 et donc $\det u_\tau = -1$.

(iii) Comme $\det : \mathbf{GL}_n(\mathbf{C}) \to \mathbf{C}^*$ est un morphisme de groupes, l'application $\sigma \mapsto \det u_\sigma$ est un morphisme de groupes. Par ailleurs, il ressort du (ii) que l'on a $\det u_\sigma = -1 = \operatorname{sign}(\sigma)$, si σ est une transposition, et comme les transpositions engendrent S_n, cela implique que les deux morphismes de groupes $\sigma \mapsto \det u_\sigma$ et $\sigma \mapsto \operatorname{sign}(\sigma)$ coïncident sur S_n.

Exercice 3.16. (i) D'après le théorème de structure, G est isomorphe à une somme directe $\oplus_{i\in \mathrm{I}}(\mathbf{Z}/p_i^{a_i}\mathbf{Z})$, où les p_i sont des nombres premiers (pas forcément distincts). On a alors $|\mathrm{G}| = \prod_{i\in \mathrm{I}} p_i^{a_i}$, et si d divise $|\mathrm{G}|$, on peut trouver des entiers b_i, avec $b_i \leqslant a_i$, tels que $d = \prod_{i\in \mathrm{I}} p_i^{b_i}$. Comme $\mathbf{Z}/p_i^{a_i}\mathbf{Z}$ est cyclique, et comme $p^{b_i} | p^{a_i}$, le groupe $\mathbf{Z}/p_i^{a_i}\mathbf{Z}$ contient un sous-groupe H_i d'ordre p^{b_i}, et $\oplus_{i\in \mathrm{I}}\mathrm{H}_i$ est un sous-groupe de G de cardinal d.

(ii) Comme $|\mathrm{A}_5| = 60 > 6 = |\mathrm{S}_3|$, la restriction de f à A_5 n'est pas injective, et comme A_5 est simple, cela implique que $f(\mathrm{A}_5) = \{\mathrm{id}\}$, et donc que f se factorise à travers $\mathrm{S}_5/\mathrm{A}_5$. Comme le cardinal de $\mathrm{S}_5/\mathrm{A}_5$ est 2, l'image de f a 1 ou 2 éléments.

(iii) Soit H un sous-groupe de S_5 d'ordre 40, et soit $\mathrm{X} = \mathrm{S}_5/\mathrm{H}$. Alors $|\mathrm{X}| = |\mathrm{S}_5|/|\mathrm{H}| = 3$. Par ailleurs, S_5 agit sur X par translation à droite, et permute les éléments de X. On en déduit l'existence d'un morphisme de groupes de S_5 dans $\mathrm{Perm}(\mathrm{X}) \cong \mathrm{S}_3$ dont l'image a au moins 3 éléments. Ceci étant en contradiction avec le (ii), cela prouve que H n'existe pas.

Exercice 3.18. (i) Comme $\mathbf{Z}/p\mathbf{Z}$ est engendré par 1, il suffit de vérifier que $x_0 \cdots x_{p-1} = 1$ implique $x_1 \cdots x_{p-1}x_0 = 1$, ce qui se démontre en multipliant la première relation à gauche par x_0^{-1} et à droite par x_0. Un point fixe de cette action est de la forme $(x, \dots, x)$ et son appartenance à X se traduit par $x^p = 1$; les points fixes sont donc en bijection avec les éléments de G d'ordre divisible par p.

(ii) La condition $x_0 \cdots x_{p-1} = 1$ peut se réécrire sous la forme $x_0 = x_{p-1}^{-1} \cdots x_1^{-1}$; on en déduit que $(x_0, \dots, x_{p-1}) \mapsto (x_1, \dots, x_{p-1})$ induit une bijection de X sur G^{p-1} et donc que $|\mathrm{X}| = |\mathrm{G}|^{p-1}$. Comme p divise $|\mathrm{G}|$ par hypothèse, il divise aussi $|\mathrm{X}|$. Maintenant, X est la réunion disjointe des orbites sous l'action de $\mathbf{Z}/p\mathbf{Z}$, et comme le cardinal d'une orbite divise celui du groupe, ces orbites ont pour cardinal 1 ou p. Comme $|\mathrm{X}|$ est divisible par p, le nombre d'orbites de cardinal 1 est divisible par p, et comme il y en a au moins une, à savoir $(1, \dots, 1)$, il y en a au moins p. Les orbites de cardinal 1 étant en bijection avec les éléments de G d'ordre divisible par p, et comme un tel élément est d'ordre p s'il n'est pas égal à 1, cela prouve que G contient des éléments d'ordre p.

Exercice 4.1. C'est un cas particulier de la prop. 4.10, mais on peut en donner une démonstration plus directe. Soit $d = \deg \mathrm{Q}$. Alors $\mathrm{K}[\mathrm{T}]/\mathrm{Q}$ est un K-espace vectoriel de dimension d (de base $(1, \dots, \mathrm{X}^{d-1})$), et si $\mathrm{P} \in \mathrm{K}[\mathrm{T}]$ n'est pas divisible par Q, la multiplication par P est injective sur $\mathrm{K}[\mathrm{T}]/\mathrm{Q}$ (si R est dans le noyau, alors PR est divisible par Q, et comme Q est irréductible et P est premier à Q, cela implique

que R est divisible par Q, et donc est nul dans K[T]/Q), et donc est surjective, ce qui prouve que tout élément non nul de K[T]/Q a un inverse.

Exercice 4.17. (i) La nullité de Δ implique, car A est premier à B, que A divise A′ (lemme de Gauss), ce qui n'est possible que si $A' = 0$, et donc si A est constant. De même, cette nullité implique que B et C sont constants, ce qui est contraire à l'hypothèse. On en déduit que $\Delta \neq 0$; l'inégalité est alors évidente.

(ii) Si z est un zéro de ABC, alors c'est un zéro d'un seul des polynômes A, B ou C puisque ceux-ci sont premiers entre eux. On peut donc, sans nuire à la généralité, supposer que c'est un zéro de multiplicité $m_z \geqslant 1$ de A. Sa multiplicité comme zéro de A′ est alors $m_z - 1$, et comme B ne s'annule pas en z, sa multiplicité comme zéro de $AB' - BA'$ est exactement $m_z - 1$.

(iii) On déduit du (ii) que P est divisible par le produit des $(T-z)^{m_z-1}$, où z parcourt les zéros de ABC, ce qui nous fournit l'inégalité $\deg P \geqslant \sum(m_z - 1)$, et comme $\sum m_z = \deg ABC = \deg A + \deg B + \deg C$ et $\sum_z 1 = r(Q)$ (par définition de $r(Q)$), on obtient $\deg P \geqslant \deg A + \deg B + \deg C - r(Q)$. Le résultat demandé s'obtient alors en comparant cette inégalité avec celle du (i).

(iv) Supposons que $A^n + B^n = C^n$, et que A, B, C ne sont pas tous constants. Comme les zéros de $A^nB^nC^n$ sont ceux de ABC, on déduit du (iii) l'inégalité $r(ABC) > n \sup(\deg A, \deg B, \deg C)$, ce qui est absurde, si $n \geqslant 3$, car $r(ABC) \leqslant \deg ABC = \deg A + \deg B + \deg C$.

Exercice 4.18. 1) (i) K et A sont clairement stables par addition, passage à l'opposé, et multiplication. Ce sont donc des sous-anneaux de $\mathbf{C}$. De plus, l'inverse de $x + iy$ est $\frac{1}{x^2+y^2}(x - iy)$ qui appartient à K, si $x, y \in \mathbf{Q}$; il en résulte que K est aussi stable par passage à l'inverse et donc est un sous-corps de $\mathbf{C}$.

(ii) On a $N(z) = |z|^2$, et le résultat suit de ce que $|z_1 z_2| = |z_1|\,|z_2|$ (on peut aussi vérifier le résultat en développant).

(iii) Si $u \in A^*$, et si v est son inverse, on a $N(u)N(v) = N(uv) = 1$. Comme $N(u)$ et $N(v)$ sont des entiers $\geqslant 0$, cela implique que $N(u) = 1$. Réciproquement, si $N(u) = 1$, alors $u\,\overline{u} = 1$ et donc u est inversible, d'inverse $\overline{u}$. Enfin, si $x, y \in \mathbf{Z}$ vérifient $x^2 + y^2 = 1$, alors l'un des deux vaut 0 et l'autre ± 1, et donc $A^* = \{1, -1, i, -i\}$.

(iv) On a $N(r) = N(b)N(\{\frac{a}{b}\})$, et comme $N(\{z\}) \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, pour tout $z \in \mathbf{C}$, on en déduit que $N(r) \leqslant \frac{1}{2}N(b) < N(b)$. Soit $c = [\frac{a}{b}]$. Alors $c \in A$ par construction, et $c + \frac{r}{b} = \frac{a}{b}$, ce qui nous donne $a = bc + r$, et prouve que $r = a - bc \in A$. D'où le résultat.

(v) Soient I un idéal de A et $b \in A^+ \cap I$ tel que $N(b)$ réalise le minimum des $N(x)$, pour $x \in I - \{0\}$. Si $a \in I$, on peut, d'après le (iv), écrire a sous la forme $a = bc + r$, avec $N(r) < N(b)$. Mais alors $r = a - bc \in I$, et la définition de b implique $r = 0$. Il en résulte que I est l'idéal principal engendré par b. Ceci permet de conclure.

2) (i) Que $\mathbf{Z} \cap (q)$ soit un idéal de $\mathbf{Z}$ est immédiat. Soient $a, b \in \mathbf{Z}$ tels que $ab \in \mathbf{Z} \cap (q)$. Comme (q) est un idéal premier de A, on a $a \in (q)$ ou $b \in (q)$, et donc $a \in \mathbf{Z} \cap (q)$ ou $b \in \mathbf{Z} \cap (q)$, ce qui prouve que $\mathbf{Z} \cap (q)$ est un idéal premier de $\mathbf{Z}$. Notons p l'élément de $\mathscr{P}$ correspondant. L'appartenance de p à $\mathbf{Z} \cap (q)$ se traduit par la divisibilité de p par q dans A ; on en déduit que p est l'unique élément de $\mathscr{P}$ divisible par q dans A. Enfin, $N(q)$ divise $N(p) = p^2$ et n'est pas égal à 1 sinon q serait inversible d'après 1) (iii) ; il ne reste donc que $N(q) = p$ et $N(q) = p^2$ comme possibilités.

(ii) Si $N(q) = p \in \mathscr{P}$ et si $q = ab$, on a $N(a)N(b) = p$, et donc $N(a) = 1$ ou $N(b) = 1$; il en résulte que a ou b est inversible, et donc que $a \in (q)$ ou $b \in (q)$. L'idéal (q) est donc premier, ce qui permet de conclure.

(iii) Comme a est de la forme $4n + 1$, l'équation $x^2 + 1 = 0$ a une solution dans $\mathbf{F}_p$, et il existe $\tilde{x} \in \{1, \ldots, p-1\}$ tel que $\tilde{x}^2 + 1$ soit divisible par p. Alors $a = \tilde{x} + i$ vérifie les conditions demandées.

Maintenant, soit $u \prod q_i$ la factorisation de a en produit de facteurs premiers dans A. Alors $N(a) = \prod N(q_i)$, et comme $p \mid N(a)$, il existe i tel que $p \mid N(q_i)$, ce qui, d'après le (i) implique que q_i divise p dans A. Il en résulte que $q_i | \mathrm{pgcd}(a, p)$, et donc que $b = \mathrm{pgcd}(a, p)$ n'est pas inversible. De plus, on a

$\mathrm{N}(b) \leqslant \mathrm{N}(a) < p^2$, et comme $\mathrm{N}(b)|p^2$, cela implique que $\mathrm{N}(b) = p$. Le (ii) montre alors que b est premier, ce qui permet de conclure.

(iv) D'après le (iii), il existe $q \in \mathscr{P}_{\mathrm{A}}$ divisant strictement p, ce qui implique $\mathrm{N}(q) = p$. Il n'y a plus qu'à écrire q sous la forme $x + iy$, avec $x, y \in \mathbf{Z}$, pour obtenir une écriture de $p = x^2 + y^2$ comme somme de deux carrés.

(v) Si $p \in \mathscr{P}$ impair n'est pas premier dans A, et si $q = x + iy$ est un diviseur premier de p, on a $\mathrm{N}(q) = p$. Or $\mathrm{N}(q) = (-i)qq^*$, et $\mathrm{N}(q^*) = \mathrm{N}(q)$ puisque $q^* = y + ix$. D'après le (ii), cela implique que $q^* \in \mathscr{P}_{\mathrm{A}}$ et donc que la factorisation de p est $(-i)qq^*$. Enfin, comme p est impair, on a $x \neq y$, et on peut, quitte à échanger les rôles de q et q^*, supposer que $x > y$ et poser $q_p = q$.

(vi) Voir la solution du (iv) de l'ex. 3.4.

(vii) D'après le (i), les éléments de $\mathscr{P}_{\mathrm{A}}$ sont les diviseurs premiers des éléments de $\mathscr{P}$. Le résultat est donc une combinaison des (v), (vi) et de ce que la factorisation de 2 est $2 = (-i)(1+i)^2$.

Exercice 5.2. La vérification de ce que d est une distance ne pose pas de problème, et comme les singletons sont ouverts puisque $\{x\} = \mathrm{B}(x, (1/2)^-)$, la topologie associée est la topologie discrète.

Exercice 5.3. Si $d'(x, y) = 0$, on a $f(x) = f(y)$ et donc $x = y$ car f est injective (strictement croissante). La symétrie est évidente et l'inégalité triangulaire suit de ce que $d'(x, z) = |f(x) - f(z)| \leqslant |f(x) - f(y)| + |f(y) - f(z)| = d'(x, y) + d'(y, z)$. Il reste à prouver que si $x \in \mathbf{R}$ et si $\varepsilon > 0$, il existe $\delta > 0$ tel que $d(x, y) < \delta$ implique $d'(x, y) < \varepsilon$ et $d'(x, y) < \delta$ implique $d(x, y) < \varepsilon$, ce qui suit de la continuité de f et de sa réciproque $g(x) = \frac{x}{1-|x|}$, si $x \in]-1, 1[$.

Exercice 5.5. C'est la topologie grossière : si $x \in \mathbf{R}$ et si U est un ouvert non vide de $\mathbf{R}$, alors U contient un élément de la forme $x + r$, avec $r \in \mathbf{Q}$, et donc tout ouvert non vide de $\mathbf{R}/\mathbf{Q}$ contient l'image de x, pour tout x, et donc est égal à $\mathbf{R}/\mathbf{Q}$.

Exercice 5.6. Soient $a \neq b$ deux points de X. Comme f est injective, on a $f(a) \neq f(b)$, et comme Y est séparé, on peut trouver des ouverts disjoints U et V de Y tels que $f(a) \in \mathrm{U}$ et $f(b) \in \mathrm{V}$. Maintenant, comme f est continue, $f^{-1}(\mathrm{U})$ et $f^{-1}(\mathrm{V})$ sont des ouverts de X, qui sont disjoints car U et V le sont, et qui contiennent respectivement a et b. Ceci permet de conclure.

Exercice 5.7. Il suffit de passer aux complémentaires.

Exercice 5.8. (i) Soit $\mathrm{U} \neq \emptyset$ un ouvert de $\mathrm{X}_1 \times \mathrm{X}_2$. Il existe alors $\mathrm{U}_1 \neq \emptyset$ ouvert de X_1 et $\mathrm{U}_2 \neq \emptyset$ ouvert de X_2 tels que U contienne $\mathrm{U}_1 \times \mathrm{U}_2$. Comme Y_1 est dense, $\mathrm{Y}_1 \cap \mathrm{U}_1$ est non vide et comme Y_2 est dense, il en est de même de $\mathrm{Y}_2 \cap \mathrm{U}_2$, ce qui montre que $(\mathrm{Y}_1 \times \mathrm{Y}_2) \cap \mathrm{U}$ qui contient $(\mathrm{Y}_1 \times \mathrm{Y}_2) \cap (\mathrm{U}_1 \times \mathrm{U}_2) = (\mathrm{Y}_1 \cap \mathrm{U}_1) \times (\mathrm{Y}_2 \cap \mathrm{U}_2)$ est non vide. On en déduit la densité de $\mathrm{Y}_1 \times \mathrm{Y}_2$.

(ii) Soient $g : \mathrm{Y} \times \mathrm{Y} \to \mathbf{R}_+$ définie par $g(x, x') = d_{\mathrm{Y}}(x, x')$ et $h : \mathrm{Y} \times \mathrm{Y} \to \mathbf{R}_+$ définie par $g(x, x') = d_{\mathrm{Z}}(f(x'), f(x'))$. On cherche à prouver que g et h sont égales. Or elles sont égales sur $\mathrm{X} \times \mathrm{X}$ par hypothèse, et comme $\mathrm{X} \times \mathrm{X}$ est dense dans $\mathrm{Y} \times \mathrm{Y}$, et Z est séparé car métrique, on peut en conclure qu'elles sont égales sur $\mathrm{Y} \times \mathrm{Y}$, en utilisant le point ci-dessus (ou l'ex. 5.11).

Exercice 5.9. (i) Comme $\overline{\mathrm{U}}$ contient U, son intérieur, qui est le plus grand ouvert contenu dans $\overline{\mathrm{U}}$ contient U. Si U est l'ouvert $]0, 1[\cup]1, 2[$ de $\mathbf{R}$, alors $\overline{\mathrm{U}} = [0, 2]$ et l'intérieur de $\overline{\mathrm{U}}$ est $]0, 2[$ qui contient strictement U. Revenons au cas d'un ouvert général U et notons V l'intérieur de son adhérence. Comme $\mathrm{U} \subset \mathrm{V}$, on a $\overline{\mathrm{U}} \subset \overline{\mathrm{V}}$, et comme $\overline{\mathrm{U}}$ est un fermé qui contient V, on a $\overline{\mathrm{V}} \subset \overline{\mathrm{U}}$, et donc $\overline{\mathrm{V}} = \overline{\mathrm{U}}$, ce qui termine la démonstration du (i).

Le (ii) se déduit du (i) en passant aux complémentaires.

Exercice 5.10. Si A n'est pas dense, son adhérence n'est pas $\mathbf{C}^2$, et il existe un polynôme $\mathrm{P} \in \mathbf{C}[\mathrm{X}, \mathrm{Y}]$ non nul s'annulant sur A. Soit donc $\mathrm{P} \in \mathbf{C}[\mathrm{X}, \mathrm{Y}]$ tel que $\mathrm{P}(n, e^n) = 0$ pour tout $n \in \mathbf{N}$. On écrit P sous la forme $\mathrm{P}(\mathrm{X}, \mathrm{Y}) = \mathrm{P}_d(\mathrm{X})\mathrm{Y}^d + \cdots + \mathrm{P}_0(\mathrm{X})$, avec $\mathrm{P}_0, \ldots, \mathrm{P}_d \in \mathbf{C}[\mathrm{X}]$. On a donc $\mathrm{P}_d(n)e^{dn} + \cdots + \mathrm{P}_0(n) = 0$

pour tout n, et en divisant par e^{dn}, on en déduit que $\mathrm{P}_d(n) \to 0$ quand $n \to +\infty$. Ceci n'est possible que si $\mathrm{P}_d = 0$. On en déduit que $\mathrm{P} = 0$; d'où la densité de A dans $\mathbf{C}^2$.

A n'est pas dense dans $\mathbf{C}^2$ pour la topologie usuelle car A ne contient aucun point de l'ouvert $\{z = (z_1, z_2),\ \sup(|z_1|, |z_2|) < 1\}$. En fait, il n'est pas difficile de voir que A est fermé dans $\mathbf{C}^2$ pour la topologie usuelle.

Exercice 5.11. Si X est métrisable, la topologie peut être définie par une métrique d, ce qui permet de supposer que (X, d) est métrique dans tout ce qui suit.

(i) Soit $a \in \mathrm{X}$. Comme les $\mathrm{B}(a, 2^{-n})$ forment une base de voisinages de a, on voit que si $a \in \overline{\mathrm{Z}}$, alors, pour tout $n \in \mathbf{N}$, il existe $x_n \in \mathrm{Z}$ avec $d(a, x_n) \leqslant 2^{-n}$; la suite $(x_n)_{n\in\mathbf{N}}$ a alors a comme limite. Réciproquement, si $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de Z ayant a pour limite, et si U est un voisinage de a, alors $x_n \in \mathrm{U}$, pour tout n assez grand, ce qui prouve que U contient des éléments de Z, et permet de montrer que $a \in \overline{\mathrm{Z}}$ (noter que ce sens n'a pas utilisé le fait que X est métrique).

(ii) Z est dense dans X si et seulement si $\overline{\mathrm{Z}} = \mathrm{X}$, et donc le résultat suit du (i).

(iii) Si $x \in \mathrm{X}$, il existe une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de Z tendant vers x. Mais alors $f(x_n)$ tend vers $f(x)$ et $g(x_n)$ tend vers $g(x)$ puisque f et g sont continues, et comme $f(x_n) = g(x_n)$ pour tout n, cela implique que $f(x)$ et $g(x)$ sont des limites de la suite $(f(x_n))_{n\in\mathbf{N}}$. Comme Y est supposé métrique et donc séparé, il y a unicité de la limite d'une suite et donc $f(x) = g(x)$.

Exercice 6.1. (i) L'ensemble A des rationnels appartenant à $[0, 1]$ est dénombrable ; soit $n \mapsto r_n$ une bijection de $\mathbf{N}$ sur A. Comme A est dense dans $[0, 1]$, l'adhérence de tout ouvert contenant A contient $[0, 1]$; il suffit donc de prendre $]a_n, b_n[=]r_n - \frac{\varepsilon}{2^{n+3}}, r_n + \frac{\varepsilon}{2^{n+3}}[$.

(ii) Comme $[0, 1]$ est compact, si les $]a_n, b_n[$, pour $n \in \mathbf{N}$, recouvrent $[0, 1]$, on peut en extraire un recouvrement fini, et le résultat suit du cas d'une famille finie. (Pour démontrer le résultat dans le cas d'une famille finie, on peut remarquer que $\sum_{n\in\mathrm{J}}(b_n - a_n)$ est l'intégrale (de Riemann) de la fonction continue par morceaux $\phi = \sum_{n\in\mathrm{J}} \mathbf{1}_{]a_n,b_n[}$. Or l'hypothèse $[0, 1] \subset \cup_{n\in\mathrm{J}}]a_n, b_n[$ se traduit par $\phi(x) \geqslant 1$, si $x \in [0, 1]$, et donc l'intégrale de ϕ est supérieure ou gale à celle de $\mathbf{1}_{[0,1]}$ qui vaut 1. L'exercice permet de montrer que l'intégrale de Lebesgue de $\mathbf{1}_{[0,1]}$ est supérieure ou égale à 1 et donc aussi égale à 1, ce qui est rassurant...)

Exercice 6.2. (i) Soit X un compact métrique, et soient $(x_n)_{n\in\mathbf{N}}$ ayant une unique valeur d'adhérence a, et U un ouvert contenant a. Alors $\mathrm{X} - \mathrm{U}$ ne contient qu'un nombre fini de termes de la suite, sinon on pourrait extraire une sous-suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ de $(x_n)_{n\in\mathbf{N}}$, dont tous les termes sont dans $\mathrm{X} - \mathrm{U}$, et comme $\mathrm{X} - \mathrm{U}$ est compact puisque fermé dans un compact, cela implique que $(x_{\varphi(n)})_{n\in\mathbf{N}}$ et donc aussi $(x_n)_{n\in\mathbf{N}}$, a une valeur d'adhérence dans $\mathrm{X} - \mathrm{U}$, contrairement à l'hypothèse. Il existe donc $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in \mathrm{U}$, si $n \geqslant \mathrm{N}$, ce qui prouve que a est la limite de la suite $(x_n)_{n\in\mathbf{N}}$.

(ii) La suite $(1 + (-1)^n)n$ admet 0 comme unique valeur d'adhérence dans $\mathbf{R}$, mais ne converge pas.

Exercice 6.3. Il suffit d'adapter la démonstration de la compacité de $\mathbf{Z}_p$ (alinéa 12.4.2) en partant du développement décimal des éléments de $[0, 1]$.

Exercice 6.4. Si f est identiquement nulle, il n'y a rien à démontrer. Sinon, il existe $x_0 \in \mathrm{E}$ tel que $|f(x_0)| > 0$, et comme f tend vers 0 à l'infini, il existe $\mathrm{M} > 0$, tel que $|f(x)| < \frac{|f(x_0)|}{2}$, si $\|x\| > \mathrm{M}$. Mais alors la boule $\mathrm{B}(0, \mathrm{M})$ contient x_0 et est compacte, puisque E est de dimension finie. Cela implique que $|f|$ atteint son maximum sur cette boule en un point x_1, et on a $|f(x_1)| \geqslant |f(x_0)| > \frac{|f(x_0)|}{2}$, ce qui prouve que $|f(x_1)|$ est aussi le maximum de $|f|$ sur E tout entier. Ceci permet de conclure.

Exercice 6.5. (i) Si $x_1, x_2 \in \mathrm{X}$, on a $d(x_1, y) \leqslant d(x_1, x_2) + d(x_2, y)$ pour tout $y \in \mathrm{F}$. En passant à la borne inférieure sur $y \in \mathrm{F}$, on en déduit que $d(x_1, \mathrm{F}) \leqslant d(x_1, x_2) + d(x_2, \mathrm{F})$. Par symétrie, on a $d(x_2, \mathrm{F}) \leqslant d(x_1, x_2) + d(x_1, \mathrm{F})$. On en déduit que $|d(x_1, \mathrm{F}) - d(x_2, \mathrm{F})| \leqslant d(x_1, x_2)$, et donc que $d(x, \mathrm{F})$ est 1-lipschitzienne.

(ii) On a $d(x,\mathrm{F})=0$, si $x\in\mathrm{F}$, et donc, par continuité, $d(x,\mathrm{F})=0$, si $x\in\overline{\mathrm{F}}$. Réciproquement, si $x\in\overline{\mathrm{F}}$, alors pour tout $n>0$, il existe $x_n\in\mathrm{F}$ avec $d(x,x_n)<2^{-n}$, ce qui implique que $d(x,\mathrm{F})<2^{-n}$, pour tout n, et donc $d(x,\mathrm{F})=0$.

(iii) La fonction $f(x)=d(x,\mathrm{F}_1)-d(x,\mathrm{F}_2)$ est continue sur X, et donc $\mathrm{U}_1=f^{-1}(\mathbf{R}_+^*)$ et $\mathrm{U}_2=f^{-1}(\mathbf{R}_-^*)$ sont deux ouverts de X (en tant qu'images inverses d'ouverts de $\mathbf{R}$ par une fonction continue) qui sont disjoints puisque $\mathbf{R}_+^*$ et $\mathbf{R}_-^*$ sont disjoints. Maintenant, si $x\in\mathrm{F}_1$, alors $d(x,\mathrm{F}_2)>0$ puisque F_2 est fermé et $x\notin\mathrm{F}_2$; donc $f(x)>0$. On en déduit que $\mathrm{F}_1\subset\mathrm{U}_1$. De même, $\mathrm{F}_2\subset\mathrm{U}_2$, ce qui permet de conclure.

(iv) La fonction $(x,y)\mapsto d(x,y)$ est continue sur $\mathrm{X}\times\mathrm{X}$. Comme $\mathrm{F}_1\times\mathrm{F}_2$ est compact comme produit de deux compacts, le minimum de $d(x,y)$ sur $\mathrm{F}_1\times\mathrm{F}_2$ est atteint en (x_0,y_0), et comme $\mathrm{F}_1\cap\mathrm{F}_2=\emptyset$, on a $d(x_0,y_0)\neq 0$, et donc $d(\mathrm{F}_1,\mathrm{F}_2)>0$.

(v) La fonction $x\mapsto d(x,\mathrm{F}_1)$ est continue sur F_2 et ne s'annule pas car $\mathrm{F}_1\cap\mathrm{F}_2=\emptyset$ et F_1 est fermé. Comme F_2 est compact, elle atteint son mimimum qui, de ce fait est >0. Or ce minimum est $\inf_{x\in\mathrm{F}_2}d(x,\mathrm{F}_1)=\inf_{x\in\mathrm{F}_2}\inf_{y\in\mathrm{F}_1}d(x,y)=d(\mathrm{F}_1,\mathrm{F}_2)$, ce qui permet de conclure.

(vi) Dans $\mathbf{R}$, on peut prendre $\mathrm{F}_1=\mathbf{N}$ et $\mathrm{F}_2=\{n+2^{-n-1},\ n\in\mathbf{N}\}$. Dans $\mathbf{R}^2$, on peut prendre $\mathrm{F}_1=\{(x,y),\,xy=1\}$ et $\mathrm{F}_2=\{(x,y),\,xy=0\}$.

Exercice 6.6. (i) Soit $g:\mathrm{X}\to\mathbf{R}$ définie par $g(x)=d(x,f(x))$. Alors g est continue comme composée de $g_1:\mathrm{X}\to\mathrm{X}\times\mathrm{X}$ envoyant x sur $(x,f(x))$ et $g_2:\mathrm{X}\times\mathrm{X}\to\mathbf{R}$ envoyant (x,y) sur $d(x,y)$. Elle atteint donc son minimum en un point x_0, et on a $f(x_0)=x_0$, sinon $d(f(f(x_0)),f(x_0))<d(f(x_0),x_0)$, ce qui est contraire à la définition de x_0. La fonction f admet donc au moins un point fixe. Si elle en admet deux $x_1\neq x_2$, on a $d(f(x_1),f(x_2))<d(x_1,x_2)$, ce qui est contraire à l'hypothèse $f(x_1)=x_1$ et $f(x_2)=x_2$. Le point fixe de f est donc unique, ce qui permet de conclure.

(ii) Soit $\delta_n=d(f^n(x),x_0)$. Comme f est strictement contractante, $\delta_{n+1}=d(f(f^n(x)),f(x_0))<\delta_n$, si $f^n(x)\neq x_0$. Maintenant, soit a une valeur d'adhérence de la suite $(f^n(x))_{n\in\mathbf{N}}$, et soit $f^{\varphi(n)}(x)$ une suite extraite tendant vers a. Si $a\neq x_0$, on a

$$\delta_{\varphi(n_0)+1}\leqslant d(f^{\varphi(n_0)+1}(x),f(a))+d(f(a),x_0)<d(f^{\varphi(n_0)}(x),a)+d(a,x_0)\leqslant d(a,x_0),$$

si n_0 est assez grand. On aboutit à une contradiction car $\delta_m\leqslant\delta_{\varphi(n_0)}<d(a,x_0)$ pour tout $m>\varphi(n_0)$, et la suite extraite $\delta_{\varphi(n)}$ tend vers $d(a,x_0)$ quand n tend vers $+\infty$. On en déduit que $a=x_0$ et donc que $f^n(x)$ a x_0 comme une unique valeur d'adhérence dans X. Comme X est compact, cela implique que $f^n(x)\to x_0$.

(iii) Soit $\delta_n=\sup_{x\in\mathrm{X}}d(f^n(x),f(x_0))$. Il s'agit de prouver que $\delta_n\to 0$. Comme f est compact et $x\mapsto d(f^n(x),f(x_0))$ est continue puisque f est continue, il existe $x_n\in\mathrm{X}$ tel que $d(f^n(x_n),x_0)=\delta_n$. On a alors $\delta_{n+1}=d(f^{n+1}(x),x_0)=d(f^n(f(x_{n+1})),x_0)\leqslant\delta_n$, ce qui montre que la suite δ_n est décroissante. Il suffit donc d'exhiber une suite extraite de $(\delta_n)_{n\in\mathbf{N}}$ tendant vers 0.

Soit a une valeur d'adhérence de la suite x_n, et soit $x_{\varphi(n)}$ une suite extraite tendant vers a. On a alors

$$\delta_{\varphi(n)}=d(f^{\varphi(n)}(x_{\varphi(n)}),x_0)\leqslant d(f^{\varphi(n)}(x_{\varphi(n)}),f^{\varphi(n)}(a))+d(f^{\varphi(n)}(a),x_0)\leqslant d(x_{\varphi(n)},a)+d(f^{\varphi(n)}(a),x_0),$$

ce qui montre que $\delta_{\varphi(n)}\to 0$ car $d(x_{\varphi(n)},a)\to 0$ par construction, et $d(f^{\varphi(n)}(a),x_0)\to 0$ d'après le (ii). Ceci permet de conclure.

Exercice 6.7. La démonstration se fait par l'absurde. Supposons X non compact, et construisons une fonction continue $\phi:\mathrm{X}\to\mathbf{R}$ non bornée. Il existe une suite $(x_n)_{n\in\mathbf{N}}$ n'ayant pas de valeur d'adhérence dans X, ce qui se traduit, pour tout $a\in\mathrm{X}$, par l'existence de $\delta_a>0$ tel que $\mathrm{B}(a,2\delta_a^-)$ contienne au plus un x_n, à savoir a si l'un des x_n vaut a. Soit $\phi_n(x)=\sup(n-n^2d(x,x_n),0)$. C'est une fonction continue sur X, nulle en dehors de $\mathrm{B}(x_n,\frac{1}{n})$ et valant n en x_n. Si $a\in\mathrm{X}$, la restriction de ϕ_n à $\mathrm{B}(a,\delta_a^-)$ est identiquement nulle, si $\frac{1}{n}<\delta_a$ et si $x_n\neq a$. Comme il n'y a qu'un nombre fini de n ne vérifiant pas ces conditions, cela montre que $\phi(x)=\sum_{n\in\mathbf{N}}\phi_n(x)$ est la somme d'un nombre fini de fonctions continues

sur $\mathrm{B}(a, \delta_a^-)$, pour tout a ; c'est donc une fonction continue sur X. Par ailleurs, on a $\phi(x_n) \geqslant n$, pour tout n, et donc ϕ est non bornée. Ceci permet de conclure.

Exercice 7.1. On sait que U est connexe par arcs, et il suffit de prouver qu'il en est de même de $\mathrm{V} = \mathrm{U} - \{x\}$. Soient donc $y_1, y_2 \in \mathrm{V}$, et soit $u : [0,1] \to \mathrm{U}$ un chemin continu joignant y_1 à y_2 dans U. Si u ne passe pas par x, il n'y a rien à faire. Sinon, il existe $r < \inf(d(x, y_1), d(x, y_2))$ tel que $\mathrm{B}(x, r) \subset \mathrm{U}$, et l'ensemble des t tels que $d(x, u(t)) \leqslant r$ admet un plus petit (resp. grand) élément t_1 (resp. t_2). Alors u permet de joindre y_1 à $u(t_1)$ et $u(t_2)$ à y_2 dans V, et on peut passer de $u(t_1)$ à $u(t_2)$ en restant sur la sphère de rayon r (il suffit de prendre l'arc de cercle délimité par le cone de sommet x et dont les bords sont les demi-droites $[x, u(t_1))$ et $[x, u(t_2))$).

Exercice 7.2. Si f est un homéomorphisme de X sur Y, alors la restriction de f à $\mathrm{X} - \{x\}$ est encore un homéomorphisme de $\mathrm{X} - \{x\}$ sur $\mathrm{Y} - \{f(x)\}$ pour tout $x \in \mathrm{X}$. Il ne peut donc pas y avoir d'homéomorphisme de $\mathbf{R}$ sur $\mathbf{R}^2$ puisque $\mathbf{R}$ privé d'un point est non connexe, alors que $\mathbf{R}^2$ privé d'un point est connexe. Les autres cas se traitent de la même manière en enlevant à $[0,1]$ n'importe quel élément différent de 0 et 1.

Exercice 7.3. Si f est une bijection de $[0,1]$ sur $]0,1[$, alors $f(]0,1]) =]0,1[- \{f(0)\}$ est non connexe, tandis que $]0,1]$ est connexe, ce qui prouve que f ne peut pas être continue.

Exercice 7.4. Si on enlève de Y les deux points de contacts, on obtient un ensemble avec 4 composantes connexes, alors que si on enlève deux points à X, le mieux que l'on puisse obtenir est 3 composantes connexes.

Exercice 7.5. (i) (a) On peut prendre une échelle avec une infinité dénombrable de barreaux et, si on retire les barreaux un par un, il ne reste que les deux montants, ce qui n'est pas connexe (i.e. F_n est la réunion des deux demi-droites verticales partant de $(0,0)$ et $(1,0)$ et des segments horizontaux $[(0,k),(1,k)]$, pour $k \geqslant n$).

(b) Si F n'est pas connexe, alors $\mathrm{F} = \mathrm{F}' \cup \mathrm{F}''$, où F' et F'' sont des fermés non vides disjoints de F. Par ailleurs, F est fermé, en tant qu'intersection de femés, et comme $\mathrm{F} \subset \mathrm{F}_0$ qui est compact, F, F' et F'' sont compacts. La distance $d = d(\mathrm{F}', \mathrm{F}'')$ est donc > 0, et $\mathrm{U}' = \{x \in \mathbf{R}^2,\ d(x, \mathrm{F}') < \frac{d}{3}\}$ et $\mathrm{U}'' = \{x \in \mathbf{R}^2,\ d(x, \mathrm{F}'') < \frac{d}{3}\}$ sont des ouverts disjoints de $\mathbf{R}^2$ contenant F' et F'' respectivement. Soit $\mathrm{Z} = \mathbf{R}^2 - (\mathrm{F}' \cup \mathrm{F}'')$. Alors Z est un fermé ne rencontrant pas F, et donc $\cap_{n \in \mathbf{N}} (\mathrm{Z} \cap \mathrm{F}_n) = \emptyset$. Comme $\mathrm{Z} \cap \mathrm{F}_n$ est un fermé de F_0 qui est compact, on en déduit l'existence de $n \in \mathbf{N}$ tel que $\mathrm{Z} \cap \mathrm{F}_n = \emptyset$. On a donc $\mathrm{F}_n = (\mathrm{U}' \cap \mathrm{F}_n) \cup (\mathrm{U}'' \cap \mathrm{F}_n)$, ce qui est en contradiction avec l'hypothèse « F_n connexe » puisque $\mathrm{U}' \cap \mathrm{F}_n$ et $\mathrm{U}'' \cap \mathrm{F}_n$ sont des ouverts disjoints de F_n qui sont non vides puisqu'ils contiennent F' et F'' respectivement. L'hypothèse « F non connexe » était donc absurde, ce qui permet de conclure.

(ii) (a) Soit X_n la réunion des segments $[x_k, x_{k+1}]$, pour $k \geqslant n$, et soit F_n l'adhérence de X_n. Alors F_n est connexe car X_n est connexe (il est même connexe par arcs), F_0 est compact car fermé par construction et borné par hypothèse, et $\mathrm{F}_{n+1} \subset \mathrm{F}_n$ car $\mathrm{X}_{n+1} \subset \mathrm{X}_n$. Il s'ensuit, d'après le (i) (b), que $\mathrm{F} = \cap_{n \in \mathbf{N}} \mathrm{F}_n$ est connexe. Montrons que F est égal à l'ensemble G des valeurs d'adhérence de la suite $(x_n)_{n \in \mathbf{N}}$, ce qui permettra de conclure.

• Si $\mathrm{Y}_n = \{x_k,\ k \geqslant n\}$ et G_n est l'adhérence de Y_n, alors $\mathrm{G} = \cap_{n \in \mathbf{N}} \mathrm{G}_n$. Or $\mathrm{Y}_n \subset \mathrm{X}_n$ et donc $\mathrm{G}_n \subset \mathrm{F}_n$, pour tout $n \in \mathbf{N}$, et $\mathrm{G} \subset \mathrm{F}$.

• Si $a \in \mathrm{F}$, alors pour tout $\varepsilon > 0$ et tout $\mathrm{N} \in \mathbf{N}$, il existe $n \geqslant \mathrm{N}$ et $x \in [x_n, x_{n+1}]$ tel que $d(x, a) < \varepsilon$. Choisissons N de telle sorte que $d(x_k, x_{k+1}) \leqslant \varepsilon$, pour tout $k \geqslant \mathrm{N}$ (c'est possible car on a supposé $d(x_{k+1}, x_k) \to 0$). On a alors $d(x_n, x) \leqslant \varepsilon$ et donc $d(x_n, a) \leqslant 2\varepsilon$. On en déduit que a est une valeur d'adhérence de la suite $(x_n)_{n \in \mathbf{N}}$, et donc que $\mathrm{F} \subset \mathrm{G}$.

Ceci permet de conclure.

(b) Il suffit de parcourir l'échelle du (i) (a) en allant d'un pied à l'autre en passant par le k-ième barreau ; comme ceci est un peu fatiguant, les pas que l'on fait sont de plus en plus petits et l'adhérence de la suite ainsi construite est constituée des deux montants (il n'est pas sûr qu'ils résistent très longtemps à ce traitement...).

Exercice 7.6. Définissons le bord du cylindre et de la bande de Moebius comme l'image de $\{0,1\}\times[0,1]$. Dans le cyclindre, on obtient deux lacets disjoints, alors que dans la bande de Moebius on n'obtient qu'un seul lacet, car $(0,0)$ est identifié à $(1,1)$. Maintenant, si x est sur le bord, alors x admet une base de voisinages constituée de demi-disques de centre x, et si on prive un de ces demi-disques de x, on obtient un ensemble contractile. Si x n'est pas sur le bord, alors tout voisinage de x contient un disque de centre x, et si on le prive de x, on obtient un ensemble non contractile. On en déduit qu'un homéomorphisme du cylindre sur la bande de Moebius induit un homéomorphisme entre les bords, mais ce n'est pas possible car le bord du cylindre n'est pas connexe, alors que celui de la bande de Moebius l'est.

Exercice 8.1. (i) Si d est ultramétrique, $d(x_m,x_{m+p})\leqslant \sup_{0\leqslant i\leqslant p-1} d(x_{m+i},x_{m+i+1})\leqslant \sup_{m\geqslant n} d(x_m,x_{m+1})$. On en déduit que si $d(x_{n+1},x_n)\to 0$, et donc si $\lim_{n\to+\infty}\big(\sup_{m\geqslant n} d(x_{m+1},x_m)\big)=0$, alors $\lim_{m\to+\infty}\big(\sup_{p\in\mathbf{N}} d(x_{m+p},x_m)\big)=0$, et la suite est de Cauchy.

(ii) Si $n\geqslant 1$, soit $i=\left[\frac{\log n}{\log 2}\right]$, de telle sorte que $n=2^i+j$, avec $0\leqslant j\leqslant 2^i-1$. Posons alors $x_n=\frac{j}{2^i}$, si i est pair et $x_n=1-\frac{j}{2^i}$, si i est impair. On vérifie que $x_{n+1}-x_n=\frac{1}{2^i}$ tend vers 0, mais que la suite $(x_n)_{n\in\mathbf{N}}$ balaie consciencieusement l'intervalle $[0,1]$ et que l'ensemble de ses valeurs d'adhérence est $[0,1]$. Elle n'est donc pas de Cauchy. On aurait aussi pu prendre $x_n=\log(n+1)$ qui tend vers $+\infty$, et donc n'est pas de Cauchy.

Exercice 8.3. (i) Soit $(\mathrm{U}_n)_{n\in\mathbf{N}}$ une famille d'ouverts denses de $\mathbf{R}$. Supposons que $\mathrm{X}=\cap_{n\in\mathbf{N}}\mathrm{U}_n$ est dénombrable, et choisissons une surjection $n\mapsto x_n$ de $\mathbf{N}$ sur X. Alors $\mathrm{V}_n=\mathrm{U}_n-\{x_n\}$ est un ouvert dense de $\mathbf{R}$ pour tout n et $\cap_{n\in\mathbf{N}}\mathrm{V}_n=\emptyset$, ce qui est contraire au lemme de Baire.

(ii) Si $(f_n)_{n\in\mathbf{N}}$ est une telle suite, et si $\mathrm{N}\in\mathbf{N}$, soit $\mathrm{F}_\mathrm{N}=\{x\in\mathbf{R},\ |f_n(x)|\leqslant \mathrm{N},\ \forall n\in\mathbf{N}\}$. Alors F_N est un fermé puisque $\mathrm{F}_\mathrm{N}=\cap_{n\in\mathbf{N}}\{x\in\mathbf{R},\ |f_n(x)|\leqslant \mathrm{N}\}$ et que chacun des ensembles de l'intersection est fermé par continuité des f_n. Par ailleurs, l'hypothèse sur la suite $(f_n)_{n\in\mathbf{N}}$ se traduit par $\cup_{\mathrm{N}\in\mathbf{N}}\mathrm{F}_\mathrm{N}=\mathbf{R}-\mathbf{Q}$. En notant U_N l'ouvert complémentaire de F_N, on obtient $\cap_{\mathrm{N}\in\mathbf{N}}\mathrm{U}_\mathrm{N}=\mathbf{Q}$, ce qui est en contradiction avec le (i) (chacun des U_N est dense dans $\mathbf{R}$ puisqu'il contient $\mathbf{Q}$).

Exercice 9.1. En revenant à la définition de la topologie produit, on voit qu'il suffit de prouver qu'on peut toujours construire une fonction continue de $\mathbf{R}$ dans $\mathbf{C}$ prenant des valeurs prescrites en un nombre fini de points. Ceci ne pose pas de problème (on peut par exemple prendre un polynôme d'interpolation de Lagrange).

Exercice 9.2. On peut prolonger $u^{(n)}$ en une fonction continue sur $\overline{\mathbf{N}}$ en posant $u^{(n)}(+\infty)=0$. On prolonge aussi u en posant $u(+\infty)=0$. Alors $u^{(n)}\to u$ uniformément sur $\overline{\mathbf{N}}$ et donc u est continue en $+\infty$, ce qui se traduit par $\lim_{k\to+\infty} u_k=0$.

On peut aussi se passer de $\overline{\mathbf{N}}$, en recopiant la démonstration du point précédent l'exercice. Soit $\varepsilon>0$. Comme $u^{(n)}\to u$ uniformément sur $\mathbf{N}$, il existe $\mathrm{N}_0\in\mathbf{N}$ tel que $|u_k^{(n)}-u_k|<\varepsilon$, quels que soient $n\geqslant \mathrm{N}_0$ et $k\in\mathbf{N}$. Choisissons $n\geqslant \mathrm{N}_0$. Comme $\lim_{k\to+\infty} u_k^{(n)}=0$, il existe $\mathrm{N}\in\mathbf{N}$ tel que $|u_k^{(n)}|<\varepsilon$, pour tout $k\geqslant \mathrm{N}$, et on a $|u_k|\leqslant |u_k^{(n)}-u_k|+|u_k^{(n)}|<2\varepsilon$, pour tout $k\geqslant \mathrm{N}$. On en déduit que $\lim_{k\to+\infty} u_k=0$.

Exercice 9.3. Comme $f_n\to f$ uniformément sur E, elle vérifie le critère de Cauchy uniforme, et on a $\lim\limits_{n\to+\infty}\big(\sup\limits_{x\in\mathrm{E},\,p\in\mathbf{N}}|f_n(x)-f_{n+p}(x)|\big)=0$. Or $|\ell_n-\ell_{n+p}|\leqslant \sup_{x\in\mathrm{E}}|f_n(x)-f_{n+p}(x)|$, et donc $\lim\limits_{n\to+\infty}\big(\sup\limits_{p\in\mathbf{N}}|\ell_n-\ell_{n+p}|\big)=0$, ce qui prouve que $(\ell_n)_{n\in\mathbf{N}}$ est de Cauchy et comme $\mathbf{C}$ est complet, elle admet une limite ℓ.

Soit maintenant $\varepsilon > 0$. Comme $f_n \to f$ uniformément sur E, il existe $\mathrm{N}_0 \in \mathbf{N}$ tel que l'on ait $|f_n(x) - f(x)| < \varepsilon$, quels que soient $n \geqslant \mathrm{N}_0$ et $x \in \mathrm{E}$. Choisissons $n \geqslant \mathrm{N}_0$. En passant à la limite, on en déduit que $|\ell_n - \ell| \leqslant \varepsilon$. Par ailleurs, il existe $\mathrm{M} > 0$ tel que $|f_n(x) - \ell_n| < \varepsilon$, si $\|x\| > \mathrm{M}$; on a donc

$$|f(x) - \ell| \leqslant |f(x) - f_n(x)| + |f_n(x) - \ell_n| + |\ell_n - \ell| < 3\varepsilon,$$

si $\|x\| > \mathrm{M}$, ce qui prouve que f tend vers ℓ à l'infini.

Exercice 10.1. (i) Si $\phi \in \mathrm{E}$, alors $\|\phi\|_\infty$ est fini car $[0,1]$ est compact et une fonction continue sur un compact est bornée. Que $\| \ \|_\infty$ soit une norme sur E est alors immédiat. Maintenant, une suite $(\phi_n)_{n\in\mathbf{N}}$ est de Cauchy pour $\| \ \|_\infty$ si et seulement si elle vérifie le critère de Cauchy uniforme sur $[0,1]$, et $\mathbf{C}$ étant complet, on sait (alinéa 9.2) que $(\phi_n)_{n\in\mathbf{N}}$ admet une limite simple ϕ qui est continue sur $[0,1]$, et que $\phi_n \to \phi$ uniformément sur $[0,1]$, ce qui signifie exatement que $\phi_n \to \phi$ pour $\| \ \|_\infty$. On en déduit la complétude de $(\mathrm{E}, \| \ \|_\infty)$.

(ii) Que $\| \ \|_1$ soit une norme est immédiat à part peut-être le fait que « $\|\phi\|_1 = 0$ » implique « $\phi = 0$ ». Mais si $\phi \neq 0$, il existe $x_0 \in [0,1]$ avec $\phi(x_0) \neq 0$, et comme ϕ est continue, il existe un intervalle I de longueur non nulle ℓ sur lequel $|\phi(x)| \geqslant |\phi(x_0)/2|$. On a alors $\|\phi\|_1 \geqslant \ell\,|\phi(x_0)/2| > 0$. Maintenant, soit $\phi_n = x^{-1/2}\mathbf{1}_{[1/n,1]}$. La suite $(\phi_n)_{n\geqslant 1}$ est de Cauchy car

$$\|\phi_{n+p} - \phi_n\|_1 = \int_{1/(n+p)}^{1/n} x^{-1/2}\,dx = 2\Big(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+p}}\Big) \leqslant \frac{2}{\sqrt{n}}.$$

Si cette suite avait une limite ϕ dans E, on aurait $\lim_{n\to+\infty} \int_0^1 |\phi - \phi_n| = 0$. Or, pour tous $a > 0$ et $n \geqslant 1/a$, on a $\int_0^1 |\phi - \phi_n| \geqslant \int_a^1 |\phi - \phi_n| = \int_a^1 |\phi(x) - x^{-1/2}|\,dx$. On devrait donc avoir $\int_a^1 |\phi(x) - x^{-1/2}|\,dx = 0$, quel que soit $a > 0$, et ϕ étant continue, cela implique que $\phi(x) = x^{-1/2}$, pour tout $x > a$ et tout $a > 0$, et donc que $\phi(x) = x^{-1/2}$ si $x \in]0,1]$. Ceci n'est pas possible car cette fonction n'est pas la restriction à $]0,1]$ d'une fonction continue sur $[0,1]$. En résumé $(\phi_n)_{n\in\mathbf{N}}$ n'a pas de limite dans E, et E n'est pas complet pour $\| \ \|_1$.

(iii) Si les normes étaient équivalentes, les suites de Cauchy seraient les mêmes dans les deux cas, et donc E serait simultanément complet ou non pour les deux normes, ce qui n'est pas le cas. On peut aussi remarquer que $\|\phi_n\|_1 \leqslant 2$ pour tout n, alors que $\|\phi_n\|_\infty \to +\infty$

Exercice 10.2. (i) $\mathrm{id} : (\mathrm{X}, \mathscr{T}_1) \to (\mathrm{X}, \mathscr{T}_2)$ est continue si et seulement si l'image réciproque de tout ouvert de $(\mathrm{X}, \mathscr{T}_2)$ par id est un ouvert de $(\mathrm{X}, \mathscr{T}_1)$, et donc si et seulement si tout élément de $\mathscr{T}_2$ est élément de $\mathscr{T}_1$.

(ii) Si $\phi_n(x) = \phi\big(\frac{x}{n}\big)$, où $\phi(x) = (1 - |x|)\mathbf{1}_{[-1,1]}(x)$, alors $\|\phi_n\|_\infty = 1$, tandis que $\|\phi_n\|_1 = n$ tend vers $+\infty$, ce qui prouve que $\mathrm{id} : (\mathscr{C}_c(\mathbf{R}), \| \ \|_\infty) \to (\mathscr{C}_c(\mathbf{R}), \| \ \|_1)$ n'est pas continue et donc que $\mathscr{T}_\infty$ n'est pas plus fine que $\mathscr{T}_1$.

De même, si $\phi_n(x) = \inf(n, |x|^{-1/2} - 1)\mathbf{1}_{[-1,1]}(x)$, alors $\|\phi_n\|_1 \leqslant \int_{-1}^1 \big(|x|^{-1/2} - 1\big)\,dx = 2$, tandis que $\|\phi_n\|_\infty = n$ tend vers $+\infty$, ce qui prouve que $\mathrm{id} : (\mathscr{C}_c(\mathbf{R}), \| \ \|_1) \to (\mathscr{C}_c(\mathbf{R}), \| \ \|_\infty)$ n'est pas continue et donc que $\mathscr{T}_1$ n'est pas plus fine que $\mathscr{T}_\infty$.

Exercice 12.2. (i) On a $|x + y|_p \leqslant |x|_p$. Si $|x + y|_p < |x|_p$, alors $x = (x + y) - y$ et donc $|x|_p \leqslant \sup(|x + y|_p, |y|_p) < |x|_p$, ce qui est absurde. Donc $|x + y|_p = |x|_p$.

(ii) Comme $u_n \to 0$, la série $\sum_{n=1}^{+\infty} u_n$ converge et si on note y sa somme, alors $|y|_p \leqslant \sup_{n\geqslant 1} |u_n|_p$. Comme on a supposé $|u_0|_p > |u_n|_p$, pour tout $n \geqslant 1$, on en déduit $|y|_p < |u_0|$, puis $|u_0 + y|_p = |u_0|_p$; en particulier, $u_0 + y = \sum_{n\in\mathbf{N}} u_n \neq 0$.

Exercice 12.5. (i) Par définition f est localement constante si et seulement si $\{x \in \mathrm{X},\ f(x) = y\}$ est voisinage de chacun des ses points (ce qui équivaut à ce qu'il soit ouvert). Il en résulte que l'image inverse de tout ensemble (en particulier d'un ouvert) est ouverte, et donc que f est continue.

(ii) $\{x \in [0,1],\ f(x) = f(0)\}$ est ouvert et fermé d'après le (i), et comme il est non vide et que $[0,1]$ est connexe, c'est $[0,1]$ tout entier. Autrement dit, les seules fonctions localement constantes sur $[0,1]$ sont les fonctions constantes.

(iii) $a + p^n\mathbf{Z}_p$ est à la fois ouvert et fermé, et donc $\{x,\ \mathbf{1}_{a+p^n\mathbf{Z}_p}(x) = 0\}$ et $\{x,\ \mathbf{1}_{a+p^n\mathbf{Z}_p}(x) = 1\}$ sont ouverts, ce qui permet d'utiliser le (i).

(iv) Si $\phi : \mathbf{Z}_p \to \mathrm{Y}$ est localement constante et si $a \in \mathbf{Z}_p$, il existe $n_a \in \mathbf{N}$ tel que ϕ soit constante sur $a + p^{n_a}\mathbf{Z}_p$. Les $a + p^{n_a}\mathbf{Z}_p$ forment un recouvrement ouvert de $\mathbf{Z}_p$ et, $\mathbf{Z}_p$ étant compact, on peut en extraire un sous-recouvrement fini par des $a + p^{n_a}\mathbf{Z}_p$, avec $a \in \mathrm{A}$ et A est un ensemble fini. Soit $n = \sup_{a\in\mathrm{A}} n_a$. Si $b \in \mathbf{Z}_p$, il existe $a \in \mathrm{A}$ tel que $b \in a + p^{n_a}\mathbf{Z}_p$ et, comme $n \geqslant n_a$, on a $b + p^n\mathbf{Z}_p \subset a + p^{n_a}\mathbf{Z}_p$ (deux boules sont soit disjointes soit l'une est incluse dans l'autre). Il en résulte que ϕ est constante sur $b + p^n\mathbf{Z}_p$ pour tout $b \in \mathbf{Z}_p$.

(v) Comme $\mathbf{Z}_p$ est compact, une fonction continue f sur $\mathbf{Z}_p$ est uniformément continue. Ceci se traduit, en notant $\|\ \|$ la norme sur $\mathbf{R}$ ou la norme p-adique sur $\mathbf{Q}_p$, par l'existence, pour tout $\varepsilon > 0$, de $n \in \mathbf{N}$, tel que $\|f(x) - f(y)\| \leqslant \varepsilon$, pour tous $x, y \in \mathbf{Z}_p$ vérifiant $|x - y|_p \leqslant p^{-n}$. Soit alors $\phi = \sum_{i=0}^{p^n-1} f(i)\mathbf{1}_{i+p^n\mathbf{Z}_p}$. Par construction, ϕ est localement constante, et on a $\|f(x) - \phi(x)\| \leqslant \varepsilon$ pour tout $x \in \mathbf{Z}_p$ (en effet, sur $i + p^n\mathbf{Z}_p$, on a $f(x) - \phi(x) = f(x) - f(i)$ et $|x - i|_p \leqslant p^{-n}$). Ceci permet de conclure.

(vi) On peut prendre la fonction qui envoie $x \in \mathbf{Z}_p$, dont l'écriture en base p est $\sum_{n=0}^{+\infty} a_n p^n$ (les a_n sont des éléments de $\{0, 1, \ldots, p-1\}$) sur $\sum_{n=0}^{+\infty} a_n p^{-1-n}$; nous laissons le soin au lecteur de vérifier que cette fonction est 1-lipschitzienne et d'imaginer à quoi elle correspond sur la description arboricole de $\mathbf{Z}_p$. L'image d'un connexe par une fonction continue est un connexe, et comme les composantes connexes de $\mathbf{Z}_p$ sont des points, toute fonction continue de $[0,1]$ dans $\mathbf{Z}_p$ est constante.

Exercice 12.6. (i) On a $\left|\left(\frac{7}{9}\right)^n\right|_7 = 7^{-n}$ et donc la série $\sum_{n=0}^{+\infty}\left(\frac{7}{9}\right)^n\binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_7, \mathbf{Q}_7)$ vers une fonction continue f. De plus, si $k \in \mathbf{N}$, alors $f(k) = \left(\frac{16}{9}\right)^k$, d'après la formule du binôme. On en déduit que $f(2k) = f(k)^2$ pour tout $k \in \mathbf{N}$, ce qui implique, compte-tenu de la densité de $\mathbf{N}$ dans $\mathbf{Z}_7$ et de la continuité de f, que $f(2x) = f(x)^2$ pour tout $x \in \mathbf{Z}_7$. Il en résulte que la somme S de la série qui nous intéresse est une racine carrée de $\frac{16}{9}$; on a donc $\mathrm{S} = \pm\frac{4}{3}$. Par ailleurs, tous les termes de la série, sauf le premier, sont dans $7\mathbf{Z}_7$, et donc $\mathrm{S} - 1 \in 7\mathbf{Z}_7$ et $\mathrm{S} = \frac{-4}{3}$, ce que l'on cherchait à démontrer.

(ii) Dans $\mathbf{R}$ la somme de la série est $\frac{4}{3}$.

Index du chapitre