UNIVERSITÉ DE NANTES

Licence de mathématiques
Licence d'économie-gestion
Licence d'informatique

CMI – PSR

2018-2019

Logique, suites numériques, dénombrement

Laurent Guillopé

Département de mathématiques, UFR Sciences et techniques
Laboratoire de mathématiques Jean Leray
Université de Nantes

Ces notes sont à la base des 9 séances de cours. Certains passages (sections 2.4-6, au fil du chapitre 3 notamment) n'ont pas été exposés: y sont développés des exemples, dont la lecture est fortement recommandée (avec une tablette de chocolat pour la fin du 1.4.4) et qui sont en lien avec le distanciel.

Version : 3 mars 2020 10:00

UNIVERSITÉ DE NANTES

Licence de mathématiques
Licence d'économie-gestion
Licence d'informatique

CMI – PSR

2018-2019

Logique, suites numériques, dénombrement

Laurent Guillopé

Département de mathématiques, UFR Sciences et techniques
Laboratoire de mathématiques Jean Leray
Université de Nantes

I : Logique et ensembles

Ces notes sont à la base des 9 séances de cours. Certains passages (sections 2.4-6, au fil du chapitre 3 notamment) n'ont pas été exposés: y sont développés des exemples, dont la lecture est fortement recommandée (avec une tablette de chocolat pour la fin du 1.4.4) et qui sont en lien avec le distanciel.

Version : 3 mars 2020 10:00

UNIVERSITÉ DE NANTES

Licence de mathématiques
Licence d'économie-gestion
Licence d'informatique

CMI – PSR

2018-2019

Logique, suites numériques, dénombrement

Laurent Guillopé

Département de mathématiques, UFR Sciences et techniques
Laboratoire de mathématiques Jean Leray
Université de Nantes

II : Suites numériques

Ces notes sont à la base des 9 séances de cours. Certains passages (sections 2.4-6, au fil du chapitre 3 notamment) n'ont pas été exposés: y sont développés des exemples, dont la lecture est fortement recommandée (avec une tablette de chocolat pour la fin du 1.4.4) et qui sont en lien avec le distanciel.

Version : 3 mars 2020 10:00

UNIVERSITÉ DE NANTES

Licence de mathématiques
Licence d'économie-gestion
Licence d'informatique

CMI – PSR

2018-2019

Logique, suites numériques, dénombrement

Laurent Guillopé

Département de mathématiques, UFR Sciences et techniques
Laboratoire de mathématiques Jean Leray
Université de Nantes

III : Dénombrement

Ces notes sont à la base des 9 séances de cours. Certains passages (sections 2.4-6, au fil du chapitre 3 notamment) n'ont pas été exposés: y sont développés des exemples, dont la lecture est fortement recommandée (avec une tablette de chocolat pour la fin du 1.4.4) et qui sont en lien avec le distanciel.

Version : 3 mars 2020 10:00

Table des matières

Chapitre 1

Logique et ensembles

> *« Le développement des mathématiques vers une plus grande précision a convergé, c'est bien connu, vers la formalisation d'une importante partie des mathématiques, de telle sorte qu'on peut démontrer n'importe quel théorème en appliquant mécaniquement juste quelques règles. »*
>
> K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I.* Monatshefte für Math. Phys. 1931.

La *logique (mathématique)* est un domaine des mathématiques qui corsète tout l'édifice même des mathématiques (et d'autres disciplines scientifiques). Elle fournit le cadre conceptuel pour le traitement des formules logiques, que ce soit les prémisses ou axiomes d'une théorie ou bien les théorèmes établis par une démonstration (formalisation, suite d'enchaînements logiques, raisonnement aux articulations plus ou moins considérables). Le théorème de complétude de Gödel[1]. (1931) assure que tout raisonnement mathématique peut être formulé dans le langage des prédicats et ses règles de calcul. La logique assure la validité des inférences, sur des objets (éléments des modèles) qui peuvent être très variés.

Insistons sur la limitation à la logique mathématique. La logique naturelle possède des attributs que la première ignore : le tiers-exclu ne donne que 2 valeurs de vérité (`Vrai`, `Faux`), les notions d'incertain, de nécessité ou de temporalité sont absentes

La formalisation d'une logique passe par la définition d'un langage (ou système) formel, à partir d'un alphabet et suivant des règles morphologiques (l'alphabet) syntaxiques (phrases et énoncés) clairement définies. Cette logique nécessite des règles d'évaluation des valeurs de vérité. Elle est réalisable dans divers domaines, à travers des modèles dont chacun précise une sémantique particulière.

Historiquement, la logique formelle se développe sous sa forme moderne à la fin

1. Kurt Gödel, 28 avril 1906, Brno, Tchéquie – 14 janvier 1978, Princeton, É.-U..

du XIXe siècle (Boole, De Morgan, Cantor, Frege,...), juste au moment où les mathématiciens s'interrogeaient sur la nature des entiers, sur celle des ensembles d'entiers et donc sur ce que sont les ensembles. Les apories de la logique et de la théorie des ensembles (face au paradoxe « l'ensemble de tous les ensembles »[2] ou celui du menteur[3]) ont été surmontées par une reprise systématique de leurs fondements. Ce cours exposera les débuts de ces théories qui sont désormais bien acceptés théoriquement et dans la pratique.

Ces systèmes logiques suffisent pour formaliser la grande majorité de raisonnements mathématiques ordinaires, comme l'affirmait Gödel déjà au début du XXe siècle. Le développement de l'informatique (tant au niveau de la puissance des unités de calcul que des outils logiciels) a permis l'apparition d'assistants de preuve. Comment démontrer le théorème de Fermat à partir de quelques axiomes et règles d'inférence? Le phénomène [2] est analogue à l'élaboration de puces complexes à partir de simples composants élémentaires (mémoire, processeurs) : ceux-ci sont combinés pour produire successivement des assemblages de plus en plus complexes, parvenant à construire des systèmes complexes défiant l'entendement (pilotage d'installations industrielles, contrôle aérien, jeux de go). Cette approche modulaire est utilisée aussi pour les assistants de preuve, capables d'élaborer des preuves de théorèmes substantiellement consistants à partir de définitions, propositions, raisonnements, abréviations, portions de codes.

Développons quelques unes des remarques précédentes

1. L'activité mathématique énonce des expressions, des assertions ou des formules, pour démontrer leur véracité ou leur fausseté, leur conférant une valeur de vérité (`Vrai` ou `Faux`)[4]. Ces processus sont basés sur le raisonnement et la démonstration[5], menant des axiomes et hypothèses par des règles logiques à cette déclaration de la valeur V ou F pour l'expression donnée. La *logique formelle* (dite parfois *logique symbolique*) a pour but de caractériser les raisonnements valides, en traitant formellement les caractères de vérité, en formalisant et justifiant l'intuition, tout en permettant le raisonnement (humain ou par machine) dans des situations complexes souvent non intuitives. Au delà de la certification du raisonnement établissant tel énoncé mathématique, la logique a des applications industrielles comme la validité de codes complexes.
2. Avec ses termes, ses constructions et ses développements, l'énoncé mathématique vise à la précision, l'absence d'ambiguïté, la clarté, la concision, la

2. Soit $A = \{x \notin A\}$: si $A \in A$, alors $A \notin A$ ce qui est contradictoire, pareillement si $A \notin A$ alors $A \in A$ tout autant contradictoire.

3. « Je mens ».

4. On considère ici les énoncés susceptibles d'avoir une valeur de vérité. Un énoncé qui n'est pas `Vrai` n'est pas nécessairement `Faux` : d'après le théorème d'incomplétude de Gödel, tout langage formel prenant en compte l'arithmétique des entiers naturels a des énoncés indécidables.

5. Les développements mathématiques présentent bien d'autres aspects : sont-ils intéressants? la résolution de ce problème est-elle pertinente? quelles applications ont-ils? On se limite ici à la logique et son apport de validation du raisonnement.

lisibilité, la justesse et la rigueur.

3. La logique formelle manipule des *éléments primitifs* constituants d'expressions ou de *formules*, appelées propositions ou prédicats. Ces formules apparaissent comme des mots construits sur un alphabet constitué de lettres ($a, \mathbb{N}, \mathrm{Z}, \aleph, \mathrm{i}, \pi, \dots$) qui sont des variables ou constantes ($\top, \bot$ les constantes `Vrai` et `Faux` resp.), de symboles ($+, \vee, \wedge, >, =, \in, \forall, \neg, \dots$ et des parenthèses (« (» et «) »), des opérations, des règles d'inférence, des quantificateurs,...) . Ces opérations produisent un raisonnement, traduisant formellement comment un ensemble d'hypothèses supposées vraies implique la véracité d'un énoncé ; cet énoncé, avec ses hypothèses, est souvent exprimé en langage naturel.

   Une proposition est dotée d'une valeur de vérité (`Vrai` ou `Faux`), un prédicat est une expression qui dépend d'une inconnue (ou d'un paramètre). Voilà un exemple de formule de la logique formelle [6] concernant la suite $\mathbf{u} = (u_n)_{n\geq 0}$.

$$\forall \mathrm{A} > 0, \quad \exists \mathrm{N} \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad (n \geq \mathrm{N} \Longrightarrow u_n \geq \mathrm{A}), \tag{1.1}$$

   où l'entier N dépend du A donné, formule logique qu'on peut exprimer de manière équivalente suivant

$$\forall \mathrm{A} > 0, \quad \exists \mathrm{N} \in \mathbb{N}, \quad \forall k \in \mathbb{N}, \quad u_{\mathrm{N}+k} \geq \mathrm{A}, \tag{1.2}$$

   ou encore de manière graphique (plus intuitive, voire heuristique) comme dans la figure I.1 où l'ensemble des réels a été représenté par la *droite réelle*. Ces formules seront traduites dans le langage vernaculaire par l'expression « *la suite* **u** *converge vers plus l'infini lorsque (l'indice)* n *tend vers l'infini* ». Cette logique symbolique représente un modèle idéal du langage mathématique et de ses expressions. La complexité des démonstrations ou de certaines expressions tend à nier des expressions intuitives ou heuristiques, ce qui est regrettable comme peut l'être tout autant la manque de clarté ou de rigueur dans le déroulé des démonstrations.

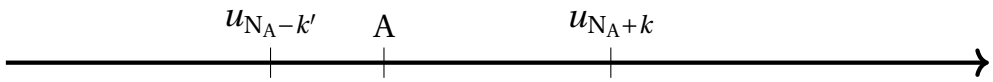

FIGURE I.1 – Traduction par un graphique intuitif de l'expression formelle (1.2). Les entiers k et k' sont supposés positifs.

4. Ces formules de la logique formelle sont compliquées. Godement [7, p. 23] écrit en 1963 « On a calculé que, si l'on cherchait à écrire en langage formalisé

6. La virgule n'est pas un élément primitif des expressions de la logique formelle : on l'utilisera néanmoins ici et *infra* pour améliorer la lisibilité des expressions formelles comme celle-ci $\forall \mathrm{A} > 0 \exists \mathrm{N} \in \mathbb{N} \forall n \in \mathbb{N} (n \geq \mathrm{N} \Longrightarrow u_n \geq \mathrm{A})$. De même, la bonne compréhension des règles de priorité d'évaluation des symboles permet d'alléger le parenthésage des formules.

un objet mathématique aussi simple (en apparence…) que le nombre 1, on trouverait un assemblage comportant plusieurs dizaines de milliers de signes (les signes fondamentaux sont un très petit nombre, mais chacun d'eux peut naturellement être répété un grand nombre de fois dans un même assemblage). »

5. Les énoncés mathématiques, affirmations du développement mathématique, sont de nature très diverse : définition, axiome, postulat, théorème, proposition (petit théorème), lemme (tout petit théorème), corollaire (conséquence directe ou quasi-immédiate d'un théorème), conjecture,… C'est en résolvant (ou assemblant) ces formules logiques qu'on parvient en théorie à démontrer la vérité de telle assertion et la validité de tel théorème, à partir des axiomes de base de la théorie logique. Mais, en pratique, on n'écrira jamais la formule logique correspondant à tel ou tel objet à partir des entités logiques de base. Cependant, on manipulera ce formalisme pour des raisonnements, mêlant la compréhension en langage naturel, l'expression de l'intuition et l'articulation logique avec les connecteurs de base et les quantificateurs.

6. Le raisonnement mathématique repose sur des notions primitives (celle d'ensemble par ex.), parfois difficiles à justifier complètement, mais qu'on adopte intuitivement aisément et où un raisonnement formalisé permet de manipuler dans le cadre axiomatique ZFC (pour Zermelo [7], Fraenkel [8] et l'axiome du choix) les propositions logiques exprimées dans des formules, d'étudier leur vérité (V) ou leur fausseté (F) et d'en créer de nouvelles syntaxiquement correctes par combinaison avec des connecteurs logiques booléens [9].

7. La logique appartient aux fondements des mathématiques et cette théorie est pratiquée par quasiment tous les chercheurs. Ses développements (en mathématiques et informatique avec la puissance accrue des processeurs) ont abouti récemment à l'élaboration d'assistants de preuve (`coq`, `Isabelle/HOL`, `lean`,…), de démonstrateurs automatiques et de systèmes experts, des programmes informatiques variés permettant de formaliser et de vérifier des démonstrations mathématiques : établir un théorème revient à trouver une formule valide qui représente le théorème dans l'ensemble des formules construites à partir des éléments primitifs.

   Ces programmes de formalisation de mathématiques se développent afin de produire un corpus complètement formalisé de mathématiques, avec des traitements algorithmiques pour traiter ce corpus de formules et s'assurer de la validité de démonstrations qui ont requis l'usage d'ordinateurs comme le théorème des quatre couleurs ou la conjecture de Kepler sur l'empilement de sphères.

7. E. Zermelo, 27 juillet 1871, Berlin, Allemagne – 21 mai 1953, Fribourg-en-Brisgau, Allemagne.
8. A. A. H. Fraenkel, 17 février 1891, Munich, Allemagne – 15 octobre 1965, Jérusalem, Israël.
9. G. Boole, 2 novembre 1815, Lincoln, Royaume-Uni – 8 décembre 1864, Ballintemple, Irlande.

1.1 Propositions, prédicats et connecteurs

1.1.1 Propositions et prédicats

La *logique propositionnelle* permet de manipuler des propositions. Définir la structure de ces assertions et des formules, c'est préciser la syntaxe du langage mathématique, employée *stricto sensu* avec plus ou moins de rigueur afin de ne pas brider excessivement l'intuition et la compréhension des notions et résultats démontrés.

Si rudimentaire soit-il, le calcul propositionnel apparaît dans tout système formel et présente bien des concepts et des méthodes simples, préparant à des systèmes plus élaborés. Il est complété par le calcul des prédicats (dit *langage du premier ordre*)par ajout de propositions dépendant de une ou plusieurs variables et la disposition des quantificateurs $\forall, \exists$.

DÉFINITION 1.1: *Une* proposition formelle *(ou* formule*)* $\mathcal{A}$ *est une assertion portant sur des objets mathématiques, objets mis en relation dans un contexte précisé. Une proposition est une suite de*

- *éléments d'un alphabet, variables propositionnelles (telles* $\mathcal{A}, p$*), constantes (*π *;* `Vrai` *:* $\top$ *de l'anglais* True *ou* V*,* `Faux` *:* $\bot = \neg\top$ *ou* F*), fonctions d'arité fixée, ;*
- *des symboles (*$\in, \int, \sum, \nabla, \ldots$*);*
- *des formules atomiques* $\mathcal{A}[x]$ *formées à partir d'une fonction* $\mathcal{A}$ *et un terme* t *(constant ou variable);*
- *parenthèses ouvrantes et fermantes;*
- *symboles logiques (ou connecteurs) (*$\wedge$ *pour «* et *»,* $\vee$ *pour «* ou *»,...).*

Chaque proposition est assortie d'une valeur de vérité : soit V *:* `Vrai`*, soit* F *:* `Faux`*, il n'y a pas de possibilité tierce. Une proposition ne peut être en même temps* `Vrai` *et* `Faux`*.*

Un prédicat est un énoncé $\mathcal{A}[x]$ *qui dépend d'un objet variable* x *(issu d'un certain domaine, parfois dit référentiel) du prédicat;* x *peut être d'arité* $k > 1$, i. e. *la variable* x *a* k *composantes* $x = (x_1, \ldots, x_k)$*. Les quantificateurs* $\forall, \exists$ *peuvent être utilisés. En donnant une valeur à* x *ou en utilisant un quantificateur, le prédicat* $\mathcal{A}[x]$ *est considéré comme une proposition avec une valeur de vérité.*

La notion d'*objet* mathématique est polymorphe : nombre, ensemble, fonction, figure, tableau, arbres,...). Voilà quelques exemples d'expressions, énoncés sans sens ou de véritables propositions avec leur valeur de vérité

▷ EXEMPLES 1.1:

1.1.1 les « 1+ », « x= », « Pour tout entier x, $x+1=2 \Longrightarrow 1$ », « 3-2) » n'ont pas de sens : ce sont formules incorrectes.

1.1.2 « La phrase suivante est fausse. La phrase précédente est vraie. ». C'est une formule incorrecte (et il n'y a pas de paradoxe !)

1.1.3 $3+\pi = e$. [F]
1.1.4 $\sqrt{2}$ est irrationnel. [V]
1.1.5 La terre est plate. [F]
1.1.6 Il fait beau [F] (à l'heure où j'écris cette liste d'exemples : demain cela pourrait être différent)
1.1.7 « Comment vas-tu ? » n'est pas une proposition, à cause de l'incertitude dans la réponse à choisir entre le vrai et le faux.
1.1.8 $14+3 = 17$. [V] (calcul en base 10), $14+3 = 11$. [V] (calcul en hexadécimal)
1.1.9 Tout entier impair > 5 est somme de trois nombres premiers (Goldbach-Helfgott). [V]
1.1.10 Un triangle ABC est rectangle si et seulement si $AB^2 = AC^2 + BC^2$. [V] ◁

et pour compléter quelques prédicats avec leur variable

▷ EXEMPLES 1.2:
1.2.1 $\log n / \log(13)$ est irrationnel. [n ?]
1.2.2 L'entier n est pair. [n ?]
1.2.3 Tout entier impair n est somme de trois nombres premiers (Goldbach-Helfgott). [n ?]
1.2.4 L'équation $x^p + y^p = z^p$ n'a pas de solutions entières avec $xyz \neq 0$ [p ?] (si $p = 2$, c'est faux, alors que si $p > 2$ c'est vrai, comme démontré par Fermat-Wiles).
1.2.5 L'aire du carré de côté de longueur a est $4a$. [a ?] (si $a = 4$ ou $a = 0$, la proposition est vraie, sinon elle est fausse).
1.2.6 La courbe $\mathscr{C}$ est un cercle passant par les points M et N. [$\mathscr{C}$?]
1.2.7 $\mathcal{P}\text{remier}[x] \Longrightarrow \mathcal{I}\text{mpair}[x]$. [$x$?] le Prédicat $\mathcal{P}\text{remier}[x]$ est $\top$ (`Vrai`) si x est non nul, au moins égal à 2 avec pour seuls diviseurs 1 et x. ◁

Le principe du tiers-exclu énonce qu'une proposition est soit `Vrai`, soit `Faux` (il correspond à l'équivalence $\mathcal{A} \vee \neg\mathcal{A} \equiv \top$), alors que le principe de non-contradiction interdit qu'elle soit `Vrai` et `Faux` ($\mathcal{A} \wedge \neg\mathcal{A} \equiv \bot$) [10]. En mathématique, une proposition est dite vraie si elle est démontrable par appel aux axiomes et prémisses de la théorie et diverses inférences.

La construction des formules syntaxiquement correctes se fait de manière inductive après le choix des symboles constitutifs : lettres désignant une proposition $\mathcal{A}, \mathcal{B}, \ldots$, parenthèses «), (», connecteurs $\neg, \wedge, \vee, \Longrightarrow, \Longleftrightarrow$, symboles lieurs $+, \times, \int, \Pi, =$ … :

THÉORÈME 1.1: *Toutes les formules sont obtenues par l'application inductive des règles élémentaires suivantes*

10. Soit $\mathcal{A}$ contradictoire, *i. e.* $\mathcal{A}$ `Vrai` et `Faux`. Soit $\mathcal{X}$ une proposition. Puisque $\neg\mathcal{A}$ est `Vrai`, alors il en est de même pour $\mathcal{A} \Longrightarrow \mathcal{X} \equiv \neg\mathcal{A} \vee \mathcal{X}$ et par suite, vu que $\mathcal{A}$ est `Vrai`, la véracité de l'assertion $\mathcal{X}$. Il en est de même pour $\neg\mathcal{X}$ et donc $\neg\mathcal{X}$ est à la fois `Vrai` et `Faux`, et ce quelle que soit la proposition $\mathcal{X}$. Ainsi, une théorie avec une seule proposition contradictoire ne contient que des énoncés contradictoires, ce qui ne laisse pas beaucoup d'assertions dont la véracité est à établir !

— *Une lettre désignant une proposition est une formule dite atomique,*
— *Si $\mathcal{A}$ est une proposition, $\neg\mathcal{A}$ en est une,*
— *Si $\mathcal{A},\mathcal{B}$ sont des propositions $\mathcal{A}\wedge\mathcal{B},\mathcal{A}\vee\mathcal{B},\mathcal{A}\Longrightarrow\mathcal{B},\mathcal{A}\Longleftrightarrow\mathcal{B}$ sont aussi des propositions.*

La valeur de vérité d'une proposition ne dépend que de celles de ses composants atomiques.

La formation des prédicats est similaire, avec ajout des quantificateurs universels $\forall$ et $\exists$ avec les formules $\forall x\mathcal{A}[x]$ et $\exists x\mathcal{A}[x]$.

1.1.2 Connecteurs et tables de vérité

Les connecteurs logiques fondamentaux mettent en relation les propositions et prédicats, permettant de construire par induction de nouvelles formules syntaxiquement correctes. La sémantique de ces formules (interprétation, validité, satisfiabilité,...) ne sera pas examinée de manière détaillée ici.

Si $\mathcal{A}$ et $\mathcal{B}$ sont deux propositions, alors on peut leur appliquer un connecteur unaire ($\neg$) ou deux connecteurs binaires ($\wedge,\vee$), les propositions obtenues ayant une valeur de vérité en lien avec celles de $\mathcal{A}$ et $\mathcal{B}$.

1. la *négation* de $\mathcal{A}$, notée $\neg\mathcal{A}$ et épelée comme « non A », est `Vrai` si et seulement si $\mathcal{A}$ est `Faux`.
2. la *disjonction* (inclusive, qui correspond au « ou » de la langue) de $\mathcal{A}$ et $\mathcal{B}$, notée $\mathcal{A}\vee\mathcal{B}$ [11] est vraie si $\mathcal{A}$ ou $\mathcal{B}$ est vraie, fausse si $\mathcal{A}$ et $\mathcal{B}$ sont fausses;
3. la *conjonction* de $\mathcal{A}$ et $\mathcal{B}$, notée $\mathcal{A}\wedge\mathcal{B}$ (voire $\mathcal{A}\,\&\,\mathcal{B}$), est vraie si $\mathcal{A}$ et $\mathcal{B}$ sont vraies, fausse si $\mathcal{A}$ ou $\mathcal{B}$ est fausse;

△ REMARQUE 1.1: Vu la formule où les deux membres ont même table de vérité

$$\mathcal{A}\wedge\mathcal{B}\equiv\neg\big((\neg\mathcal{A})\vee(\neg\mathcal{B})\big),$$

il suffit d'introduire les connecteurs $\vee$ et $\neg$. ▽

DÉFINITION 1.2: *Deux propositions $\mathcal{A}$ et $\mathcal{B}$ sont dites* équivalentes logiquement *si elles sont vraies simultanément ou bien fausses simultanément.*

Si deux formules $\mathcal{P}$ et $\mathcal{Q}$ contiennent les $k\geq 1$ propositions $\mathcal{A}_1,\ldots\mathcal{A}_k$ comme sous-formule, on établira les 2^k valeurs de vérité des deux propositions $\mathcal{P}$ et $\mathcal{Q}$ suivant les valeurs de vérité des k formules $\mathcal{A}_1,\ldots,\mathcal{A}_k$: ces valeurs seront rangées dans une table, dite table de vérité.

Voilà quelques exemples de formules logiques (proposition ou prédicat) avec des connecteurs fondamentaux. Le symbole $\equiv$ indique l'équivalence des propositions qui l'encadrent : $\mathcal{A}\equiv\mathcal{B}$ indiquent que $\mathcal{A}$ et $\mathcal{B}$ sont équivalents.

▷ EXEMPLES 1.3:

11. voire $\mathcal{A}\mid\mathcal{B}$, au risque de confondre avec l'opérateur de division $|$.

1.3.1 $\mathcal{A} \equiv$ (6 est un nombre pair) $\equiv (2 \mid 6)$ [V]
1.3.2 $\mathcal{B} \equiv$ (21 est un multiple de 4) $\equiv (4 \mid 21)$ [F]
1.3.3 $\mathcal{A} \wedge \mathcal{B} \equiv ((2 \mid 6)$ et $(4 \mid 21))$ [F]
1.3.4 $\mathcal{A} \vee \mathcal{B} \equiv ((2 \mid 6)$ ou $(4 \mid 21))$ [V]
1.3.5 $\neg\mathcal{B} \equiv$ (21 n'est pas un multiple de 4) [F]
1.3.6 $\mathcal{C}[n] \equiv$ (2019 n'est pas un multiple de n) [n ?] $(2019 = 3 * 673)$
1.3.7 $\mathcal{C}[n = 4] \wedge \mathcal{C}[3] \wedge \mathcal{C}[n]$
1.3.8 Si $\mathrm{A} = \{a, b\}$, l'ensemble des parties $\mathscr{P}(\mathrm{A})$ a quatre éléments

$$\mathscr{P}(\mathrm{A}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\},$$

à moins que a et b coïncident auquel cas $\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$ a 2 éléments. De manière générale on pourra montrer par récurrence que si A est fini avec k éléments alors $\mathscr{P}(\mathrm{A})$ a 2^k éléments (cf. la proposition 3.4 du troisième chapitre.) ◁

Afin de clarifier le calcul des valeurs de vérité, il est parfois opportun de dresser des *tables de vérité* récapitulant les valeurs de vérité issues de certaines combinaisons de propositions et de connecteurs logiques. Suivant la représentation (V,F ou 1,0 ou $\top, \bot$) des constantes `Vrai` et `Faux`, on a la table de vérité associée au connecteur de négation $\neg$:

$\mathcal{A}$	$\neg\mathcal{A}$
V	F
F	V

$\mathcal{A}$	$\neg\mathcal{A}$
1	0
0	1

$\mathcal{A}$	$\neg\mathcal{A}$
$\top$	$\bot$
$\bot$	$\top$

TABLE I.1 – Table de vérité du connecteur unaire $\neg$.

Ainsi la table I.2 considère les valeurs de vérité de formules construites à partir de deux propositions $\mathcal{A}, \mathcal{B}$ et des connecteurs $\wedge, \vee, \neg$ On remarque les mêmes co-

$\mathcal{A}$	$\mathcal{B}$	$\neg\mathcal{A}$	$\neg\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	$\neg(\mathcal{A} \wedge \mathcal{B})$	$(\neg\mathcal{A}) \vee (\neg\mathcal{B})$	$\neg(\mathcal{A} \vee \mathcal{B})$	$(\neg\mathcal{A}) \wedge (\neg\mathcal{B})$
V	V	F	F	V	V	F	F	F	F
V	F	F	V	F	V	V	V	F	F
F	V	V	F	F	V	V	V	F	F
F	F	V	V	F	F	V	V	V	V

TABLE I.2 – Tables de vérités de diverses formules binaires.

lonnes de valeurs de vérité dans les colonnes 7 et 8, 9 et 10, correspondant aux lois de Morgan du théorème 1.2 ci-dessous.

$$\neg(\mathcal{A} \wedge \mathcal{B}) \equiv (\neg\mathcal{A}) \vee (\neg\mathcal{B}), \quad \neg(\mathcal{A} \vee \mathcal{B}) \equiv (\neg\mathcal{A}) \wedge (\neg\mathcal{B}).$$

À partir de ces connecteurs de base, on en construit d'autres qui sont éventuellement abrégés par le choix de symboles particuliers, par exemple les quatre connecteurs binaires introduits ci-dessous, avec comme tables de vérité dans la table I.3 :

TABLE I.3 – La table de vérité des connecteurs $\Longrightarrow$, $\Longleftrightarrow$ et $\oplus$, ainsi que celle de la contraposée.

$\mathcal{A}$	$\neg\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}\Longrightarrow\mathcal{B}$	$\mathcal{A}\Longleftrightarrow\mathcal{B}$	$\mathcal{A}\oplus\mathcal{B}$	$(\neg\mathcal{B})\Longrightarrow(\neg\mathcal{A})$
V	F	V	V	V	F	V
V	F	F	F	F	V	F
F	V	V	V	F	V	V
F	V	F	V	V	F	V

1. L'*implication* $\Longrightarrow$: la proposition « $\mathcal{A}\Longrightarrow\mathcal{B}$ » est `Vrai` si et seulement si soit $\mathcal{A}$ est `Faux`, soit $\mathcal{A}$ et $\mathcal{B}$ sont `Vrai`. Ainsi la proposition « $(\mathcal{A}\Longrightarrow\mathcal{B})$ » est une réécriture de $(\neg\mathcal{A})\vee\mathcal{B}$. Sa négation est donnée par $\neg(\mathcal{A}\Longrightarrow\mathcal{B})\equiv(\mathcal{A}\wedge\neg\mathcal{B})$
2. L'*équivalence* $\Longleftrightarrow$: la proposition « $\mathcal{A}\Longleftrightarrow\mathcal{B}$ » est définie comme la double implication « $(\mathcal{A}\Longrightarrow\mathcal{B})\wedge(\mathcal{B}\Longrightarrow\mathcal{A})$ ». On dira que « $\mathcal{A}$ *équivaut à* $\mathcal{B}$ ».
3. Le « *ou exclusif* » $\oplus$: il est défini par diverses formules
$$\mathcal{A}\oplus\mathcal{B}\equiv\big((\mathcal{A}\wedge\neg\mathcal{B})\vee(\mathcal{B}\wedge\neg\mathcal{A})\big)\equiv\big((\mathcal{A}\vee\mathcal{B})\wedge(\neg\mathcal{A}\vee\neg\mathcal{B})\big).$$
4. La *contraposée* $\neg\mathcal{B}\Longrightarrow\neg\mathcal{A}$: elle est équivalente à l'implication $\mathcal{A}\Longrightarrow\mathcal{B}$ [12]. La table I.3 indique les valeurs de vérité de diverses formules, dont notamment une implication et sa contraposée. Voir aussi au début de la section 1.3 et la sous-section 1.3.3 ci-dessous.

Les premières propriétés de ces connecteurs logiques sont rassemblées dans le théorème suivant qui indique le caractère booléen de ces opérations sur les propositions : on comparera ces opérations sur les propositions avec celles opérant sur les parties d'un ensemble suivant les propriétés de la proposition 1.2.

Les équivalences de ce théorème sont utiles pour simplifier les formules, voire les normaliser (garder les opérateurs $\neg$ et $\wedge$, mais faire disparaître les $\vee$) ou les restructurer.

THÉORÈME 1.2: *Soient $\mathcal{A},\mathcal{B},\mathcal{C}$ des propositions avec valeurs de vérité `Vrai` ou `Faux`. Les équivalences suivantes ont lieu : les membres de gauche ont même valeur de vérité que ceux de droite.*

1. *commutativité :* $\mathcal{A}\wedge\mathcal{B}\equiv\mathcal{B}\wedge\mathcal{A}$, $\mathcal{A}\vee\mathcal{B}\equiv\mathcal{B}\vee\mathcal{A}$,
2. *associativité :* $\mathcal{A}\wedge(\mathcal{B}\wedge\mathcal{C})\equiv(\mathcal{A}\wedge\mathcal{B})\wedge\mathcal{C}$, $\mathcal{A}\vee(\mathcal{B}\vee\mathcal{C})\equiv(\mathcal{A}\vee\mathcal{B}\vee\mathcal{C})$,

12. On ne confondra pas avec l'*implication réciproque* $\mathcal{B}\Longrightarrow\mathcal{A}$.

3. *idempotence :* $\mathcal{A} \wedge \mathcal{A} \equiv \mathcal{A}$, $\mathcal{A} \vee \mathcal{A} \equiv \mathcal{A}$,
4. *distributivité :* $\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \equiv (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$,
   $\mathcal{A} \vee (\mathcal{B} \wedge \mathcal{C}) \equiv (\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{A} \vee \mathcal{C})$,
5. *double négation :* $\neg(\neg\mathcal{A}) \equiv \mathcal{A}$,
6. *lois de Morgan :* $\neg(\mathcal{A} \vee \mathcal{B}) \equiv (\neg\mathcal{A}) \wedge (\neg\mathcal{B})$,
   $\neg(\mathcal{A} \wedge \mathcal{B}) \equiv \neg\mathcal{A} \vee (\neg\mathcal{B})$,
7. *tiers-exclu :* $\mathrm{A} \wedge \neg\mathrm{A} \equiv \bot$, $\mathrm{A} \vee \neg\mathrm{A} \equiv \top$,
8. *absorption :* $\mathcal{A} \wedge \bot \equiv \bot$, $\mathcal{A} \wedge (\mathcal{A} \vee \mathcal{B} \equiv \mathcal{A}$, $\mathcal{A} \vee \top \equiv \top$, $\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B} \equiv \mathcal{A}$,
9. *neutre :* $\mathrm{A} \wedge \top \equiv \mathcal{A}$, $\mathcal{A} \vee \bot \equiv \mathcal{A}$.

DÉMONSTRATION. Chacune de ces équivalences est établie en vérifiant que les membres de gauche et de droite ont même table de vérité, *i. e.* sont `Vrai` ou `Faux` en même temps quelque soient les valeurs de vérité des propositions élémentaires $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$.

Par exemples, Le tableau I.4 démontre la loi de Morgan exprimant l'équivalence $\neg(\mathcal{A} \vee \mathcal{B}) \equiv (\neg\mathcal{A}) \wedge (\neg\mathcal{B})$. Le tableau I.5 établit les équivalences dites « absorption » et « neutre ». □

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	$\neg(\mathcal{A} \vee \mathcal{B})$	$\neg\mathcal{A}$	$\neg\mathcal{B}$	$(\neg\mathcal{A}) \wedge (\neg\mathcal{B})$
V	V	V	F	F	F	F
V	F	V	F	F	V	F
F	V	V	F	V	F	F
F	F	F	V	V	V	V

TABLE I.4 – Loi de Morgan : $\neg(\mathcal{A} \vee \mathcal{B}) \equiv (\neg\mathcal{A}) \wedge (\neg\mathcal{B})$.

$\bot$	$\top$	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	$\mathcal{A} \wedge (\mathcal{A} \vee \mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	$\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B})$	$\mathcal{A} \wedge \bot$	$\mathcal{A} \vee \top$	$\mathcal{A} \wedge \top$	$\mathcal{A} \vee \bot$
F	V	V	V	V	V	V	V	F	V	V	V
F	V	V	F	V	V	F	V	F	V	V	V
F	V	F	V	V	F	F	F	F	V	F	F
F	V	F	F	F	F	F	F	F	V	F	F

TABLE I.5 – Équivalences dites « absorption » et « neutre ».

On peut reformuler cette équivalence de la manière suivante : la négation de la disjonction « $\mathcal{A}$ *ou* $\mathcal{B}$ » est la conjonction « $\neg\mathcal{A}$ *et* $\neg\mathcal{B}$ ». Par ex. la négation de « L'entier N est divisible par 3 ou 5 » est « L'entier N n'est divisible ni par 3 ni par 5 ».

D'autres équivalences ont lieu, par exemple $(\mathcal{A} \oplus \mathcal{B}) \oplus \mathcal{C} \equiv \mathcal{A} \oplus (\mathcal{B} \oplus \mathcal{C})$.

1.1.3 Quantificateurs : $\forall, \exists$

Au delà des combinaisons de propositions exposées précédemment, il y a besoin parfois d'exprimer qu'un prédicat dépendant d'une variable $x \in \mathrm{X}$ est `Vrai` pour toute valeur de $x \in \mathrm{X}$, ou à l'opposé pour au moins une valeur de $x \in \mathrm{X}$. Le langage abstrait des propositions ne permet pas de traduire formellement ces expressions du langage naturel, comme « Tout humain est mortel ». Un prédicat dépendant d'une variable (déjà introduite par Aristote [13], permet l'usage des quantificateurs :

DÉFINITION 1.3: *Soit $\mathcal{A}[x]$ un prédicat.*

Le quantificateur $\forall$ [14], épelé suivant « Pour tout », est dit quantificateur universel *: la formule $\forall x \mathcal{A}[x]$ assure que la propriété $\mathcal{A}[x]$ est `Vrai` pour tout x (présumé parcourir un ensemble* X*);*

Le quantificateur $\exists$, épelé suivant « Il existe » est dit quantificateur existentiel *: la formule $\exists x \mathcal{A}[x]$ assure que la propriété $\mathcal{A}[x]$ est `Vrai` pour au moins un x (présumé parcourir un ensemble* X*).*

△ REMARQUES 1.2:

1. On utilise parfois le quantificateur existentiel $\exists!$ marquant une existence unique : « Il existe un unique … », qui peut s'exprimer par une formule équivalente à partir des connecteurs de base et les quantificateurs $\forall, \exists$.

$$\exists! x \mathcal{A}[x] \equiv \exists x \mathcal{A}[x] \wedge \forall y (\mathcal{A}[y] \Longrightarrow (x = y)).$$

2. Si x appartient à un nombre fini d'objets $x_1, \ldots, x_k$, les quantificateurs universels peuvent être exprimés par des formules équivalentes avec les connecteurs élémentaires

$$\forall x \mathcal{A}[x] \equiv \mathcal{A}[x_1] \wedge \ldots \wedge \mathcal{A}[x_k], \quad \exists x \mathcal{A}[x] \equiv \mathcal{A}[x_1] \vee \ldots \vee \mathcal{A}[x_k].$$

▽

Un prédicat $\mathcal{A}[x]$, précédé par un ou plusieurs quantificateurs universels ou existentiels peut être considéré comme une proposition avec valeur de vérité (`Vrai` ou `Faux`) et être inséré dans les formules. On verra ci-dessous comment l'opérateur de négation $\neg$ opère sur des formules contenant des quantificateurs.

▷ EXEMPLES 1.4:

1.4.1 $\exists x \in \mathbb{R}, x^4 + 1 = 0$ [F]

1.4.2 $\exists x \in \mathbb{C}, x^4 + 1 = 0$ [V] (le contexte a changé : on est dans $\mathbb{C}$)

1.4.3 $\forall x \in \mathbb{R}, x^4 + 1 > 0$ [V]

13. Aristote, 384 av. J.-C., Stagire – 322 av. J.-C., Chalcis.

14. Les quantificateurs sont notés graphiquement par une lettre symétrisée, A et $\forall$, E et $\exists$, initiales de « all » et « exists » en anglais. Le symbole $\forall$ a été introduit par le logicien C. S. Pierce, 10 septembre 1839 Cambridge, Massachusetts, É.-U. – 19 avril 1914, Milford, Pennsylvania, É.-U.

1.4.4 $\forall$P polynôme non constant , $\exists z \in \mathbb{C}$ racine de P [V] (théorème dit de d'Alembert-Gauß). ◁

En terme d'ensemble (cf. infra), affirmer que tel prédicat $\mathcal{A}[x]$ est `Vrai` pour tout $x \in \mathrm{E}$ est équivalent à affirmer que la partie de E

$$\mathrm{A} = \{x \in \mathrm{E}, \mathcal{A}[x] \text{ est } \texttt{Vrai}\}$$

est égale à E, ou encore que le complémentaire $\overline{\mathrm{A}}$ est vide. De manière analogue, déclarer l'existence d'un $x \in \mathrm{E}$ vérifiant le prédicat $\mathcal{A}[x]$ signifie que la partie A n'est pas vide et que son complémentaire est distinct de E.

PROPOSITION 1.1: *Les deux quantificateurs $\exists$ et $\forall$ sont reliés par l'opérateur de négation $\neg$: la négation de « $\forall x, \mathcal{A}[x]$ » est « $\exists x$, Non $(\mathcal{A}[x])$ », aussi a-t-on les équivalences*

$$\neg\big(\forall x \in \mathrm{E}\, \mathcal{A}[x]\big) \equiv \exists x \in \mathrm{E}\, \neg(\mathcal{A}[x]), \quad \neg\big(\exists x \in \mathrm{E}\, \mathcal{A}[x]\big) \equiv \forall x \in \mathrm{E}\, \neg(\mathcal{A}[x]).$$

L'ordre d'écriture des quantificateurs importe, comme les propositions suivantes le montrent

$$\begin{aligned} &\forall n \in \mathbb{N}, \quad \exists m \in \mathbb{N}, \quad n < m, \\ &\exists m \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad n < m, \end{aligned}$$

la première étant vraie (le m dépend de n), la seconde fausse s'il existe, le m est un majorant de $\mathbb{N}$). Néanmoins, il y a possibilité de regrouper les quantificateurs de même type. La proposition

$$\forall n \in \mathbb{N}, \quad \forall m \in \mathbb{N}, \quad m + n \in \mathbb{N}$$

est abrégée en

$$\forall (n, m) \in \mathbb{N}^2, \quad m + n \in \mathbb{N},$$

voire

$$\forall n, m \in \mathbb{N}, \quad m + n \in \mathbb{N},$$

ce qui permet de contracter les formules logiques. Certaines variables quantifiées dans un énoncé sont substituables (elles sont dites muettes) : elles peuvent même parfois disparaître totalement. Ainsi du prédicat

$$\begin{aligned} \text{L'entier } n \text{ est pair } &\equiv \text{L'entier } n \text{ est tel qu'il } \exists m \in \mathbb{N}, n = 2m \\ &\equiv \text{L'entier } n \text{ est le double d'un entier} \end{aligned}$$

La négation de propositions avec quantificateurs est parfois complexe, ainsi par exemple

$$\forall x \in \mathbb{R}, \quad \forall \varepsilon > 0, \quad \exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad |x - y| \leq \delta \Longrightarrow |f(x) - f(y)| \leq \varepsilon$$

est

$$\exists x \in \mathbb{R}, \quad \exists \varepsilon > 0, \quad \forall \delta > 0, \quad \exists y \in \mathbb{R}, \quad |x-y| \leq \delta \quad \text{et} \quad |f(x)-f(y)| > \varepsilon$$

Pour un dernier exemple, considérons l'ensemble E des êtres sur une planète parmi lesquels il y a des humains et des mortels, avec les prédicats $\mathcal{H}[x]$ et $\mathcal{M}[x]$ correspondants. En début des propositions suivantes, il est sous-entendu que x est un élément de E (ainsi, on a substitué à la forme complète « $\forall x \in \mathrm{E}$ » la forme « $\forall x$ »)

Seuls les humains sont mortels	$\forall x(\mathcal{M}[x] \Longrightarrow \mathcal{H}[x])$
Tous les humains sont mortels	$\forall x(\mathcal{H}[x] \Longrightarrow \mathcal{M}[x])$
Il existe un humain immortel	$\exists x(\mathcal{H}[x] \wedge \neg\mathcal{M}[x])$
Il n'existe pas d'humain mortel	$\forall x(\mathcal{H}[x] \longrightarrow \neg\mathcal{M}[x])$

Les seconde et troisième propositions sont la négation l'une de l'autre.

Continuons avec le caractère mortel des hommes du syllogisme grec

1. Tout homme est un animal
2. Tout animal est mortel
3. Donc, tout homme est mortel

Le contenu de cette déduction n'a rien à voir avec la véracité ou la fausseté des propositions constitutives : cet énoncé est une instanciation de la proposition suivante

1. Tout $\mathcal{A}$ est $\mathcal{B}$
2. Tout $\mathcal{B}$ est $\mathcal{C}$
3. Donc tout $\mathcal{A}$ est $\mathcal{C}$

qui se récrit en formule logique, toujours `Vrai`, suivant

$$\big[(\forall x(\mathcal{A}[x] \Longrightarrow \mathcal{B}[x]) \wedge (\forall x(\mathcal{B}[x] \Longrightarrow \mathcal{C}[x]))\big] \Longrightarrow (\forall x(\mathcal{A}[x] \Longrightarrow \mathcal{C}[x]).$$

DÉFINITION 1.4: *Une variable x qui apparaît dans une formule* **F** *est dite* libre *si elle n'est pas quantifiée dans* **F**. *Elle est dite* liée *(ou* muette*) si elle est quantifiée,* i. e. *si elle apparaît dans une sous-formule de* **F** *du type* $\forall x\mathbf{G}$ *ou* $\exists x\mathbf{G}$*, tout en étant libre dans la formule* **G**.

Une formule avec au moins une variable libre est dite ouverte. *Une formule dont toutes les variables sont liées est dite* close.

La clôture universelle *(resp.* clôture existentielle*) d'une formule* **F** *est la formule obtenue en adjoignant au début de la formule les quantificateurs* $\forall x \forall y \ldots$ *(resp.* $\exists x \exists y$*) correspondant aux variables libres* $x, y, \ldots$ *de la formule* **F**.

On notera $\mathbf{F}(x,y,z)$ pour indiquer que la formule $\mathbf{F}$ possède x,y,z comme variables libres. Par exemple, $\mathbf{F}(x,z)=\mathcal{A}[x]\wedge\exists y\mathcal{B}[x,y,z]$ est une formule ouverte où x et z sont libres. Une formule fermée est une proposition.

▷ EXEMPLES 1.5:

1.5.1 La formule $\mathcal{A}[x]\vee\mathcal{B}[y]$ contient les variables x et y comme variables libres. C'est un prédicat en les variables x,y.

1.5.2 La formule « $x+2=4$ » est un prédicat, avec valeur de vérité `Vrai` (en arithmétique des entiers naturels) seulement pour $x=2$, alors que les formules « $\forall x(x+2=4)$ » et « $\exists x(x+2=4)$ » sont des propositions `Faux` et Vrai resp..

1.5.3 La formule « $\forall x\forall y(\mathcal{A}[x]\vee\mathcal{B}[y])$ » a toutes ses variables liées : c'est une proposition qui contient les variables x et y comme variables liées.

1.5.4 Dans la formule (syntaxiquement correcte)

$$\forall x\big(\mathcal{A}[x,y]\Longrightarrow\big[(\forall x\mathcal{B}[x])\vee(\exists y\mathcal{C}[x,y])\big]\big),$$

les variables x et y ont des occurrences libres et liées. Afin d'éviter les erreurs de lecture et d'interprétation, il convient d'écrire cette formule suivant

$$\forall x\big(\mathcal{A}[x,y]\Longrightarrow[(\forall z\mathcal{B}[z])\vee(\exists t\mathcal{C}[x,t])]\big),$$

où les variables t,x,z sont liées et y libre. ◁

1.2 Ensembles

C'est à Cantor [15] qu'est attribuée l'introduction de la théorie des ensembles, théorie aux fondements des mathématiques d'aujourd'hui. Il formulait ce qu'est un ensemble ainsi « N'importe quelle collection d'objets définis et distinguables de notre pensée ou de notre intuition »

La théorie élémentaire des ensembles, tel que l'a formulée son créateur Cantor, admet un certain nombre de paradoxes : les deux donnés ci-dessous sont assez caractéristiques, avec un auto-référencement similaire au paradoxe du menteur affirmant « Je ne mens pas », paradoxe déjà connu du temps d'Aristote.

[Russell [16]] Considérons la partie $\mathrm{A}=\{x|x\notin x\}$. Alors l'assertion $\mathrm{A}\in\mathrm{A}$ est équivalente à sa négation $\mathrm{A}\notin\mathrm{A}$, contradiction inacceptable. Une théorie contenant une assertion et sa négation n'est pas cohérente.

[Berry [17]] Soit $\mathcal{A}[n]$ la propriété « n est un entier définissable par une phrase française d'au plus 100 caractères ». Alors l'ensemble $\mathrm{A}=\{n\in\mathbb{N}|\mathcal{A}[n]\ \texttt{Vrai}\}$ ne peut exister. En effet, supposons son existence. Il n'y a, en comptant les blancs, qu'au plus 27^{100} phrases françaises d'au plus 100 caractères, chacune de ces phrases ne définissant qu'au plus un entier Ainsi, l'ensemble A a au plus 27^{100} éléments, et son complémentaire (partie non vide l'ensemble

15. G. Cantor, 3 mars 1845, Saint-Pétersbourg, Russie — 6 janvier 1918, Halle-sur-Saale, Allemagne.
16. Bertrand A. W. Russell, 18 mai 1872, Trellech, Monmouthshire, UK – 2 février 1970, Penrhyndeudraeth, Caernarfonshire, Wales, UK.
17. G. G. Berry, 1867 -– 1928.

infini $\mathbb{N}$) est non vide. Vu que toute partie non vide d'entiers possède un plus petit élément, le complémentaire de A doit posséder un plus petit élément, soit n_A qui appartient donc au complémentaire de A : l'entier n_A est non définissable par une phrase françaises d'au plus 100 caractères. Mais « l'entier n_A est le plus petit entier non définissable par une phrase française d'au plus 100 caractères » est une définition pour n_A, qui comporte 96 caractères : le nombre n_A appartient aussi à A, contradiction!
Le paradoxe de Berry vient du sens imprécis que l'on donne au mot « définir ». Il faut distinguer le langage mathématique, formalisé, celui dans lequel sont définis les entiers, du métalangage (tel notre langage ordinaire), dans lequel est formulée la phrase de Berry.

Une axiomatisation reposant sur des formalisations adéquates a permis de définir des théories des ensembles non contradictoires, et donc utilisables.

1.2.1 Ensembles et parties

Pour une théorie élémentaire des ensembles, nous retiendrons les définitions informelles suivantes, si lacunaires soit-elles mais en faisant confiance à notre intuition : une formalisation est nécessaire autant pour les mathématiciens que les informaticiens.

DÉFINITION 1.5: *Un* ensemble *(ou* espace*)* E *est une collection d'objets, appelés* éléments *ou* membres. *La collection n'est pas ordonnée, sans répétition.*

L'ensemble sans élément est l'ensemble vide, noté $\emptyset$.

Le regroupement de certains éléments de E *constitue une* partie *(ou* sous-ensemble*, lui-même un ensemble) : si* A *est une partie de* E*, l'appartenance de l'élément* a *à l'ensemble* A *sera notée* $a \in A$*, la négation* $a \notin A \equiv \neg(a \in A)$.

La partie A *est incluse dans la partie* B*, soit «* $A \subset B$ *», si tout élément de* A *appartient aussi à* B.

*L'*ensemble des parties $\mathscr{P}(E)$ *est défini comme l'*ensemble des parties *de* E.

Les éléments sont très divers : nombres, points, droites, tas, piles, graphes, intervalles de la droite réelle, ensembles,... Cette liberté suggère qu'un ensemble peut être n'importe quoi : cette latitude amène des paradoxes (comme celui de Russell évoqué ci-dessus), ce qui est évité par le choix de systèmes axiomatiques.

Un ensemble est décrit soit par une caractérisation (telle « les nombres rationnels négatifs »), soit par une énumération explicite de ces éléments. Les signes $\in$ et $\subset$ qui viennent d'être introduits, sont parmi les signes de base, précédant les signes de combinaison de parties $\cup, \cap, \Delta, \ldots$

Le choix d'ensembles est crucial pour le développement des différents domaines des mathématiques, par ex. analyse *vs* algèbre, géométrie réelle *vs* géométrie complexe,. Voilà quelques ensembles, sous-ensembles ou pas.

⊳ EXEMPLES 1.6:

1.6.1 $\{a\}$ (ensemble à un élément).

1.6.2 si $a \neq b$, les ensembles $\{a, b\}$ et $\{b, a\}$ sont des ensembles identiques, $\{a, a, a\}$ est identique à $\{a\}$.

1.6.3 L'ensemble $\{\{a\}\}$ est un ensemble à 1 élément qui peut être considéré comme la partie $\{a\}$ de l'ensemble $\{a,b,c,d,e,\ldots,x,y,z\}$.
1.6.4 $\mathbb{N}$, $\{$nombres entiers impairs$\}$, $\mathbb{D}$.
1.6.5 $[\![1,n]\!] = \{1,2,\ldots,n-1,n\} = [1,n]\cap\mathbb{N}$ ensemble des n entiers non nuls de 1 à n ; ensemble fini.
1.6.6 $\mathscr{C}([0,1])$ l'ensemble des applications continues sur $[0,1]$ à valeurs réelles.
1.6.7 $\{x$ congru à $0,2,4,6,8,10$ modulo $10\} = 2\mathbb{Z}$
1.6.8 Les solutions x,y entières de l'équation de Pell [18] $x^2-y^2=61$.
1.6.9 $\operatorname{argmin} f = \{x\in \mathrm{E} | f(x) = \min_{y\in \mathrm{E}} f(y)\}$, l'ensemble des minima d'une fonction $f : \mathrm{E}\to\mathbb{R}$, ensemble qui peut être vide, comme par exemple pour exp : $x\in\mathbb{R}\mapsto \mathrm{e}^x$.
1.6.10 Plan et ses points, droites, courbes,...
1.6.11 $\mathbb{R}^*\times\mathbb{R}^*$, $\mathbb{R}^2\setminus\{(0,0)\}$.
1.6.12 si E est l'ensemble à deux éléments $\{0,1\}$, alors $\mathscr{P}(\mathrm{E}) = \{\emptyset,\{0\},\{1\},\{0,1\}\}$.
1.6.13 Si a est un élément de A, le singleton (partie à un élément) $\{a\}$ est un élément de l'ensemble des parties $\mathscr{P}(\mathrm{A})$. Les notations $\emptyset$, $\{\emptyset\}$ et $\{\{\emptyset\}\}$ ont diverses interprétations. $\emptyset$ est l'ensemble vide et aussi la partie vide, et unique, de l'ensemble $\emptyset$: $\mathscr{P}(\emptyset) = \{\emptyset\}$. Par suite le singleton $\{\emptyset\}$ est l'unique partie à un élément de $\mathscr{P}(\emptyset)$: c'est un élément de $\mathscr{P}(\mathscr{P}(\emptyset))$. Le singleton $\{\{\emptyset\}\}$ est un élément de $\mathscr{P}(\mathscr{P}(\mathscr{P}(\emptyset)))$. ◁

La relation d'appartenance lie un élément a de E et une partie A : l'élément a appartient à A (ou bien a est élément de A ou encore la partie A contient a) qu'on écrira $a\in\mathrm{A}$ ou $\mathrm{A}\ni a$. La non appartenance de l'élément a à l'ensemble A est notée $a\notin\mathrm{A}$. L'inclusion de A dans B revient à dire l'appartenance à B de tout élément appartenant à A. L'ensemble vide $\emptyset$ est inclus dans tout ensemble A.

1.2.2 Prédicats et parties

Soit le prédicat $\mathcal{A}[x]$ pour x dans E. La question de la vérité ou non de $\mathcal{A}[x]$ revient à l'étude de la partie [19]

$$\mathrm{E}(\mathcal{A}) = \{x\in\mathrm{E} | \mathcal{A}[x] \text{ est } \texttt{Vrai}\}$$

des éléments de E pour lesquels le prédicat $\mathcal{A}[x]$ a `Vrai` comme valeur de vérité. Inversement, étant donnée la partie $\mathrm{A}\subset\mathrm{E}$, cette partie A apparaît comme le sous-ensemble des éléments a de E vérifiant la proposition « $\mathcal{A}[x] : x\in\mathrm{A}$ ». Cette correspondance entre prédicats et parties explique comment des propriétés du calcul des prédicats se retrouvent dans celles applicables aux parties d'un ensemble.

18. J. Pell, 1er mars 1611, Southwick, West Sussex – 12 décembre 1685, Westminster, Formation.
19. Les séparateurs « |,; » seront utilisés indifféremment entre partie désignant le sous-ensemble et partie prédicat.

▷ EXEMPLE 1.7: Dans le plan $\mathbb{R}^2$, les prédicats « $\mathcal{A}[x,y] : xy = 0$ », « $\mathcal{A}[x,y] : (x = 0) \wedge (y = 0)$ » correspondent à la réunion des axes et à la partie réduite à l'origine resp.. ◁

Ainsi, le calcul logique apparaît de manière équivalente comme une arithmétique des propositions ou des parties. Pour les parties A et B associées aux prédicats $\mathcal{A}[x]$ et $\mathcal{B}[x]$ resp., on a pour les connecteurs de base et les opérations ensemblistes élémentaires les équivalences :

1. intersection $\cap$ *versus* conjonction $\wedge$: $\mathrm{A} \cap \mathrm{B} = \{x \in \mathrm{E} | (\mathcal{A}[x] \wedge \mathcal{B}[x])\ \texttt{Vrai}\}$
2. union $\cup$ *versus* disjonction $\vee$: $\mathrm{A} \cup \mathrm{B} = \{x \in \mathrm{E} | (\mathcal{A}[x] \vee \mathcal{B}[x])\ \texttt{Vrai}\}$
3. complémentaire *versus* négation $\neg$: $\overline{\mathrm{A}} = \{x \in \mathrm{E} | (\neg \mathcal{A}[x]\ \texttt{Vrai})\}$.

1.2.3 Algèbre des parties, produits

Les opérateurs d'intersection, d'union et de complémentaire munissent l'ensemble des parties de l'ensemble E d'une structure dite d'*algèbre de Boole*[20]. Les définitions de parties particulières et de leurs propriétés sont rassemblées dans la proposition suivante :

PROPOSITION 1.2: *Soient* E *un ensemble et* A, B, C *des parties de* E. *Les opérations binaires d'union et d'intersection et unaire de prise du complémentaire sont définies pour des parties* A *et* B *de l'ensemble* E *suivant*

1. *union :* $\mathrm{A} \cup \mathrm{B} := \{a \in \mathrm{E} | (x \in \mathrm{A}) \vee (x \in \mathrm{B})\}$,
2. *intersection :* $\mathrm{A} \cap \mathrm{B} := \{a \in \mathrm{E} | (x \in \mathrm{A}) \wedge (x \in \mathrm{B})\}$,
3. ${}^c\mathrm{A} := \overline{\mathrm{A}} := \complement\mathrm{A} = \complement_{\mathrm{E}}\mathrm{A} = \{x \in \mathrm{E} | x \notin \mathrm{A}\}$.

Alors, ces opérations vérifient les propriétés suivantes

1. union *:* $\mathrm{A} \cup \mathrm{B} = \mathrm{B} \cup \mathrm{A}$ *;*
2. intersection *:* $\mathrm{A} \cap \mathrm{B} = \mathrm{B} \cap \mathrm{A}$ *;*
3. neutres *:* $\emptyset \cup \mathrm{A} = \mathrm{A}$, $\mathrm{E} \cap \mathrm{A} = \mathrm{A}$, $\mathrm{E} \cup \mathrm{A} = \mathrm{E}$, $\emptyset \cap \mathrm{A} = \emptyset$ *;*
4. complémentaire *:* $\overline{\emptyset} = \mathrm{E}$ *et* $\overline{\overline{\mathrm{A}}} = \mathrm{A}$, $\overline{\mathrm{A}} \cup \mathrm{A} = \mathrm{E}$, $\overline{\mathrm{A}} \cap \mathrm{A} = \emptyset$ *;*
5. distributivité *:* $\mathrm{A} \cup (\mathrm{B} \cap \mathrm{C}) = (\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{A} \cup \mathrm{C})$, $\mathrm{A} \cap (\mathrm{B} \cup \mathrm{C}) = (\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{A} \cap \mathrm{C})$ *;*
6. lois de Morgan *:* $\overline{\mathrm{A} \cap \mathrm{B}} = \overline{\mathrm{A}} \cup \overline{\mathrm{B}}$, $\overline{\mathrm{A} \cup \mathrm{B}} = \overline{\mathrm{A}} \cap \overline{\mathrm{B}}$ *;*

20. Un ensemble ordonné $(\mathrm{X}, \leq, \vee, \wedge, 0, 1)$ est une algèbre de Boole si – chaque paire $(x,y) \in \mathrm{X}^2$ d'éléments de X possède une borne supérieure notée $x \vee y$ et une borne inférieure $x \wedge y$), – l'opérateur $\vee$ est distributif par rapport à l'opération $\vee$, et vice versa, *i. e.* $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ – l'élément 0 est un minimum, 1 est un maximum, – pour tout $x \in \mathrm{X}$, il existe un élément ${}^c x$ tel que $x \vee {}^c x) = 1$ et $x \wedge {}^c x) = 0$. Pour un ensemble E, l'espace $(\mathscr{P}(\mathrm{E}), \subset, \cup, \cap, \emptyset, \mathrm{E})$ est une algèbre de Boole et toute algèbre de Boole X de cardinal fini est de cette forme. L'ensemble des formules du calcul propositionnel où deux formules propositionnelles sont confondues quand elles ont même table de vérité est une algèbre de Boole.

7. différence : $A\backslash B := \{x \in A \wedge x \notin B\}$;
8. différence symétrique : $A\Delta B := (A \setminus B) \cup (B \setminus A)$ *avec* $A\Delta B = B\Delta A$.

À ces opérateurs s'ajoutent les relations entre parties

1. inclusion : $A \subset B$ *si tout élément de* A *est dans* B ;
2. égalité : $A = B \equiv (A \subset B$ *et* $B \subset A)$.

DÉMONSTRATION. Contentons-nous d'établir à titre d'exemple une des lois de Morgan :

$$\begin{aligned}\overline{A \cap B} &= \{\neg(x \in A \cap B)\} = \{\neg((x \in A) \wedge (x \in B))\} = \{\neg(x \in A) \vee \neg(x \in B)\} \\ &= \left\{(x \in \overline{A}) \vee (x \in \overline{B})\right\} = \left\{x \in (\overline{A} \cup \overline{B})\right\} = \overline{A} \cup \overline{B}.\end{aligned}$$

Les autres relations sont établies pareillement, en cohérence avec les règles du calcul propositionnel du théorème 1.2. □

La notion de couple est définie intuitivement, comme celle d'ensemble

DÉFINITION 1.6: *Un couple* (a, b) *est la donnée de deux objets* a *et* b*, distincts ou égaux et écrits de manière ordonnée. Pour un entier* k *au moins égal à 1, un* k*-uplet est une suite ordonnée* $(a_1, a_2, \ldots, a_k)$ *de* k *objets (distincts ou pas).*

L'espace produit (di cartésien*)* $E \times F$ *des ensembles* E *et* F *est l'ensemble constitué des couples* (e, f) *d'éléments des ensembles* E *et* F*,*

$$E \times F = \left\{(e, f) | e \in E, f \in F\right\}.$$

L'espace produit des k*-uplets* $e = (e_1, \ldots, e_n)$ *avec comme composante* e_i $(i = 1, \ldots, k)$ *un élément de* E_i *est l'ensemble*

$$E_1 \times E_2 \times \ldots \times E_k = \left\{(e_1, \ldots, e_k) | e_i \in E_i, i = 1, \ldots, k\right\}.$$

Les espaces produits permettent d'introduire de multiples autres ensembles, avec des parties particulières : graphes d'application, de relations,... On a les cas particuliers $E \times E = E^2$, $E^n = E \times \cdots \times E$ (avec n facteurs) : si $a \neq b$, les triplets (a, b, b) et (b, a, b) sont des éléments de E^3 distincts.

En conclusion de cette partie, on constate la simplicité à construire des ensembles de plus en plus complexes.

1.2.4 Applications et fonctions

DÉFINITION 1.7: *Une* application *(ou* fonction*)* f *est un objet mathématique établi par la donnée d'un ensemble* E *comme* espace source *(ou* ensemble de départ*), d'un ensemble* F *comme* espace but *(ou* ensemble d'arrivée*) et une règle d'association à tout élément* $x \in E$ *d'un unique élément* $y \in F$ *qui sera noté* $f(x)$*. On notera ainsi*

*« $f : E \to F$ » ou de manière plus précise « $f : x \in E \mapsto f(x) \in F$ ». Si $y = f(x)$, on dit que y est l'*image *de x par f et que x est un* antécédent *de y.*

L'espace des applications de source E *et de but* F *est noté* F^E *ou* $\mathscr{F}(E,F)$.

*L'*application identité [21] *de* E *dans* E *est l'application* $\mathbb{1}_E : x \in E \mapsto x \in E$.

Le graphe Gr_f *de l'application f est la partie* $\mathrm{Gr}_f = \{(x, f(x)) | x \in E\}$ *du produit cartésien* $E \times F$.

La composée *de l'application $f : E \to F$ et (suivie) de $g : F \to G$ est l'application de* E *dans* G *qui à chaque élément $x \in E$ associe l'élément $g(f(x))$ de* G. *Cette composée est notée $g \circ f$.*

△ REMARQUE 1.3: Le terme de *fonction* est essentiellement synonyme d'application, mais avec des variations légères : pour certains, une fonction est une application avec ensemble des réels $\mathbb{R}$ ou $\mathbb{C}$ comme espace but. D'autres entendent par fonction une application dont le domaine de définition est éventuellement strictement inclus dans l'espace source : ce distinguo entre fonction et application est variable historiquement. Les deux termes seront employés ici de manière équivalente. Le terme de *correspondance* est aussi employé, notamment pour désigner une bijection $f : E \to F$ comme une *correspondance biunivoque* entre les espaces E et F, associant à $x \in E$ l'unique image $y = f(x) \in F$ et réciproquement à $y \in F$ l'unique antécédent $x = f^{-1}(y) \in F$. ▽

▷ EXEMPLES 1.8:

1.8.1 Une application $u : n \in \mathbb{N} \mapsto u(n) \in \mathbb{R}$ induit une suite $\mathbf{u} = (u_n)_{n\geq 0}$ avec $u_n = u(n)$ pour $n \geq 0$ et inversement, une suite réelle n'est rien d'autre qu'une application de $\mathbb{R}^{\mathbb{N}}$. On devrait écrire donc $u(n)$ à la place de u_n, mais la tradition a imposé la forme indicée, sauf dans certains cas où la forme $(u(n))_{n\geq 0}$ est préférée. Il y a cependant une petite différence entre les deux points de vue : la suite $\mathbf{u} = (u_n)_{n\geq 0}$ conserve un mode d'énumération standard $u_0, u_1, \ldots$ par termes d'indices croissants, là où l'application $u : \mathbb{N} \to \mathbb{R}$ associe simplement à tout entier n le nombre $u(n)$. Il convient aussi de bien distinguer une suite de l'ensemble de ses valeurs (pouvant être réduit à un seul élément!).

1.8.2 Considérant les complexes comme des nombres autant que les réels, on introduit pareillement les suite de nombres complexes $(u_n)_{n\geq 0}$ éléments de $\mathbb{C}^{\mathbb{N}}$. Avec ses parties réelles et imaginaires, une application à valeurs dans $\mathbb{C}$ (et donc une suite complexe) $u : n \in \mathbb{N} \mapsto u(n) \in \mathbb{C}$ induit une suite complexe $(u_n)_{n\geq 0}$, et par là même deux suites réelles, $(\Re e(u_n))_{n\geq 0}$ et $(\Im m(u_n))_{n\geq 0}$ et réciproquement.

1.8.3 Soit $\mathscr{P}(E)$ l'ensemble des parties de E (cf. définition 1.5). La fonction caractéristique χ_A associée à la partie $A \in \mathscr{P}(E)$ est l'application $\chi_A : E \to \mathbb{R}$

21. Cette application *Identité* est parfois notée Id_A, on ne confondra pas avec l'application qui vaut 1 sur A et 0 sur $\overline{A}$.

définie par

$$\chi_A(x) = \begin{cases} 1 \text{ si } x \in A, \\ 0 \text{ si } x \notin A. \end{cases}$$

Au lieu de l'espace d'arrivée $\mathbb{R}$, prenons comme espace but de χ_A l'ensemble $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ comme espace but avec $\chi_A(x) = \overline{0}$ ou $\overline{1}$ suivant que $x \in A$ ou $x \notin A$. Malgré le changement d'espace but de $\mathbb{R}$ à $\mathbb{Z}/2\mathbb{Z}$, notons pareillement cette application χ_A. On obtient une application χ définie suivant

$$\chi : A \in \mathscr{P}(E) \mapsto \chi_A \in \mathscr{F}(E, \mathbb{Z}/2\mathbb{Z}).$$

Par ailleurs, à une application $\theta : E \to \mathbb{Z}/2\mathbb{Z}$, on associe la partie A_θ de E

$$A_\theta := \{x \in E | \theta(x) = \overline{1}\} := \widehat{\theta}^{-1}(\{\overline{1}\}) = \theta^{-1}(1),$$

où les deux derniers membres reprennent les notation de la définition 1.9 ci-dessous. On obtient les identités

$$A_{\chi_A} = A, \quad A \in \mathscr{P}(E), \qquad \chi_{(A_\theta)} = \theta, \quad \theta \in \mathscr{F}(E, \mathbb{Z}/2\mathbb{Z})$$

ce qui établit la bijectivité[22] de l'application $A \in \mathscr{P}(E) \to \chi_A \in \mathscr{F}(E, \mathbb{Z}/2\mathbb{Z})$ avec application réciproque $\theta \to A_\theta$. ◁

LEMME 1.1: *Soit f appartenant à $\mathscr{F}(E,F)$ et g appartenant à $\mathscr{F}(F,E)$. En général les applications $g \circ f$ et $f \circ g$ ne sont pas égales.*

Soit f appartenant à $\mathscr{F}(E,F)$, g appartenant $\mathscr{F}(F,G)$ et h appartenant $\mathscr{F}(G,H)$. Alors

$$(h \circ g) \circ f = h \circ (g \circ f).$$

DÉMONSTRATION. Pour le premier alinéa, il suffit de trouver un contre-exemple à la commutativité. Si $E \neq F$, les espaces source de $g \circ f$ et $f \circ g$ sont distincts, et donc aussi les composées. Si $E = F$, on peut aussi exhiber des composées distinctes : soit l'application $L_{a,b} : x \in \mathbb{R} \mapsto ax + b \in \mathbb{R}$. Alors

$$L_{a,b} \circ L_{a',b'}(x) = a(a'x + b') + b = L_{aa',ab'+b}(x)$$

égale à $L_{a',b'} \circ L_{a,b}$ si et seulement si $ab' + b = a'b + b'$, condition restrictive.

Pour le second alinéa, on a

$$\big[(h \circ g) \circ f\big](x) = (h \circ g)(f(x))h\big[g(f(x))\big] = h\big[[(g \circ f)(x)\big] = \big[h \circ (g \circ f)\big](x)$$

ce qui signifie bien l'énoncé. □

22. cf. ci-après pour la définition d'application bijective.

La définition 1.7 a introduit la notion de graphe G_f pour la fonction $f : E \to F$: c'est la partie $G_f = \{(x, f(x)) \in E \times F | x \in E\}$. Ainsi, une partie G de $E \times F$ est le graphe d'une application $f : E \to F$ si $(x, y), (x, y') \in G$ implique $y = y'$ et si pour tout $x \in E$, il existe un $(x, y) \in G$ (et alors $y = f(x)$). Les graphes de deux fonctions de E dans F distinctes sont des parties distinctes du produit cartésien $E \times F$: une telle fonction détermine un seul graphe et l'ensemble des applications $\mathscr{F}(E, F)$ des applications $f : E \to F$ est une partie de $\mathscr{P}(E \times F)$!

On a toujours une application $\emptyset \to F$ (dont le graphe est la partie vide du produit $E \times F$), mais, si E est non vide, il n'y a pas d'application de $E \to \emptyset$. Il convient (et on prend l'habitude) de faire attention aux propriétés de l'ensemble vide, apparemment paradoxales, mais compatibles avec la logique : l'ensemble vide est toujours partie d'un ensemble E et on a $B \setminus B = \emptyset$.

DÉFINITION 1.8: *Une* application $f : E \to F$ *est dite*

1. injective *si tout élément* y *du but* F *est l'image d'au plus un élément* x *de la source* E. *Autrement dit,* f *est injective si, lorsque deux éléments quelconques* x_1, x_2 *de* E *ont même image* $f(x_1) = f(x_2)$, *alors* $x_1 = x_2$.
2. surjective *si tout élément* y *du but* F *est l'image d'au moins un élément* x *de la source* E. *Autrement dit, pour* $y \in F$, *il existe au moins un élément* x *de* E *tel que* $f(x) = y$.
3. bijective *si elle est injective et surjective.*

Si $f : E \to F$ *est bijective, son application réciproque est l'application notée* f^{-1} *d'espace source* F *et d'espace but* E *qui associe à* $y \in F$ *l'unique élément* $x \in E$ *tel que* $f(x) = y$. *On vérifie* $f \circ g = \mathbb{1}_F$ *et* $g \circ f = \mathbb{1}_E$.

▷ EXEMPLES 1.9:

1.9.1 $x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$: ni surjective, non injective.
1.9.2 $x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}^+$: surjective, non injective.
1.9.3 $x \in \mathbb{N} \mapsto x^2 \in \mathbb{N}$ (injective, non surjective.
1.9.4 $x \in [0, +\infty[\mapsto x^2 \in [0, +\infty[$ (bijective avec $\sqrt{\ }$ comme fonction réciproque)
1.9.5 $x \in [2, +\infty[\mapsto x^2 \in [0, +\infty[$ (injective, non surjective)
1.9.6 $x \in E \mapsto \{x\} \in \mathscr{P}(E)$, injective, non surjective
1.9.7 $x = (u, v) \in \mathbb{R}^2 \mapsto u$, projection u de x sur l'axe horizontal (surjective, non injective)
1.9.8 $f : x \in [0, 1[\to f(x) = 1/(1 - x^2) \in \mathbb{R}$ (non surjective,injective)
1.9.9 $f : x \in \mathbb{R} \to f(x) = x/(1 + |x|) \in]-1, 1[$, bijective de fonction réciproque $f^{-1} : y \in]-1, 1[\to f^{-1}(y) = y/(1 - |y|)$
1.9.10 $Z : \varphi \in [0, 1] \to Z(\varphi) = \cos\varphi + i\sin\varphi \in \{z \in \mathbb{C}, |z| = 1\}$ (surjective, non injective) ◁

PROPOSITION 1.3: *Soient* E, F *des ensembles non vides,* $x_0 \in E$ *et* f *une application de* E *dans* F.

— *L'application* f *est injective si et seulement si il existe une application* g *de* F *dans* E *telle que* $g \circ f = \mathbb{1}_E$.
— *L'application* f *est surjective si et seulement si il existe une application* g *de* F *dans* E *telle que* $f \circ g = \mathbb{1}_F$.
— *L'application* f *est bijective si et seulement si il existe une application* g *de* F *dans* E *telle que* $f \circ g = \mathbb{1}_F$ *et* $g \circ f = \mathbb{1}_E$.

DÉMONSTRATION. — Soit f injective. On définit $g : F \to E$ telle que

$$g(y) = \begin{cases} x & \text{si } y \in \operatorname{Im} f \text{ avec } f(x) = y \text{ (par injectivité un tel } x \text{ est unique),} \\ x_0 & \text{si } y \notin \operatorname{Im} f. \end{cases}$$

On a alors $g \circ f(x) = x$ pour tout $x \in E$, soit $g \circ f = \mathbb{1}_E$.
Réciproquement, si $g \circ f = \mathbb{1}_E$, alors si $y_1 = f(x_1) = f(x_2)$, on obtient $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$ et donc l'unicité de l'antécédent de y_1.

— Soit f surjective. On choisit pour chaque $y \in F$ un élément $x_y \in E$ tel que $f(x_y) = y$, définissant ainsi une application $g : y \in F \mapsto x_y \in E$. On a alors $f \circ g(y) = f(x_y) = y$, soit $f \circ g = \mathbb{1}_F$.
Réciproquement, si g vérifie $f \circ g = \mathbb{1}_F$, alors pour tout $y \in F$, on a $f(g(y)) = y$ ce qui assure que cet $y \in F$ a au moins un antécédent (soit $g(y)$) par f : c'est la surjectivité de f.

— Supposons f bijective. D'après les deux alinéa précédents, il existe g, g' (*a priori* non égaux) tels que $g \circ f = \mathbb{1}_E$, $f \circ g' = \mathbb{1}_F$. En multipliant par g la dernière égalité, on obtient

$$g = g \circ \mathbb{1}_F = g \circ (f \circ g') = (g \circ f) \circ g' = \mathbb{1}_E \circ g' = g'$$

et donc $g = g'$, ce qui était à démontrer.
Pour la réciproque, le g donné vérifie $g \circ f = \mathbb{1}_E$, $f \circ g = \mathbb{1}_F$, ce qui assure l'injectivité et la surjectivité resp. de f, et donc son caractère bijectif. □

DÉFINITION 1.9: *L'application* $f : E \to F$ *a une extension* $\widetilde{f} : \mathscr{P}(E) \to \mathscr{P}(F)$ *telle que*

$$\widetilde{f}(A) = \{f(x) | x \in A\}, \quad A \in \mathscr{P}(E),$$

et induit l'application $\widehat{f}^{-1} : \mathscr{P}(F) \to \mathscr{P}(E)$ *définie suivant*

$$\widehat{f}^{-1}(B) = \{x \in E | f(x) \in B\}, \quad B \in \mathscr{P}(F).$$

La partie $\widetilde{f}(A)$ *(qu'on notera souvent simplement* $f(A)$*) est appelée* image directe *de la partie* A *de* E. *La partie* $\widehat{f}^{-1}(B)$ *est appelée* image réciproque *de la partie* B *de* f. *Pour* $y \in E$, *on notera* $f^{-1}(y)$ *la partie* $\widehat{f}^{-1}(\{y\})$.

Soit f *une application de* E *dans* F, E_1 *une partie de* E *et* F_1 *une partie de* F *contenant l'image* $f(E_1)$. *La* restriction *de* f *à* E_1 *avec comme espace but* F_1 *est l'application notée* $f_{|E_1,F_1}$ *(ou simplement* $F_{|E_1}$ *de* E_1 *dans* F_1 *telle que* $f_{|E_1}(x) = f(x)$ *pour tout* $x \in E_1$.

△ REMARQUES 1.4:

1. On vérifie que
$$\widetilde{f}(\{x\}) = \{f(x)\}, \quad x \in \mathrm{E}, \qquad \widehat{f}^{-1}(\{y\}) = \{x \in \mathrm{E}, f(x) = y\}, \quad y \in \mathrm{F},$$
i. e. l'image directe d'un singleton (un ensemble à un élément) est un singleton, alors que l'image réciproque d'un singleton n'est pas forcément un singleton.
Si f est bijective, il en est de même pour $\widetilde{f}$ et $\widehat{f}$ avec $\widetilde{f}^{-1} = \widehat{f}$. Suivant le contexte, et en prenant garde aux conséquences de cet abus, on notera simplement par f les applications image directe ou image réciproque associées à l'application $f : \mathrm{E} \to \mathrm{F}$.
2. La considération de restrictions permet de faire apparaître des fonctions avec des propriétés (injectivité ou surjectivité, différentiabilité,...) « meilleures », on pourra prendre comme illustration de cette remarque les fonctions sin et arcsin.
3. Les notions d'injectivité, de surjectivité ou bijectivité peuvent être considérées en termes d'existence et d'unicité des solutions de l'équation $f(x) = y$ à résoudre en la variable x : si f est injective, alors pour tout $y \in \mathrm{E}$, l'équation $f(x) = y$ a au plus une solution, si f est surjective, pour tout $y \in \mathrm{E}$, alors l'équation $f(x) = y$ a au moins une solution, si f est bijective, alors pour tout $y \in \mathrm{E}$, l'équation $f(x) = y$ a exactement une solution. ▽

DÉFINITION 1.10: *Les ensembles* E *et* F *sont dits de même cardinal s'il existe une bijection de* E *sur* F.

L'ensemble vide est dit de cardinal 0.

L'ensemble E *est dit fini de cardinal* $n \in \mathbb{N}^*$ *si* E *est de même cardinal que l'intervalle des entiers* $[\![1, n]\!]$. *L'ensemble* E *est dit* dénombrable *s'il existe une bijection de* E *sur* $\mathbb{N}$.

▷ EXEMPLES 1.10:

1.10.1 Associant tout nombre entier naturel pair $2k$ à l'entier k et tout nombre entier naturel impair à un entier strictement négatif $2k+1 \mapsto -k-1$, on construit une bijection de $\mathbb{N}$ sur $\mathbb{Z}$, qui sont donc de même cardinal.

1.10.2 Tout entier non nul est de manière unique le produit $\mathrm{P} = 2^k(2\ell+1)$ d'une puissance de 2 et d'un entier impair, ainsi l'application $\mathrm{P} : (k,\ell) \in \mathbb{N}^2 \mapsto 2^k(2\ell+1) \in \mathbb{N}^*$ est une bijection, de même que l'application $(k,\ell) \in \mathbb{N}^2 \mapsto 2^k(2\ell+1) - 1 \in \mathbb{N}$. Une autre bijection est fournie par l'application $(p,q) \in \mathbb{N}^2 \mapsto (p+q)(p+q+1)/2 + q \in \mathbb{N}$: l'espace $\mathbb{N}^2$ est parcouru successivement suivant les diagonales $\mathrm{D}_d = \{(p,q) \in \mathbb{N}^2 | p+q = d\}$, un point (p,q) déterminant la diagonale D_{p+q+1}, avec le numéro d'ordre $\sigma + q$ où $\sigma = 1+2+\cdots+d = d(d+1)/2$ et $q \in [\![1, d+1]\!]$ sur cette diagonale. L'ensemble $\mathbb{N}^2$ est dénombrable.

1.10.3 L'ensemble $\mathbb{Q}$ des rationnels est dénombrable, mais $\mathbb{R}$ ne l'est pas. On démontre l'existence d'une bijection de $\mathscr{P}(\mathbb{N})$ sur $\mathbb{R}$. Les démonstrations de ces assertions ne seront pas précisées ici. ◁

1.2.5 Partition

DÉFINITION 1.11: *Soit* E *un ensemble. Une* partition $\mathscr{A}$ *de* E *est une collection* $(A_i)_{i\in I}$ *de parties non vides de* E, *deux à deux disjointes et dont l'union* $\cup_{i\in I}A_i$ *est égale à* E *tout entier. L'ensemble d'indices* I *est un numérotage des éléments de la collection. Les parties* A_i *sont appelées* atomes *de la partition,* I *son ensemble d'indexation.*

Si l'ensemble E est fini, l'ensemble d'indice I est fini et on pourra prendre comme ensemble d'indices I l'intervalle $[\![1,\alpha]\!]$. On notera

$$\mathscr{A} = (A_1,\dots,A_\alpha) = (A_i)_{i\in[\![1,\alpha]\!]}.$$

Une partition peut-être associée comme une partie de l'ensemble des parties de E vérifiant certaines propriétés.

▷ EXEMPLES 1.11:

1.11.1 On peut avoir des partitions avec des parties ou des ensembles d'indice infinis

$$\mathbb{R} = \bigcup_{i\in\mathbb{R}}\{i\}, \quad \mathbb{R} = \bigcup_{j\in J} j+\mathbb{Q}$$

où on a noté $j+\mathbb{Q}$ la partie $\{j+q, q\in\mathbb{Q}\}$. L'ensemble J est difficile à décrire et son existence dépend de l'axiome du choix.

1.11.2 La partie $\mathbb{I}$ des entiers impairs et $\mathbb{P}$ celle des entiers pairs déterminent une partition $\{\mathbb{I},\mathbb{P}\}$ de l'ensemble des entiers relatifs $\mathbb{Z}$. Plus généralement, étant donné $k\in\mathbb{N}^*$ les k parties $\mathbb{P}_j = \{j+pk, p\in\mathbb{Z}\}$ pour $j = 0,1,\dots,k-1$ déterminent une partition de $\mathbb{Z}$ en k parties, les congruences des entiers modulo k.

1.11.3 Soit $f : E\to F$ une application surjective. Alors l'égalité $E = \cup_{y\in F} f^{-1}(y)$ assure que $(f^{-1}(y))_{y\in F}$ est une partition de E.
De manière plus générale, une surjection de X sur Y est caractérisée par la donnée d'une partition $\mathscr{P}$ de X constituée de p parties $X_1,\dots,X_p$ non vides disjointes, puis d'une bijection qui associe à chaque atome X_π un élément $y(\pi)\in Y$. ◁

La notion de partitions est liée à celle de relation (binaire) sur un ensemble E.

DÉFINITION 1.12: *Soit* E *un ensemble. Une* relation $\mathscr{R}$ *entre éléments de* E *est une partie* R *de* $E\times E$ *: les deux éléments* x, y *de* E *sont dits* en relation $\mathscr{R}$) *si le couple* (x,y) *est un élément de* R.

La relation R *est dite*

— *réflexive si tout couple* (x,x) *est dans* R *;*
— *symétrique si tout couple* (x,y) *est dans* R *si et seulement si* (y,x) *est dans* R *;*
— *transitive si les couples* $(x,y),(y,z)$ *étant dans* R, *il en est de même pour* (x,z) *;*
— *d'équivalence si la relation* R *est réflexive, symétrique et transitive.*

Pour une relation d'équivalence R, *la partie* $C(x) = \{y\in E | (x,y)\in R\}$ *est appelée* classe d'équivalence de x *et l'ensemble de ces parties constitue une partition de* E.

▷ EXEMPLES 1.12:

1.12.1 Soit d entier non nul. La relation sur $\mathbb{Z}$ de divisibilité « x en relation avec y si et seulement si d divise $x-y$ » est d'équivalence. On a $R_d = \{(x,x+kd), x,k\in\mathbb{Z}\}$ et il y a d classes d'équivalence. Cette partition détermine l'ensemble fini des *entiers modulo* d.

1.12.2 La partition de E associée à une application surjective[23] $f : \mathrm{E} \to \mathrm{F}$ peut être vue comme déterminée par la relation d'équivalence « x et x' ont même image par f »

◁

1.3 Quelques types usuels de raisonnement

Démontrer des théorèmes, c'est établir que telle assertion est `Vrai`. La démonstration se déroule dans un contexte

— géométrie euclidienne : points, droites,...,
— arithmétique : $\mathbb{N}$,
— fonctions d'une variable réelle : $\mathbb{R}$, calcul différentiel et intégral.

avec des hypothèses, voire des prémisses (axiomes et faits), rassemblées dans l'assertion $\mathcal{H}$ (par exemples, pour le domaine *Arithmétique*, on supposera connu, et on utilisera, la division euclidienne ainsi que la décomposition en produit de facteurs premiers). La démonstration vise à démontrer la véracité des conclusions, exprimées dans la proposition $\mathcal{C}$. Parfois, ces propositions sont des prédicats portant sur une variable x (précisée par le contexte du domaine d'étude) : l'implication est alors équivalente à une inclusion

$$\mathrm{H} = \{x|\mathcal{H}[x]\} \subset \mathrm{C} = \{x|\mathcal{C}[x]\}$$

Les raisonnements développés pour démontrer des théorèmes sont extrêmement variés. Outre le raisonnement par récurrence, trois types de raisonnement interviennent fréquemment : ils sont présentés ici.

Les démonstrations complexes peuvent emprunter dans leurs différentes étapes (ou après une *disjonction* des cas) des types différents de raisonnement. L'étude des hypothèses (à quelle étape telle hypothèse est utilisée?), du contexte ainsi posé, des règles d'inférence permet aussi de mieux comprendre un énoncé, éventuellement en simplifiant une première démonstration. Les démonstrations informelles appliquent parfois plusieurs règles d'inférence en même temps, oublient parfois de mentionner les règles utilisées : en utilisant un langage normalisé, les démonstrations par ordinateur échappent à ces manques.

Il y a néanmoins un schéma général, incarné par l'exemple suivant et ou le connecteur $\Longrightarrow$ joue un rôle important. Soit la proposition $\mathcal{C}$ (les *conclusions* de la démonstration) dont on veut démontrer la valeur de vérité `Vrai`. On introduit la proposition $\mathcal{X}$ pour laquelle on démontre que la conjonction « $\mathcal{X}$ et $\mathcal{X} \Longrightarrow \mathcal{C}$ » est `Vrai` : dans les équivalences

$$\big(\mathcal{X} \wedge (\mathcal{X} \Longrightarrow \mathcal{C})\big) \equiv \big(\mathcal{X} \wedge (\neg\mathcal{X} \vee \mathcal{C})\big) \equiv \big(\mathcal{X} \wedge \neg\mathcal{X}\big) \vee \big(\mathcal{X} \wedge \mathcal{C}\big) \equiv \mathcal{X} \wedge \mathcal{C},$$

le premier membre est `Vrai`, alors que le caractère `Vrai` du dernier membre impose que $\mathcal{C}$ le soit. En général la proposition $\mathcal{C}$ sera impliquée par une proposition $\mathcal{X}$

23. La condition de surjectivité est souvent affirmée, afin semble-t-il d'éviter des parties vides dans la partition de $\mathrm{E} = \cup_{y\in\mathrm{F}} f^{-1}(y)$ et accessoirement de montrer que F est fini : elle peut disparaître.

incluant les hypothèses suffisantes (qui peuvent varier au cours de la mise au point de la démonstration) pour la véracité de $\mathcal{C}$, résultat de celle $\mathcal{X} \Longrightarrow \mathcal{C}$ ou de variantes.

Si les deux assertions $\mathcal{X}$ et $\mathcal{X} \Longrightarrow \mathcal{C}$ sont `Vrai`, alors $\mathcal{C}$ est `Vrai`. On dira de manière équivalente :

— les hypothèses $\mathcal{X}$ sont des *conditions suffisantes* de $\mathcal{C}$,
— les conditions $\mathcal{C}$ sont des *conditions nécessaires* de $\mathcal{X}$.

1.3.1 Par exhibition d'un contre-exemple

On cherche à montrer que « $\forall x, \mathcal{C}[x]$ » est `Vrai` ou `Faux`. La négation de cette assertion est $\exists x_0, \neg\mathcal{C}[x_0]$. Si un tel x_0 avec $\neg\mathcal{C}[x_0]$ `Vrai` existe, alors l'assertion $\forall x, \mathcal{C}[x]$ est `Faux`, vu que sa négation est `Vrai`.

▷ EXEMPLES 1.13:

1.13.1 L'assertion « Le périmètre et l'aire d'un rectangle sont égaux » a comme formule propositionnelle

$$\forall (a,b) \in (\mathbb{R}^+)^2, 2(a+b) = ab$$

où il a été convenu que a, b sont les longueurs de deux côtés adjacents du rectangle. Sa négation $\exists (a_0, b_0), 2(a_0+b_0) = a_0 b_0$ ce qui est en général `Faux` : prendre par (contre-)exemple, $a_0 = b_0 = 1$ pour lesquels $2 \cdot (1+1) \neq 1 \cdot 1$.

1.13.2 « Une suite réelle qui tend vers $+\infty$ est croissante » Cette assertion est fausse, comme le contre-exemple $u_n = n + (-1)^n, n \in \mathbb{N}^*$ en convainc. ◁

1.3.2 Raisonnement par déduction directe

Il s'agit de démontrer que la proposition $\mathcal{C} \Longrightarrow \mathcal{C}$ est vraie. La démonstration part des hypothèses représentées par la proposition $\mathcal{H}$ et par l'appel à une succession d'axiomes, définitions et règles d'inférence, on parvient à démontrer que la proposition $\mathcal{C}$ (représentant le théorème) est `Vrai`.

▷ EXEMPLES 1.14:

1.14.1 « Si $x^3 \geq 0$, alors $x \geq 0$ » : si $x = 0$, l'implication est claire, sinon on peut diviser par x^2 (non nul) la première inégalité dont le sens est conservé, donnant ainsi l'inégalité à démontrer.

1.14.2 « Si les entiers a, b sont des multiples de l'entier naturel d, alors $a+b$ est un multiple de d » : par hypothèse, il existe des entiers p, q tels que $a = pd, b = qd$ et par suite $a+b = (p+q)d$, ce qui exprime que $a+b$ est un multiple de d.

1.14.3 « Si n est divisible par 2 et 3, alors n est divisible par 6 ». Soit n divisible par 2 et 3. Ainsi, il existe des entiers p, q tels que $n = 2p = 3q$. Vu[24] que

24. On a utilisé implicitement l'existence d'entiers a, b tels que $3a - 2b = 1$ pour les entiers 2,3 premiers entre eux.

$n = 3n - 2n$, on peut écrire $n = 3(2p) - 2(3q) = 6(p-q)$, ce qui démontre que n est divisible par 6. ◁

Il sera instructif de reprendre la démonstration de cet exemple pour chacun des types de raisonnement introduits ci-dessous.

1.3.3 Raisonnement par contraposée

Pour démontrer l'implication $\mathcal{A} \Longrightarrow \mathcal{B}$, on étudie la proposition (dite *implication contraposée*) $\neg\mathcal{B} \Longrightarrow \neg\mathcal{A}$. L'implication et sa contraposée ont mêmes valeurs de vérité suivant celles des propositions $\mathcal{A}$ et $\mathcal{B}$.

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Longrightarrow \mathcal{B}$	$\neg\mathcal{B}$	$\neg\mathcal{A}$	$\neg\mathcal{B} \Longrightarrow \neg\mathcal{A}$
V	V	V	F	F	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

avec les équivalences

$$(\mathcal{A} \Longrightarrow \mathcal{B}) \equiv (\neg\mathcal{A} \vee \mathcal{B}) \equiv (\neg\mathcal{A} \vee \neg(\neg\mathcal{B})) \equiv (\neg(\neg\mathcal{B}) \vee \neg\mathcal{A}) \equiv (\neg\mathcal{B} \Longrightarrow \neg\mathcal{A}).$$

Cela a été développé dans la sous-section 1.1.2, avec le tableau de vérité I.3.

▷ EXEMPLES 1.15:

1.15.1 À démontrer « *Soit x réel tel que $x \leq \varepsilon$ pour tout $\varepsilon > 0$. Alors $x \leq 0$* », soit

$$(\forall \varepsilon > 0, x \leq \varepsilon) \Longrightarrow (x \leq 0)$$

avec contraposée

$$(x > 0) \Longrightarrow (\exists \varepsilon > 0, x > \varepsilon).$$

Il suffit de prendre $\varepsilon = x/2$ dans la contraposée.

1.15.2 Soit la proposition

$$\text{si } x \notin \{0,1\}, \text{ alors } x(1-x) \neq 0$$

avec contraposée

$$x(1-x) = 0 \Longrightarrow x \in \{0,1\}.$$

qui est `Vrai` (les racines du polynôme $x(1-x)$ sont 0 et 1).

1.15.3 Reprenons l'exemple précédent 1.14.3 et cherchons à démontrer la contraposée « si n n'est pas divisible par 6, alors il n'est pas divisible par 2 ou par 3 ».

La division euclidienne affirme l'existence d'entiers q et $r \in [\![0,5]\!]$ tels[25] que $n = 6q + r$: vu que n n'est pas divisible par 6, r est non nul. Si $r = 1,3$ ou 5 (resp.), on a

$$\begin{aligned} n &= 6q + 1 = 2 \times (3q) + 1, \\ n &= 6q + 3 = 2 \times (3q) + 3 = 2 \times (3q + 1) + 1, \\ n &= 6q + 5 = 2 \times (3q) + 5 = 2 \times (3q + 2) + 1 \text{ resp.}, \end{aligned}$$

ce qui donne n impair, *i. e.* non divisible par 2 ; si $r = 2$ ou 4 (resp.), on a pareillement

$$\begin{aligned} n &= 6q + 2 = 3 \times (2q) + 2, \\ n &= 6q + 4 = 3 \times (2q) + 4 = 3 \times (2q + 1) + 1 \text{ resp.}, \end{aligned}$$

et donc n est non divisible par 3. Ainsi, il a été montré que 2 ou 3 ne divisent pas n, ce qui achève la démonstration par contraposée. ◁

1.3.4 Raisonnement par l'absurde

On démontre que la conclusion $\mathcal{C}$ est vraie à partir des hypothèses $\mathcal{H}$ en montrant que l'assertion constituée par la conjonction $\mathcal{H} \wedge \neg\mathcal{C}$ des hypothèses $\mathcal{H}$ et de la négation $\neg\mathcal{C}$ de la conclusion $\mathcal{C}$, conduit à une contradiction. Ainsi l'assertion $\mathcal{H} \wedge \neg\mathcal{C}$ est fausse, et sa négation

$$\neg\big(\mathcal{H} \wedge \neg\mathcal{C}\big) \equiv \neg\mathcal{H} \vee \neg(\neg\mathcal{C}) \equiv \neg\mathcal{H} \vee \mathcal{C} \equiv \big(\mathcal{H} \Longrightarrow \mathcal{C}\big)$$

est vraie, de même que la contraposée $\neg\mathcal{C} \Longrightarrow \neg\mathcal{H}$ et donc aussi l'implication $\mathcal{H} \Longrightarrow \mathcal{C}$ à démontrer.

Dans la pratique, on commence le raisonnement par « Supposons $\mathcal{H}$ `Vrai` et $\mathcal{C}$ `Faux` » et on cherche une assertion contradictoire (à la fois `Vrai` et `Faux`)

▷ EXEMPLES 1.16:

1.16.1 Démontrons *ab absurdo* le théorème « Le nombre $\sqrt{2}$ est irrationnel[26] ». En effet, supposons $\sqrt{2} = p/q$ avec p et q premiers entre eux, *i. e.* p et q sans facteur premier commun. Alors, élevant au carré l'égalité $\sqrt{2} = p/q$, on a $2q^2 = p^2$, ce qui assure que 2 divise p, puis 4 divise $p^2 = 2q^2$, puis 2 divise q^2 et donc 2 divise q : ainsi 2 est un facteur commun de p et q, ce qui contredit ce qui avait été supposé au moment de l'introduction des p et q. L'hypothèse « $\sqrt{2}$ rationnel » est donc fausse et le théorème « Le nombre $\sqrt{2}$ est irrationnel » est démontré.

25. La notation $[\![m,n]\!]$ désigne l'intervalle d'entiers naturels compris en m et n, soit $[\![m,n]\!] = \{m, m+1, \ldots, n-1, n\}$.

26. Hippase de Métaponte, VIe s. avant J.-C.

1.16.2 L'irrationalité de π a été établie par Lambert[27] emprunta la voie *ab absurdo*. La preuve a été simplifiée depuis lors, avec utilisation d'arguments issus du calcul intégral, tout en gardant la voie du raisonnement par l'absurde.

1.16.3 « L'ensemble des nombres premiers est infini », comme l'a démontré Euclide[28]. Euclide suppose que cela ne soit pas le cas : il existe alors une liste finie $p_1,\dots,p_n$ de nombres premiers et l'entier $\mathrm{P} = 1+\prod_{i=1}^{n} p_i$ a nécessairement tous ses facteurs premiers hors de la liste $p_1,\dots,p_n$, ce qui contredit l'hypothèse : il y a donc une infinité de nombres premiers. Ici l'hypothèse $\mathcal{H}$ implicite consiste en la vérité des bases de l'arithmétique, en particulier les résultats de division et de factorisation d'un naturel en un produit de facteurs premiers, produit unique à réordonnancement près de ses facteurs.

1.16.4 Pour l'exemple traité en 1.14.3 et 1.15.3, supposons que, outre n divisible par 2 et 3, que n n'est pas divisible par 6 : ces trois conditions donnent l'existence de m,p,q,r tels que $n=2m=3p$ et $n=6q+r$ avec $r\in[\![1,5]\!]$. Ainsi

$$r = n-6q = 2m-6q = 3p-6q,$$

ce qui donne r divisible par 2 et 3, ce qui n'est pas possible vu que r est un des chiffres $1,2,3,4$ ou 5. Cette contradiction permet de dire que l'hypothèse *n non divisible par 6* est absurde, ce qui clôt la démonstration. ◁

1.3.5 Raisonnement par récurrence (ou induction)

Il s'agit de démontrer la validité d'un prédicat $\mathcal{A}[n]$ (nommée souvent *propriété de récurrence*) dépendant d'un entier n avec $n\geq n_0$ (en général $n_0=0$ ou 1). Ce type de raisonnement repose sur la formule

$$\Big(\mathcal{A}[n_0]\wedge\forall(k\geq n_0)\big(\mathcal{A}[k]\Longrightarrow\mathcal{A}[k+1]\big)\Big)\Longrightarrow\Big((\forall(n\geq n_0)\mathcal{A}[n]\Big)$$

On commence par démontrer dans une étape d'*initialisation* l'assertion $\mathcal{A}[n_0]$, puis on exécute l'étape d'*hérédité* (ou de *transmission*) : $\mathcal{A}[k]\Longrightarrow\mathcal{A}[k+1]$ pour tout $k\geq n_0$.

Si les deux étapes sont exécutées avec une conclusion `Vrai`, alors la propriété $\mathcal{A}[n]$ est `Vrai` pour tout $n\geq n_0$.

DÉMONSTRATION. Considérons l'ensemble

$$\mathrm{A}=\big\{n\in\mathbb{N},n\geq n_0,\ \mathcal{A}[n]\text{ est fausse}\big\}.$$

Si A est non vide, soit n_A son plus petit élément (l'ensemble des entiers naturels $\mathbb{N}$ a la propriété que toute partie non vide de $\mathbb{N}$ a un plus petit élément). L'égalité $n_\mathrm{A}=n_0$

27. Jean-Henri Lambert, 26 août 1728, Mulhouse, République de Mulhouse – 25 septembre 1777, Berlin, Prusse.

28. Euclide, -300 avant J.-C.

n'est pas valable car on a montré « $\mathcal{A}[n_0]$ » `Vrai`. Alors $n_A > n_0$ et « $\mathcal{A}[n_A - 1]$ » `Vrai`, ce qui implique « $\mathcal{A}[n_A]$ » `Vrai`, ce qui contredit l'appartenance de n_A à A. Ainsi la partie A est vide, ce qui indique la véracité de « $\mathcal{A}[n]$ » pour tout $n \geq n_0$. □

On rédigera l'hypothèse de récurrence $\mathcal{A}[n]$ avec soin.

▷ EXEMPLES 1.17:

1.17.1 Les nombres $31,331,3\,331,\ldots,33\,333\,331$ sont tous premiers, mais pas $333\,333\,331 = 17 \times 19\,607\,843$

1.17.2 Pour toutes les valeurs de $n \in [\![0,39]\!]$, le nombre n^2+n+41 est premier[29] : on pourrait être tenté d'initier un une récurrence avec hypothèse du type « Pour tout entier n, le nombre n^2+n+41 est premier ». Mais, cela ne peut qu'être vain puisque le nombre $40^2+40+41 = 41^2$ est composé. Cet exemple, comme le précédent, souligne que ce n'est pas parce qu'une propriété $\mathcal{A}[n]$ est `Vrai` pour quelques valeurs de n qu'elle l'est pour tout n !

1.17.3 Une démonstration par récurrence établit la relation $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$ pour tout entier n. Encore faut-il deviner le membre de droite !

1.17.4 Reprenons l'exemple déjà traité trois fois (1.14.3, 1.15.3 et 1.16.4) pour le montrer par récurrence. Formulons l'hypothèse de récurrence

$$\mathcal{R}[\mathrm{N}] : \begin{array}{l}\text{si } n \in [\![6\mathrm{N}, 6\mathrm{N}+5]\!] \text{ est divisible par 2 et 3,}\\ \text{alors } n \text{ est divisible par 6}\end{array}$$

Cette hypothèse est vérifiée pour $\mathrm{N} = 0$: aucun entier parmi $1,2,3,4,5$ n'est divisible à la fois par 2 et 3, alors que 0 est divisible par $2,3$ et en même temps par 6.

Supposons $\mathcal{R}[\mathrm{N}]$ vérifiée. Pour établir sa validité pour $\mathrm{N}+1$, considérons un entier n dans l'intervalle $[\![6(\mathrm{N}+1), 6(\mathrm{N}+1)+5]\!]$: alors $n-6 \in [\![6\mathrm{N}, 6\mathrm{N}+5]\!]$, auquel on peut appliquer l'hypothèse de récurrence $\mathcal{R}[\mathrm{N}]$. Si cet entier $n-6$ est divisible par 2 et 3, alors il est divisible par 6 : il en est de même pour $n = (n-6)+6$, ce qui achève d'établir la validité de la propriété de récurrence au rang $\mathrm{N}+1$. La démonstration par récurrence est achevée. ◁

Étant donnée une propriété $\mathcal{A}[n]$ à considérer à partir de l'entier n_0, il est parfois plus aisé d'établir la récurrence pour la propriété $\mathcal{B}[n]$ définie pour $n \geq n_0$ suivant

$$\mathcal{B}[n] : \mathcal{A}[k], \quad k = n_0, \ldots, n.$$

La validité de $\mathcal{B}[n]$ pour tout $n \geq n_0$ implique celle de $\mathcal{A}[n]$ pour tout $n \geq n_0$ (et réciproquement).

La découpe d'une tablette de chocolat fournit un exemple de telle récurrence (dite *forte*).

▷ EXEMPLE 1.18: On cherche à établir par récurrence le nombre de cassures nécessaires à découper une tablette de chocolat [5] rectangulaire en petits carrés.

29. n^2+n+41 : 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281 , 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971 , 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601, $1681 = 40^2+40+41 = 41^2$.

$\mathcal{C}$[N] Soit $n \leq \mathrm{N}$: la tablette de chocolats rectangulaire à n carreaux se découpe en $n-1$ cassures.

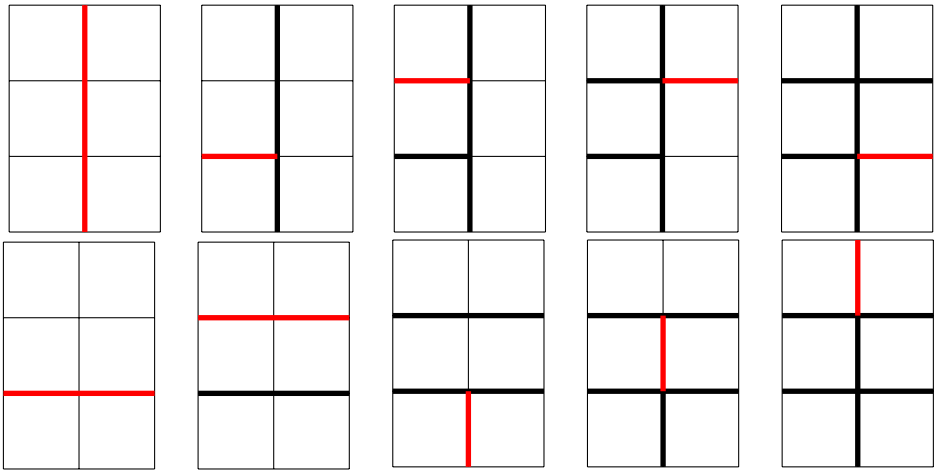

FIGURE I.2 – Une tablette à 6 carrés et deux manières de la réduire en morceaux par 5 cassures.

La propriété $\mathcal{C}$[N] est vraie pour $\mathrm{N}=1$ (rien à casser!), $\mathrm{N}=2, \mathrm{N}=3$ et $\mathrm{N}=5$ (une seule configuration), $\mathrm{N}=4$ (deux configurations). Supposons la vraie pour l'entier N. Pour la démontrer au rang $\mathrm{N}+1$, il suffit de considérer les tablettes à $\mathrm{N}+1$ carreaux, le nombre de découpes étant assuré comme étant $n-1$ pour les tablettes à n avec $n < \mathrm{N}+1$ d'après l'hypothèse de récurrence. Prenons donc une tablette de chocolat à $\mathrm{N}+1$ carreaux. Une découpe produit 2 tablettes à n_1 et n_2 carreaux avec $\mathrm{N}+1 = n_1+n_2$ carreaux globalement, chaque tablette se découpant en n_1-1 et n_2-1 découpes resp. Le nombre total de découpes est donc $1+(n_1-1)+(n_2-1) = \mathrm{N}$, ce qui démontre la propriété de récurrence au rang $\mathrm{N}+1$. ◁

Terminons par le développement du binôme de Newton[30] et sa démonstration par récurrence.

LEMME 1.2: *Pour n entier non nul et a, b deux éléments qui commutent (par ex. nombres complexes, polynôme, fraction rationnelles ; des matrices a, b commutantes,* i. e. *$ab = ba$), la formule du binôme est*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad (\mathcal{R}[n])$$

où $\binom{k}{n} = n!/[k!(n-k)!]$ et la factorielle $n!$ est définie par récursivité : $n! = n(n-1)!$ si $n > 0$ et $0! = 1$. On a convenu que a^0 et b^0 sont égaux à l'élément 1 de l'espace où les variables a, b sont réalisées[31]

30. I. Newton, 25 décembre Woolsthorpe, Grande-Bretagne – 20 mars 1727, Londres, Grande-Bretagne.

31. Le carré $(a+b)^2$ est égal à $a^2+ab+ba+b^2$, alors que le membre de gauche de la formule du binôme écrit ici est égal à $b^2+2ab+a^2$: l'égalité du binôme impose $ab = ba$.

DÉMONSTRATION. La propriété $\mathcal{R}[1]$ est « $a+b=b+a$ » qui est bien établie. Supposons $\mathcal{R}[n]$ `Vrai`. Alors

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b)\\
&= \left[\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\right](a+b)\\
&= \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}a + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}b\\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1} b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1}\\
&= \sum_{\mathrm{K}=1}^{n+1}\binom{n}{\mathrm{K}-1}a^{\mathrm{K}} b^{n-\mathrm{K}+1} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1}\\
&= \binom{n}{n}a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1}+\binom{n}{k}\right]a^k b^{n-k+1} + \binom{n}{0}b^{n+1}\\
&= a^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k} + b^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}$$

où on a utilisé l'hypothèse de récurrence dès la seconde égalité, puis utilisé la commutativité du produit pour écrire notamment $a^k b^{n-k}a = a^{k+1}b^{n-k}$, puis changé de variable de sommation dans le terme de gauche de la cinquième égalité et finalement utilisé l'identité $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ dans la cinquième. On a donc établi la formule du binôme au rang $n+1$. □

Chapitre 2

Suites numériques

Ce chapitre est tout entier consacré aux propriétés de convergence de suites numériques, notées suivant [1]

$$\mathbf{u} = (u_n)_{n\geq 0} = (u_n).$$

On entend par terme général le nombre u_n d'indice n (ou u_k d'indice k). Ce terme u_n est en général un réel (et la suite est est dite réelle) ou un complexe. Une suite $\mathbf{u}$ à termes complexes est équivalente à la donnée de deux suites à valeurs réelles

$$\mathbf{u} = \big(u_n = a_n + \mathrm{i}b_n\big)_{n\geq 0} \Longleftrightarrow \mathbf{a} = \big(a_n = \Re e\, u_n\big)_{n\geq 0}, \quad \mathbf{b} = \big(b_n = \Im m\, u_n\big)_{n\geq 0}.$$

Une inégalité du type $|x-\ell| < \varepsilon$ est employée pour exprimer que x est près de ℓ (qui apparaît par ex. dans la définition 2.1 ci-dessous) peut s'exprimer géométriquement comme l'appartenance de x au petit intervalle $]\ell-\varepsilon, \ell+\varepsilon[$. De même, remplaçant « valeur absolue de réel » par le « module de nombre complexe », on exprime la proximité du complexe z avec c par l'affirmation de l'appartenance de z au disque $\mathrm{D}_c(\varepsilon)$ de centre c et de rayon (petit) ε défini par $\mathrm{D}_c(\varepsilon) = \big\{z \in \mathbb{C}, |z-c| < \varepsilon\big\}$.

Ces différents points de vue permettent d'étendre quasi-immédiatement aux suites à valeurs complexes certains résultats établis pour les suites à valeurs réelles. Il arrive même qu'une suite $\mathbf{u}$ soit à valeurs dans $\mathbb{R}^d$ avec $d \geq 3$ (ou $d = 2$ sans rapport avec l'algèbre des nombres complexes : on écrira son terme général suivant $u_n = (u_n(1), \ldots, u_n(d))$; pour des petites valeurs de d, par exemple $d = 3$ ou 2, on écrira $u_n = (x_n, y_n, z_n)$ si $d = 3$ ou simplement $u_n = (x_n, y_n)$ si $d = 2$. Certaines propriétés énoncées dans la suite pour des suites numériques restent valables pour ces suites à valeurs dans $\mathbb{R}^d$: distinguer lesquelles est un bon exercice de compréhension de ces propriétés!

Une autre variation minime concerne la définition du domaine des indices de la suite. En général, il est pris comme l'ensemble des entiers naturels $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, mais il est parfois préférable de le restreindre, par exemple à $\mathbb{N}^* = \{1, 2, 3, \ldots\}$ pour la suite $(1/n)_{n\geq 1}$.

1. Dans cet imprimé, la lettre grasse $\mathbf{u}$ désignera la suite de terme général u_n défini pour $n \geq 0$ (ou plus généralement $n \geq n_0$ pour un certain entier n_0). Au tableau, on se contentera de la forme soulignée $\underline{\underline{u}}$ une ou deux fois.

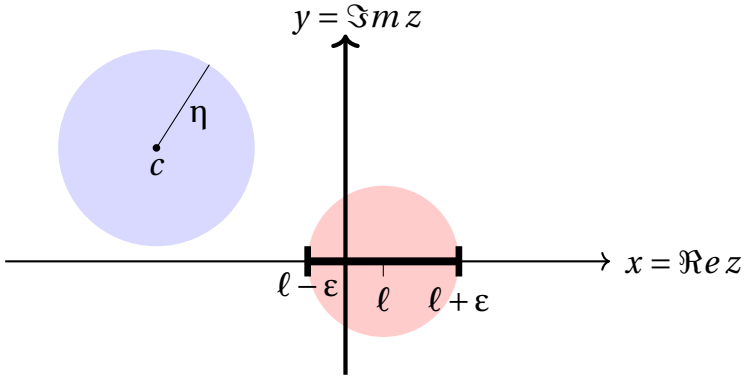

FIGURE II.1 – Dans le plan complexe avec la variable $z = \Re e\, z + \mathrm{i}\Im m\, z \simeq (x, y)$, la droite réelle est représentée par l'axe horizontal $\{(x,0) | x \in \mathbb{R}\}$: l'intervalle (réel) $]\ell - \varepsilon, \ell + \varepsilon[$ est l'intersection de l'axe réel et du disque $\mathrm{D}_\ell(\varepsilon) = \{z \in \mathbb{C}, |z - \ell| < \varepsilon\}$. Le disque complexe $\mathrm{D}_c(\eta)$ centré en c (hors de l'axe réel) et de rayon (petit) η est une illustration géométrique de la proximité $|z - c| < \eta$ entre les complexes z et c.

Ce distinguo n'est en rien gênant, car l'objectif du cours consiste en l'étude des propriétés asymptotiques d'une suite, *i. e.* le comportement des termes u_n quand n est grand (et même de plus en plus grand).

Donnons un exemple typique

▷ EXEMPLE 2.1: Les deux suites $\mathbf{u} = (u_n)_{n\geq 1}$ et $\mathbf{v} = (v_n)_{n\geq 1}$ définies suivant

$$u_n = \left(1 + \frac{1}{n}\right)^n, \quad v_n = 1 + \frac{1}{1} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}, \qquad n \geq 1$$

convergent vers la même limite, à savoir le nombre d'Euler [2] (la base des logarithmes népériens)

$$\mathrm{e} = 2.71828\ 18284\ 59045\ 23536\ldots$$

les convergences sont de rapidité très différente, comme l'indiquent les quelques approximations suivantes où on a souligné les décimales erronées

$$u_4 = 2.\underline{44141}\ldots, \quad u_{64} = 2.\underline{69734}\ldots, \quad u_{1024} = 2.71\underline{696}\ldots$$
$$v_4 = 2.\underline{66666}\ldots, \quad v_{16} = 2.71828\ 18284\ 5\underline{8994}\ldots$$

◁

Ce chapitre va donner la définition de la convergence d'une suite, puis établir la convergence de quelques suites basiques avant d'étudier la convergence de suites plus compliquées en s'appuyant sur une algèbre des convergences. Ces résultats généraux seront suivis de l'étude de suites particulières généralisant les suites arithmético-géométriques.

2. Leonhard Euler, 15 avril 1707, Bâle Suisse – le 7 septembre 1783, Saint-Pétersbourg, Empire russe.

Terminons cette introduction avec quelques propriétés précisant la forme d'une suite **u** complexe (ou réelle au besoin)

1. La suite **u** est *constante* si tous ses termes ont même valeur. Si v est cette valeur, on identifiera parfois v et la suite constante $(v)_{n\geq 0} = (v, v, v, \dots)$.
2. La suite **u** est *stationnaire* si elle est constante à partir d'un certain indice, *i. e.* il existe $\mathrm{N} \in \mathbb{N}^*$ tel que $u_{\mathrm{N}} = u_{\mathrm{N}+n}$ pour tout $n \geq 0$.
3. La suite **u** est *périodique* de période $\mathrm{T} \in \mathbb{N}^*$ si $u_{n+\mathrm{T}} = u_n$ pour tout $n \geq 0$.
4. Une *suite extraite* (ou *sous-suite*) de la suite **u** est toute suite de la forme $\left(u_{\varphi(n)}\right)$ avec l'application $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante.
5. La suite **u** est bornée si il existe un réel B telle que $|u_n| \leq \mathrm{B}$ pour tout $n \in \mathbb{N}$.

Pour les suites réelles, on a des propriétés relatives à l'ordre

1. La suite **u** est majorée (minorée resp.) s'il existe un réel M (resp. m) tel que $u_n \leq \mathrm{M}$ (resp. $u_n \geq m$) pour tout indice $n \geq 0$. Une suite réelle est bornée si et seulement si elle est minorée et majorée.
2. La suite **u** est *croissante* si $u_n \leq u_{n+1}$ pour tout $n \geq 0$.
3. La suite **u** est *décroissante* si $u_n \geq u_{n+1}$ pour tout $n \geq 0$.
4. La suite **u** est *strictement (dé)croissante* si les inégalités précédemment introduites sont strictes.
5. La suite **u** est *monotone* si elle est croissante ou décroissante.
6. La suite **u** est majorée (minorée resp.) s'il existe un réel M (resp. m) tel que $u_n \leq \mathrm{M}$ (resp. $u_n \geq m$) pour tout indice $n \geq 0$. Une suite est bornée si et seulement si elle est minorée et majorée.

Mentionnons à nouveau que ce qui nous importe ici, ce sont les propriétés du terme u_n de la suite **u** pour un indice n suffisamment grand. Les propriétés précédentes peuvent être assorties de cette (légère) réserve : « Pour n assez grand ». Une suite bornée à partir d'un certain rang est bornée, mais en général une suite croissante pour n assez grand, ne l'est pas toujours : la suite $\left(|n-5|\right)_{n\geq 5}$ est croissante, mais pas la suite $\left(|n-5|\right)_{n\geq 0}$.

Donnons quelques exemples de suites avec certaines des propriétés précédentes :

⊳ EXEMPLES 2.2:

2.2.1 Soit $\mathrm{T} \in \mathbb{N}^*$ et a un réel. La suite de terme général $\sin\left(2n\pi/\mathrm{T} + a\right)$ est périodique de période T, la suite complexe de terme général $\left((1-\mathrm{i})/\sqrt{2}\right)^n = \mathrm{e}^{-\mathrm{i}n\pi/4}$ est périodique de période $\mathrm{T} = 8$.

2.2.2 La suite des décimales d'un nombre rationnel est, à partir d'un certain entier, périodique : $1/90 = 0.011111\dots$, $53/2475 = 0.021414\dots$ (admis).

2.2.3 La suite $\left(u_n = \mathrm{A}^n/n!\right)_{n\geq 0}$ est décroissante à partir d'un certain rang : le quotient $u_n/u_{n-1} = \mathrm{A}/n$ est strictement inférieur à 1 si $\mathrm{A}/n < 1$, *i. e.* $n > \mathrm{A}$. Ainsi la suite $(u_n)_{n\geq[\mathrm{A}]+1}$ est décroissante.

2.2.4 La suite **u** a comme suite extraite celle des termes d'indice pair $\mathbf{u}_p = (u_{2k})_{k\geq 0}$ et celle des termes impairs $\mathbf{u}_i = (u_{2k+1})_{k\geq 0}$.

2.2.5 La suite **u** de terme général $\sin\left(2\pi\sqrt{n}\right)$ a comme suite extraite la suite $\left(u_{k^2} = \sin(2\pi k)\right)_{k\geq 0}$ qui est constante nulle. On montre que pour tout réel x, il existe une suite extraite de cette suite **u** qui converge vers $\sin x$. ◁

2.1 Convergence et limite

Soit **u** une suite de nombres. La convergence de cette suite vers le nombre ℓ signifie (intuitivement) que si on se place dans un petit voisinage de ℓ (un intervalle $\mathrm{I}_\ell(\varepsilon) =]\ell-\varepsilon, \ell+\varepsilon[$ avec ε petit), alors tous les termes u_k de la suite s'y trouvent, pourvu qu'on considère des termes d'indice k assez élevé. La définition formelle est la suivante

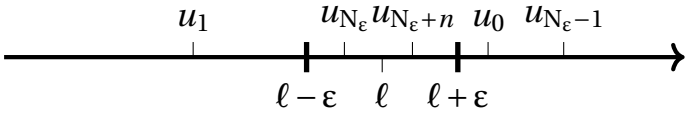

FIGURE II.2 – La suite réelle **u** converge vers ℓ : étant donné ε, il existe N_ε tel que $u_{\mathrm{N}_\varepsilon+n} \in]\ell-\varepsilon, \ell+\varepsilon[$ pour tout $n \geq 0$.

DÉFINITION 2.1: *La suite* **u** *est dite convergente vers le nombre* ℓ *si pour tout réel* ε *strictement positif, il existe un entier* N_ε *tel que la condition* $n \geq \mathrm{N}_\varepsilon$ *implique pour l'entier* n *l'inégalité* $|u_n - \ell| \leq \varepsilon$. *On dit que* ℓ *est la limite de la suite et on écrit*

$$\ell = \lim_{n\to\infty} u_n \quad ou \quad u_n \xrightarrow{n\to\infty} \ell.$$

Cette propriété de convergence s'exprime en logique formelle suivant

$$\forall \varepsilon > 0, \quad \exists \mathrm{N}_\varepsilon \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad (n \geq \mathrm{N}_\varepsilon \Longrightarrow |u_n - \ell| \leq \varepsilon). \tag{2.1}$$

△ REMARQUES 2.1:

1. L'inégalité $|u_n - \ell| \leq \varepsilon$ de la définition peut être remplacée par l'inégalité stricte $|u_n - \ell| < \varepsilon$ (remplacer ε par 2ε, mais le ε positif doit l'être strictement.
2. L'entier N_ε dépend de la suite **u** et du $\varepsilon > 0$. Pour insister sur cette dépendance (en général effective), on a inscrit un indice ε à cet entier N_ε. ▽

On a une définition purement analogue pour une suite complexe $\mathbf{u}$ convergeant vers la limite $\ell \in \mathbb{C}$, soit

$$\forall \varepsilon > 0, \quad \exists N \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad (n \geq N \Longrightarrow |u_n - \ell| \leq \varepsilon).$$

En langage moins formalisé qui débutait cette section, il faut donc remplacer

$$\text{« l'intervalle } I_\ell(\varepsilon) =]\ell - \varepsilon, \ell + \varepsilon[\text{ »}$$

par

$$\text{« le disque } D_\ell(\varepsilon) = \{z \in \mathbb{C}, |z - \ell| < \varepsilon\} \text{ ».}$$

L'application *module* $z \in \mathbb{C} \mapsto |z| \in \mathbb{R}^+$ est un prolongement à $\mathbb{C}$ de l'application *valeur absolue* sur $\mathbb{R}$, la valeur absolue $|x|$ ou le module $|z|$ étant interprétés comme la longueur de x (dans $\mathbb{R}$) ou z (dans le plan complexe $\mathbb{C}$).

Par une translation $(x \mapsto x - \ell)$, on peut se ramener au cas particulier où $\ell = 0$. En effet la suite $\mathbf{u}$ converge vers ℓ si et seulement si la suite $\mathbf{u} - \ell = (u_n - \ell)_{n \geq 0}$ converge vers 0 : cela provient dans la définition (2.1) pour $u_n \to \ell$ et $u_n - \ell \to 0$ de l'identité $u_n - \ell = (u_n - \ell) - 0$ utilisée dans la définition de la convergence des suites $\mathbf{u}$ et $\mathbf{u} - \ell$.

Graphiquement, on peut considérer le graphe de la suite réelle $\mathbf{u}$ dans le plan $\mathbb{N}_n \times \mathbb{R}_u$: les points (n, u_n) s'accumulent asymptotiquement le long de la droite $u = \ell$. Pour la suite complexe $\mathbf{u}$, on peut représenter dans le plan complexe les disques $D_\ell(\varepsilon)$: pour $n \geq N_\varepsilon$ le complexe u_n y est contenu ; si la suite est réelle, on peut considérer cette figure en restriction à l'axe réel, où le disque $D_\ell(\varepsilon) = \{|z - \ell| \leq \varepsilon\}$ y est remplacé par l'intervalle $]\ell - \varepsilon, \ell + \varepsilon[$.

La définition de la limite suppose qu'on connaisse la limite : peut-on avoir un critère d'existence de la limite sans la connaître explicitement ? On apportera une réponse positive dans certains cas.

Donnons quelques exemples, avec la donnée explicite du N_ε de la définition 2.1.

▷ EXEMPLES 2.3 :

2.3.1 Soit $\mathbf{u}$ une suite stationnaire : il existe un entier N tel que $u_n = u_N$ pour tout $n \geq N$. Il en résulte que la suite $\mathbf{u}$ est convergente avec limite $\ell = u_N$.

2.3.2 La suite $\left(u_n = \dfrac{1}{n}\right)_{n \geq 1}$ converge vers 0 : étant donné $\varepsilon > 0$, si on prend[3] $N_\varepsilon = \left\lfloor \dfrac{1}{\varepsilon} \right\rfloor + 1$, la minoration

$$n \geq N_\varepsilon \geq \frac{1}{\varepsilon}$$

assure

$$\left| \frac{1}{n} - 0 \right| = \frac{1}{n} \leq \varepsilon.$$

C'est la bonne condition énonçant la convergence de la suite $\left(\dfrac{1}{n}\right)_{n \geq 1}$ vers 0.

3. La partie entière du réel x est notée $\lfloor x \rfloor$.

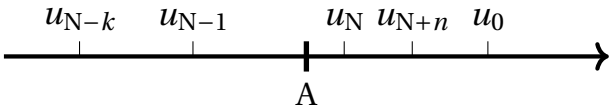

FIGURE II.3 – La suite réelle **u** qui tend vers $+\infty$: $u_{N+n} \geq A$ pour $n \geq 0$.

2.3.3 Soit d réel positif non nul. Le même raisonnement vaut pour la suite dite de Riemann $\left(u_n = \dfrac{1}{n^d}\right)_{n\geq 1}$ convergente vers 0 : étant donné un $\varepsilon > 0$, si on prend $N_\varepsilon = \left\lfloor \dfrac{1}{\varepsilon^{1/d}} \right\rfloor + 1$, la minoration

$$n \geq N_\varepsilon \geq \frac{1}{\varepsilon^{1/d}}$$

assure

$$\frac{1}{n} \leq \varepsilon^{1/d} \text{ et donc } \frac{1}{n^d} \leq \varepsilon,$$

soit

$$\left|\frac{1}{n^d} - 0\right| = \frac{1}{n^d} \leq \varepsilon.$$

2.3.4 La suite $\left(u_n = \dfrac{n+1}{n}\right)_{n\geq 1}$ converge vers $\ell = 1$: on a

$$u_n - 1 = \frac{n+1}{n} - 1 = \frac{1}{n}$$

et on prendra donc $N_\varepsilon = \left\lfloor \dfrac{1}{\varepsilon} \right\rfloor + 1$ correspondant au $\varepsilon > 0$. ◁

On a une définition analogue pour une suite tendant vers $+\infty$ ($-\infty$ resp.), *i. e.* une suite dont les valeurs sont de plus en plus grandes (négatives avec valeur absolue de plus en plus grande resp.) lorsque l'indice tend vers $+\infty$.

DÉFINITION 2.2: *La suite* **u** *est dite tendre vers* $+\infty$ *si pour tout réel* A*, il existe un entier* N *tel que, si* $n \geq N$, $u_n \geq A$*, soit de manière formelle*

$$\forall A \in \mathbb{R}, \quad \exists N \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad (n \geq N \Longrightarrow u_n \geq A).$$

et on écrira

$$+\infty = \lim_{n\to\infty} u_n \quad ou \quad u_n \xrightarrow{n\to\infty} +\infty.$$

De manière analogue l'énoncé « La suite **u** tend vers $-\infty$ » est formulé suivant

$$\forall A \in \mathbb{R}, \quad \exists N \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad \big(n \geq N \Longrightarrow u_n \leq A\big).$$

Parfois, on considère une suite $\mathbf{u}$ qui « tend vers l'infini », signifiant que la suite $(|\mathbf{u}|)_{n\geq 0}$ des valeurs absolues tend vers $+\infty$:

$$\forall A \in \mathbb{R}, \quad \exists N \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad |u_{N+n}| \geq A.$$

Dans la définition 2.2, on peut bien évidemment se limiter aux réels $A > 0$.

Les symboles ∞, $+\infty$, $-\infty$ ne sont pas des nombres et il n'est pas possible de définir sur l'ensemble $\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$ un prolongement des opérations classiques $+, \times$. On dira que « la suite $\mathbf{u}$ converge vers ℓ » et que « la suite $\mathbf{u}$ tend vers $+\infty$ » pour bien marquer la différence des deux situations.

▷ EXEMPLE 2.4: Soit $d > 0$. Le raisonnement précédent utilisé pour la suite $\left(n^{-d}\right)_{n\geq 1}$ s'adapte aisément à l'étude de la convergence de la suite $\left(n^{d}\right)_{n\geq 1}$ qui tend vers $+\infty$. Le nombre A étant fixé, soit l'entier $N_A = \lfloor A^{1/d} \rfloor + 1$. La minoration $n \geq N_A \geq A^{1/d}$ assure $n^d \geq N_A^d \geq A$, ce qui justifie la convergence de la suite $\left(n^{d}\right)_{n\geq 1}$ vers $+\infty$. ◁

Les deux définitions 2.1 et 2.2 sont liées, comme le lemme suivant l'indique

LEMME 2.1: *Soit* $\mathbf{u}$ *une suite de réels strictement positifs. La suite* $\mathbf{u}$ *converge vers* 0 *si et seulement si la suite* $1/\mathbf{u} = (1/u_n)_{n\geq 1}$ *tend vers* $+\infty$.

Même si le contenu de ce lemme semble clair, nous allons le démontrer en partant de la définition 2.1.

DÉMONSTRATION. Supposons la suite $\mathbf{u}$ convergente vers $\ell = 0$. Soit $A > 0$ et considérons $\varepsilon = \dfrac{1}{A}$ et le N_ε afférent donné par la definition 2.1. Ainsi, si $n \geq N_\varepsilon$, on a

$$u_n = |u_n| \leq \varepsilon = A^{-1}$$

et donc $u_n^{-1} \geq A$. On a donc montré que $\left(u_n^{-1}\right)$ tend vers $+\infty$.

Réciproquement, il suffit de reprendre le même schéma. Soit $\varepsilon > 0$, $A = \varepsilon^{-1}$ et le N_A afférent pour la suite $\left(u_n^{-1}\right)$ tendant vers $+\infty$. Alors pour $n \geq N_A$, on a $u_n^{-1} \geq A$ et donc $|u_n| = u_n \leq A^{-1} = \varepsilon$, ce qui établit que la suite $\mathbf{u}$ converge vers $\ell = 0$. □

Quelques propriétés liées à la convergence de suites

PROPOSITION 2.1: *Soit* $\mathbf{u}$ *une suite à valeurs réelles ou complexes.*

1. *La convergence, ou la non-convergence, de la suite* $\mathbf{u}$ *ne dépend pas de ses premiers termes. Il en est de même de la valeur de sa limite.*
2. *Si la suite* $\mathbf{u}$ *est convergente, elle a une unique limite.*
3. *Si la suite* $\mathbf{u}$ *est convergente, elle est bornée.*
4. *Toute sous-suite* $\mathbf{v}$ *de la suite* $\mathbf{u}$ *supposée convergente vers* ℓ *est elle-même convergente de même limite* ℓ.
5. *Soit* $\mathbf{v}$ *une suite réelle convergeant vers* 0 *et* C *une constante strictement positive. Si la suite* $\mathbf{u}$ *vérifie* $|u_n| \leq C v_n, n \geq 1$, *alors la suite*[4] $\mathbf{u}$ *converge vers* 0.

4. On dit que la suite $\mathbf{u}$ est dominée par la suite $\mathbf{v}$, à la constante multiplicative C près.

6. *Soit* **v** *une suite réelle tendant vers* $+\infty$ *et* **u** *une suite réelle. Si il existe une constante* C *strictement positive telle que* $u_n \geq Cv_n$ *pour* $n \geq 1$, *alors la suite* **u** *tend vers* $+\infty$.

DÉMONSTRATION. On peut aisément démontrer chacune de ces assertions en faisant appel aux définitions et leurs ε. On peut s'en convaincre par des arguments plus littéraires (et le soutien de graphiques).

Pour la seconde assertion, supposons l'existence de deux limites ℓ_1 et ℓ_2 distinctes. Dessinons dans le plan complexe deux petits disques $D_{\ell_1}(\varepsilon)$ et $D_{\ell_2}(\varepsilon)$ centrés en ℓ_1 et ℓ_2 disjoints : alors pour n assez grand, le terme u_n est dans chacun de ces disques, ce qui n'est pas possible.

Pour la troisième, il suffit de considérer le disque $D_0(|\ell|+1)$ contenant le disque $D_\ell(1)$, qui lui-même contient toutes les valeurs u_n pour $n > N_1$ (où l'entier N_1 sort de la définition 2.1) en prenant $\varepsilon = 1$). Alors en prenant un majorant M de $|\ell|+1$ et des modules $|u_1|,\dots,|u_{N_1}|$ (en nombre fini), le caractère borné de la suite **u** est établi.

Pour la quatrième, considérons l'application injective croissante $\varphi : \mathbb{N} \to \mathbb{N}$ décrivant la suite extraite **v**, soit le terme général $v_k = u_{\varphi(k)}$ pour $k \geq 1$. Pour $\varepsilon > 0$, on prend le petit disque $D_\ell(\varepsilon)$ centré en ℓ et un $N = N_\varepsilon$ tel que toutes les valeurs de u_n pour $n \geq N$ sont dans ce disque. Alors, vu que $\varphi(k) \geq k$, les $v_k = u_{\varphi(k)}$ sont aussi dans ce disque pour $k \geq N_\varepsilon$, ce qui établit la convergence de la suite **v**.

Pour la cinquième, soit un $\varepsilon > 0$. Il existe un $N = N_\varepsilon$, tel que pour $n \geq N_\varepsilon$, les termes v_n sont dans le petit disque $D_0(C^{-1}\varepsilon)$; alors, pour $n \geq N$, les termes u_n vérifient $|u_n| \leq Cv_n \leq C[C^{-1}\varepsilon] = \varepsilon$, ce qui les situe dans le disque $D_0(\varepsilon)$. On vient d'établir la convergence de le suite **u** vers 0.

Pour la dernière, pour $A > 0$, il existe un entier $N = N_A$ tel que les termes v_n sont dans la demi-droite $[A/C, +\infty[$ (*i. e.* vérifient $v_n \geq \dfrac{A}{C}$) à partir de ce rang N, alors, à partir de ce même rang N, les valeurs u_n, qui satisfont

$$u_n \geq Cv_n \geq C\left[\frac{A}{C}\right] = A,$$

se trouvent dans la demi-droite $[A, +\infty[$, ce qui signifie que **u** tend vers $+\infty$. □

△ REMARQUE 2.2: Une suite bornée n'est pas nécessairement convergente, comme l'indique la suite de terme général $u_n = \cos(\pi n) = (-1)^n$: sa sous-suite des termes d'indice pair (resp. impair) est constante, ces deux sous-suites ayant des limites opposées ± 1.

Par ailleurs, une suite non bornée ne tend pas nécessairement vers l'infini : la suite $\left(\sqrt{n+1} - (-1)^n\sqrt{n}\right)$ n'est pas bornée (sa sous-suite des éléments d'ordre impair $u_{2k+1} = \sqrt{2k+2} + \sqrt{2k+1}$ tend vers $+\infty$) et ne tend pas vers $+\infty$, ni vers $-\infty$ (sa sous-suite des éléments d'indice pair $u_{2k} = \sqrt{2k+1} - \sqrt{2k} = \dfrac{1}{\sqrt{2k+1}+\sqrt{2k}}$ converge vers 0). ▽

▷ EXEMPLE 2.5: On va montrer[5] $\lim_{n\to\infty} \sqrt[n]{n} = 1$. En effet, tout d'abord, la suite $\left(r_n = \sqrt[n]{n} - 1\right)$ est positive : vu la stricte croissance de $u \in \mathbb{R}^+ \mapsto u^n \in \mathbb{R}^+$, on a $\sqrt[n]{n} > 1$ si et seulement si $n = (\sqrt[n]{n})^n > 1$.

D'après la formule du binôme et $\sqrt[n]{n} = 1 + r_n$.

$$n = (1+r_n)^n = \sum_{k=0}^{n} \binom{n}{k} r_n^k > \binom{n}{2} r_n^2 = \frac{n(n-1)}{2} r_n^2$$

ainsi

$$0 < r_n^2 < n\frac{2}{n(n-1)} = \frac{2}{n-1} =$$

soit $0 < r_n < \sqrt{\dfrac{2}{n-1}} = \sqrt{2}(n-1)^{1/2}$. Vu que la suite majorante $\left(\sqrt{2}(n-1)^{1/2}\right)$ de r_n converge vers 0, il en est de même pour la suite de terme général r_n d'après l'alinéa 5 de la proposition 2.1. Vu que $r_n = \sqrt[n]{n} - 1$, on déduit la convergence de la suite $\left(\sqrt[n]{n}\right)_{n\geq 1}$ vers 1.

On en déduit $\sqrt[n]{c} \to 1$ pour tout réel positif non nul. Il suffit de le montrer pour $c > 1$: si $c < 1$, l'identité $\sqrt[n]{c} = \left[\sqrt[n]{c^{-1}}\right]^{-1}$ ramène le cas $c < 1$ au cas $c > 1$ via l'assertion « l'inverse d'une suite convergente vers k non nulle converge vers l'inverse k^{-1} » (cf. sixième colonne du tableau II.2, alors que si c=1, $\sqrt[n]{c} = 1$ pour tout n. Soit donc $c > 1$. On a alors $1 \leq \sqrt[n]{c} \leq \sqrt[n]{n}$ si $n \geq c$, soit

$$0 \leq \sqrt[n]{c} - 1 \leq \sqrt[n]{n} - 1, \quad n \geq c,$$

ce qui implique la convergence vers 0 de la suite $\left(\sqrt[n]{c} - 1\right)_{n\geq 1}$, et donc vers 1 de la suite $\left(\sqrt[n]{c}\right)$. ◁

Les deux limites suivantes sont basiques

LEMME 2.2: *Si a est un réel tel que $a > 1$, q un complexe tel que $|q| < 1$ et d un entier naturel, alors*

$$\lim_{n\to\infty} \frac{a^n}{n^d} = +\infty, \qquad \lim_{n\to\infty} q^n n^d = 0$$

DÉMONSTRATION. Commençons par le cas $d = 0$. On écrit $a = 1+h$ avec $h > 0$, puis on utilise la formule du binôme de Newton

$$a^n = (1+h)^n = 1 + nh + \cdots \geq hn$$

où les termes ignorés sont tous positifs ou nuls. Vu que $hn \to +\infty$ lorsque $n \to \infty$, il en est de même par comparaison (cf. le dernier alinéa de la proposition 2.1) pour la suite (a^n).

Le cas $d \in \mathbb{N}^*$ se traite de la même manière en négligeant tous les termes du binôme sauf un seul pour obtenir une minoration de a^n/n^d qui tende vers $+\infty$.

$$(1+h)^n = 1 + nh + \cdots + \binom{n}{d+1} h^{d+1} + \cdots \geq \frac{n(n-1)\ldots(n-d)}{(d+1)!} h^{d+1}$$

et par suite, pour $n \geq 2d$, inégalité équivalente à $\dfrac{n}{2} \geq d$ ou encore $n - d \geq \dfrac{n}{2}$,

$$\frac{a^n}{n^d} = \frac{(1+h)^n}{n^d} \geq \frac{n(n-1)\ldots(n-d)}{n^d} \frac{h^{d+1}}{(d+1)!} \geq \frac{(n-d)^d}{n^d} \frac{h^{d+1}}{(d+1)!} n \geq 2^{-d} \frac{h^{d+1}}{(d+1)!} n$$

5. On peut aussi le montrer via la formule $\sqrt[n]{n} = \exp((\ln n)/n)$: on prend le parti ici de coller au plus près des définitions basiques.

En posant $m_{h,d} = 2^{-d} h^{d+1}/(d+1)!$, le terme général a^n/n^d est minoré par $m_{h,d}n$, terme général d'une suite qui converge vers $+\infty$: il en est de même pour $\left(a^n/n^d\right)_{n\geq 1}$ à nouveau en invoquant le sixième alinéa de la proposition 2.1.

On peut faire cette démonstration en utilisant des propriétés dites *algèbre des limites* qui seront vues ci-dessous.

Soit donc la suite **u** de terme général $u_n = a^n/n^d$ pour $n \in \mathbb{N}^*$ et la suite **v** de terme général $v_n = u_{n+1}/u_n$. On a

$$v_n = \frac{a^{n+1}}{(n+1)^d} \Big/ \frac{a^n}{n^d} = \frac{a^{n+1}}{a^n} \frac{n^d}{(n+1)^d} = \frac{a}{(1+1/n)^d},$$

et donc $v_n \to a$ (d'après l'algèbre des limites). Prenons b dans l'intervalle (ouvert) $]1, a[$: l'intervalle $]b, 2a-b[$ est centré en a et de longueur $2(a-b)$. D'après la définition de la limite de **v** (qui converge vers a), il existe N tel que, pour tout $n \geq \mathrm{N}$, v_n soit dans l'intervalle $]b, 2a-b[$ et donc $v_n \geq b$. Ainsi

$$u_{\mathrm{N}+n+1} = \frac{u_{\mathrm{N}+n+1}}{u_{\mathrm{N}+n}} \frac{u_{\mathrm{N}+n}}{u_{\mathrm{N}+n-1}} \dots \frac{u_{\mathrm{N}+1}}{u_{\mathrm{N}}} u_{\mathrm{N}} = v_{\mathrm{N}+n} v_{\mathrm{N}+n-1} \dots v_{\mathrm{N}} u_{\mathrm{N}} \geq b^{n+1} u_{\mathrm{N}} \to +\infty$$

En résulte que la suite **u** domine[6] la suite (b^n) à partir de l'indice N : la suite (b_n) tend vers $+\infty$, ce qui implique la même convergence pour la suite **u** (en vertu du dernier alinéa de la proposition 2.1).

Pour la deuxième assertion, si $|q| = 0$, alors la suite $(q^n n^d)$ est constante avec valeur nulle. Si q est non nul, nous posons $a = 1/|q|$ qui est strictement supérieur à 1 : ainsi, vu $|q^n n^d| = \left(a^n/n^d\right)^{-1}$, la première partie assure que l'inverse de $|q^n n^d|$ tend vers $+\infty$ et donc, vu le lemme 2.1, la suite $(|q^n n^d(|$, et donc aussi $(q^n n^d)$, converge vers 0. □

COROLLAIRE 2.1: *Soit d entier naturel non nul. On a*

$$\lim_{n\to\infty} \frac{\ln n}{n^d} = 0$$

DÉMONSTRATION. Posons $\mathrm{X} = \ln n$ et $\mathrm{N} = \lfloor \mathrm{X} \rfloor + 1$. Alors

$$0 \leq \frac{\ln n}{n^d} = \frac{\mathrm{X}}{\mathrm{e}^{d\mathrm{X}}} \leq \frac{\mathrm{N}}{\mathrm{e}^{d(\mathrm{N}-1)}} \leq \mathrm{e}^d \frac{\mathrm{N}}{\mathrm{e}^{d\mathrm{N}}}$$

où le dernier facteur converge vers 0 lorsque n (et par suite $\mathrm{N} = \lfloor \ln n \rfloor + 1$) tend vers $+\infty$. □

Le tableau II.1 reprend quelques convergences de base qui viennent d'être montrées pour d entier. Elles sont en fait valables pour d réel : par exemple, avec D entier tel que $\mathrm{D} \geq d$, on écrit $a^n n^{-d} \geq a^n n^{-\mathrm{D}}$, le second membre tendant vers $+\infty$,et donc aussi le premier d'après l'alinéa 6 de la proposition 2.1.

D'une part, on a vu dans l'exemple 2.4 que pour $d > 0$ la suite $\left(n^d\right)_{n\geq 0}$ tend vers $+\infty$. On peut l'établir à nouveau en utilisant que la suite $\left(n^d\right)$ est croissante : d'après le corollaire 2.2, il suffit d'en exhiber une sous-suite tendant vers $+\infty$ pour en déduire que la suite $\left(n^d\right)$ tend aussi vers $+\infty$. Soit donc k entier tel que kd soit au moins égal à 1. Alors la suite extraite $\left(\left(n^k\right)^d = n^{kd}\right)_{n\geq 1}$ (correspondant à l'injection

6. cf. note 4.

$n \in \mathbb{N}^* \mapsto n^k \in \mathbb{N}^*$) de la suite $\left(n^d\right)_{n\geq 1}$ est minorée par la suite $(n)_{n\geq 1}$ tendant vers $+\infty$, la suite $\left(n^{kd}\right)$ tend donc vers $+\infty$ (cf. dernière alinéa de la proposition 2.1) et donc aussi la suite croissante $\left(n^d\right)_{n\geq 1}$ dont $\left(n^k d\right)_{n\geq 0}$ est une sous-suite [7].

D'autre part, et comme précédemment, il suffit d'étudier le comportement de la suite $\left(\dfrac{a^n}{n^d}\right)$ avec $a > 1$ et $d > 0$ quand n tend vers l'infini. Dans ce cas, vu que $d \leq \lfloor d \rfloor + 1$, on a $\left(\dfrac{a^n}{n^d}\right) \geq \dfrac{a^n}{n^{\lfloor d \rfloor + 1}}$: le membre de droite de l'inégalité tendant vers $+\infty$, il en est de même pour le membre de gauche $\dfrac{a^n}{n^d}$.

n^d si $d > 0$	$\dfrac{1}{n^d}$ si $d > 0$	$\dfrac{a^n}{n^d}$ si $a > 1$ et $d \in \mathbb{R}$	$\dfrac{a^n}{n^d}$ si $\lvert a\rvert < 1$ et $d \in \mathbb{R}$	$\dfrac{\ln n}{n^d}$ si $d > 0$
$+\infty$	0	$+\infty$	0	0

TABLE II.1 – Limites basiques

2.2 Algèbre des limites

Très souvent dans des études de limites, on commence par réduire l'analyse d'une expression à celle de ses sous-expressions (somme, produit,...).

Cette démarche est justifiée par des énoncés du type « la somme (le produit resp.) de deux suites convergentes est convergente avec comme limite la somme (le produit resp.) des limites » : ces règles apparaissent dans les premières lignes du tableau suivant, y compris avec certaines suites supposées tendre vers $\pm\infty$.

Commençons par préciser ces opérations élémentaires sur les suites, induites par les opérations algébriques [8] sur les nombres réels ou complexes.

DÉFINITION 2.3: *Soit* $\mathbf{u}$, $\mathbf{v}$ *deux suites. Leur somme* $\mathbf{u}+\mathbf{v}$ *, leur produit* $\mathbf{uv}$ *, leur quotient* $\mathbf{u}/\mathbf{v}$ *sont définis suivant*

$$(\mathbf{u}+\mathbf{v})_n = u_n + v_n, \quad (\mathbf{uv})_n = u_n v_n, \quad \left(\frac{\mathbf{u}}{\mathbf{v}}\right)_n = \frac{u_n}{v_n}, \quad n \geq 0,$$

7. On a utilisé le fait qu'une suite croissante ayant une sous-suite tendant vers $+\infty$, tend elle-même vers $+\infty$: c'est établi dans le corollaire 2.2 ci-dessous.

8. Ces propriétés sur les suites peuvent pour certaines être reformulées en terme d'algèbre linéaire. Ainsi, l'espace S_0 des suites numériques $(u_n)_{n\geq 0}$ est un espace vectoriel : l'addition de deux suites et la multiplication d'une suite par un scalaire sont définies naturellement et vérifient les propriétés d'espace vectoriel. La partie $S_{c,0}$ des suites $\mathbf{u} \in S_0$ convergentes en est un sous-espace vectoriel et l'application L qui à une suite convergente $\mathbf{u}$ de $S_{c,0}$ associe sa limite $L(\mathbf{u}) = \lim(u_n)$ est une application linéaire.

où il est supposé f_n non nul pour au moins $n \geq n_0$.

Pour ℓ, C scalaires (réel ou complexe) identifiés aux suites constantes $\mathbf{C}, \ell$, avec les conventions

$$C\mathbf{u} := \mathbf{Cu} \quad \text{i. e.} \quad (C\mathbf{u})_n = Cu_n, \quad \mathbf{u} + \ell := \mathbf{u} + \ell \quad \text{i. e.} \quad (\mathbf{u} + \ell)_n = u_n + \ell, \qquad n \geq 0.$$

On a alors le début du tableau II.2

THÉORÈME 2.1: *Soient* $\mathbf{u}$, $\mathbf{v}$ *deux suites convergentes,* λ *scalaire. Alors les suites* $\mathbf{u}+\mathbf{v}$, $\lambda\mathbf{u}$, $\mathbf{uv}$ *et* $\mathbf{u}/\mathbf{v}$ *(a supposer que* $\lim \mathbf{v}$ *est non nulle) sont convergentes, avec pour limite*

$$\lim(\mathbf{u}+\mathbf{v}) = \lim \mathbf{u} + \lim \mathbf{v}, \qquad \lim(\lambda\mathbf{u}) = \lambda \lim \mathbf{u},$$
$$\lim(\mathbf{uv}) = \lim \mathbf{u} \cdot \lim \mathbf{v}, \qquad \lim(\mathbf{u}/\mathbf{v}) = \lim \mathbf{u} / \lim \mathbf{v}.$$

DÉMONSTRATION. La démonstration est préparée par la présentation suivante

$$u_n + v_n - (k+l) = (u_n - k) + (v_n - \ell)$$
$$u_n v_n - kl = (u_n - k)\, v_n + k(v_n - \ell)$$
$$\frac{1}{v_n} - \frac{1}{\ell} = \frac{\ell - v_n}{v_n \ell}$$

qui donne les estimations

$$|u_n + v_n - (k+\ell)| \leq |u_n - k| + |v_n - \ell|$$
$$|u_n v_n - k\ell| \leq |u_n - k| \cdot |v_n| + |k| \cdot |v_n - \ell|$$
$$\left| \frac{1}{v_n} - \frac{1}{\ell} \right| = \frac{|v_n - \ell|}{|v_n| \cdot |\ell|}$$

Ligne après ligne, il existe un réel $C > 0$ tel que les expressions à droite soient majorées par la somme de quantités petites du type $C\varepsilon$ quand l'indice est suffisamment grand (reprendre la définition de convergence et le fait que toute suite convergente est bornée, cf. l'alinéa 3 de la proposition 2.1). Si le cas de la somme est aisé, quelques précisions sont bienvenues pour les autres cas :

— pour le produit, la suite $\mathbf{v}$ est bornée (car convergente) : il existe $C > 0$ telle que $|v_n| \leq C$ et $|k| \leq C$, d'où la majoration supplémentaire par $C|u_n - k| + C|v_n - \ell|$)

— vue l'hypothèse ℓ non nul, il existe un entier N tel que si $n \geq N$ alors $|v_n - \ell| \leq |\ell|/2$ et donc $|v_n| \geq |\ell| - |v_n - \ell| \geq |\ell|/2$. En résulte la majoration

$$\left| \frac{1}{v_n} - \frac{1}{\ell} \right| = \frac{\ell - v_n|}{|v_n| \cdot |\ell|} \leq C|v_n - \ell|$$

avec $C = 2/|\ell|^2$.

Remarquons que ces calculs de limites de suites convergentes (vers un nombre) valent autant pour des suites réelles que complexes. □

Pour les combinaisons qui incluent des $\pm\infty$, les énoncés ne portent que sur des suites réelles : pour ces expressions basiques dont un terme tend vers $+\infty$, le traitement est analogue, à base d'inégalités justifiées par les hypothèses et l'intuition.

Montrons par exemple que si $u_n \to +\infty$ et $v_n \to \ell$ avec $\ell > 0$, alors le produit $(u_n v_n)$ tend vers $+\infty$. En effet, pour n assez grand, on a d'une part u_n positif et d'autre part v_n "proche" de ℓ (et loin du zéro 0), par ex. $|v_n - \ell| \leq \ell/2$, ce qui implique v_n positif minoré par $\ell/2$. On a alors $u_n v_n > \dfrac{\ell}{2} u_n$ pour tous ces n assez grands. On peut appliquer donc la propriété (6) de la proposition 2.1, pour conclure que $(u_n v_n)$ tend vers $+\infty$.

Cette « algèbre » des limites est efficace, avec comme restriction les formes indéterminées indiquées par un point d'interrogation dans le tableau II.2 il n'y a pas de règle générale pour leur analyse.

TABLE II.2 – Convergence de suites obtenues par des opérations algébriques où k, ℓ sont des limites de $\mathbf{u}$ et $\mathbf{v}$.

$\mathbf{u}$	$(\lvert u_n\rvert)$	$\mathbf{v}$	$\mathbf{u}+\mathbf{v}$	$\mathbf{uv}$	$\dfrac{1}{\mathbf{u}}$	$\mathbf{u}/\mathbf{v}$	(u_n^α) si $u_n > 0, \forall n$
k	$\lvert k\rvert$	ℓ	$k+\ell$	$k\ell$	k^{-1} si $k \neq 0$	$\dfrac{\ell}{k}$ si $k \neq 0$	k^α
$+\infty$	$+\infty$	$+\infty$	$+\infty$	$+\infty$	0	?	$+\infty$
$-\infty$	$+\infty$	$+\infty$	?	$-\infty$	0	?	–
$+\infty$	$+\infty$	$\ell > 0$	$+\infty$	$+\infty$	0	0	$+\infty$
$+\infty$	$+\infty$	0	$+\infty$	?	0	0	$+\infty$

PROPOSITION 2.2: *Le tableau II.2 indique si telle suite converge, ou tend vers, suivant les propriétés des suites constituant les combinaisons algébriques (basées sur les opérations $+, *, -, /$). Les première et troisième colonnes sont préremplies, induisant la complétion des autres.*

Les combinaisons suivantes

$$+\infty + (-\infty), \quad 0 \times \pm\infty, \quad \frac{0}{0}, \quad \frac{\pm\infty}{\pm\infty}$$

donnent lieu à indétermination, qui est signalée avec un point d'interrogation.

▷ EXEMPLES 2.6:

2.6.1 Étudiant la convergence de la suite $\mathbf{u} = \left(\dfrac{3n^2 - n - 1}{-n^2 - 3n + 4}\right)_{n \geq 0}$, on constate deux formes indéterminées : d'une part au numérateur avec les deux pre-

miers termes en position $+\infty-\infty$, d'autre part entre numérateur et dénominateur avec une forme du type $\frac{+\infty}{-\infty}$. Avant d'étudier la convergence, on modifie l'expression des termes de la suite en tenant compte des termes dominants[9] (par ex. en remplaçant $3n^2-n-1$ par $n^2\left(3-\frac{1}{n}-\frac{1}{n^2}\right)$) et en les isolant de manière convenable, faisant disparaître les formes indéterminées :

$$u_n=\frac{3n^2-n-1}{-n^2-3n+4}=\frac{n^2\left(3-\frac{1}{n}-\frac{1}{n^2}\right)}{n^2\left(-1-\frac{3}{n}+\frac{4}{n^2}\right)}=\frac{3-\frac{1}{n}-\frac{1}{n^2}}{-1-\frac{3}{n}n^2+\frac{4}{n^2}}\xrightarrow[n\to\infty]{}\frac{3-0-0}{-1-0+0}=-3$$

2.6.2 L'exemple suivant montre combien l'analyse des indéterminations donne des résultats variés : soit, pour $d\in\mathbb{Z}$ les suites

$$\mathbf{u}(d)=(n^d)_{n\geq 0},\qquad \mathbf{U}(\mathrm{A},d)=u(d)-\mathrm{A}(u(d)+u(d+1)),$$

où on a écrit de manière condensée

$$[\mathbf{U}(\mathrm{A},d)]_n=n^d-\mathrm{A}\left(n^d+n^{d+1}\right)=(1-\mathrm{A})n^d-\mathrm{A}n^{d+1},\quad n\geq 1.$$

Alors, on établit pour $\mathrm{A}>0$

$$\mathrm{U}(\mathrm{A},p)_n=\begin{cases}-n^{d+1}\to-\infty & \text{si } \mathrm{A}=1 \text{ et } d>-1,\\ -n^{d+1}\to 0 & \text{si } \mathrm{A}=1 \text{ et } d<-1,\\ -1\to-1 & \text{si } \mathrm{A}=1 \text{ et } d=-1,\\ n^{d+1}\left(-\mathrm{A}+(1-\mathrm{A})n^{-1}\right)\to-\infty & \text{si } \mathrm{A}\neq 1 \text{ et } d>-1,\\ n^{d+1}\left(-\mathrm{A}+(1-\mathrm{A})n^{-1}\right)\to 0 & \text{si } \mathrm{A}\neq 1 \text{ et } d<-1,\\ -\mathrm{A}+(1-\mathrm{A})n^{-1}\to-1 & \text{si } \mathrm{A}\neq 1 \text{ et } d=-1,\end{cases}$$

◁

2.3 Monotonie et convergence

Le résultat suivant est intimement lié à la propriété de l'ensemble des nombres réels suivant laquelle toute partie majorée non vide admet une borne supérieure (*i. e.* un plus petit majorant) :

9. cf. la première définition dans 2.5 ou l'avant-dernier alinéa de l'énumération de la proposition 2.1.

THÉORÈME 2.2: *Une suite réelle* **u** *monotone bornée est convergente.*
Sa limite ℓ *vaut*

$$\ell = \sup\{u_n | n \geq 0\} \qquad ou \qquad \ell = \inf\{u_n | n \geq 0\},$$

suivant que la suite **u** *est croissante ou décroissante.*
Si la suite réelle **u** *croissante (resp. décroissante) n'est pas majorée (resp. minorée), alors* **u** *tend vers* $+\infty$ *(resp.* $-\infty$*).*

▷ EXEMPLES 2.7:

2.7.1 Soit x réel. La suite de ses approximations décimales $\mathbf{d} = (10^{-n}\lfloor 10^n x\rfloor)_{n\geq 0}$ est croissante : d'après la caractérisation de la partie entière ($\lfloor y\rfloor$ est le plus grand entier inférieur ou égal à y), on a $\lfloor 10^n x\rfloor \leq 10^n x$, puis $10\lfloor 10^n x\rfloor \leq 10^{n+1}x$ et $10\lfloor 10^n x\rfloor \leq \lfloor 10^{n+1}x\rfloor$, soit finalement

$$d_n = 10^{-n}\lfloor 10^n x\rfloor \leq 10^{-n-1}\lfloor 10^{n+1}x\rfloor = d_{n+1}.$$

De plus, en multipliant l'inégalité

$$10^n x - 1 \leq \lfloor 10^n x\rfloor \leq 10^n x$$

par 10^{-n}, on obtient

$$x - 10^{-n} \leq d_n \leq x$$

ce qui établit le caractère borné de la suite **d** et sa convergence de limite ℓ : passant à la limite dans les inégalités précédentes suivant le théorème 2.4 ci-dessous, on a $x \leq \lim d_n \leq x$ et donc $x = \lim \mathbf{d}$.
La suite **d** est la suite des approximations décimales par défaut de x, alors que la suite $(d_n + 10^{-n})_{n\geq 0}$ celle des approximations décimales par excès.

2.7.2 La suite **e** de terme général $e_n = \sum_{k=0}^{n} \frac{1}{k!}$ est convergente, avec limite le nombre d'Euler e comme il est démontré par ailleurs. Cette suite est croissante parce que

$$e_{n+1} = e_n + \frac{1}{(n+1)!}.$$

Minorant par 2 chaque facteur autre que le premier dans $k!$, on obtient l'inégalité $k! \geq 2^{k-1}$, ce qui permet de majorer

$$e_n = \sum_{k=0}^{n} \frac{1}{k!} \leq 1 + \sum_{k=1}^{n} \frac{1}{2^{k-1}} = 1 + \frac{1-2^{-n}}{1-2^{-1}} \leq 1 + \frac{1}{1/2} = 3, \quad n \geq 1,$$

et de conclure à la convergence de la suite **e**.

2.7.3 La suite **E** de terme général $E_n = \sum_{k=1}^{n} k^{-2}$ est convergente[10] car croissante et majorée. En effet, pour $k \geq 2$, on a

$$\frac{1}{k^2} \leq \frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k},$$

10. En 1644, Pietro Mengoli (1626 ou 1627, Bologne – 7 juin 1686) posa la question de la valeur exacte de cette limite, cette question est connue comme le *problème de Bâle*. En 1735,âgé de 28 ans, L. Euler la donna comme étant $\pi^2/6$ au terme d'une démonstration qu'il rendit rigoureuse en 1742.

et donc, par annulations dites *télescopiques*,

$$E_n \le 1 + \left[\frac{1}{1} - \frac{1}{2}\right] + \cdots + \left[\frac{1}{k-1} - \frac{1}{k}\right] + \cdots + \left[\frac{1}{n-1} - \frac{1}{n}\right] = 1 + 1 - \frac{1}{n} \le 2, \quad n \ge 1.$$

2.7.4 Soit la suite dite harmonique $\mathbf{H} = \left(\sum_{k=1}^{n} \frac{1}{k}\right)_{n\ge1}$. Minorons chacun des 2^k termes consécutifs

$$\frac{1}{2^k+1}, \frac{1}{2^k+2}, \ldots, \frac{1}{2^k+2^k} = \frac{1}{2^{k+1}}$$

par $2^{-(k+1)}$: la somme de ces termes est minorée par $2^k \cdot 2^{-(k+1)} = 1/2$, minorant indépendant de k. En minorant les n différentes sommes de ces termes regroupés dans H_{2^n} en lien avec la partition de $[\![1, 2^n]\!]$ en $n+1$ paquets suivant

$$[\![1, 2^n]\!] = [\![1]\!] \cup [\![2]\!] \cup [\![2+1, 2^2]\!] \cup [\![2^2+1, 2^3]\!] \cup \ldots \\ \cup [\![2^k+1, 2^{k+1}]\!] \cup \cdots \cup [\![2^{n-1}+1, 2^n]\!],$$

on obtient $H_{2^n} \ge 1 + n/2$: ainsi donc la sous-suite $(H_{2^n})_{n\ge0}$ tend vers $+\infty$; vu que la suite $\mathbf{H}$ est monotone, cela implique que la suite (H_n) tend vers $+\infty$. En effet, vu la définition de la convergence de la suite (H_{2^n}) vers $+\infty$, étant donné $A > 0$, il existe N tel que $H_{2^n} \ge A$ pour $n \ge N$. Alors pour $k > 2^N$, vu la croissance de la suite $\mathbf{H}$, on a $H_k \ge H_{2^N} \ge A$, ce qui signifie la convergence vers $+\infty$ de la suite $\mathbf{H}$. ◁

DÉMONSTRATION. On peut se limiter au cas d'une suite $\mathbf{u}$ croissante : si la suite $\mathbf{u}$ est décroissante (majorée/minorée resp.), la suite $\mathbf{v} = -\mathbf{u}$ est croissante (resp. minorée/majorée). Si la suite $\mathbf{u}$ converge vers ℓ (tend vers $\pm\infty$ resp.), alors la suite $\mathbf{v}$ converge vers $-\ell$ (tend vers $\mp\infty$ resp.).

Supposons $\mathbf{u}$ croissante bornée. La partie $\{u_n, n \ge 0\}$ de $\mathbb{R}$ étant non vide bornée admet une borne supérieure (un plus petit majorant) ℓ. Soit $\varepsilon > 0$. Le réel $\ell - \varepsilon$ n'est pas un majorant de l'ensemble des valeurs de $\mathbf{u}$: il existe N tel que $u_N \ge \ell - \varepsilon$. On a alors, pour tout $n \ge N$,

$$\ell - \varepsilon \le u_N \le u_n \le \ell$$

où la deuxième inégalité provient de la croissante de la suite $\mathbf{u}$ et la dernière du fait que ℓ est un majorant des valeurs de $\mathbf{u}$. Ainsi, pour $n \ge N$ on a $|u_n - \ell| = \ell - u_n \le \varepsilon$: on vient donc de montrer que la suite $\mathbf{u}$ converge vers ℓ.

Si la suite $\mathbf{u}$ croissante n'est pas bornée, elle n'est pas majorée (elle est minorée par u_0) : pour tout $A \ge 0$, il existe un entier N tel que $u_N \ge A$ et donc $u_n \ge u_N \ge A$ pour $n \ge N$: ainsi la suite $\mathbf{u}$ tend vers $+\infty$. □

On a un corollaire, qui a été utilisé dans la discussion du tableau II.1 lorsqu'on a montré que (n^d) tend vers $+\infty$:

COROLLAIRE 2.2: *Si la suite réelle* $\mathbf{u}$ *est croissante et a une sous-suite* $\left(v_n = u_{\varphi(n)}\right)$ *tendant vers* $+\infty$, *alors la suite* $\mathbf{u}$ *tend vers* $+\infty$.

DÉMONSTRATION. La suite $\mathbf{u}$ n'est pas bornée, puisque sa sous-suite ne l'est pas. Ainsi la suite $\mathbf{u}$ tend donc vers $+\infty$ d'après le théorème 2.2. □

On a des théorèmes importants concernant des suites comparables.

THÉORÈME 2.3: *Soient* $\mathbf{u}$, $\mathbf{v}$ *deux suites réelles telles que* $u_n \leq v_n$ *pour tout* n *au moins égal à* N. *Si ces deux suites sont convergentes de limites respectives* k *et* ℓ, *alors* $k \leq \ell$.

Ce théorème est souvent utilisé dans la situation d'une suite $\mathbf{u}$ dominée par une autre suite $\mathbf{v}$ convergente vers 0 à un nombre réel C près (comme on l'a vu dans la proposition 2.1) : $\mathbf{v}$ est une suite convergente vers 0, C est une constante, $\mathbf{u}$ est une suite telle que $|u_n| \leq \mathrm{C}v_n$ pour tout n, alors $\mathbf{u}$ converge vers 0.

DÉMONSTRATION. Supposons par l'absurde que $d = k - \ell > 0$. Pour n assez grand, u_n est dans l'intervalle $\left[k - \frac{d}{3}, k + \frac{d}{3}\right]$ et v_n dans l'intervalle $\left[\ell - \frac{d}{3}, \ell + \frac{d}{3}\right]$. Ainsi

$$u_n \geq k - \frac{d}{3} \text{ et } v_n \leq \ell + \frac{d}{3} < 0$$

et donc

$$v_n - u_n \leq \ell + \frac{d}{3} - \left[k - \frac{d}{3}\right] = -\frac{d}{3},$$

ce qui est contradictoire avec l'hypothèse ($u_n \leq v_n$ pour tout n assez grands). On a donc $k \leq \ell$. □

△ REMARQUE 2.3: Il n'est pas vrai (en général) que les inégalités $u_n < v_n$, $n \geq \mathrm{N}$ implique l'inégalité stricte des limites. Par exemple, la suite $\mathbf{u}$ telle que $u_n = 1/n > 0$ pour $n \geq 1$, avec limite nulle pour les deux suites. ▽

Le théorème suivant est connu sous le *lemme des gendarmes* ou *lemme du sandwich.*

THÉORÈME 2.4: *Soient* $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ *trois suites réelles telles que* $u_n \leq v_n \leq w_n$ *pour* n *au moins égal à un certain* n_0.
Si les deux suites $\mathbf{u}$, $\mathbf{w}$ *convergent vers la même limite* ℓ, *alors la suite* $\mathbf{v}$ *converge vers le nombre* ℓ.
Si une des trois suites tend vers $+\infty$ *et la suite* $\mathbf{w} - \mathbf{u}$ *est bornée, alors les deux autres convergent vers* $+\infty$.

▷ EXEMPLES 2.8:

2.8.1 la suite $\left(\sin(n^{-k})/n\right)_{n\geq 1}$ converge vers 0. En effet, les inégalités

$$-1 \leq \sin\left(n^{-k}\right) \leq 1 \text{ et donc } -\frac{1}{n} \leq \frac{\sin\left(n^{-k}\right)}{n} \leq \frac{1}{n}$$

permettent d'appliquer le lemme du sandwich. En fait, la simple majoration $\left|\sin\left(n^{-k}\right)\right|/n \leq n^{-1}$ suffit à établir la convergence vers 0 : en général, il n'y a pas une unique voie pour établir la convergence (ou son absence) d'une suite.

2.8.2 Soit $\mathbf{u}$ bornée et $\mathbf{v}$ convergente vers 0. Alors, si M désigne une borne de $|\mathbf{u}|$, on a $0 \leq |u_n v_n| \leq \mathrm{M}|v_n|$ avec la suite $\mathrm{M}\mathbf{v}$ tendant vers 0 et donc $\mathbf{uv}$ converge vers 0. ◁

Le théorème suivant énonce la convergence de suites dites *adjacentes*, que nous définissons.

DÉFINITION 2.4: *Les deux suites réelles* $\mathbf{u},\mathbf{v}$ *sont dites* adjacentes *si la suite* $\mathbf{u}$ *est croissante, la suite* $\mathbf{v}$ *décroissante et la suite* $\mathbf{u}-\mathbf{v}$ *convergente vers* 0.

THÉORÈME 2.5: *Deux suites adjacentes* $\mathbf{u}$, $\mathbf{v}$ *sont toutes deux convergentes, de même limite.*

▷ EXEMPLES 2.9:

2.9.1 Les deux suites $\left(u_n = \mathrm{E}_n = \sum_{k=1}^{n} k^{-2}\right)_{n\geq 1}$ et $\left(v_n = u_n + \frac{1}{n}\right)_{n\geq 1}$ sont adjacentes.

On a en effet

$$v_{n+1} - v_n = \frac{1}{(n+1)^2} + \frac{1}{n+1} - \frac{1}{n} = -\frac{1}{n(n+1)^2} \leq 0,$$

soit la décroissance de la suite $\mathbf{v}$. La croissance de $\mathbf{u}$ et la convergence de $(v_n - u_n)_{n\geq 1}$ sont claires.

2.9.2 La suite $\left(u_n = \sum_{k=1}^{n} \frac{1}{k!}\right)_{n\geq 1}$ est croissante alors que la suite de terme général $v_n = u_n + \frac{1}{nn!}$ est décroissante vu que

$$v_{n+1} - v_n = \frac{1}{(n+1)(n+1)!} + \frac{1}{(n+1)!} - \frac{1}{nn!} = -\frac{1}{n(n+1)(n+1)!} < 0.$$

Leur différence $\mathbf{u}-\mathbf{v}$ converge vers 0 : ces deux suites sont ainsi adjacentes, elle convergent vers la base e du logarithme népérien (primitive s'annulant en $t=1$ de la fonction $t \in \mathbb{R}^+ \to t^{-1}$).

Montrons par l'absurde que cette limite $\ell = \mathrm{e}$ est irrationnelle [11] : supposons que $\ell = \frac{p}{q}$ pour deux entiers p et q. Vu l'hypothèse, le nombre

$$q!(\ell - u_q) = \frac{p}{q}q! - \left[q! + \frac{q!}{1!} + \frac{q!}{2!} + \frac{q!}{3!} + \cdots + \frac{q!}{q!}\right]$$

11. L'étude de e comme limite de deux suites adjacentes est reprise dans la section 2.5.4 ci-dessous.

est un entier naturel s non nul et

$$q!(u_{q+n}-u_q) = q!\left[\frac{1}{(q+1)!}+\frac{1}{(q+2)!}+\frac{1}{(q+3)!}+\cdots+\frac{1}{(q+n)!}\right]$$
$$= \frac{1}{q+1}+\frac{1}{(q+1)(q+2)}+\cdots+\frac{1}{(q+1)(q+2)\ldots(q+n)}$$

En utilisant la minoration

$$(q+1)(q+2)\ldots(q+n) > (q+1)^n, \quad n \geq 0,$$

on obtient, pour $n \geq 0$, la majoration

$$q!(u_{q+n}-u_q) < \frac{1}{q+1}+\frac{1}{(q+1)^2}+\frac{1}{(q+1)^3}+\ldots\frac{1}{(q+1)^n}$$
$$= \frac{1}{q+1}\frac{1-(q+1)^{-n}}{1-(q+1)^{-1}} = \frac{1-(1+q)^{-n}}{q} < \frac{1}{q}$$

et donc en passant à la limite lorsque $n \to \infty$

$$0 < s = q!(\ell-u_q) = \lim_{n\to\infty} q!(u_{q+n}-u_q) \leq \frac{1}{q} < 1,$$

ce qui contredit le fait que s soit entier non nul. Ainsi le nombre d'Euler e est irrationnel : il doit cette propriété au fait qu'il est bien approché par les rationnels !

◁

Démonstration du théorème 2.4 dit du sandwich . Considérons la première assertion où les deux suites **u** et **w** convergent vers ℓ. Les inégalités $u_n \leq v_n \leq w_n$ pour tout n permettent les majorations (passage de la première à la seconde ligne)

$$|v_n-\ell| \leq |v_n-w_n|+|w_n-\ell| = w_n-v_n+|w_n-\ell|$$
$$\leq w_n-u_n+|w_n-\ell| = w_n-\ell-(u_n-\ell)+|w_n-\ell|$$
$$\leq 2|w_n-\ell|+|u_n-\ell|.$$

Les deux termes du dernier membre convergent vers 0, il en est donc de même pour le premier membre (dominé par le dernier membre), ce qui signifie la convergence de la suite **v** vers ℓ.

Une suite parmi $\mathbf{u},\mathbf{v},\mathbf{w}$ étant choisie, alors les deux autres s'en déduisent par ajout d'une suite bornée : par exemple, les suites **v** et **w** se déduisent de **u** suivant $v_n = u_n+(v_n-u_n)$ et $w_n = u_n+(w_n-u_n)$ avec les suites (v_n-u_n) et (w_n-u_n) bornées vu que la suite (w_n-u_n) est supposée bornée. Ainsi, si l'une des trois suites tend vers $+\infty$, alors les deux autres tendent vers $+\infty$. □

Démonstration du théorème 2.5 des suites adjacentes. On a $u_n \leq v_n$ pour tout n. Sinon, on aurait pour un entier m l'inégalité $u_m > v_m$ et par suite

$$u_{m+p} \geq u_m > v_m \geq v_{m+p}, \quad p \geq 0,$$

et la suite $\left(u_{m+p}-v_{m+p}\right)_{p\geq 0}$, aux termes minorés par $u_m-v_m > 0$, ne pourrait pas converger vers 0. On a donc $u_{n+p} \leq v_{n+p}$ pour tous m et p et par suite

$$u_n \leq u_{n+p} \leq v_{n+p} \leq v_n, \quad n,p \in \mathbb{N},$$

ce qui permet d'affirmer que la suite **u** est croissante majorée et que la suite **v** est décroissante minorée : ces deux suites sont donc convergentes de limites respectives k et ℓ. La convergence vers 0 de la suite $(u_n - v_n)$ donne $k - \ell = 0$, soit $k = \ell$, ce qui achève cette démonstration. □

Il est utile de comparer des suites : différents cas sont rassemblés dans la définition suivante

DÉFINITION 2.5: *Soient* **u** *et* **v** *deux suites réelles, avec tous les termes* v_n *non nuls.*

1. *La suite* **u** *est dite* dominée *par* **v** *si la suite* (u_n/v_n) *est bornée,* i. e. *il existe une constante* C *telle que* $|u_n| \leq C v_n$. *On écrira* $u_n = \mathcal{O}(v_n)$;
2. *La suite* **u** *est négligeable devant la suite* **v** *si la suite* (u_n/v_n) *tend vers* 0 ; *on écrira* $u_n = o(v_n)$;
3. *La suite* **u** *est équivalente à la suite* **v** *si la suite* (u_n/v_n) *tend vers* 1. *On écrira* $u_n \sim v_n$.

△ REMARQUE 2.4: Ces trois différents cas peuvent s'exprimer suivant les propositions

$$\begin{aligned}
&\exists C \in \mathbf{R} \quad \forall n \in \mathbf{N} \quad |u_n| \leq C|v_n| \\
&\forall \varepsilon > 0 \quad \exists N_\varepsilon \quad \forall n \geq N_\varepsilon \quad |u_n| \leqslant \varepsilon |v_n| \\
&\forall \varepsilon > 0 \quad \exists N_\varepsilon \quad \forall n \geq N_\varepsilon \quad |u_n - v_n| \leq \varepsilon |v_n|,
\end{aligned}$$

la dernière étant équivalente à $\forall \varepsilon > 0 \quad \exists n_0 \quad \forall n \geq n_0 \quad |u_n - v_n| \leq \varepsilon |u_n|$ puisque l'une énonce que $\lim u_n/v_n = 1$ et l'autre $\lim v_n/u_n = 1$. ▽

▷ EXEMPLES 2.10:

2.10.1 $\sqrt{1+\pi n^2} = \mathcal{O}(n)$, $\sqrt{1+6n^2} = o(n^2)$, $\sqrt{1+3n^2} \sim \sqrt{3}n$;

2.10.2 Soit a, r des réels strictement positif.

Alors $(1+r)^n = o(n!)$, $n^a = o((1+r)^n)$, $\ln(n) = o(n^a)$. ◁

2.4 Suites et fonctions

Les liens des suites avec la théorie des fonctions sont importants. Par exemple, une fonction $f :]a,b[\to \mathbb{R}$ est continue en $m \in]a,b[$ si et seulement si pour toute suite **u** à valeurs dans $]a,b[$ et convergente vers $m \in]a,b[$, alors la suite $f(\mathbf{u})$, définie suivant $f(\mathbf{u})_n = f(u_n)$ pour $n \geq n_0$, est convergente de limite $f(m)$.

La proposition suivante nous sera utile, elle résulte simplement du critère de continuité d'une fonction qui vient d'être rappelé.

PROPOSITION 2.3: *Soit* $f :]a,b[\to]a,b[$ *et* $\mathbf{u}$ *une suite à valeurs dans* $]a,b[$. *Supposons* f *continue,* $\mathbf{u}$ *convergente de limite* $\ell \in]a,b[$. *Alors* $\ell = f(\ell)$.

2.5 Exemples de suites

Dans cette section, on examine des suites définies par des relations de récurrence $u_{n+1} = f(u_n), n \geq 0$ qui apparaissent comme des généralisations des suites arithmético-géométriques, que ce soit des récurrences linéaires d'ordre $d \geq 2$ ou des homographies. Leurs propriétés de convergence (ou plus généralement leur comportement quand l'indice n tend vers l'infini) apparaissent naturellement, une fois le cadre (linéaire ou homographique) bien établi.

2.5.1 Suites arithmético-géométriques

Cette sous-section est consacrée aux suites linéaires récurrentes d'ordre 1, notamment en rapport avec les suites arithmético-géométriques. Avant de commencer, on donne quelques indications sur ces suites linéaires récurrentes (à coefficients constants) d'ordre $d \in \mathbb{N}^*$. Les suites linéaires récurrentes d'ordre 2 seront étudiées dans la sous-section suivante.

DÉFINITION 2.6: *Une suite* $\mathbf{u}$ *est dite* linéaire récurrente à coefficients constants d'ordre $d \in \mathbb{N}^*$ *si elle satisfait aux relations*

$$u_{n+d} = a_1 u_{n+d-1} + \cdots + a_{d-1} u_{n+1} + a_d u_n + k_n, \quad n \geq 0 \tag{2.2}$$

où $a_1, \ldots, a_d$ *sont des nombres avec* $a_d \neq 0$ *et* $\mathbf{k}$ *est une suite numérique.*
Le problème homogène associé à (2.2) porte sur les suites $\mathbf{v}$ *vérifiant les relations*

$$v_{n+d} = a_1 v_{n+d-1} + \cdots + a_{d-1} v_{n+1} + a_d v_n, \quad n \geq 0. \tag{2.3}$$

Le polynôme

$$\mathrm{P}_c(\mathrm{X}) = \mathrm{X}^d - a_1 \mathrm{X}^{d-1} - \cdots - a_{d-1}\mathrm{X} - a_d. \tag{2.4}$$

est appelé polynôme caractéristique *de la récurrence linéaire (2.2).*

△ REMARQUE 2.5: Le terme k_n est appelé parfois *second membre*. Cela provient de l'écriture de (2.2) suivant

$$u_{n+d} - a_1 u_{n+d-1} - \cdots - a_{d-1} u_{n+1} - a_d u_n = k_n, \quad n \geq 0$$

▽

À l'ordre $d = 1$, nous avons les récurrences, homogènes et non homogènes,

$$u_{n+1} = a_1 u_n, \qquad u_{n+1} = a_1 u_n + k_n.$$

Soit r non nul. La suite géométrique (r^n) vérifie (2.3) si et seulement si

$$r^{n+d} = a_1 r^{n+d-1} + \cdots + a_d r^n, \quad n \geq 0$$

soit si et seulement si

$$r^d = a_1 r^{d-1} + \cdots + a_{d-1} r + a_d$$

i. e. si et seulement si r est une racine du polynôme caractéristique $\mathrm{P}_c(\mathrm{X})$ introduit dans (2.4). Vu que le coefficient a_d est non nul, le polynôme caractéristique P_c n'a pas de racine nulle : les solutions exponentielles $(r^n)_{n\geq 0}$ sont supposées toujours non nulles.

On admettra le lemme suivant.

LEMME 2.3: *Soit* $\mathbf{u}$ *une suite vérifiant la récurrence linéaire homogène à coefficients constants*

$$u_{n+d} = a_1 u_{n+d-1} + \cdots + a_{d-1} u_{n-1} + a_d u_n, \quad n \geq 0.$$

avec polynôme caractéristique

$$\mathrm{P}_c(\mathrm{X}) = \mathrm{X}^d - a_1 \mathrm{X}^{d-1} - \cdots - a_{d-1}\mathrm{X} - a_d$$

Supposons que ce polynôme admet d *zéros* $\lambda_1, \lambda_2, \ldots$ *comptés avec multiplicités* m_j *: le polynôme* P_c *admet une factorisation en facteurs linéaires*

$$\mathrm{P}_c(\mathrm{X}) = \prod_{j=1}^{e} (\mathrm{X} - \lambda_j)^{m_j},$$

où $d = \sum_{j=1}^{e} m_j$ *. Alors le terme général de la suite* $\mathbf{u}$ *s'écrit de manière unique suivant*

$$u_n = \sum_{j=1}^{e} \sum_{i_j=0}^{m_j-1} \alpha_{j i_j} n^{i_j} \lambda_j^n, \quad n \geq 0, \tag{2.5}$$

où les $\alpha_{j i_j}, i_j = 1, \ldots, m_j, j = 1, \ldots, e$ *sont des nombres uniquement déterminés.*

DÉMONSTRATION. Soit S l'application qui associe à la suite $\mathbf{u}$ la suite $(u_{n+1})_{n\geq 0}$. D'une part, si P est un polynôme de degré au plus d, alors

$$(\mathrm{S} - \lambda)\big((\mathrm{P}(n)\lambda^n)_{n\geq 0}\big) = \big(\widetilde{\mathrm{P}}(n)\lambda^n\big)_{n\geq 0},$$

avec le polynôme $\widetilde{\mathrm{P}}$ de degré au plus $d-1$, vu que $\widetilde{\mathrm{P}}(n) = \lambda\big(\mathrm{P}(n+1) - \mathrm{P}(n)\big)$. Ainsi $(\mathrm{S} - \lambda)^d\big((\mathrm{P}(n)\lambda^n)\big)$ est de degré au plus $\deg \mathrm{P} - d$, et donc nul si $\deg \mathrm{P} < d$.

Par ailleurs, la propriété (2.3) de récurrence linéaire homogène à coefficients constants pour la suite $\mathbf{u}$ est exprimée exactement par la nullité $\mathrm{P}_c(\mathrm{S})(\mathbf{u}) = 0$. Ainsi, si $(\mathrm{X} - \lambda)^d$ est un facteur du polynôme caractéristique P_c, les suites $(n^p\lambda^n)_{n\geq 0})$ avec $p < d$ sont annulées par $\mathrm{P}_c(\mathrm{S}) = \mathrm{Q}(\mathrm{S})(\mathrm{S} - \lambda)^d$ et donc vérifie la propriété (2.3). Avec des arguments d'algèbre linéaire [12] on montre que la solution générale de (2.3) est combinaison linéaire de ces solutions particulières $(n^p\lambda^n)$. □

12. L'étude des suites vérifiant des relations de récurrence linéaire est en fait celle de l'application S introduite ci-dessus, en tant qu'*opérateur linéaire* sur l'espace des suites exponentielle-polynôme. Les premières propriétés (relativement générales) peuvent être étudiées de manière élémentaire.

La différence entre (2.2) et (2.3) est la nullité des termes de second membre k_n. Si $\mathbf{u}$ et $\mathbf{w}$ sont deux solutions de (2.2), alors leur différence $\mathbf{u}-\mathbf{w}$ est une solution de (2.3) et inversement si $\mathbf{u}$ et $\mathbf{v}$ sont solutions de (2.2) et de (2.3) resp., alors la somme $\mathbf{u}+\mathbf{v}$ est solution de (2.2). En outre, si $\widehat{\mathbf{u}}$ ($\widetilde{\mathbf{u}}$ resp.) est solution de (2.2) avec comme second membre $\widehat{\mathbf{k}}$ ($\widetilde{\mathbf{k}}$ resp.) alors $\alpha\widetilde{\mathbf{u}}+\beta\widehat{\mathbf{u}}$ est solution de (2.2) avec second membre $\alpha\widetilde{\mathbf{k}}+\beta\widehat{\mathbf{k}}$. Ainsi suffit-il de traiter les récurrences linéaires (2.2) avec second membre du type $(\rho^n n^d)_{n\geq 0}$, celles avec comme second membre du type $(\rho^n \mathrm{P}(n))_{n\geq 0}$ s'en déduisant par sommation des solutions pour des exponentielle-monôme comme second membre.

En général, le lemme précédent décrit précisément les solutions (2.5) des récurrences homogènes à coefficients constants, alors que le problème non homogène est plus difficile : il ne sera résolu ici que pour des suites $\mathbf{k}$ de type exponentielle-polynôme $\left(r^n \mathrm{P}(n)\right)_{n\geq 0}$ où r dans $\mathbb{R}$ ou $\mathbb{C}$ et P est un polynôme.

Pour la description des solutions de (2.2), on se limitera donc à trouver une solution de (2.2) à laquelle on ajoutera une solution quelconque de l'équation homogène (2.3) : on aura ainsi toutes les solutions de (2.2), dépendant des d paramètres α_{ji_j} de (2.5) qui seront ajustés avec les valeurs initiales $u_0,\dots,u_{d-1}$ de la suite $\mathbf{u}$.

Le lemme précédent souligne le rôle crucial des suites exponentielle-polynôme $(\rho^n n^d)_{n\geq 0}$ (où $d\in\mathbb{N}^*$ et $\rho\in\mathbb{C}$) dans la description des suites vérifiant les relations de récurrence homogènes (2.3). Par ailleurs, pour la relation de récurrence linéaire (2.2) avec second membre (k_n), il existe une suite exponentielle-polynôme qui la vérifie. Dans la suite, nous allons examiner ces deux aspects dans le cas $d=1$ (première généralisation des suites arithmético-géométrique, avec suite $\mathbf{k}$ au-delà d'une simple constante) et $d=2$ (autre généralisation avec des solutions exponentielle-polynôme dès l'équation homogène (2.5)).

Reprenons la discussion des suites récurrentes d'ordre $d=1$. Une suite arithmétique (géométrique resp.) est caractérisée par une relation de récurrence :

[A] Suite arithmétique $\mathbf{a}$: $a_{n+1}=a_n+a,\quad n\geq 0,$

[G] Suite géométrique $\mathbf{g}$: $g_{n+1}=qg_n,\quad n\geq 0,\quad q\neq 0.$

Ceci vaut si a,q,a_0,g_0 sont réels ou complexes. Le cas $q=0$ (correspondant à la condition $a_1\neq 0$) est écarté. Si $q=1$, on retrouve une suite arithmétique de raison a nulle : la suite est constante.

L'étude asymptotique est simple :

[A] Une récurrence établit la formule

$$a_n=na+a_0,\quad n\geq 0.$$

Si $a=0$, la suite (a_n) est constante ; sinon elle tend vers $\mathrm{sign}(a)\infty$ si a est réel, vers l'infini asymptotiquement dans la direction de a si a est complexe non réel

[G] Une récurrence établit la formule

$$g_n=q^n g_0,\quad n\geq 0.$$

— Si $q = 1$, la suite **g** est constante (comme une suite arithmétique de raison $a = 0$).
— Si $q = -1$, la suite **g** est 2-périodique.
— Si $|q| < 1$, la suite **g** converge vers 0 (en étant stationnaire si et seulement si $g_0 = 0$).
— Si $q > 1$ et $g_0 \neq 0$, la suite **g** tend vers $+\infty$ ou $-\infty$ suivant le signe de g_0
— Le comportement asymptotique de la suite $(q^n)_{n\geq 0}$ dans le plan complexe avec le rapport $q \in \{w \in \mathbb{C}; |w| = 1\} \setminus \mathbb{R}$ est plus riche. On considère la forme exponentielle du rapport $q = e^{2i\pi\theta}$. Si θ est rationnel, *i. e.* $\theta = \alpha/\beta$ avec α, β entiers, la suite de terme général

$$\left(e^{2i\pi\theta}\right)^n = e^{2i\pi n\alpha/\beta}, \quad n \geq 0$$

est β-périodique. Si θ est irrationnel, la suite $(e^{2i\pi\theta n})$ ne converge pas et n'est pas périodique.

DÉFINITION 2.7: *La suite* **u** *est dite* arithmético-géométrique *si elle vérifie la relation de récurrence*

$$u_{n+1} = qu_n + a, \quad n \geq 0, \tag{2.6}$$

où q est supposé non nul.

C'est donc un cas particulier d'une suite vérifiant une relation (2.2) de récurrence linéaire à coefficients constants d'ordre 1 avec la suite **k** constante. Son étude se ramène à l'étude de suites arithmétique ou géométrique. Remarquons que si la suite **u** vérifiant (2.6) converge vers ℓ, alors

$$\ell = q\ell + a,$$

d'où le rôle particulier de $\ell = a/(1-q)$ lorsque $q \neq 1$ et l'identité issue de (2.6) par soustraction de (2.5.1)

$$u_{n+1} - \ell = q(u_n - \ell), \quad n \geq 0.$$

LEMME 2.4: *Soit* **u** *la suite définie par la relation de récurrence*

$$u_{n+1} = qu_n + a, \quad n \geq 0$$

et son terme initial u_0.

1. *Si $q = 1$, la suite* **u** *est une suite arithmétique de raison a et terme initial u_0 : $u_n = na + u_0$ pour $n \geq 0$.*
2. *Si $q \neq 1$, soit $\ell = a/(1-q)$. La suite $\mathbf{v} = \mathbf{u} - \ell$ est une suite géométrique de rapport q et de terme initial $v_0 = u_0 - \ell$ de telle manière que $v_n = q^n v_0$, donc, vu que $\mathbf{u} = \mathbf{v} + \ell$*

$$u_n = q^n(u_0 - \ell) + \ell, \quad n \geq 0$$

Si $|q| < 1$, alors la suite **u** *converge vers ℓ.*
Si q est réel avec $|q| > 1$, la suite **u** *tend vers $+\infty$ ou ∞ suivant le signe de $u_0 - \ell$, avec* **u** *stationnaire si $u_0 = \ell$.*

Soit S_n *la somme des* $n+1$ *premiers termes de la suite* $\mathbf{u}$. *Alors*

$$S_n = u_0 + \cdots + u_n = \begin{cases} \dfrac{n(n+1)}{2}a + (n+1)u_0 & \text{si } q = 1, \\ \dfrac{1-q^{n+1}}{1-q}(u_0 - \ell) + (n+1)\ell & \text{sinon.} \end{cases}$$

DÉMONSTRATION. Les affirmations pour $q = 1$ sont immédiates. Sinon, soit ℓ solution de l'équation linéaire $\ell = q\ell + a$, soit $\ell = a/(1-q)$. Alors, la suite $\mathbf{v}$ de terme général $v_n = u_n - \ell$ pour $n \geq 0$ vérifie

$$v_{n+1} = u_{n+1} - \ell = qu_n + a - \ell = qu_n - q\ell = q(u_n - \ell) = qv_n$$

et est donc une suite géométrique de rapport q et de terme initial $v_0 = u_0 - \ell$. Ainsi

$$u_n - \ell = v_n = q^n v_0 = q^n(u_0 - \ell), \quad n \geq 0$$

et

$$u_n = q^n(u_0 - \ell) + \ell, \quad n \geq 0$$

et par conséquent

$$S_n = \sum_{k=0}^{n} \left[q^k(u_0 - \ell) + \ell \right] = (u_0 - \ell)\frac{1-q^{n+1}}{1-q} + (n+1)\ell, \quad n \geq 0.$$

Pour une suite arithmétique, la somme

$$S_n = \sum_{k=0}^{n} [ka + u_0] = a\frac{n(n+1)}{2} + (n+1)u_0, \quad n \geq 0.$$

est calculée grâce à la formule $1 + \cdots + n = n(n+1)/2$. □

Pour les relations de récurrence linéaire d'ordre 1, l'équation homogène (2.3) est $u_{n+1} = qu_n$ avec polynôme caractéristique $P_C(X) = X - q$. Sa solution $\mathbf{u}$ est la suite géométrique

$$u_n = q^n u_0, \quad n \geq 0.$$

Les relations (2.2) sont du type $u_{n+1} = qu_n + r^n P(n)$ et une solution particulière de (2.3) est donnée par la proposition (cf. la proposition 2.6 ci-dessous en ordre $d \geq 2$)

PROPOSITION 2.4: *Soit la récurrence linéaire d'ordre 1*

$$u_{n+1} = qu_n + \rho^n P(n), \quad n \geq 0. \tag{2.7}$$

où P *est un polynôme de degré* d_P, ρ *et* q *des nombres.*

- *Si* $q \neq \rho$, *il existe une unique solution* $\mathbf{u}$ *de (2.7) de la forme* $\mathbf{u} = \left(\rho^n Q(n)\right)_{n\geq 0}$ *avec* Q *polynôme de degré au plus* d_P.
- *Si* $q = \rho$, *il existe une unique solution* $\mathbf{u}$ *de (2.7) de la forme* $\mathbf{u} = \left(\rho^n nQ(n)\right)_{n\geq 0}$ *avec* Q *polynôme de degré au plus* s_P.

DÉMONSTRATION. Le premier cas revient à montrer l'existence d'un polynôme Q tel que

$$\rho^{n+1}Q(n+1) = q\rho^n Q(n) + \rho^n P(n), \quad n \geq 0$$

équivalent à

$$\rho Q(n+1) = qQ(n) + P(n), \quad n \geq 0$$

soit l'équation portant sur la variable qu'est le polynôme Q et où les nombres ρ, q et le polynôme P de degré d_P sont donnés. Utilisant le fait qu'un polynôme est nul si et seulement si il a une infinité de zéros (ici tous les entiers naturels $\mathbb{N}$), on obtient l'équation

$$\rho Q(X+1) - qQ(X) = P(X) \tag{2.8}$$

qu'on considérera comme une équation dans l'espace $\mathbb{R}_{d_P}[X]$ des polynômes de degré au plus d_P. On montre [13] via des outils d'algèbre linéaire qu'un tel Q existe de manière unique dans l'espace $\mathbb{R}_{d_P}[X]$.

Le deuxième cas où $q = \rho$ amène à l'équation

$$\rho^{n+1}Q(n+1) = \rho^{n+1}Q(n) + \rho^n P(n), \quad n \geq 0 \tag{2.9}$$

et de manière similaire au cas précédent à l'équation

$$\rho\big[Q(X+1) - Q(X)\big] = P(X), \tag{2.10}$$

pour laquelle l'algèbre linéaire [14] affirme une unique solution XQ(X) avec Q polynôme dans $\mathbb{R}_{d_P}[X]$. □

La suite (2.7) à récurrence linéaire d'ordre 1 avec second membre $\mathbf{k} = (P(n))$ correspond exactement à une suite arithmético-géométrique (2.6) avec un polynôme P de degré 0 (*i. e.* P est constant) $\rho = 1$. Si $q \neq \rho = 1$, on a une solution particulière constante $\big(\rho^n P(n)\big)$, égale à $Q = P/(1-q)$: c'est le $\ell = a/(1-q)$ du lemme 2.4.

▷ EXEMPLE 2.11: On considère la somme $u_n = \sum_{k=0}^{n}\big[3k^2 + 2k + 1\big]$ comme vérifiant la relation récurrente linéaire avec second membre

$$u_{n+1} = u_n + 3(n+1)^2 + 2(n+1) + 1 = u_n + 3n^2 + 8n + 6, \quad n \geq 0, \tag{2.11}$$

avec $u_0 = 1$. La suite $\mathbf{u}$ vérifie $u_{n+1} = u_n + P(n)$ avec $P(X) = 3X^2 + 8X + 6$ polynôme de degré 2.

13. Soit $\mathbb{R}_{d_P}[X]$ l'espace des polynômes de degré au plus d. Cette équation (2.8) est résoluble pour tout P si et seulement si l'application $Q(X) \in \mathbb{R}_{d_P}[X] \mapsto rQ(X+1) - qQ(X) \in \mathbb{R}_{d_P}[X]$ est surjective ou si et seulement si elle est injective ou encore si et seulement si l'équation $rQ(X+1) - qQ(X) = 0$ n'a comme solution que la solution nulle, ce qui est le cas : il suffit de regarder le terme de degré maximal du polynôme $rQ(X+1) - qQ(X)$ en fonction de celui de Q.

14. L'application $Q(X) \in X\mathbb{R}_d[X] \mapsto Q(X+1) - Q(X) \in \mathbb{R}_{d_P}[X]$ est une application linéaire bien définie entre les espaces de même dimension $d+1$), application qui est injective : l'équation (2.10) a donc une et seule solution de la forme $Q(X) = XR(X)$ avec R de degré au plus d.

Vu que 1 est racine caractéristique de la récurrence linéaire $u_{n+1} = u_n$ et que le second membre est de la forme $1^n P(n)$ (soit $\rho = 1$ dans l'énoncé de la proposition 2.4), on cherche une solution particulière avec comme terme général $nQ(n)$ où Q est un polynôme de degré 2. Le terme général de la solution de (2.11) sera donc de la forme $nQ(n) + \lambda(1^n)$ pour $\lambda \in \mathbb{R}$, somme d'une solution particulière $nQ(n)$ de l'équation avec second membre $(P(n))$ et d'une solution quelconque $\lambda(1^n)$ de l'équation homogène $u_{n+1} = u_n$ (dont toute solution est une suite constante). Le polynôme Q de degré 2 est déterminé par 3 coefficients a, b, c tels que $Q(X) = aX^2 + bX + c$, déterminés par les valeurs initiales de la suite $\mathbf{u}$:

$$u_0 = 1, \quad u_1 = u_0 + P(0) = 7, \quad u_2 = u_1 + P(1) = 24, \quad u_3 = u_2 + P(2) = 58,$$

soit le système à résoudre

$$\begin{aligned} 1 &= 0 * Q(0) + \lambda = \lambda, \\ 7 &= 1 * Q(1) + \lambda = a + b + c + \lambda, \\ 24 &= 2 * Q(2) + \lambda = 2(4a + 2b + c) + \lambda, \\ 58 &= 3 * Q(3) + \lambda = 3(9a + 3b + c) + \lambda \end{aligned}$$

avec solution $a = 1$, $b = c = 5/2$ et $\lambda = 1$ soit

$$u_n = \lambda + nQ(n) = n^3 + \frac{5}{2}n^2 + \frac{5}{2}n + 1, \quad n \geq 0.$$

On vérifie bien cette formule avec les formules (plus ou moins connues) $1 + \cdots + n = n(n+1)/2$ et $1^2 + \cdots + n^2 = n(n+1)(2n+1)/6$. ◁

Terminons cette section par la notion de *série* (ou *fonction*) *génératrice* associée à une suite, qui est sujet ici à calcul explicite pour des suites arithmético-géométriques. La notion générale de fonction génératrice et les calculs associés sont développés dans la section 2.5.6 ci-dessous. On peut calculer aisément les fonctions génératrices des suites arithmétique et géométrique. Cela repose sur l'inversibilité du polynôme $1 - X$ dans l'espace des séries formelles, dont l'inverse noté $(1-X)^{-1}$ est donné par

$$(1-X)^{-1} = \frac{1}{1-X} = 1 + X + X^2 + \ldots + X^n + \ldots = \sum_{n=0}^{\infty} X^n,$$

série formelle qui vérifie l'identité formelle $(1-X)(1+X+X^2+X^3+\ldots) = 1$ et qu'on usera à sa guise.

LEMME 2.5: *Pour la suite arithmétique* $\mathbf{a} = (na + u_0)_{n\geq 0}$ *de raison* a *et la suite géométrique* $\mathbf{g} = (u_0 q^n)_{n\geq 0}$ *de rapport* q*, toutes deux étant de premier terme* u_0*, on a*

$$S_{\mathbf{a}}(X) = u_0(1-X)^{-1} + aX(1-X)^{-2}, \quad S_{\mathbf{g}}(X) = g_0(1-qX)^{-1}.$$

DÉMONSTRATION. On effectue les calculs de manière formelle. Pour la suite arithmétique, on dérive formellement l'identité $\sum_{n=0}^{\infty} X^n = (1-X)^{-1}$ obtenant ainsi [15]

$$\sum_{n=0}^{\infty} nX^{n-1} = (1-X)^{-2}$$

15. On vérifie $(1-X)^2(1+2X+3X^2+\ldots) = (1-2X+X^2)\sum_{n=0}^{\infty} nX^{n-1} = 1$.

d'où la fonction génératrice de la suite arithmétique

$$S_{\mathbf{a}}(X) = \sum_{n=0}^{\infty} u_0 X^n + \sum_{n=0}^{\infty} naX^n = u_0(1-X)^{-1} + aX\sum_{n=0}^{\infty} nX^{n-1} = u_0(1-X)^{-1} + aX(1-X)^{-2}.$$

Pour la suite géométrique, on a

$$S_{\mathbf{g}}(X) = \sum_{n=0}^{\infty} g_0 q^n X^n = g_0 \sum_{n=0}^{\infty} (qX)^n = \frac{g_0}{1-qX}.$$ □

2.5.2 Récurrences linéaires d'ordre 2

Rappelons la définition

DÉFINITION 2.8: *Une suite* **u** *obéit à une* récurrence linéaire à coefficients constants d'ordre $d = 2$ *s'il existe des nombres* a_1, a_2, *avec* a_2 *non nul, et une suite* $\mathbf{k} = (k_n)_{n\geq 0}$ *tels que*

$$u_{n+2} = a_1 u_{n+1} + a_2 u_n + k_n, \quad n \geq 0. \tag{2.12}$$

Si la suite **k** *est nulle, l'équation (2.12) est dite* homogène.

▷ EXEMPLE 2.12: Une suite de Fibonacci [16] $\mathbf{f} = (f_n)_{n\geq 0}$ est linéaire d'ordre 2, vu qu'elle est définie par la récurrence linéaire

$$f_{n+2} = f_{n+1} + f_n, \quad n \geq 0.$$

◁

Soit r nombre non nul. La suite géométrique $(r^n)_{n\geq 0}$ est solution de la récurrence linéaire homogène associée à (2.12) si et seulement si

$$r^{n+2} = a_1 r^{n+1} + a_2 r^n, n \geq 0$$

d'où découle l'équation caractéristique

$$r^2 = a_1 r + a_2.$$

Le polynôme $P_c(X) = X^2 - a_1 X - a_2$ a été introduit dans (2.4) comme polynôme caractéristique associé à la récurrence linéaire homogène (2.12).

16. Leonardo Fibonacci, v. 1175 à Pise – v. 1250.

PROPOSITION 2.5: *Soit* $P_c(X) = X^2 - a_1 X - a_2$ *le polynôme caractéristique associé à la récurrence linéaire homogène*

$$u_{n+2} = a_1 u_{n+1} + a_2 u_n, \quad n \geq 0. \tag{2.13}$$

1. *Si le polynôme* P_c *a deux racines distinctes* r_1, r_2, *alors toute suite* $\mathbf{u}$ *vérifiant la récurrence linéaire homogène (2.13) est une combinaison linéaire (unique) des suites* $\mathbf{r}_1 = \left(r_1^n\right)_{n\geq 0}$ *et* $\mathbf{r}_2 = \left(r_2^n\right)_{n\geq 0}$, i. e. *il existe des nombres* λ_1, λ_2 *uniques tels que*

$$u_n = \lambda_1 r_1^n + \lambda_2 r_2^n, \quad n \geq 0. \tag{2.14}$$

2. *Si le polynôme caractéristique* P_c *a une racine double* r *non nulle, alors toute suite* $\mathbf{u}$ *vérifiant la récurrence homogène (2.13) est une combinaison linéaire (unique) des suites* $\mathbf{r} = (r^n)_{n\geq 0}$ *et* $\mathbf{s} = (nr^n)_{n\geq 0}$, i. e. *il existe des nombres* λ, μ *uniques tels que*

$$u_n = \lambda r^n + \mu n r^n, \quad n \geq 0.$$

3. *Si la récurrence linéaire est à coefficients réels avec un polynôme caractéristique à racines complexes non réelles* $\rho e^{\pm i\theta}$ *avec* $\rho > 0$ *et* $\theta \in]0, \pi[$, *alors toute suite réelle* $\mathbf{u}$ *vérifiant la récurrence linéaire homogène (2.13) est une combinaison linéaire (unique) des suites* $\mathbf{c} = \left(\rho^n \cos(n\theta)\right)_{n\geq 0}$ *et* $\mathbf{s} = \left(\rho^n \sin(n\theta)\right)_{n\geq 0}$, i. e. *il existe des nombres réels* λ, μ *uniques tels que*

$$u_n = \lambda \rho^n \cos(n\theta) + \mu \rho^n \sin(n\theta), \quad n \geq 0.$$

△ REMARQUE 2.6: Les deux premiers cas valent autant pour des suites complexes ou réelles, avec les paramètres de la récurrence a_1, a_2 complexes ou réels. Le dernier cas de cette proposition suppose les paramètres a_1, a_2 réels, de telle manière que si la suite $\mathbf{u}$ (complexe) vérifie la récurrence, il en est de même pour la suite conjuguée $\overline{\mathbf{u}} = \left(\overline{u_n}\right)_{n\geq 0}$. À côté des suites géométriques de rapport complexe

$$\mathbf{u}_+ = \left(\left(\rho e^{i\theta}\right)^n\right)_{n\geq 0} = \left(\rho^n e^{in\theta}\right)_{n\geq 0}, \quad \mathbf{u}_- = \left(\left(\rho e^{-i\theta}\right)^n\right) = \left(\rho^n e^{-in\theta}\right)_{n\geq 0},$$

les suites réelles constituées des parties réelles ou imaginaires sont aussi solutions de (2.13)

$$\Re e\, u_{n+2} = a_1 \Re e\, u_{n+1} + a_2 \Re e\, u_n, \quad \Im m\, u_{n+2} = a_1 \Im m\, u_{n+1} + a_2 \Im m\, u_n, \quad n \geq 0.$$

donnant une paire de solutions fondamentales de (2.12), permettant d'écrire toute suite vérifiant (2.12) comme combinaison linéaire de ces deux suites à coefficients réels. ▽

DÉMONSTRATION. Vu la relation de récurrence, une suite $\mathbf{u}$ vérifiant (2.13) est déterminée par ses deux premiers termes u_0 et u_1. Par ailleurs, vu que r_1 et r_2 sont des racines du polynôme caractéristique P_c, les suites (r_1^n), (r_2^n) et $(\lambda_1 r_1^n + \lambda_2 r_2^n)$ vérifient les relations (2.13). Les nombres λ_1, λ_2 sont contraints par le système linéaire des deux premiers termes u_0, u_1

$$u_0 = \lambda_1 + \lambda_2, \quad u_1 = \lambda_1 r_1 + \lambda_2 r_2$$

résolu, vu que $r_1 \neq r_2$, de manière unique suivant

$$\lambda_1 = \frac{u_0 r_2 - u_1}{r_2 - r_1}, \quad \lambda_2 = \frac{u_0 r_1 - u_1}{r_1 - r_2} \tag{2.15}$$

En cas de racine $r = a_1/2$ double, le polynôme caractéristique a la forme $\mathrm{P}_c(\mathrm{X}) = (\mathrm{X} - a_1/2)^2$ avec $a_2 = -a_1^2/4$ et la suite $\left(n r_{n\geq 0}^n\right)$ vérifie la récurrence (2.13) :

$$\begin{aligned}(n+2)r^{n+2} - a_1(n+1)r^{n+1} - a_2 n r^n &= r^n[(n+2)r^2 - a_1(n+1)r - a_2 n] \\ &= r^n[(n+2)(a_1^2/4) - a_1(n+1)a_1/2 - a_1^2/4n] \\ &= 0.\end{aligned}$$

Les conditions initiales $u_n = \lambda r^n + \mu n r^n$ pour $n = 0, 1$ déterminent λ, μ

$$u_0 = \lambda, \quad u_1 = \lambda r + \mu r$$

soit

$$\lambda = u_0, \quad \mu = (u_1 - u_0 r)/r$$

Vu l'hypothèse $a_2 \neq 0$, le polynôme $\mathrm{P}_c(r)$ ne peut avoir 0 comme racine et donc r est non nul.

Si a_1, a_2 sont réels, le polynôme caractéristique P_c est réel et si r non réel en est une racine, sa conjuguée $\overline{r}$ l'est aussi : les suites $(r^n)_{n\geq 0}$ et $(\overline{r}^n)_{n\geq 0}$, ainsi que les suites « partie réelle » $(\Re e\, r^n)_{n\geq 0}$ et « partie imaginaire » $(\Im m\, r^n)_{n\geq 0}$ tels que

$$\Re e\, r^n = \frac{r^n + \overline{r}^n}{2} = \rho^n \cos(n\theta), \quad \Im m\, r^n = \frac{r^n - \overline{r}^n}{2\mathrm{i}} = \rho^n \sin(n\theta), \quad n \geq 0,$$

sont solutions de (2.12). Une suite $\mathbf{u}$ vérifiant (2.12) est combinaison linéaire unique

$$u_n = \lambda \rho^n \cos(n\theta) + \mu \rho^n \sin(n\theta),$$

les λ, μ déterminés par les coefficients u_0, u_1

$$u_0 = \lambda, \quad u_1 = \lambda \rho \cos\theta + \mu \rho \sin\theta$$

soit

$$\lambda = u_0, \quad \mu = \frac{u_1 - u_0 \rho \cos\theta}{\rho \sin\theta}$$

avec $\rho \sin\theta$ est non nul car $r = \rho \mathrm{e}^{\mathrm{i}\theta}$ est complexe non réel. □

▷ EXEMPLE 2.13: La suite de Fibonacci **f** vérifie la relation de récurrence linéaire avec données initiales f_0, f_1

$$f_{n+2} = f_{n+1} + f_n, \quad n \geq 0, \qquad f_0 = 0, f_1 = 1.$$

soit

$$f_0 = 0, f_1 = 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, \ldots$$

Le polynôme caractéristique $\mathrm{P}_f(\mathrm{X}) = \mathrm{X}^2 - \mathrm{X} - 1$ a comme racines $\varphi_\pm = \left(1 \pm \sqrt{5}\right)/2$ (où φ_+ est appelé *nombre d'or*). La formule (2.15) donne

$$f_n = \frac{\varphi_+^n - \varphi_-^n}{\sqrt{5}} = \frac{\left[\dfrac{1+\sqrt{5}}{2}\right]^n - \left[\dfrac{1-\sqrt{5}}{2}\right]^n}{\sqrt{5}}.$$

Développant ces deux puissances suivant le binôme de Newton, les termes de degré pair avec $(\sqrt{5})^{2k}$ en facteur s'annulent mutuellement, alors que la différence des termes de degré impair $(\sqrt{5})^{2k+1}/\sqrt{5}$ voient les facteurs racines $\sqrt{5}$ disparaître : f_n est bien un entier. Par ailleurs, dans la formule donnant f_n, le second terme converge vers 0 exponentiellement vite alors que le premier tend vers $+\infty$ exponentiellement.

La suite de Fibonacci **f** est une suite d'entiers qui tend vers $+\infty$. Le quotient f_{n+1}/f_n vérifie

$$\frac{f_{n+1}}{f_n} = \varphi_+ \frac{1 - \left(\varphi_-/\varphi_+\right)^{n+1}}{1 - \left(\varphi_-/\varphi_+\right)^n}$$

avec les termes $|\varphi_-/\varphi_+| < 1$. Le quotient f_{n+1}/f_n, représente le taux de croissance des termes de la suite de Fibonacci : il tend vers φ_+ lorsque $n \to \infty$. ◁

La résolution de récurrences linéaires non homogènes est faisable quand la suite (k_n) est une suite exponentielle-polynôme :

PROPOSITION 2.6: *Soit la relation récurrente linéaire à coefficients constants*

$$u_{n+2} = a_1 u_{n+1} + a_2 u_n + k_n, \quad n \geq 0. \tag{2.16}$$

de polynôme caractéristique P_c*, avec la suite exponentielle-polynôme* $\mathbf{k} = (\rho^n \mathrm{P}(n))_{n\geq 0}$ *où* P *est un polynôme de degré* d_P *et* ρ *un nombre.*
Si ρ *est une racine caractéristique de multiplicité* m *(*$m = 0, 1$ *ou* 2*), alors il existe une solution unique vérifiant (2.16) du type* $(\rho^n n^m \mathrm{Q}(n))_{n\geq 0}$ *avec* Q *polynôme de degré au plus* d_P*.*

DÉMONSTRATION. La démonstration est analogue à celle de la proposition 2.4 basée sur deux notes 13 et 14, qu'il suffit de reprendre pour les cas $m = 0$ et $m = 1$. Pour $m = 2$, la suite $(\rho^n \mathrm{Q}(n))_{n\geq 0}$ est solution de l'équation non homogène (2.12) si et seulement si

$$\rho^2 \mathrm{Q}(n+2) - a_1 \rho \mathrm{Q}(n+1) - a_2 \mathrm{Q}(n) = \mathrm{P}(n), \quad n \geq 0$$

On considère le polynôme Q de degré $d+2$ tel que $Q(X) = AX^{d+2} + BX^{d+1} + R(X)$ avec R de degré au plus d et on lui applique l'opérateur

$$Q \mapsto \widetilde{Q}(X) = \rho^2 Q(X+2) - a_1 \rho Q(X+1) - a_2 Q(X)$$

pour lequel on trouve comme termes de degré $d+2$ et $d+1$

$$\widetilde{Q}(X) = AP_c(\rho)X^{d+2} + \left[A\rho d(2\rho - a_1) + BP_c(\rho)\right]X^{d+1} + \ldots,$$

les coefficients étant nuls du fait que ρ est racine du polynôme caractéristique (donc $P_c(\rho) = 0$), racine double (et donc $\Delta = a_1^2 + 4a_2 = 0$). Il en résulte que l'application linéaire $Q \in X^2\mathbb{R}_{d_P}[X] \mapsto \widetilde{Q} \in \mathbb{R}_{d_P}[X]$ est bien définie, et injective de surcroît. Vu l'égalité des dimensions cette application est une bijection et (2.16) a bien une solution $(\rho^n n^2 Q(n))_{n\geq 0}$ unique avec Q de degré d si $(k_n = \rho^n P(n))$ avec P de degré d. □

▷ EXEMPLES 2.14:

2.14.1 La récurrence linéaire à coefficients constants

$$u_{n+2} = 5u_{n+1} - 6u_n + 100 \cdot 7^n$$

admet 2 et 3 comme racines (simples) de son polynôme caractéristique. On peut donc trouver comme solution particulière une solution du type $(A \cdot 7^n)$. En substituant dans l'équation, on trouve la solution particulière $\mathbf{u} = (5 \cdot 7^n)_{n\geq 0}$.

2.14.2 Soit la récurrence linéaire à coefficients constants et avec second membre

$$u_{n+2} = 5u_{n+1} - 6u_n + 3^n(6n+30). \tag{2.17}$$

Le polynôme caractéristique est $P_c(X) = X^2 - 5X + 6$ avec comme racines 2 et 3. Ainsi, il existe une solution particulière du type $\left(3^n n(an+b)\right)_{n\geq 0}$ où les constantes a, b sont déterminées par la relation de récurrence valable pour tout entier $n \in \mathbb{N}$

$$3^2(n+2)(a(n+2)+b) = 5 \cdot 3(n+1)(a(n+1)+b) - 6 \cdot n(an+b) + 6n + 30$$

soit trois conditions linéaires déterminant a et b en isolant les coefficients des monômes $n^2, n, 1$

$$\begin{aligned} 9a &= 15a - 6a \\ 9(2a+b+2a) &= 15(a+b+a) - 6b + 6 \\ 9 \cdot 2(2a+b) &= 15(a+b) + 30 \end{aligned}$$

qui a comme unique solution $a = 1, b = 3$. La solution générale de (2.17) est donc de la forme $\mathbf{u} = \left(\lambda 2^n + \mu 3^n + 3^n n(n+3)\right)$, les constantes λ, μ étant uniquement déterminées par les 2 premiers termes u_0, u_1 de la suite $\mathbf{u}$:

$$u_0 = \lambda + \mu, \quad u_1 = 2\lambda + 3\mu + 12,$$

soit

$$\lambda = 12 + 3u_0 - u_1, \quad \mu = -12 - 2u_0 + u_1$$

◁

2.5.3 Suites homographiques

DÉFINITION 2.9: *Soient a,b,c,d réels avec $ad-bc$ non nul.*
L'application T *définie par*

$$\mathrm{T} : x \in \mathbb{R} \mapsto \mathrm{T}(x) = \frac{ax+b}{cx+d} \in \mathbb{R}, \quad x \in \mathbb{R} \setminus \left\{-\frac{d}{c}\right\}. \tag{2.18}$$

est appelée homographie. *Si $c=0$, cette définition est à comprendre suivant*

$$\mathrm{T} : x \in \mathbb{R} \mapsto \mathrm{T}(x) = \frac{ax+b}{d} \in \mathbb{R}, \quad x \in \mathbb{R}. \tag{2.19}$$

L'hypothèse de non nullité de $ad-bc$ assure que l'application T est non constante et injective

$$\mathrm{T}'(x) = \frac{ad-bc}{(cx+d)^2}, \qquad \mathrm{T}(x)-\mathrm{T}(x') = \frac{(ad-bc)(x-x')}{(cx+d)(cx'+d)}, \quad x,x' \in \mathbb{R} \setminus \left\{-\frac{d}{c}\right\},$$

à l'opposé de ce qui est quand $ad-bc=0$, par exemple si d non nul

$$\frac{ax+b}{cx+d} = \frac{\frac{bc}{d}x+b}{cx+d} = \frac{b}{d}\frac{cx+d}{cx+d} = \frac{b}{d}.$$

et cette remarque[17] vaut aussi pour les T du type (2.19) : $\mathrm{T}'(x) = a/d, \mathrm{T}(x)-\mathrm{T}(x') = a/d(x-x')$. Si $ad-bc=ad=0$, alors soit $d=0$ et T n'est pas défini, soit $a=0$ auquel cas T' est nul et T est constante.

L'objet de cette section est l'étude des suites (réelles) $\mathbf{x}=(x_n)_{n\geq 0}$ définies par la relation de récurrence

$$x_{n+1} = \mathrm{T}(x_n) = \frac{ax_n+b}{cx_n+d}, \quad n \geq 0,$$

avec x_0 réel et T une homographie. On suppose dans la suite que T n'est pas l'identité (cas $b=0$, $c=0$: la suite (x_n) est constante).

△ REMARQUE 2.7: Une suite arithmético-géométrique (2.6) est un cas particulier de suite homographique : si q non nul, la suite vérifiant $u_{n+1} = qu_n + a$ est déterminée par l'homographie $x \mapsto (qx+a)/(0\cdot x+1) = qx+a$. ▽

Afin de ne considérer que des applications bien définies et avec mêmes source et but, on ajoute à $\mathbb{R}$ un point noté ∞, obtenant l'ensemble $\widehat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$. On prolonge alors l'application T définie par (2.18) en une application, dite encore *homographie*, $\widehat{\mathrm{T}} : \widehat{\mathbb{R}} \to \widehat{\mathbb{R}}$, (prolongement souvent noté T afin de ne pas alourdir les notations) selon la définition suivante :

17. Dans la suite, on omettra parfois la vérification que telle formule est aussi valable pour ces applications affines avec un $c=0$.

DÉFINITION 2.10: *Soient a,b,c,d réels avec $ad-bc$ non nul. L'application* T *définie par*

$$\mathrm{T}(x)=\begin{cases}\dfrac{ax+b}{cx+d} & si\ x\in\mathbb{R}\setminus\left\{-\dfrac{d}{c}\right\},\\ \infty & si\ x=-\dfrac{d}{c},\\ \dfrac{a}{c} & si\ x=\infty.\end{cases}\tag{2.20}$$

est appelée homographie. Si $c=0$, cette définition est à comprendre suivant

$$\mathrm{T}(x)=\begin{cases}\dfrac{ax+b}{d} & si\ x\in\mathbb{R},\\ \infty & si\ x=\infty.\end{cases}\tag{2.21}$$

Le lemme suivant est vérifié aisément. L'image inverse de y par T s'obtient en résolvant l'équation $y=\dfrac{ax+b}{cx+d}$ selon

$$y(cx+d)=ax+b\Longleftrightarrow x(cy-a)=-dy+b\Longleftrightarrow x=\frac{-dy+b}{cy-a}.$$

Le lemme suivant est basé sur une vérification simple des propriétés d'inverse de T et son T^{-1} associé.

LEMME 2.6: *L'homographie* T *définie par (2.20) est une bijection de* $\widehat{\mathrm{R}}$ *sur* $\widehat{\mathrm{R}}$*, d'application réciproque* T^{-1} *formulée suivant*

$$\mathrm{T}^{-1}(y)=\begin{cases}\dfrac{-dy+b}{cy-a} & si\ y\in\mathbb{R}\setminus\left\{\dfrac{a}{c}\right\},\\ \infty & si\ y=\dfrac{a}{c},\\ -\dfrac{d}{c} & si\ y=\infty.\end{cases}$$

Si $c=0$ la formule précédente est à comprendre suivant

$$\mathrm{T}^{-1}(y)=\begin{cases}\dfrac{dy-b}{a} & si\ y\in\mathbb{R},\\ \infty & si\ y=\infty,\end{cases}$$

La condition $ad-bc$ non nul pour T perdure pour son inverse T^{-1} : $(-d)(-a)-bc\neq 0$. L'application réciproque T^{-1} d'une homographie T est donc encore une homographie. Les homographies avec $c=0$ déterminent les suites arithmético-géométriques : les récurrences homographiques livrent une extension des récurrences arithmético-géométriques, récurrences avec une homographie T qui a ∞ comme point fixe (et donc de type (2.19)).

Dans l'espace $\widehat{\mathbb{R}}$, il est agréable de disposer de notions de convergence (et de continuité) : d'une part, si ℓ est réel, la convergence de $\mathbf{x}$ vers ℓ est celle considérée pour des suites réelle dans la définition 2.1. D'autre part, la convergence de $\mathbf{x}$ vers ∞ est analogue à celle de la définition 2.2

$$\forall \mathrm{A} \in \mathbb{R}, \quad \exists \mathrm{N} \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \quad (|u_{\mathrm{N}+n}| \geq \mathrm{A} \text{ ou } x_{\mathrm{N}+n} = \infty).$$

On vérifie que les transformations $\widehat{\mathrm{T}}$ de (2.20) et (2.21) sont continues au sens suivant : pour tout $\lambda \in \widehat{\mathbb{R}}$: si $x_n \to \lambda$ dans $\widehat{\mathbb{R}}$, alors $\mathrm{T}x_n \to \mathrm{T}\lambda$ (dans $\widehat{\mathbb{R}}$). D'ailleurs le prolongement (2.20) de (2.18) peut se voir comme un prolongement par continuité relativement à cette convergence.

LEMME 2.7: *La composée* $\mathrm{T}_2 \circ \mathrm{T}_1$ *de deux homographies* $\mathrm{T}_1, \mathrm{T}_2$ *est une homographie.*

DÉMONSTRATION. Sous couvert de vérification de l'absence de division par 0, on a

$$\frac{a_2 \dfrac{a_1 x + b_1}{c_1 x + d_1} + b_2}{c_2 \dfrac{a_1 x + b_1}{c_1 x + d_1} + d_2} = \frac{(a_2 a_1 + b_2 c_1)x + a_2 b_1 + b_2 d_1}{(c_2 a_1 + d_2 c_1)x + c_2 b_1 + d_2 d_1} \tag{2.22}$$

de la forme $(\mathrm{A}x + \mathrm{B})/(\mathrm{C}x + \mathrm{D})$ avec $\mathrm{A} = a_2 a_1 + b_2 c_1, \mathrm{B} = a_2 b_1 + b_2 d_1$, etc. et la non nullité de

$$\mathrm{AD} - \mathrm{BC} = (a_1 d_1 - b_1 c_1)(a_2 d_2 - b_2 c_2).$$

La discussion est un peu longue : il s'agit de vérifier que la composée $\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1$ (application de $\widehat{\mathrm{R}}$ dans $\widehat{\mathrm{R}}$) est bien une homographie $\widehat{\mathrm{T}}$ réelle prolongée à $\widehat{\mathrm{R}}$ suivant les définitions (2.20) et (2.21). On séparera cette vérification suivant les cas de nullité ou non nullité des coefficients c_1 et c_2.

Le cas $c_1 = c_2 = 0$ (où d_1, d_2 sont non nuls vu l'hypothèse de non nullité des $a_j d_j - b_j c_j$ pour $j = 1, 2$) est le plus simple (on manipule des fonctions affines et leur prolongement) : d'une part pour x réel

$$\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1(x) = \mathrm{T}_2 \circ \mathrm{T}_1(x) = \frac{a_2}{d_2}\left(\frac{a_1 x + b_1}{d_1}\right) + \frac{b_2}{d_2} = \frac{a_2 a_1}{d_2 d_1} x + \frac{b_1 a_2}{d_1 d_2} + \frac{b_2}{d_2}, \quad x \in \mathbb{R}, \tag{2.23}$$

qui sera notée T (application de $\mathbb{R}$ dans $\mathbb{R}$), d'autre part $\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1(\infty) = \widehat{\mathrm{T}}_2(\infty) = \infty$. La composée $\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1$ est le prolongement à $\widehat{\mathrm{R}}$ de l'application affine T définie sur $\mathbb{R}$ par (2.23) et selon (2.21). Pour le cas $c_1 \neq 0$ et $c_2 = 0$, on a $d_2 \neq 0$. Alors, pour x réel distinct de $-d_1/c_1$, on a

$$\mathrm{T}_2 \circ \mathrm{T}_1(x) = \mathrm{T}_2\left(\frac{a_1 x + b_1}{c_1 x + d_1}\right) = \frac{a_2\left(\frac{a_1 x + b_1}{c_1 x + d_1}\right) + b_2}{d_2} = \frac{(a_2 a_1 + b_2 c_1)x + a_2 b_1 + b_2 d_1}{d_2 c_1 x + d_1 d_2},$$

alors que $\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1(-d_1/c_1) = \widehat{\mathrm{T}}_2(\infty) = \infty$ et

$$\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1(\infty) = \mathrm{T}_2(a_1/c_1) = \frac{a_2 \frac{a_1}{c_1} + b_2}{d_2} = \frac{a_2 a_1 + b_2 c_1}{c_1 d_2},$$

le dernier membre provenant des coefficients respectifs des définitions (2.20) et (2.21). On vient de montrer que la composée $\widehat{\mathrm{T}}_2 \circ \widehat{\mathrm{T}}_1$ est bien du type (2.20). Considérons la situation où le coefficient c_1 de T_1 est non nul, alors que le c_2 de T_2 est nul.

$$\mathrm{T}_2 \circ \mathrm{T}_1(-d_1/c_1) = \mathrm{T}_2(\infty) = \infty, \quad \mathrm{T}_2 \circ \mathrm{T}_1(\infty) = \mathrm{T}_2\left(\frac{a_1}{c_1}\right) = \frac{a_2\left(\frac{a_1}{c_1}\right) + b_2}{d_2} = \frac{a_2 a_1 + c_1 b_2}{d_2 c_1}$$

et

$$\mathrm{T}_2 \circ \mathrm{T}_1(x) = \frac{a_2 \dfrac{a_1 x + b_1}{c_1 x + d_1} + b_2}{d_2} = \frac{(a_2 a_1 + b_2 c_1)x + a_2 b_1 + b_2 d_1}{d_2(c_1 x + d_1)}, \quad x \in \mathbb{R} \setminus \{-d_1/c_1\}$$

d'image $\mathbb{R}\setminus\{(a_2a_1+c_1b_2)/(d_2c_1)\}$. Vu que $a_2d_2-b_2c_2$ est non nul et c_2 nul, d_2 est certainement non nul.

Finalement, traitons des cas où ni T_1 ni T_2 ne laisse ∞ fixe. On a ainsi c_1c_2 non nul.

La première configuration consiste en $T_2\circ T_1(\infty)=\infty$: c'est équivalent à $T_1(\infty)=T_2^{-1}(\infty)$, soit $a_1/c_1=-d_2/c_2$ ou encore $C=a_1c_2+d_2c_1=0$ avec C le coefficient d'homographie de $T_2\circ T_1$ dans (2.22). La nullité de C assure que $T=T_2\circ T_1$ est le prolongement de l'application affine $x\in\mathbb{R}\mapsto(Ax+B)/D\in\mathbb{R}$ de (2.22) laissant fixe ∞.

Dans la seconde, $T_1(\infty)=a_1/c_1$ (dans $\mathbb{R}$) et

$$T_2(T_1(\infty))=\frac{a_2\frac{a_1}{c_1}+b_2}{c_2\frac{a_1}{c_1}+d_2}=\frac{a_2a_1+b_2c_1}{c_2a_1+d_2c_1}=\frac{a_2a_1+b_2c_1}{C}$$

où le dénominateur $C=c_2a_1+d_2c_1$ n'est pas nul (la nullité est le cas qui vient d'être étudié). Par ailleurs

$$(T_2\circ T_1)^{-1}(\infty)=T_1^{-1}\big(T_2^{-1}(\infty)\big)=T_1^{-1}\left(\frac{-d_2}{c_2}\right)=\frac{-d_1\left(\frac{-d_2}{c_2}\right)+b_1}{c_1\left(\frac{-d_2}{c_2}\right)-a_1}=-\frac{d_1d_2+b_1c_2}{c_1d_2+a_1c_2}$$

qui est un réel vu la non-nullité du dénominateur $C=c_1d_2+a_1c_2$. Ainsi l'application $T=T_2\circ T_1$ envoie ∞ sur le réel $x_\infty=T_2\circ T_1(\infty)$, le réel $y_\infty=(T_2\circ T_1)^{-1}(\infty)$ sur ∞ et la partie $\mathbb{R}\setminus\{x_\infty\}$ sur $\mathbb{R}\setminus\{y_\infty\}$. Cette composée est bien une homographie sur $\widehat{\mathbb{R}}$. □

La discussion sur les homographies réelles vaut en fait complètement (et sans difficulté autre que des calculs algébriques à vérifier) pour les homographies (réelles ou complexes) avec espaces source et but « complété » $\widehat{\mathbb{C}}=\mathbb{C}\cup\{\infty\}$ de $\mathbb{C}$. Nous verrons qu'il est fructueux (dernier cas du théorème suivant 2.6) de considérer les homographies réelles avec espaces source et but le complété $\widehat{\mathbb{C}}$.

Revenons à la suite $\mathbf{x}$ à valeurs dans $\widehat{\mathbb{R}}$ définie par récurrence suivant

$$x_0\in\widehat{\mathbb{R}}\text{ et }x_{n+1}=T(x_n),\qquad n\geq 0.$$

Si la suite $\mathbf{x}$ est convergente vers $\ell\in\mathbb{R}$, sa limite ℓ doit être un point fixe de T. L'équation aux points fixes de T restreinte dans $\mathbb{R}$

$$T(x)=x\Longleftrightarrow ax+b=x(cx+d)$$

est une équation du second degré. L'équation au point fixe $Tx=x, x\in\widehat{\mathbb{R}}$ n'a ∞ comme solution que si T est une application affine ($x\mapsto T(x)=\alpha x+\beta$ supposée non triviale ($(\alpha,\beta)\neq(1,0)$) et non constante ($\alpha\neq 0$), auquel cas il y a au plus un point fixe de T dans $\mathbb{R}$. On a trois cas bien différents, suivant le nombre de points fixes (déterminant chacun une suite constante) de T dans $\widehat{\mathbb{R}}$.

THÉORÈME 2.6: *Soit* $\mathrm{T} : \widehat{\mathbb{R}} \to \widehat{\mathbb{R}}$ *une homographie réelle (distincte de l'identité) et la suite* $\mathbf{x}$ *vérifiant la relation de récurrence* $x_{n+1} = \mathrm{T}(x_n)$ *pour* $n \geq 0$ *et de donnée initiale* $x_0 \in \widehat{\mathbb{R}}$.

- *Si* T *admet* $\mathrm{F_T} = 2$ *points fixes distincts dans* $\widehat{\mathrm{R}}$, *alors*
  - *soit la suite* $\mathbf{x}$ *est* 2*-périodique pour tout* x_0 *distinct des points fixes,*
  - *soit la suite* $\mathbf{x}$ *converge vers un des points fixes quelle que soit la donnée initiale* x_0 *exceptée l'autre point fixe, auquel cas la suite* $\mathbf{x}$ *stationne sur ce point fixe.*
- *Si* T *admet* $\mathrm{F_T} = 1$ *point fixe dans* $\widehat{\mathrm{R}}$, *la suite* $\mathbf{x}$ *tend vers cet unique point fixe quelle que soit la donnée initiale* x_0.
- *Si* T *admet* $\mathrm{F_T} = 2$ *points fixes non réels (donc conjugués), il n'y a jamais convergence de la suite* $\mathbf{x}$ *: le comportement asymptotique de la suite* $\mathbf{x}$ *est décrit suivant*
  - *soit il existe un entier* $m > 1$ *tel que* T *a une puissance* m*-ème égale à l'identité, auquel cas la suite* $\mathbf{x}$ *est* m*-périodique,*
  - *soit la suite* $\mathbf{x}$ *se répartit de manière dense sur la droite étendue* $\widehat{\mathbb{R}}$.

DÉMONSTRATION. Une application affine $\mathrm{T} : x \mapsto (ax+b)/d$ induit une suite homographique vérifiant une récurrence $x_{n+1} = qx_n + t$ de type arithmético-géométrique dont les propriétés asymptotiques ont été déjà étudiées et se retrouvent dans un des deux premiers cas du théorème. Pour éviter ces cas, on supposera dans la suite que $\mathrm{T} : x \mapsto (ax+b)/(cx+d)$ n'a pas ∞ comme point fixe, *i. e.* T a tous ses points fixes réels, racines du trinôme $x(cx+d) = ax+b$.

La méthode de démonstration est commune aux trois principaux cas : changer la suite $\mathbf{x}$ en une suite $\mathbf{y} = (y_n = \Phi(x_n))$ pour une homographie Φ convenable. Ainsi la suite $\mathbf{y}$ est définie aussi par une relation de récurrence $y_{n+1} = \widetilde{\mathrm{T}}(y_n)$ où

$$\widetilde{\mathrm{T}} = \Phi \circ \mathrm{T} \circ \Phi^{-1},$$

la transformation $\widetilde{\mathrm{T}}$ étant une application affine, induisant donc une suite géométrique ou une suite arithmétique. Avec ce changement de coordonnée de x à $y = \Phi(x)$ pour une homographie Φ bien choisie, on est ainsi ramené à une récurrence arithmético-géométrique pour la suite $\mathbf{y} = \Phi(\mathbf{x})$. Ce changement de variable est symbolisé par le diagramme décrivant les relations entre les applications $\widetilde{\mathrm{T}}$ et T, Φ :

$$\begin{array}{ccc} x & \xrightarrow{\quad\mathrm{T}\quad} & \mathrm{T}(x) \\ \big\downarrow \Phi & & \big\downarrow \Phi \\ y & \xrightarrow[\widetilde{\mathrm{T}} = \Phi \circ \mathrm{T} \circ \Phi^{-1}]{} & \widetilde{\mathrm{T}}(y) \end{array}$$

La transformation Φ transporte un point fixe α de T en le point fixe $\Phi(\alpha)$ de $\widetilde{\mathrm{T}}$.

Considérons le cas où l'application T a deux point fixes réels α, β distincts. On considère l'application $\Phi_{\alpha,\beta}(x) = \dfrac{x-\alpha}{x-\beta}$ (qu'on notera simplement Φ pour alléger) : cette application applique α, β sur $0, \infty$ resp. Alors l'application $\widetilde{\mathrm{T}} = \Phi \circ \mathrm{T} \circ \Phi^{-1}$ a 0

et ∞ comme points fixes

$$\widetilde{\mathrm{T}}(0) = \Phi \circ \mathrm{T} \circ \Phi^{-1}(0) = (\Phi \circ \mathrm{T})(\alpha) = \Phi(\alpha) = 0$$

et l'identité analogue $\widetilde{\mathrm{T}}(\infty) = \infty$. Si $\widetilde{\mathrm{T}}(y) = (\widetilde{a}y + \widetilde{b})/(\widetilde{c}y + \widetilde{d})$, l'égalité $\widetilde{\mathrm{T}}(0) = 0$ implique $\widetilde{b}/\widetilde{d} = 0$ alors que $\widetilde{\mathrm{T}}(\infty) = \infty$ implique $\widetilde{a}/\widetilde{c} = \infty$, ces deux contraintes imposant $\widetilde{b} = \widetilde{c} = 0$ et $\widetilde{\mathrm{T}}(y) = \widetilde{a}/\widetilde{d}\,y$ que nous écrirons $\widetilde{\mathrm{T}}(y) = \widetilde{q}y$ pour un $\widetilde{q}$ réel. L'étude de la convergence de la suite $\mathbf{x}$ est équivalente à l'étude de la suite $\big(y_n = \Phi(x_n)\big)$ qui vérifie $y_{n+1} = \widetilde{q}y_n$ pour $n \geq 0$. La discussion se fera selon les cas $|\widetilde{q}| < 1$, $\widetilde{q} = -1$ et $|\widetilde{q}| > 1$ sur la suite $\mathbf{y}$ avant de revenir à la suite $\mathbf{x}$ via l'application Φ. Si $|\widetilde{q}| < 1$, il y a convergence de $\mathbf{y}$ vers 0, donc de $\mathbf{x} = \Phi^{-1}(\mathbf{y})$ vers α (sauf si $x_0 = \beta$). Si $\widetilde{q} = -1$, la suite $\mathbf{y}$ (avec y_0 non nul, ni ∞) oscille entre y_0 et $-y_0$: il en est de même pour $\mathbf{x}$ qui oscille avec période 2 entre x_0 et $\mathrm{T}(x_0)$ (pourvu que x_0 soient distincts des points fixes α, β). Enfin si $|\widetilde{q}| > 1$, la suite $(y_n = \widetilde{q}^n y_0)$ tend vers ∞ (sans distinction de signe).

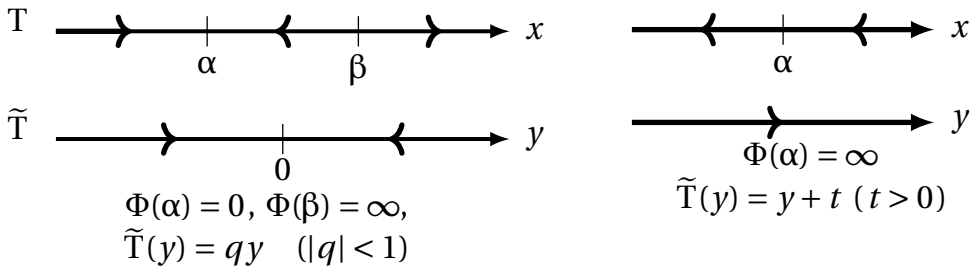

FIGURE II.4 – Les points limite, avant et après changement de variable $x \mapsto y = \Phi(x)$. Les flèches indiquent le sens d'une itération de la suite $\mathbf{x}$ convergente vers ou provenant d'un point fixe sur la droite réelle complétée $\widehat{\mathbb{R}}$.

Traitons le cas où l'application T a été supposée n'avoir qu'un point fixe α réel. En considérant l'application $\Psi : x \mapsto (x-\alpha)^{-1}$ d'application réciproque $y \mapsto \alpha + y^{-1}$, l'application $\widetilde{\mathrm{T}} = \Psi \circ \mathrm{T} \circ \Psi^{-1}$ a ∞ comme point fixe : ainsi $\widetilde{\mathrm{T}}(y) = (\widetilde{a}y + \widetilde{b})/\widetilde{d}$. Si $\widetilde{a}/\widetilde{d} \neq 1$, il y a un point fixe (outre ∞), ce qui n'est pas. Donc $\widetilde{\mathrm{T}}$ est de la forme $\widetilde{\mathrm{T}}(y) = y + t$ avec t réel non nul. Ainsi, à moins de stationner en ∞, la suite $(y_n = \widetilde{\mathrm{T}}^n(y_0) = y_0 + nt)$ tend vers ∞ et donc $\mathbf{x} = \Psi(\mathbf{y})$ converge vers le point fixe $\alpha = \Psi^{-1}(\infty)$ de T.

Venons en au cas où l'application $\mathrm{T} : \mathbb{R} \mapsto \mathbb{R}$ n'a pas de point fixe qui soit réel ou ∞. Si on considère le prolongement de T à $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ par les mêmes formules que celles définissant T à coefficients réels (2.18) et (2.19) et appliquant $\widehat{\mathbb{C}}$ en lui même, cette application (encore notée T) a deux points fixes complexes non réels $\zeta, \bar{\zeta}$, conjugués l'un de l'autre. Reprenant les notations du premier cas ci-dessus, l'application

$$\Phi_{\zeta,\bar{\zeta}} : z \in \widehat{\mathbb{C}} \mapsto w = \frac{\zeta - z}{\bar{\zeta} - z} \in \widehat{\mathbb{C}}$$

La transformation $\Phi_{\zeta,\bar{\zeta}}$ a pour inverse

$$\Phi^{-1}_{\zeta,\bar{\zeta}} : w \in \widehat{\mathbb{C}} \mapsto z = \frac{w\bar{\zeta} - \zeta}{w - 1} \in \widehat{\mathbb{C}}$$

et applique la droite réelle complétée $\widehat{\mathbb{R}} = \{\Im m\, z = 0\} \cup \{\infty\}$ sur le cercle $\mathrm{S}^1 = \{|w| = 1\}$ vu que

$$\left|\Phi_{\zeta,\bar{\zeta}}(x)\right| = \left|\frac{\zeta - x}{\bar{\zeta} - x}\right| = 1, \quad x \in \mathbb{R}$$

et $\Phi^{-1}_{\zeta,\bar\zeta}$ ramène le cercle unité S^1 sur l'axe horizontal complété $\widehat{\mathbb{R}} = \{\Im m\, z = 0\} \cup \{\infty\}$

$$\Im m\left(\Phi^{-1}_{\zeta,\bar\zeta}(w)\right) = \Im m\left(\frac{w\bar\zeta - \zeta}{w-1}\right) = \frac{\Im m\left((w\bar\zeta-\zeta)(\overline{w}-1)\right)}{|w-1|^2}$$
$$= \frac{\Im m\,(w\overline{w}\bar\zeta - \bar\zeta w - \zeta\overline{w} + \zeta)}{|w-1|^2} = 0, \quad w \in \mathrm{S}^1$$

et donc l'homographie $\Phi_{\zeta,\bar\zeta} : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ applique bijectivement $\widehat{\mathbb{R}}$ sur le cercle S^1. Par un argument pleinement analogue aux considérations du cas de deux points fixes réels ci-dessus, l'application $\widetilde{\mathrm{T}}$ est donnée par $\widetilde{\mathrm{T}}(y) = \widetilde{q}y$. L'application $\widetilde{\mathrm{T}}$ laisse invariante le cercle S^1 (car T laisse invariante la droite réelle). Ainsi $\widetilde{q}$ est de module 1 : $\widetilde{q}$ est soit une racine m-ème de l'unité, auquel cas $\mathrm{T}^{\circ m} = \mathrm{Id}$ et la suite $\mathbf{x} = \Phi^{-1}_{\zeta,\bar\zeta}(\mathbf{y})$ est m-périodique, soit un complexe de module 1 qui n'est pas une racine de l'unité, auquel cas la suite $(\widetilde{q}^n y_0)_{n\in\mathbb{N}}$, avec $y_0 \in \mathrm{S}^1$, est "dense" dans le cercle, et par suite la suite $\mathbf{x} = \Phi^{-1}_{\zeta,\bar\zeta}(\mathbf{y})$ est dense dans la droite complétée $\widehat{\mathbb{R}} = \mathrm{R} \cup \{\infty\}$.

□

▷ EXEMPLES 2.15:

2.15.1 Soit q non nul. L'homographie $\mathrm{H}_{q,a} : x \mapsto qx + a$ détermine la suite arithmético-géométrique vérifiant $u_{n+1} = qu_n + a$. Si $q = 1$ et a non nul, la transformation $\mathrm{H}_{q,a}$ a un seul point fixe, soit ∞ ; si $q \neq 1$, $\mathrm{H}_{q,a}$ en a deux, soit $a/(1-q)$ et ∞.

2.15.2 L'application T définie par $\mathrm{T}(x) = \dfrac{3x+2}{x+4}$ a deux points fixes réels $x = 1$ et $x = -2$. Conjuguée par l'application $\Phi : x \mapsto \dfrac{x-1}{x+2}$ d'application réciproque $\Phi^{-1} : y \mapsto \dfrac{1+2y}{1-y}$, l'application T prend la forme $\widetilde{\mathrm{T}} = \Phi \circ \mathrm{T} \circ \Phi^{-1}(y) = \dfrac{2}{5}y$. Ainsi la suite $\mathbf{x}$ converge vers $x_\infty = 1 = \Phi^{-1}(0)$ quel que soit le point initial $x_0 \in \mathbb{R}$, excepté $x_0 = -2$.

2.15.3 L'application $\mathrm{T} : x \mapsto (7x-12)/(3x-5)$ a $x = 2$ comme unique point fixe. Si $\Phi : x \mapsto (x-2)^{-1}$, alors $\Phi \circ \mathrm{T} \circ \Phi^{-1}$ prend la forme $\widetilde{\mathrm{T}} : y \mapsto y + 3$.

2.15.4 L'application T définie par $\mathrm{T} : x \in \widehat{\mathbb{C}} \mapsto \dfrac{x - \sqrt{3}}{\sqrt{3}x + 1}$ a $\pm\mathrm{i}$ comme points fixes. L'application $\Phi : x \mapsto \dfrac{x-\mathrm{i}}{x+\mathrm{i}}$ a comme inverse $\Phi^{-1} : y \mapsto \mathrm{i}\dfrac{1+y}{1-y}$ et l'application $\widetilde{\mathrm{T}} = \Phi \circ \mathrm{T} \circ \Phi^{-1}$ est définie par $\widetilde{\mathrm{T}}(z) = \tau z$, le nombre $\tau = -\dfrac{\sqrt{3}\mathrm{i}+1}{2}$ étant une racine troisième de l'unité. On vérifie que $\mathrm{T}^3 = \mathrm{Id}_{\widehat{\mathbb{R}}}$: la suite $\mathbf{x}$ est périodique de période 3, soit $x_0, x_1 = \mathrm{T}(x_0), x_2 = \mathrm{T} \circ \mathrm{T}(x_0), x_3 = x_0, \ldots$.

2.15.5 Soit T_a l'homographie (complexe) définie par $\mathrm{T}_a(x) = a^2/x$. On considère Φ_a et sa réciproque Φ_a^{-1} définies par

$$\Phi_a(x) = \frac{x-a}{x+a}, \quad \Phi_a^{-1}(y) = a\frac{1+y}{1-y}$$

On vérifie que

$$\Phi_a \circ \mathrm{T}_a \circ \Phi_a^{-1}(y) = -y$$

Cette famille de T_a, restreinte aux homographies (complexes) de paramètre a tel que $T_a(\widehat{\mathbb{R}}) \subset \widehat{\mathbb{R}}$, illustre l'analyse générale : pour a réel (deux points fixes) et a imaginaire pur (pas de point fixe réel), T_a est 2-périodique. ◁

2.5.4 Le nombre d'Euler e

Soit les suites p et s définies par

$$p_n = \left(1+\frac{1}{n}\right)^n, \quad s_n = 1+\frac{1}{1!}+\cdots+\frac{1}{n!}$$

LEMME 2.8: *La suite $p=(p_n)_{n\geq 1}$ est strictement croissante.*

DÉMONSTRATION. On a d'une part

$$\begin{aligned}\left(1+\frac{1}{n}\right)^n &= \sum_{k=0}^{n}\binom{n}{k}\left(\frac{1}{n}\right)^k \\ &= \sum_{k=0}^{n}\frac{1}{k!}\frac{n(n-1)(n-2)\ldots(n-k+1)}{n\cdot n\cdot n\ldots n} \\ &= \sum_{k=0}^{n}\frac{1}{k!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right),\end{aligned}$$

et d'autre part

$$\begin{aligned}\left(1+\frac{1}{n+1}^{n+1}\right) &= \sum_{k=0}^{n+1}\frac{1}{k!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\ldots\left(1-\frac{k-1}{n+1}\right) \\ &= \sum_{k=0}^{n}\frac{1}{k!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\ldots\left(1-\frac{k-1}{n+1}\right) \\ &\quad + \frac{1}{(n+1)!}\left(\frac{n}{n+1}\right)\left(\frac{n-1}{n+1}\right)\ldots\left(\frac{1}{n+1}\right) \\ &= \sum_{k=0}^{n}\frac{1}{k!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\ldots\left(1-\frac{k-1}{n+1}\right)+\left(\frac{1}{n+1}\right)^{n+1}\end{aligned}$$

L'inégalité provient de la comparaison des coefficients respectifs de $\frac{1}{k!}$

$$\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right) < \left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\ldots\left(1-\frac{k-1}{n+1}\right).$$

□

LEMME 2.9: *On a $p_n < s_n < 3$ pour $n \geq 2$.*

DÉMONSTRATION. On a

$$\begin{aligned}p_n = \left(1+\frac{1}{n}\right)^n &= \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k} \\ &= 1+n\frac{1}{n}+\frac{n(n-1)}{2!}n^{-2}+\cdots+\frac{n(n-1)(n-2)\cdot\ldots\cdot 2\cdot 1}{n!}n^{-n} \\ &< 1+\frac{1}{1!}+\cdots+\frac{1}{n!} = s_n.\end{aligned}$$

et par ailleurs

$$\begin{aligned}s_n &= 2+\frac{1}{2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{1\cdot 2\cdot 3\cdot\ldots\cdot n} \\ &< 2+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{n-1}} = 3-\frac{1}{2^{n-1}} < 3\end{aligned}$$

□

Ces deux lemmes assurent que les suites (p_n) et (s_n) sont croissantes bornées : elles sont donc convergentes. Notons par p_∞, s_∞ les limites respectives. Vu que $p_n \le s_n$, on a $p_\infty \le s_\infty$.

Pour n, N entiers avec $n \ge \mathrm{N}$, on a

$$\begin{aligned} p_n &= 1 + \frac{1}{1!} + \frac{1}{2!}\left(1-\frac{1}{n}\right) + \cdots + \frac{1}{n!}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{n-1}{n}\right) \\ &\ge 1 + \frac{1}{1!} + \frac{1}{2!}\left(1-\frac{1}{n}\right) + \cdots + \frac{1}{\mathrm{N}!}\left(1-\frac{1}{n}\right)\cdots\cdots\left(1-\frac{\mathrm{N}-1}{n}\right) \end{aligned}$$

où on a ôté les termes (positifs) d'indice $k = \mathrm{N}+1, \mathrm{N}+2, \ldots, , n$ dans la première ligne pour avoir la seconde ligne comme minorant. Faisant tendre $n \to \infty$ en laissant N fixe, on obtient $p_\infty \ge s_\mathrm{N}$ pour tout N, puis $p_\infty \ge s_\infty$ et leur égalité $p_\infty = s_\infty$ par suite : on notera par e cette limite.

On peut préciser un peu la position relative de e vis à vis de la suite (p_n).

LEMME 2.10: *On a l'inégalité*

$$\left(1+\frac{1}{n}\right)^n < \mathrm{e} < \left(1+\frac{1}{n}\right)^{n+1}, \quad n > 1$$

La suite $\widetilde{s} = (s_n + 1/(n \cdot n!))$ *est décroissante.*

DÉMONSTRATION. Ce résultat résulte de la décroissance de la suite $\left((1+\frac{1}{n})^{n+1}\right)$ qui résulte à nouveau du bon usage de l'inégalité arithmético-géométrique. Cette décroissance est équivalente à l'inégalité

$$\left(\left[1+\frac{1}{n+1}\right]^{n+2}\right)\frac{1}{n+1} \le \frac{n\left(1+\frac{1}{n+1}\right)+\left(1+\frac{1}{n+1}\right)^2}{n+1} \le 1+\frac{1}{n}$$

La dernière inégalité est démontrée en comparant

$$\begin{aligned} n\left(1+\frac{1}{n+1}\right)+\left(1+\frac{1}{n+1}\right)^2 &= n + \frac{n}{n+1} + 1 + \frac{2}{n+1} + \frac{1}{(n+1)^2} \\ &= \frac{(n+1)^3 + (n+2)(n+1) + 1}{(n+1)^2} \end{aligned}$$

avec $(n+1)(1+1/n) = (n+1)^2/n$: leur différence est

$$\begin{aligned} &\frac{(n+1)^3 + (n+2)(n+1) + 1}{(n+1)^2} - (n+1)^2/n \\ &\qquad = \frac{n[(n+1)^3 + (n+2)(n+1) + 1] - (n+1)^4}{n(n+1)^2} = \frac{-1}{n(n+1)^2} \end{aligned}$$

ce qui confirme l'inégalité annoncée. Finalement

$$\widetilde{s}_{n+1} - \widetilde{s}_n = \frac{1}{(n+1)!} + \frac{1}{(n+1)(n+1)!} - \frac{1}{n \cdot n!} = -\frac{1}{n(n+1)(n+1)!},$$

ce qui assure la décroissance de la suite $\widetilde{s}$. □

Ainsi le nombre d'Euler e est-il la limite des deux suites de rationnels adjacentes (p_n) et $\widetilde{s}_n)$. La première approximation n'est pas très rapide, alors que l'autre suite approche e a une convergence bien meilleure.

THÉORÈME 2.7:

$$0 < \mathrm{e} - \left(1 + \frac{1}{1!} + \cdots + \frac{1}{n!}\right) < \frac{1}{n n!}$$

Le nombre e *est irrationnel.*

DÉMONSTRATION. On a

$$\begin{aligned} e - s_n &= \lim_{k\to\infty}\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots+\frac{1}{(n+k)!}\right)\\ &= \lim_{k\to\infty}\frac{1}{(n+1)!}\left(1+\frac{1}{n+2}+\frac{1}{(n+2)(n+3)}+\cdots+\frac{1}{(n+2)(n+3)\ldots(n+k)}\right)\\ &\le \frac{1}{(n+1)!}\lim_{k\to\infty}\left(1+\frac{1}{n+2}+\frac{1}{(n+2)^2}+\cdots+\frac{1}{(n+2)^{k-1}}\right)\\ &\le \frac{1}{(n+1)!}\frac{1}{1-\dfrac{1}{n+2}} = \frac{n+2}{(n+1)!(n+1)} = \frac{1}{n!n}\frac{n(n+2)}{(n+1)^2} < \frac{1}{n!n}. \end{aligned}$$

Supposons que e soit rationnel : il existe deux entiers p, q avec $q > 1$ tels que

$$0 < \frac{p}{q} - \left(1+\frac{1}{1!}+\cdots+\frac{1}{q!}\right) < \frac{1}{qq!}$$

et donc, en multipliant par $q!$

$$0 < p(q-1)! - q!\left(1+\frac{1}{1!}+\cdots+\frac{1}{q!}\right) < \frac{1}{q}$$

il existerait un entier entre 0 et q^{-1}, ce qui est absurde : le nombre e est irrationnel. □

2.5.5 Approximation de racine carrée

Héron [18] est connu pour sa formule donnant l'aire A d'un triangle en fonction des longueurs de ses côtés ℓ_1, ℓ_2, ℓ_3 et de son demi-périmètre $p = (\ell_1+\ell_2+\ell_3)/2$:

$$\mathrm{A} = \sqrt{p(p-\ell_1)(p-\ell_2)(p-\ell_3)}.$$

Amené donc à calculer des racines carrées, il a proposé la suite définie par récurrence

$$u_{n+1} = \frac{u_n}{2} + \frac{a}{2u_n}, \quad n \ge 0, \qquad u_0 > \sqrt{a}$$

pour approcher la racine carrée d'un réel positif $a > 0$. Avec l'hypothèse $u_0 > \sqrt{a}$, la suite est clairement à termes strictement positifs non nuls. Vu que pour $x > 0$

$$\frac{x}{2} + \frac{a}{2x} = \frac{x^2+a}{2x} = \frac{(x-\sqrt{a})^2}{2x} + \sqrt{a} \ge \sqrt{a},$$

on a $u_n \ge \sqrt{a}$ pour $n \ge 1$ et la suite **u** est décroissante

$$u_{n+1} - u_n = \frac{u_n}{2} + \frac{a}{2u_n} - u_n = \frac{a-u_n^2}{2u_n} \le 0.$$

La suite **u** décroissante minorée est convergente : sa limite $\ell > 0$ (on a remarqué ci-dessous $u_n > \sqrt{a}$) vérifie $\dfrac{\ell}{2} + \dfrac{a}{2\ell} = \ell$ et est donc égale à $\sqrt{a}$. On a la majoration

$$u_n - \sqrt{a} = \frac{u_{n-1}}{2} + \frac{a}{2u_{n-1}} - \sqrt{a} = \frac{(u_{n-1}-\sqrt{a})^2}{2u_{n-1}} \le \frac{(u_{n-1}-\sqrt{a})^2}{2\sqrt{a}}, \quad n \ge 2$$

Ainsi

$$0 \le \frac{u_n-\sqrt{a}}{2\sqrt{a}} \le \frac{(u_{n-1}-\sqrt{a})^2}{(2\sqrt{a})^2} \le \left(\frac{u_{n-2}-\sqrt{a}}{2\sqrt{a}}\right)^{2^2} \le \cdots \le \left(\frac{u_{n_0}-\sqrt{a}}{2\sqrt{a}}\right)^{2^{n-n_0}}$$

18. Héron d'Alexandrie, premier siècle apr. J.-C.

où n_0 est assez grand tel que $\theta = \dfrac{u_{n_0} - \sqrt{a}}{2\sqrt{a}} < 1$. Posant $C = \log_{10}(\theta^{-1})$ et D tel que $10^D = 2\sqrt{a}\theta^{2^{-n_0}}$, on a

$$0 \leq u_n - \sqrt{a} \leq 2\sqrt{a}\theta^{2^{-n_0}}\theta^{2^n} = 10^{D-2^nC}, \quad n \geq n_0.$$

La majoration $u_n - \sqrt{a} \leq 10^{D-2^nC}$ indique 2^nC décimales exactes (à la constante additive D près) pour l'approximation u_n de $\sqrt{a}$: à chaque itération de la suite u_n, il y a doublement du nombre de décimales exactes.

Ce phénomène de convergence très rapide est connu en général pour toute suite **u** définie par récurrence suivant

$$u_{n+1} = u_n - \frac{f(u_n)}{f'(u_n)}$$

qui converge vers le zéro ℓ de la fonction f à supposer que u_1 soit assez proche de la racine ℓ. Cette suite est dite de Newton-Raphson [19], redonnant la suite de Héron pour la fonction $f_a : x \mapsto x^2 - a$.

2.5.6 Série formelle et fonction génératrice

Comme il a été expliqué à la fin de l'étude des suites arithmético-géométriques (cf. section 2.5.1), une suite peut être représentée par une série formelle (sa fonction génératrice), le calcul sur ces séries permettant d'en préciser la forme ainsi que des expressions pour les suites associées. On a étudié les suites sujettes à une récurrence linéaire d'ordre 1 : on va étudier les récurrences d'ordre supérieur, en fait d'ordre 2 pour rester dans la simplicité.

Revenons à quelques généralités sur les séries formelles, généralisation des polynômes. Une série formelle S est une somme formelle de monômes rangés en ordre de degré croissant

$$S = \sum_{n=0}^{+\infty} s_n X^n$$

à coefficients s_n complexes (on peut préférer s_n dans $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, voire $\mathbb{Z}_2$ ou $\mathbb{Z}$). Dénoté $\mathbb{C}[[X]]$, l'espace de séries formelles contient les polynômes et les opérations arithmétiques déployées pour les polynômes s'y prolongent naturellement. Nul souci de la convergence des séries manipulées (si on en venait à substituer une valeur numérique au symbole X), les calculs entre ces séries peuvent être justifiés rigoureusement. Par exemple, les manipulations menant à la formule finale (2.25) peuvent être pleinement justifiées, ou établies directement (par une récurrence par exemple). Pour $S = \sum_{n=0}^{+\infty} s_n X^n$ et $T = \sum_{n=0}^{+\infty} t_n X^n$ on a les opérations

1. addition : $S + T = \sum_{n=0}^{+\infty} (s_n + t_n) X^n$,
2. multiplication par un scalaire : $\lambda S = \sum_{n=0}^{+\infty} \lambda s_n X^n$,
3. multiplication : $ST = \sum_{n=0}^{+\infty} p_n X^n$ avec $p_n = \sum_{k=0}^{n} s_k t_{n-k}$,
4. inversion : $(1-X)^{-1} = \sum_{n=0}^{+\infty} X^n$,
5. séries de séries,
6. produits infinis de séries.

Pour l'opération d'inversion, il faut comprendre simplement que dans l'espace des séries formelles la série $S_0 = \sum_{n=0}^{+\infty} X^n$ vérifie $S_0(1-X) = (1-X)S_0 = 1$ (multiplication bien définie), alors qu'il n'y a pas de polynôme P_0 qui vérifie $P_0(1-X) = 1$. En général, le calcul de l'inverse est un peu délicat : une série formelle $S = \sum_{n=0}^{+\infty} s_n X^n$ est inversible si et seulement si son coefficient s_0 du terme de degré 0 est non nul. En effet sous cette hypothèse, on a $S = s_0(1 - XT)$ pour une certaine série formelle T, l'inversion de S découle de celle de $1 - XT$. La série formelle $\widetilde{T} = 1 + \sum_{n=1}^{+\infty} X^n T^n$ est bien définie vu que le terme $X^n T^n$ ne contient que des monômes de degré au moins n : le terme de degré k de $\widetilde{T}$ provient des k premiers termes de la série T. On vérifie que le produit du membre de droite

$$s_0^{-1} S\widetilde{T} = s_0^{-1}[s_0(1-XT)]\widetilde{T} = (1-XT)\left(1 + \sum_{n=1}^{+\infty} X^n T^n\right) = 1$$

19. Joseph Raphson, v. 1648, Middlesex, Angleterre – v. 1715, Angleterre.

est égal à 1, assurant l'inverse de S comme étant $s_0^{-1}\widetilde{\mathrm{T}}$, le facteur dans le produit du membre de gauche. On écrira par convention $(1-\mathrm{XT})^{-1}$ comme la série formelle $1+\sum_{n=1}^{+\infty}\mathrm{X}^n\mathrm{T}^n$ qui rend inversible S.

Pour les séries de séries ou produits de séries

$$\sum_{n\geq 0}\mathrm{S}_n := \sum_{n\geq 0:}\mathrm{X}^{d_n}\widetilde{\mathrm{S}}_n, \quad \prod_{n\geq 0}(1+\mathrm{S}_n) := \prod_{n\geq 0}(1+\mathrm{X}^{d_n}\widetilde{\mathrm{S}}_n)$$

où la suite (d_n) des degrés minimaux des séries S_n tendent vers $+\infty$ (à moins que la suite de séries (S_n) ne soit un polynôme pour n assez grand), il y a convergence de la série ou du produit dans l'espace des séries formelles.

Ainsi, les calculs algébriques effectués dans l'espace de séries formelles $\mathbb{C}[[\mathrm{X}]]$ développés dans la suite sont pleinement justifiables, sans que nous développions les arguments appropriés plus avant ici.

DÉFINITION 2.11: *À toute suite* **u** *est associée la* série formelle $\mathrm{S}_{\mathbf{u}}(\mathrm{X})$

$$\mathrm{S}_{\mathbf{u}}(\mathrm{X}) = \sum_{n=0}^{\infty} u_n\mathrm{X}^n,$$

dite fonction génératrice *de la suite* **u**.

La manipulation de séries à partir de la fonction génératrice permet parfois de gagner dans la compréhension de la suite **u**, ainsi du premier exemple :

▷ EXEMPLE 2.16: Soit a_n note le nombre de manières de partitionner n en des entiers deux à deux distincts (*i. e.* $n = j_1 + \cdots + j_k$ avec les j_k entiers distincts deux à deux). Alors

$$\sum_{n=0}^{\infty} a_n x^n = \prod_{j=1}^{\infty}(1+x^j) = \prod_{j=1}^{\infty}\frac{1-x^{2j}}{1-x^j} = \prod_{k=0}^{\infty}\frac{1}{1-x^{2k+1}} = \prod_{k=0}^{\infty}\sum_{j_k=0}^{\infty} x^{j_k(2k+1)} = \sum_{n=0}^{\infty} b_n x^n$$

vu la disparition du facteur $1-x^{2j}$ dans les numérateurs et dénominateurs du second produit infini. Le dernier produit infini distingue les entiers somme d'entiers impairs (avec répétition éventuelle). Il en résulte l'égalité du nombre de partitions de n par des entiers distincts avec celui de partitions de n avec des entiers impairs. ◁

Dans le cadre des suites à récurrence linéaire, l'usage des séries formelles permet de donner forme aux suites solution. Reprenons l'exemple des suites de Fibonacci (cf. exemple 2.13).

▷ EXEMPLE 2.17: À la suite **u** vérifiant la relation linéaire $u_{n+2} = u_{n+1} + u_n$ (suite de type Fibonacci) est associée la série formelle $\mathrm{S}_u = \sum_{n=0}^{+\infty} u_n\mathrm{X}^n$. Sommant les relations linéaires pondérées par le monôme X^n pour la relation à l'ordre $n+1$, nous obtenons

$$\sum_{n=0}^{+\infty} u_{n+2}\mathrm{X}^{n+2} = \sum_{n=0}^{+\infty}\left[u_{n+1}\mathrm{X}^{n+2} + u_n\mathrm{X}^{n+2}\right],$$

soit

$$\mathrm{S}_u - u_0 - u_1\mathrm{X} = \mathrm{X}(\mathrm{S}_u - u_0) + \mathrm{X}^2\mathrm{S}_u$$

et donc

$$\mathrm{S}_u = \frac{u_0 + (u_1 - u_0)\mathrm{X}}{1-\mathrm{X}-\mathrm{X}^2}.$$

Le polynôme[20] $1-\mathrm{X}-\mathrm{X}^2$ a comme racines

$$\gamma_+ = \frac{-1+\sqrt{5}}{2} = \frac{2}{1+\sqrt{5}}, \quad \gamma_- = \frac{-1-\sqrt{5}}{2} = \frac{2}{1-\sqrt{5}},$$

20. Ce polynôme P est relié au polynôme P_c caractéristique de la récurrence par $\mathrm{P}_c\left(\mathrm{X}^{-1}\right) = \mathrm{P}(\mathrm{X})$.

de telle sorte que

$$\frac{1}{1-X-X^2} = -\frac{1}{X-\gamma_+}\frac{1}{X-\gamma_-} = \frac{1}{\gamma_+-\gamma_-}\left[\frac{\gamma_+^{-1}}{1-\gamma_+^{-1}X} - \frac{\gamma_-^{-1}}{1-\gamma_-^{-1}X}\right]$$
$$= \frac{1}{\gamma_+-\gamma_-}\left[\sum_{n=0}^{+\infty}\gamma_+^{-n-1}X^n - \sum_{n=0}^{+\infty}\gamma_-^{-n-1}X^n\right],$$

soit finalement

$$S_u = \frac{u_0+(u_1-u_0)X}{\gamma_+-\gamma_-}\left[\sum_{n=0}^{+\infty}\left[\gamma_+^{-n-1}-\gamma_-^{-n-1}\right]X^n\right]. \tag{2.24}$$

Pour $u_0 = u_1 - 1 = 0$, on obtient ainsi

$$S_u = \frac{X}{\gamma_+-\gamma_-}\left[\sum_{n=0}^{+\infty}\left[\gamma_+^{-n-1}-\gamma_-^{-n-1}\right]X^n\right] = \frac{\sum_{n=0}^{+\infty}\left[\gamma_+^{-n-1}-\gamma_-^{-n-1}\right]X^{n+1}}{\sqrt{5}}$$

soit

$$u_n = \frac{\left[\frac{1+\sqrt{5}}{2}\right]^n - \left[\frac{1-\sqrt{5}}{2}\right]^n}{\sqrt{5}}, \quad n \geq 0 \tag{2.25}$$

formule établie par Euler en 1765 et redécouverte par Binet[21] en 1843. Le nombre $(1+\sqrt{5})/2$ est appelé le nombre d'or.

Pour $u_0 = u_1 = 1$, on obtient pour la suite $\mathbf{u}$ les coefficients de la série S_u dans (2.24)

$$u_n = \frac{\gamma_+^{-n-1}-\gamma_-^{-n-1}}{\sqrt{5}} = \frac{\left[\frac{1+\sqrt{5}}{2}\right]^{n+1} - \left[\frac{1-\sqrt{5}}{2}\right]^{n+1}}{\sqrt{5}}.$$

◁

21. Jacques Philippe Marie Binet, 2 février 1786, Rennes – 12 mai 1856, Paris.

Chapitre 3

Dénombrement

« faire partout des dénombrements si entiers, et des revues si générales, que je fusse assuré de ne rien omettre »
R. Descartes, Le discours de la méthode

Le dénombrement, ou analyse combinatoire, a pour but de compter un (ou des) ensemble E (dépendant d'un paramètre n éventuellement), c'est à dire déterminer le cardinal $|\mathrm{E}|$. Au besoin, cet ensemble sera structuré et on cherchera à éviter une énumération globale, élément à élément, surtout quand le dit ensemble est de cardinal grand. En plus de ce comptage, apparaît aussi la tâche d'étiquetage des éléments de E par des nombres, c'est-à-dire la détermination d'une bijection entre E et un autre ensemble plus familier comme $[\![1,n]\!]$ où $n = |\mathrm{E}|$ [1]

Quand ces ensembles sont caractérisés par des propriétés arithmétiques, géométriques ou probabilistes, le dénombrement prendra avantage de ces structures. Ainsi, ces méthodes de comptage sont utilisées dans des domaines variés : probabilités sur des ensembles finis, graphes, théorie des nombres, etc Les résultats d'un décompte (d_n) avec un paramètre n seront éventuellement asymptotiques, *i. e.* un équivalent avec des fonctions classiques, faisant appel à l'analyse fine du comportement de suites associées (d_n) quand n tend vers $+\infty$. L'exemple basique est le cardinal $n!$ des bijections internes à un ensemble E fini de cardinal $|\mathrm{E}| = n$. Les paragraphes apparaissant en petite taille n'ont pas été abordés pendant le cours oral.

3.1 Cardinal

Reprenons les définitions déjà présentées dans le chapitre précédent.

DÉFINITION 3.1: *Deux ensembles sont dits de même cardinal s'il existe une bijection de l'un sur l'autre.*
L'ensemble E *est dit* fini de cardinal $n \in \mathbb{N}^*$ *s'il existe une bijection de* E *sur l'intervalle* $[\![1,n]\!]$. *Par convention, l'ensemble vide a pour cardinal l'entier* 0.
Un ensemble non fini est dit infini. *Un ensemble est dit* dénombrable *s'il a même cardinal que* $\mathbb{N}$.

Si E est fini, son cardinal de E est diversement noté : $\mathrm{card}\,\mathrm{E} = |\mathrm{E}| = \#\mathrm{E}$. Si E n'est pas vide, c'est l'entier n tel que E soit en bijection avec $[\![1,n]\!]$.

1. Pour m,n entiers avec $m \leq n$, la notation $[\![m,n]\!]$ désigne l'intervalle d'entiers naturels compris entre m et n, soit $[\![m,n]\!] = \{m, m+1, \ldots, , n-1, n\}$. Ainsi, $|[\![m,n]\!]| = n-m+1$.

△ REMARQUES 3.1:

1. On montre par récurrence (sur n) que l'intervalle $[\![m,n]\!]$ avec $m \leq n$ est de cardinal $n-m+1$, ou en exhibant la bijection

$$x \in [\![m,n]\!] \longmapsto x-m+1 \in [\![1,n-m+1]\!].$$

2. Décompter un ensemble E est souvent réalisé en construisant une bijection de E sur un ensemble dont le cardinal est connu. La difficulté réside dans cette construction. Par ex. on montre que $\mathbb{Q}$ est en bijection avec $\mathbb{N}$ et qu'il n'y a pas de bijection entre $\mathbb{N}$ et $\mathbb{R}$. ▽

LEMME 3.1: *Si l'ensemble* E *est fini, alors toute partie* F *de* E *est finie ainsi que son complémentaire* $\overline{\mathrm{F}}$ *dans* E*, avec la relation* $|\mathrm{F}| = |\mathrm{E}| - \left|\overline{\mathrm{F}}\right|$.

Tout ensemble infini contient une partie N *en bijection avec l'ensemble des entiers naturels* $\mathbb{N}$.

Un ensemble E *est fini si et seulement si il n'est en bijection avec aucune partie propre* F *(*i. e. *distincte de* E*) de l'ensemble* E.

DÉMONSTRATION. Soit $n \in \mathbb{N}$ le cardinal de l'ensemble fini E : il existe une bijection $\varphi : \mathrm{E} \to [\![1,n]\!]$ qui nous permettra, après avoir traité le cas où $\mathrm{E} = [\![1,n]\!]$, de ramener les résultats établis pour $[\![1,n]\!]$ dans un ensemble E quelconque de cardinal n. Une partie F de $[\![1,n]\!]$ est constituée d'entiers entre 1 et n : ils sont en nombre fini; notons p et q les cardinaux de F et $\overline{\mathrm{F}}$ respectifs. Si F est vide, le cardinal $p = |\mathrm{F}|$ est nul et le complémentaire $\overline{\mathrm{F}}$ dans $[\![1,n]\!]$ est $[\![1,n]\!]$ de cardinal $q = n$: on obtient $|\mathrm{F}| + \left|\overline{\mathrm{F}}\right| = 0 + n = |[\![1,n]\!]|$, soit $p+q = n$. L'égalité vaut aussi si $\mathrm{F} = [\![1,n]\!]$. Si F est non vide et distinct de $[\![1,n]\!]$, la partie F est en bijection avec $[\![1,p]\!]$ en ordonnant dans $[\![1,n]\!]$ ses éléments suivant $a_1 < a_2 < \cdots < a_p$, alors que la partie $\overline{\mathrm{F}}$ est en bijection avec $[\![p+1,p+q]\!]$ suivant l'énumération ordonnée $b_{p+1} < b_{p+2} < \ldots < b_{p+q}$. Les parties F et $\overline{\mathrm{F}}$ sont disjointes, leur union égale à $[\![1,n]\!]$: on en déduit la relation $p+q = n$, soit $|\mathrm{F}| + \left|\overline{\mathrm{F}}\right| = |[\![1,n]\!]|$, ce qui achève de montrer $|\mathrm{F}| + \left|\overline{\mathrm{F}}\right| = |\mathrm{E}|$ pour F une partie de $\mathrm{E} = [\![1,n]\!]$. Le cas général pour E de cardinal n s'ensuit grâce au transfert sur E via la bijection $\varphi : \mathrm{E} \to [\![1,n]\!]$ mentionnée ci-dessus

$$|\mathrm{F}| + \left|\overline{\mathrm{F}}\right| = \left|\varphi(\mathrm{F})\right| + \left|\varphi(\overline{\mathrm{F}})\right| = \left|\varphi(\mathrm{F})\right| + \left|\overline{\varphi(\mathrm{F})}\right| = |[\![1,n]\!]| = \left|\varphi(\mathrm{E})\right| = |\mathrm{E}|, \quad \mathrm{F} \subset \mathrm{E}.$$

Soit E infini. Toute partie F_n finie de E avec n éléments peut être complétée par un élément (n'appartenant pas à F_n) pour constituer une partie F_{n+1} à $n+1$ éléments. Si ce n'était pas le cas, il existerait un entier k et une partie finie F_k égale à E et donc E serait finie. On construit alors une suite $(e_n)_{n\geq 1}$ d'éléments de E en choisissant un e_1 dans E, puis, par récurrence, la suite $(e_1,\ldots,e_n)$ étant déterminée, on lui adjoint un élément e_{n+1} distinct des n premiers éléments $e_1,\ldots,e_n$. L'ensemble $\mathrm{N} = \{e_1,e_2,\ldots,e_n,\ldots\}$ des valeurs de la suite $(e_n)_{n\geq 1}$ convient comme partie N de E en bijection avec $\mathbb{N}$.

Si E est fini de cardinal $|E|$, une partie propre de E est de cardinal inférieur à $|E|-1$ et donc F ne peut être en bijection avec E. Réciproquement et par contraposée, si E est infini, il existe une bijection $\varphi : \mathbb{N} \to N$ avec N partie de E : la partie $E \setminus \{\varphi(0)\}$ est une partie propre de E en bijection avec E via l'application $\Phi : E \to E \setminus \{\varphi(0)\}$ telle que $\Phi(x) = x$ si $x \notin N$ et $\Phi(\varphi(n)) = \varphi(n+1)$ pour $n \in \mathbb{N}$. Ainsi Φ réalise une application de E sur une partie propre de E, ce qui établit la contraposée de la dernière assertion du lemme. □

PROPOSITION 3.1: *Soient* E, F *finis de même cardinal et* $f : E \to F$. *Alors les propriétés de surjectivité, injectivité et bijectivité pour* f *sont équivalentes.*

△ REMARQUE 3.2: Ainsi, si on a $\varphi : E \to F$ entre deux espaces de même cardinal, l'injectivité (surjectivité resp.) de φ suffit à conclure à la bijectivité de φ. Cela permet donc parfois, dans la situation d'égalité des deux cardinaux, d'établir la bijectivité (vue comme un étiquetage des éléments de F par ceux de E) en démontrant la surjectivité (ou l'injectivité) seule. ▽

DÉMONSTRATION. Supposons f surjective. Si f n'est pas injective, il existe p, q distincts tels que $f(p) = f(q)$. On a donc au plus $|E|-1$ images (des points de $E \setminus \{p, q\}$ outre l'unique image de p et q). Ainsi f n'est pas surjective, ce qui contredit l'hypothèse.

Supposons f injective. Supposons f non surjective. Ainsi il existe $p \in F$ qui n'a pas d'antécédent et donc $f(E) \subset F \setminus \{p\}$ et par suite $|E| = |f(E)| \leq |F \setminus \{p\}| < |F|$, l'inégalité $|E| < |F|$ étant contradictoire avec l'hypothèse de l'égalité $|E| = |E|$ des cardinaux.

Le reste des implications coule de source. □

△ REMARQUE 3.3: L'hypothèse de finitude sur les ensembles E et F de la proposition précédente est essentielle : les équivalences qu'elle affirme ne sont pas valides pour un ensemble infini, par exemple $\mathbb{N}$: l'application $S : n \in \mathbb{N} \mapsto n+1 \in \mathbb{N}$ n'est pas surjective bien qu'injective, l'application $D : n \in \mathbb{N} \mapsto \lfloor n/2 \rfloor \in \mathbb{N}$ est surjective, sans être injective.

Si E est infini, il contient une partie N en bijection $\varphi : N \to \mathbb{N}$ avec $\mathbb{N}$ d'après le lemme 3.1. Les applications précédentes S, N sur $\mathbb{N}$ transportées par φ sur N en $S_\varphi = \varphi^{-1} \circ S \circ \varphi$, $D_\varphi = \varphi^{-1} \circ D \circ \varphi$ sur N peuvent être prolongées à E, en les applications $\widetilde{S}_\varphi, \widetilde{D}_\varphi$ définies suivant

$$\widetilde{D}_\varphi(e) = \begin{cases} D_\varphi(e) \text{ si } e \in N \\ e \text{ si } e \in E \setminus N, \end{cases} \qquad \widetilde{S}_\varphi(e) = \begin{cases} S_\varphi(e) \text{ si } e \in N \\ e \text{ si } e \in E \setminus N. \end{cases}$$

Les applications $\widetilde{D}_\varphi$ et $\widetilde{S}_\varphi$ sont surjectives et injectives resp., mais ni injectives ni surjectives resp. ▽

PROPOSITION 3.2: *Soient* $F_1, \ldots, F_k$ *des ensembles finis non vides.*
Le produit cartésien $F_1 \times \cdots \times F_k$ *est fini, de cardinal* $\prod_{j=1}^{k} |F_j|$.

DÉMONSTRATION. On effectue une récurrence sur le nombre k de facteurs avec la propriété

$$\text{« } \mathcal{C}[k] : \quad \text{Le cardinal de } \mathrm{F}^k \text{ est } |\mathrm{F}|^k \text{ ».}$$

Pour $k = 1$, le produit est réduit à un facteur, la propriété est vraie. Supposons vraie la propriété au rang k : un élément $(f_1, \ldots, f_{k+1})$ du produit $\prod_{j=1}^{k+1} \mathrm{F}_j$ à $k+1$ facteurs est déterminé par le choix de $(f_1, \ldots, f_k)$ dans le produit $\mathrm{F}_1 \times \cdots \times \mathrm{F}_k$, soit $\prod_{j=1}^{k} |\mathrm{F}_j|$ possibilités d'après l'hypothèse de récurrence, et de $|\mathrm{F}_{k+1}|$ choix pour $f_{k+1} \in \mathrm{F}_{k+1}$, soit $\left[\prod_{j=1}^{k} |\mathrm{F}_j|\right] |\mathrm{F}_{k+1}|$ choix possibles en tout, ce qui est la propriété au rang $k+1$. □

△ REMARQUE 3.4: Si on prend les F_i de la proposition tous égaux à l'ensemble F, le produit F^n et l'ensemble $\mathscr{F}([\![1, n]\!], \mathrm{F})$ des applications de $[\![1, n]\!]$ dans F ont mêmes cardinaux. Les bijections sont

$$(e_1, \ldots, e_n) \in \mathrm{F}^n \mapsto f := (i \in [\![1, n]\!] \mapsto e_i \in \mathrm{F}) \in \mathscr{F}([\![1, n]\!], \mathrm{F})$$

et

$$f \in \mathscr{F}([\![1, n]\!], \mathrm{F}) \mapsto (f(1), \ldots, f(n)) \in \mathrm{F}^n.$$

Leur cardinal (comme entier naturel) est donc $|\mathscr{F}([\![1, n]\!], \mathrm{F})| = |\mathrm{F}^n| = |\mathrm{F}|^n$. ▽

PROPOSITION 3.3: *Soient* E, F *des ensembles finis non vides. L'ensemble* $\mathscr{F}(\mathrm{E}, \mathrm{F})$ *des applications de* E *dans* F *est fini, de cardinal* $|\mathrm{F}|^{|\mathrm{E}|}$.

DÉMONSTRATION. Avec une bijection $\varphi : [\![1, n]\!] \to \mathrm{E}$, on construit l'application

$$\Phi : f \in \mathrm{F}^{\mathrm{E}} \mapsto f \circ \varphi \in \mathrm{F}^{[\![1,n]\!]},$$

qui est une bijection de F^{E} sur $\mathrm{F}^{[\![1,n]\!]}$, d'application réciproque donnée par

$$\Phi^{-1} : g \in \mathrm{F}^{[\![1,n]\!]} \mapsto g \circ \varphi^{-1} \in \mathrm{F}^{\mathrm{E}}.$$

Il suffit de montrer l'assertion $|\mathrm{F}^{\mathrm{E}}| = |\mathrm{F}|^{|\mathrm{E}|}$ pour $\mathrm{E} = [\![1, n]\!]$, ce qui a été établi dans la remarque suivant la proposition précédente 3.2. □

△ REMARQUE 3.5: La formule $\left|\mathrm{F}^{\mathrm{E}}\right| = |\mathrm{F}|^{|\mathrm{E}|}$ justifie la notation F^{E} pour l'ensemble des applications de E dans F. On utilise aussi la notation $\mathscr{F}(\mathrm{E}, \mathrm{F})$. ▽

Une partie A de l'ensemble E est caractérisée par l'application $\chi_{\mathrm{A}} : \mathrm{E} \to \mathbb{Z}_2$ définie suivant

$$\chi_{\mathrm{A}}(x) = \begin{cases} 1 & \text{si } x \in \mathrm{A}, \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, avec $\mathbb{Z}_2$ identifié naturellement avec $\{0, 1\}$, l'application

$$\mathrm{A} \in \mathscr{P}(\mathrm{E}) \longmapsto \chi_{\mathrm{A}} \in (\mathbb{Z}_2)^{\mathrm{E}} = \mathscr{F}(\mathrm{E}, \{\mathbb{Z}_2\})$$

est une bijection de l'ensemble des parties $\mathscr{P}(\mathrm{E})$ de E sur l'ensemble $(\mathbb{Z}_2)^{\mathrm{E}}$ des applications de E vers $\mathbb{Z}_2 = \{0, 1\}$. Munissons $\mathbb{Z}_2$ de l'addition et de la multiplication

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

TABLE III.1 – Addition et multiplication dans $\mathbb{Z}_2$.

induites par celles de $\mathbb{Z}$ (cf. tableau III.1). Pour deux applications $f, g : E \to \mathbb{Z}_2$, ces opérations sont utilisées pour induire la somme $f+g$ et le produit fg des deux applications : par définition, $(f+g)(x) := f(x)+g(x)$ et $fg(x) := f(x)g(x)$ pour tout $x \in E$. L'ensemble $(\mathbb{Z}_2)^E = \mathscr{F}(E, \{0,1\})$ est muni d' opérations algébriques (produit, addition) en correspondance avec les opérations ensemblistes (intersection, différence symétrique) définies en terme d'algèbre de Boole (cf. proposition 1.2 de la première partie).

$$\chi_{A\cap B} = \chi_A \chi_B, \quad \chi_{A\cup B} = \chi_A + \chi_B - \chi_{A\cap B}, \quad \chi_A + \chi_B = \chi_{A\Delta B}, \quad \chi_{\overline{A}} = 1 - \chi_A.$$

Si l'ensemble E est fini, on a vu dans le lemme 3.2 que $\left|(\mathbb{Z}_2)^E\right| = |\mathbb{Z}_2|^{|E|} = 2^{|E|}$, on a donc établi la première partie de la proposition suivante

PROPOSITION 3.4: *Soit* E *un ensemble fini. Alors l'ensemble* $\mathscr{P}(E)$ *des parties de* E *est fini de cardinal* $2^{|E|}$.
Si E *est infini, il n'y a pas de surjection de* E *sur* $\mathscr{P}(E)$.

DÉMONSTRATION. On peut aussi prouver la première assertion par récurrence en considérant uniquement les ensembles $[\![1,n]\!]$. En effet, une bijection φ entre E et F induit la bijection entre les ensembles de parties

$$\Phi : A \in \mathscr{P}(E) \mapsto \varphi(A) \in \mathscr{P}(F)$$

de bijection réciproque

$$\Phi^{-1} : B \in \mathscr{P}(F) \mapsto \varphi^{-1}(B) \in \mathscr{P}(E).$$

Il suffit donc d'établir la formule du cardinal de l'ensemble des parties pour les intervalles entiers $[\![1,n]\!]$. La propriété de récurrence pour $n \geq 1$ est

$$\mathcal{C}[n] : \text{le cardinal de } \mathscr{P}([\![1,n]\!]) \text{ est } 2^n.$$

Elle est vraie pour $n = 1$: $\mathscr{P}([\![1,1]\!]) = \{\emptyset, \{1\}\}$. Supposons l'assertion vraie pour l'entier n. Les parties de l'ensemble $[\![1,n+1]\!]$ sont de deux sortes, exclusives l'une de l'autre : celles qui contiennent l'entier $n+1$, celles qui ne le contiennent pas. Ainsi l'ensemble P des parties du premier type est en bijection avec l'ensemble S de celles du second type en ôtant l'entier $n+1$ à chacune des parties de P, soit $|P| = |S|$. De plus, les parties P et S sont disjointes, avec union l'ensemble $\mathscr{P}([\![1,n+1]\!])$, ainsi

$|\mathscr{P}([[1,n+1]])| = |\mathrm{P}| + |\mathrm{S}|$. Enfin, la partie S est en bijection avec l'ensemble des parties de $[[1,n]]$, soit $|\mathrm{S}| = |\mathscr{P}([[1,n]])| = 2^n$ d'après l'hypothèse de récurrence. On a donc

$$|\mathscr{P}([[1,n+1]])| = |\mathrm{P}| + |\mathrm{S}| = 2|\mathrm{S}| = 2|\mathscr{P}([[1,n]])| = 2\cdot 2^n = 2^{n+1}$$

ce qui établit la formule au rang $n+1$ et achève la démonstration par récurrence. La formule est aussi vraie pour $n=0$: $\mathscr{P}(\emptyset) = \{\emptyset\}$ de cardinal 1.

Supposons qu'il existe une surjection de E sur $\mathscr{P}(\mathrm{E})$. Soit A la partie de E des éléments $e \in \mathrm{E}$ hors de $f(e)$, *i. e.*

$$\mathrm{A} = \left\{e \in \mathrm{E} | e \notin f(e)\right\}.$$

Par surjectivité, il existe un élément $a \in \mathrm{E}$ tel que $\mathrm{A} = f(a)$. L'élément a n'est ni dans A (sinon, on aurait $a \in \mathrm{A} = f(a)$, et donc a hors de $f(a) = \mathrm{A}$: contradictoire!), ni hors de A (sinon, $a \in f(a) = \mathrm{A}$, impliquant $a \in \mathrm{A}$, contradictoire!). □

3.2 Décompositions (somme, produit, partition)

De multiples dénombrements sont basés sur l'un des deux principes suivants (on les a déjà utilisés dans la démonstration des premiers alinéa de la proposition 3.2 et du lemme 3.1) :

— *Principe de la somme* : choisir un objet a parmi m ou (indépendamment) un objet b parmi n, c'est effectuer un choix d'un des objets a ou b avec $m+n$ choix,

— *Principe du produit* : choisir un objet a parmi m, puis choisir un objet b parmi n, c'est choisir les objets a puis b de $m\cdot n$ façons.

Ces deux situations se traduisent en termes ensemblistes

— Si A et B sont deux parties finies disjointes d'un ensemble E, alors la partie $\mathrm{A}\cup\mathrm{B}$ est finie et $|\mathrm{A}\cup\mathrm{B}| = |\mathrm{A}| + |\mathrm{B}|$.

— Si A et B sont deux ensembles finis, alors le produit $\mathrm{A}\times\mathrm{B}$ est fini et $|\mathrm{A}\times\mathrm{B}| = |\mathrm{A}|\cdot|\mathrm{B}|$.

À ces situations s'ajoute le comptage par une partition[2] provenant d'une application surjective[3]

LEMME 3.2: *Soit* $f : \mathrm{E} \to \mathrm{F}$ *surjective avec* E *fini. Alors* F *est fini et*

$$|\mathrm{E}| = \sum_{y\in\mathrm{F}} \left|f^{-1}(y)\right|.$$

2. Une partition de l'ensemble E est une collection $(\mathrm{A}_i)_{i\in\mathrm{I}}$ de parties, appelées atomes, de E deux à deux disjointes et dont l'union $\cup_{i\in\mathrm{I}}\mathrm{A}_i$ est égale à E tout entier. Il se peut que certains atomes soient la partie vide, même si souvent ce n'est pas le cas.

3. La condition de surjectivité est souvent affirmée, afin semble-t-il d'éviter des parties vides dans la partition de $\mathrm{E} = \cup_{y\in\mathrm{F}} f^{-1}(y)$ et accessoirement de montrer que F est fini : elle peut disparaître.

DÉMONSTRATION. On a $E = \bigcup_{y\in F} f^{-1}(y)$ où les parties $f^{-1}(y)$, avec $y \in F$, sont non vides, deux à deux distinctes. Les parties $f^{-1}(y)$ de E sont de cardinal fini non nul. L'ensemble E étant fini et chaque $f^{-1}(y)$ de cardinal au moins 1, on a $|E| \geq \sum_{y\in F} 1 \geq |F|$ et l'ensemble F est aussi fini. Les parties $f^{-1}(y)$ étant disjointes et d'union E, la somme de leurs cardinaux est le cardinal de E. □

▷ EXEMPLES 3.1:

3.1.1 Depuis 2009, les codes minéralogiques françaises sont constitués de 2 lettres, 3 chiffres, puis 2 lettres. Le triplet de chiffres débute par 001 (et se termine en 999), Les lettres *I*, *O* et *U* sont exclues, les blocs *SS* et *WW* sont exclues dans la partie gauche, le bloc *SS* dans le bloc de droite

$$N = [(23 \times 23) - 2] \times 999 \times [(23 \times 23) - 1] = 277\,977\,744.$$

Introduit en 1950, l'ancien système basé sur les 101 départements contenait un bloc de 1 à 4 chiffres, un bloc de 1 à 3 lettres (avec des exclusions de combinaison, *PQ*, *SS* par ex.) et le code du département dans le bloc de droite

3.1.2 Soit $p_1 < p_2 < \ldots < p_n$ des entiers premiers et $a_1 < \cdots < a_n$ des entiers positifs. Le nombre des diviseurs entiers naturels du produit $\prod_{i=1}^n p_i^{a_i}$ est $\prod_{i=1}^n (1 + a_i)$. En effet, un diviseur du produit est caractérisé par la décomposition $\prod_{i=1}^n p_i^{k_i}$ avec $0 \leq k_i \leq a_i$, soit $1 + a_i$ choix pour l'exposant k_i.

3.1.3 Bourbaki [4] énonce le principe des bergers. La tradition décrit un berger comptant les pattes de son troupeau pour en déduire le nombre de moutons : il use donc de l'application $m : P \to M$ qui associe à une patte son mouton propriétaire. On a donc $|P| = 4|M|$ soit $|M| = |P|/4$. ◁

Avant de compter les permutations de E, introduisons la fonction *factorielle*, fonction à valeurs entières ultra-présente dans les problèmes de dénombrement.

DÉFINITION 3.2: *La factorielle d'un entier n non nul est le nombre entier noté $n!$ égal au produit des entiers de 1 à n. Par convention, on pose $0! = 1$,*

La factorielle $n \in \mathbb{N} \mapsto n! \in \mathbb{N}$ est un exemple typique d'une fonction définie récursivement :

```
def factorial(n):
   if n=1:
      return(1)
   else:
      return(factorial(n-1) * n)
```

La convention $0! = 1$ permet souvent d'élargir des formules de dénombrement pour des valeurs nulles des variables. La notation $n!$ a été introduite au début du XIXe siècle par Kramp [4].

La factorielle $n \in \mathbb{N} \mapsto n! \in \mathbb{N}$ est une fonction à croissante très rapide (comme bien d'autres fonctions combinatoires) : le calcul de ses valeurs pose des problèmes du fait de sa croissance extrêmement rapide : elle domine toute fonction polynomiale, toute fonction exponentielle. Pour un jeu à 32 cartes, une bijection $f \in \mathfrak{S}([\![1,32]\!])$ dans lui même correspond à la donne $f(1), f(2), \ldots, f(32)$ une fois une donne de référence $1, 2, \ldots, 32$ fixée par une numérotation des cartes de 1 à 32 : il y a 32! donnes possibles [5]

$$32! = 263130836933693530167218012160000000$$

soit $32! \simeq 2.631 \cdot 10^{35}$. Pour décrire la croissance de la factorielle, on a la formule de Stirling [6] donnant un équivalent de $n!$

$$n! \simeq \sqrt{2\pi n}\left(\frac{n}{e}\right)^n, \qquad n \to +\infty$$

4. Christian Kramp, 8 juillet 1760, Strasbourg – 13 mai 1826, Strasbourg.
5. Les calculs ont été réalisés avec `sagemath`.
6. James Stirling, mai 1692, Garden, Stirling – 5 décembre 1770, Édimbourg.

ou encore soit

$$32! \sim_{\text{Stir.}} 1.4667 \cdot 10^{42}, \quad 52! \simeq 8.065 \cdot 10^{67} \sim_{\text{Stir.}} 8.052 \cdot 10^{67}, \quad 78! \simeq 1.1324 \cdot 10^{115} \sim_{\text{Stir.}} 1.1312 \cdot 10^{115}$$

pour des jeux de 32, 52 et 78 cartes.

Dénombrons les *permutations*[7] d'un ensemble fini E : une permutation de E est une application bijective de E dans E.

THÉORÈME 3.1: *Soit* E *fini de cardinal* n. *L'ensemble* $\mathfrak{S}(\mathrm{E})$ *des permutations de* E *est fini, de cardinal* $n!$.

DÉMONSTRATION. Soit φ une bijection de E sur $[\![1,n]\!]$: elle induit une bijection $\Phi : f \in \mathfrak{S}(\mathrm{E}) \mapsto \varphi \circ f \circ \varphi^{-1} \in \mathfrak{S}([\![1,n]\!])$. Ainsi, il suffit de montrer le théorème pour les permutations de l'ensemble $[\![1,n]\!]$. Une telle permutation f est un arrangement ordonné, sans répétition de ces n éléments. Pour définir f, on choisit l'image $f(1)$ du premier élément parmi ces n éléments en l'enlevant de $[\![1,n]\!]$, puis la seconde $f(2)$ parmi les $n-1$ éléments restants de $[\![1,n]\!]$ en l'ôtant pareillement, puis la troisième $f(3)$ ..., et ce jusqu'au dernier élément restant. On détermine ainsi une permutation f en n étapes : il y a n choix possibles pour le $f(1)$ de la première étape, $n-1$ choix pour le $f(2)$ de la deuxième étape, ..., et finalement (sans choix véritable de possible) 1 élément parmi $[\![1,n]\!] \setminus \{f(1),\dots,f(n-1)\}$, soit $n(n-1)\dots 2\times 1 = n!$ permutations possibles[8]. □

3.3 Arrangements et combinaisons

DÉFINITION 3.3: *Soit* E *un ensemble de cardinal* $n = |\mathrm{E}| > 0$ *et* $k \in [\![1,n]\!]$. *Un* arrangement *(sans répétition) de* k *éléments de l'ensemble* E, *ou de* k *objets parmi* n, *est le choix de* k *éléments distincts dans* E, *avec numérotation de* 1 *à* k *de ces éléments. Un arrangement de* k *éléments dans* E *s'identifie à une injection de* $[\![1,k]\!]$ *dans* E.

PROPOSITION 3.5: *Soient* k,n *des entiers avec* $1 \le k \le n$. *Le nombre* A_n^k *d'arrangements à* k *objets parmi* n *est donné par*

$$\mathrm{A}_n^k = n(n-1)\dots(n-(k-1)) = \frac{n!}{(n-k)!}.$$

Si $k > n$, *il n'y a pas d'arrangement à* k *éléments parmi* n.

7. Le terme de *substitution*, voire *transformation* est aussi employé, induisant la notation $\mathfrak{S}(\mathrm{E})$ pour l'ensemble des bijections de E dans E.

8. Par exemple, on écrit 376498521 pour définir une permutation f de $[\![1,9]\!]$, le i-ème chiffre étant $f(i)$ pour $i \in [\![1,9]\!]$.

DÉMONSTRATION. Le calcul de A_n^k est analogue au décompte des permutations : le décompte se fait en k étapes indépendantes, avec estimation du nombre de choix possibles à chaque étape :

— n possibilités lors du premier choix,
— $n-1$ possibilité lors d'une seconde étape,
— ...
— $n-k+1$ lors de la k-ème étape

soit

$$\begin{aligned} A_n^k &= n(n-1)\dots(n-k+1) \\ &= n(n-1)\dots(n-k+1)\frac{(n-k)(n-k-1)\dots 2\times 1}{(n-k)(n-k-1)\dots 2\times 1} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

choix possibles au final. □

▷ EXEMPLE 3.2: Un alphabet à 26 lettres permet de construire $A_{26}^3 = 26\cdot 25\cdot 24 = 15\,600$ mots de 3 lettres distinctes deux à deux. Sans imposer des lettres distinctes, on peut élaborer $26^3 = 17\,576 = |\mathscr{F}(\{1,2,3\},[\![1,26]\!])|$ mots de 3 lettres. ◁

DÉFINITION 3.4: *Soit* E *un ensemble de cardinal* $n = |E| > 0$ *et* $k \in [\![0,n]\!]$. *Une* combinaison[9] *de* k *éléments pris dans l'ensemble* E *de cardinal* n *(ou de* k *éléments parmi* n*) est une partie à* k *éléments dans l'ensemble* E.

▷ EXEMPLE 3.3: Dans $[\![1,4]\!]$, on a 6 combinaisons à 2 éléments parmi 4 : $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$ et $\{3,4\}$.

Il y a 12 arrangements de 2 éléments parmi 4 : $(1,2)$, $(2,1)$, $(1,3)$, $(3,1)$, $(1,4)$, $(4,1)$, $(2,3)$, $(3,2)$, $(2,4)$, $(4,2)$, $(3,4)$ et $(4,3)$.

Il y a une seule combinaison de 0 élément parmi n éléments, à savoir l'ensemble vide $\emptyset$. ◁

△ REMARQUES 3.6:

1. Les nombres de combinaison $\binom{n}{k}$ apparaissent dans le développement du binôme (cf. ($\mathcal{R}[n]$)), ce qui justifie la définition de *coefficient binomial*.
2. Une combinaison est une liste d'éléments sans répétition, ni ordre.
3. Les coefficients binomiaux $\binom{n}{k}$ pour des petites valeurs de k sont simples et valent d'être calculés de manière élémentaire

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{2} = \frac{n(n-1)}{2}$$

9. On parle de *bloc* aussi.

et correspondent au nombre de parties vides, de parties à 1 élément (singletons) et de parties à 2 éléments resp. d'un ensemble à n éléments. Le nombre de parties à 2 éléments parmi n s'obtient à partir des n^2 paires (k,ℓ), d'où on a retiré les paires doubles (k,k) et regroupé les deux paires symétriques $(k,l),(l,k)$ pour en faire la partie $\{k,l\}$.

4. Il y a d'autres notations pour ce coefficient binomial : $\binom{n}{k} = C_n^k = C_{n,k}$. ▽

PROPOSITION 3.6: *Soient k,n des entiers avec $0 \leq k \leq n$. Le nombre $\binom{n}{k}$ de combinaisons de k éléments/objets parmi n est égal à*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n\cdot(n-1)\cdot\cdots\cdot(n-k-1)}{k!}.$$

Si $k > n$, il n'y a pas de combinaisons de k parmi n.

DÉMONSTRATION. Dans une combinaison de k éléments parmi n, les éléments ne sont pas ordonnés : à chaque combinaison (ou sous-ensemble) de k éléments correspondent $k!$ arrangements, soit

$$\binom{n}{k} = C_{n,k} = C_n^k = \frac{A_n^k}{k!} = \frac{n!}{(n-k)!k!}.$$

On peut reprendre la démonstration en utilisant le principe de la surjection. Soit $0 < k \leq n$, $\mathscr{A}_k(E)$ l'ensemble des injections $\varphi : [\![1,k]\!] \to E$, $\mathscr{B}_k(E)$ l'ensemble des combinaisons à k éléments dans E. On a l'application

$$\Phi : \varphi \in \mathscr{A}_k(E) \longmapsto \varphi([\![1,k]\!]) \in \mathscr{B}_k(E)$$

qui est surjective. Vu que $B \in \mathscr{B}_k(E)$ est de cardinal k, l'image réciproque $\Phi^{-1}(B)$ est constituée des injections d'image B au nombre de $k!$. Ainsi

$$|\mathscr{A}_k(E)| = \sum_{B\in\mathscr{B}_k(E)} \left|\Phi^{-1}(B)\right| = \sum_{B\in\mathscr{B}_k(E)} k! = |\mathscr{B}_k(E)|\,k!$$

On a vu $|\mathscr{A}_k(E)| = \dfrac{n!}{(n-k)!}$, ainsi

$$|\mathscr{B}_k(E)| = \frac{n!}{(n-k)!k!},$$

ce qui conclut. On aura remarqué que $\binom{n}{0} = 1$ correspondant à l'unique partie vide.

□

▷ EXEMPLES 3.4:

3.4.1 Il y a $\binom{4}{2} = 4\cdot 3/2! = 6$ parties à 2 éléments dans un ensemble de cardinal 4 : $\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}$.

3.4.2 On veut tester la compatibilité de 15 médicaments en groupes de 4. Il y a $\binom{15}{4} = 15\cdot 14\cdot 13\cdot 12/4! = 1\,365$ groupes de 4 médicaments possibles. ◁

Pour l'interprétation combinatoire des nombres de combinaison de k éléments parmi n, la fonction binomiale $\binom{n}{k}$ a des arguments entiers k, n avec $n \geq k \geq 0$. Cette fonction peut être prolongée à une fonction définie sur $\mathbb{N} \times \mathbb{R}$

$$(k,n) \in \mathbb{N} \times \mathbb{R} \longmapsto \binom{n}{k} = \begin{cases} \dfrac{n(n-1)\ldots(n-k+1)}{k!} & \text{si } k > 0, \\ 1 & \text{si } k = 0, \\ 0 & \text{si } k < 0. \end{cases}$$

On remarquera que $\binom{n}{n+p} = 0$ si $p > 0$.

Les coefficients binomiaux $\binom{n}{k}$ obéissent à de multiples relations (cf. [8]). On en a sélectionné 9 dans le tableau III.2.

1.	$\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$	$p \geq k \geq 0$	développement factoriel
2.	$\binom{p}{k} = \binom{p}{p-k}$	$p \geq 0$	symétrie
3.	$\binom{p}{k} = \dfrac{p}{k}\binom{p-1}{k-1}$	$k \neq 0$	absorption/extraction
4.	$\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$		addition/induction
5.	$\binom{p}{m}\binom{m}{k} = \binom{p}{k}\binom{p-k}{m-k}$		transformation trinomiale
6.	$\sum_{k=0}^{p}\binom{p}{k}x^k y^{p-k} = (x+y)^p$	$p \geq 0$	binôme
7.	$\binom{p+q}{k} = \sum_{\ell=0}^{k}\binom{p}{\ell}\binom{q}{k-\ell}$		Convolution de Vandermonde
8.	$\sum_{k=m}^{n}\binom{k}{m} = \binom{n+1}{m+1}$	$n \geq m \geq 0$	sommation du haut
9.	$\sum_{k=0}^{n}\binom{m+k}{k} = \binom{m+n+1}{n}$	$n, m \geq 0$	sommation parallèle

TABLE III.2 – Coefficients binomiaux : 9 identités remarquables, k, n, p, q entiers, éventuellement avec quelques restrictions.

DÉMONSTRATION. Les identités du tableau peuvent être établies en général soit suivant le calcul des factorielles, soit par une interprétation combinatoire (décompte

d'un ensemble de deux manières différentes ou explicitation d'une bijection entre deux ensembles dont l'un a son cardinal connu).

1. Valable pour $p \geq k \geq 0$, ce développement en factorielles provient de la définition.

2. Considérons la bijection de $\mathscr{P}([\![1,p]\!])$ dans lui-même qui fait correspondre à une partie A de k éléments son complémentaire $\overline{\mathrm{A}}$ à $p-k$ éléments dans $[\![1,p]\!]$, qui induit une bijection de la partie des combinaisons à k éléments parmi p sur celle des combinaisons à $p-k$ éléments parmi p.

3. Au sein d'un groupe de p personnalités, on veut choisir un comité de k personnes avec un président : il y a $\binom{p}{k}$ choix possibles de comité et donc $\binom{p}{k}k$ choix possibles au final pour le président et le comité. On peut aussi commencer par choisir le président, avec p choix de présidents, qu'on complète par le choix de $k-1$ membres parmi les $p-1$ personnalités restantes : on obtient au total $p\binom{k-1}{p-1}$ possibilités, soit au final l'égalité $\binom{p}{k}k = p\binom{p-1}{k-1}$.

   On peut aussi développer les définitions factorielles des deux membres de l'égalité (qui n'explique guère la méthode précédente basée sur un double comptage)

$$\frac{p}{k}\binom{p-1}{k-1} = \frac{p(p-1)!}{k(k-1)!(p-k)!} = \frac{p!}{k!(p-k)!} = \binom{p}{k}$$

4. Soit E fini de cardinal p. On fixe un élément e de E. Une combinaison A à k éléments est de deux sortes. En premier lieu, la combinaison A contient e et alors A est de la forme $\mathrm{A}' \cup \{e\}$ avec A' combinaison de $k-1$ éléments de $\mathrm{E} \setminus \{e\}$, il y a donc $\binom{p-1}{k-1}$ combinaisons de cette sorte. Dans le second type, la combinaison A ne contient par e et s'identifie dons à une combinaison de k éléments de $\mathrm{E} \setminus \{e\}$, soit $\binom{p-1}{k}$ possibles. On obtient donc $\binom{p}{k} = \binom{p-1}{k-1} + \binom{p-1}{k}$.

   Cette relation est lue sur le tableau triangulaire de Pascal [10] des valeurs de ces coefficients binomiaux. Dans ce tableau triangulaire III.4 qui liste ligne par ligne les coefficients binomiaux des combinaisons de $k = 0, 1, \ldots, p-1, p$ objets parmi p, on obtient un coefficient $\binom{p}{\ell}$ par somme des deux coefficients qui l'encadrent dans la ligne immédiatement supérieure : sont distingués sur notre triangle III.4 les sommes $3+3=6$ et $35+21=56$.

5. Dans un ensemble E de cardinal $p = |\mathrm{E}|$, on énumère les combinaisons A de m objets parmi p, puis les combinaisons B de k objets parmi m. Cette succession de choix est équivalente au choix de combinaisons $\widetilde{\mathrm{B}}$ de k objets parmi p, suivi du choix de combinaisons $\widetilde{\mathrm{A}}$ de $m-k$ objets parmi $p-k$, avec $\mathrm{A} = \widetilde{\mathrm{A}} \cup \widetilde{\mathrm{B}}$ et $\mathrm{B} = \widetilde{\mathrm{B}}$. L'identité $\binom{p}{m}\binom{m}{k} = \binom{p}{k}\binom{p-k}{m-k}$ en résulte. Elle peut aussi être

10. Blaise Pascal, 19 juin 1623, Clermont – 19 août 1662, Paris.

obtenue par développement factoriel :

$$\binom{p}{m}\binom{m}{k} = \frac{p!}{m!(p-m)!}\frac{m!}{k!(m-k)!} = \frac{p!}{k!(m-k)!(p-m)!}$$
$$= \frac{p!}{k!(p-k)!}\frac{(p-k)!}{(m-k)!(p-m)!} = \binom{p}{k}\binom{p-k}{m-k}$$

6. La formule du binôme de Newton a été établie au premier chapitre (cf. $\mathcal{R}[n]$ du Lemme 1.2), où il a été fortement utilisé la troisième formule dite d'addition/induction ci-dessus. D'autres identités entre coefficients binomiaux proviennent de cette formule du binôme par des choix judicieux des x, y, soit $x = y = 1$ (on a $2^p = \sum_{k=1}^{p}\binom{p}{1}$: on justifie cette égalité combinatoirement en comptant dans $\mathscr{P}([\![1,p]\!])$ les 2^n parties suivant leur cardinal k de 0 à p), $x = -y = 1$, $x = 1, y = \mathrm{i}$ (et prise de la partie réelle) ou après dérivation de la formule du binôme avec $y = 1$.

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n \qquad \sum_{k=0}^{n}\binom{n}{k}(-1)^k = 0$$
$$\sum_{k=0}^{n}\binom{n}{2k}(-1)^k = 2^{n/2}\cos(n\pi/4) \qquad \sum_{k=0}^{n}k\binom{n}{k}x^{k-1} = n(1+x)^{n-1}$$

7. On applique le développement binomial aux différents facteurs de l'identité

$$(x+y)^{p+q} = (x+y)^p(x+y)^q$$

et on sélectionne dans les deux membres de cette égalité

$$\sum_{k=0}^{p+q}\binom{p+q}{k}x^k y^{p+q-k} = \left[\sum_{\ell=0}^{p}\binom{p}{\ell}x^\ell y^{p-\ell}\right]\left[\sum_{n=0}^{q}\binom{q}{n}x^n y^{q-n}\right]$$

le monôme de type $x^k y^{p+q-k}$ à gauche, les produits de type $x^\ell y^{p-\ell}x^n y^{q-n}$ avec $\ell + n = k$ (ℓ variant de 0 à k) à droite.

8. Soient $n+1$ tickets numérotés de 0 à n. L'entier $m \leq n$ étant fixé, on va dénombrer les $\binom{n+1}{m+1}$ combinaisons de $m+1$ parmi $n+1$, en les regroupant suivant le numéro k le plus haut des $m+1$ tickets de chaque combinaison. Soit $k \in [\![m,n]\!]$. À la prise $\{0 \leq n_1 < n_2 < \ldots < n_m < n_{m+1} = k\}$ de $m+1$ tickets parmi ces $n+1$ tickets telle que son plus grand numéro de ticket soit k est associée la partie $\{0 \leq n_1 < n_2 < \ldots < n_m < k\}$ de $[\![0,k-1]\!]$. Cette correspondance est bijective. On obtient donc $\binom{n+1}{m+1} = \sum_{k=m}^{n}\binom{k}{m}$.

9. On a

$$\sum_{k=0}^{n}\binom{m+k}{k} = \sum_{k=0}^{n}\binom{m+k}{m} = \sum_{\mathrm{K}=m}^{m+n}\binom{\mathrm{K}}{m} = \binom{m+n+1}{m+1} = \binom{m+n+1}{n}$$

où on a fait le changement de variable $\mathrm{K} = m+k$ dans la seconde égalité, puis utilisé la sommation précédente dans la première

□

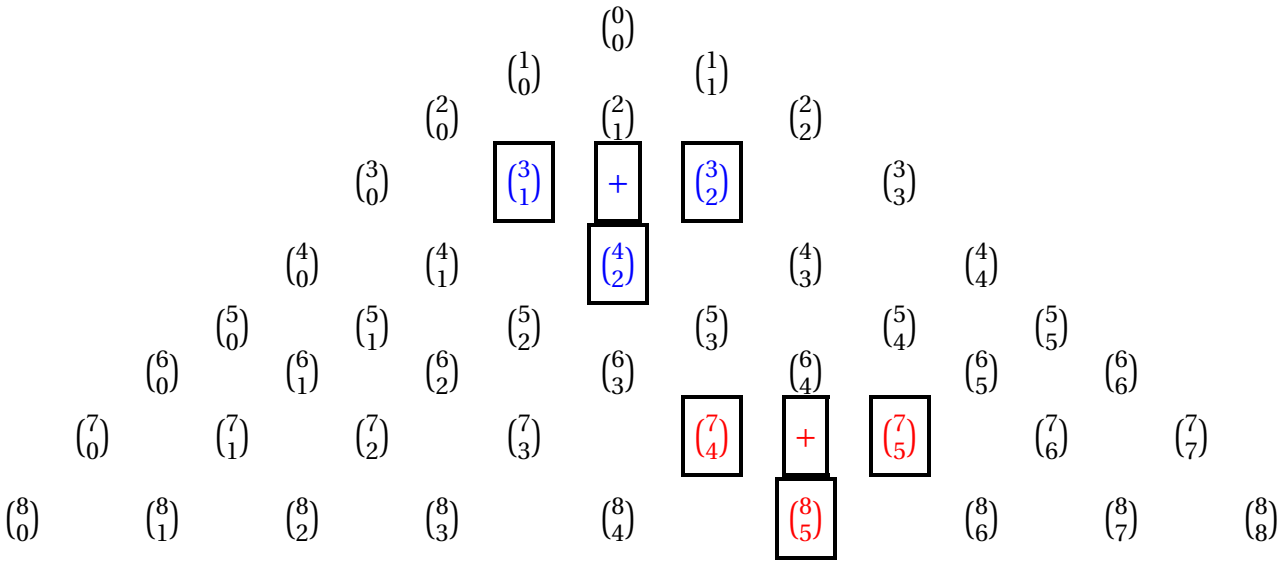

TABLE III.3 – Le triangle de Pascal des coefficients binomiaux.

n																	
0								1									
1							1		1								
2						1		2		1							
3					1		3	+	3		1						
4				1		4		6		4		1					
5			1		5		10		10		5		1				
6		1		6		15		20		15		6		1			
7	1		7		21		35		35	+	21		7		1		
8	1	8		28		56		70		56		28		8		1	

TABLE III.4 – Le triangle de Pascal des valeurs binomiales.

Le dénombrement de différentes situations est incarné par celui du tirage de boules dans une urne avec ou sans ordre (l'ordre importe pour dénombrer les plaques minéralogiques, ce qui n'est pas le cas pour les nombres issus d'un tirage du loto), avec ou sans répétition (autrement dit avec ou sans remise). Ces quelques exemples montrent l'ubiquité combinatoire des combinaisons (ou arrangements) de k parmi n dans les formules de comptage.

La suite considère un ensemble de n boules distinctes numérotées de 1 à n, chacune confondue avec son numéro. L'ensemble $\mathrm{N} = \{1,2,3\}$ servira d'exemple de

lot de n boules ($n = 3$ ci-dessous). On différenciera un tirage (*simple* ou *unitaire* : une unique boule est tirée) et un k-tirage (constitué de k tirages successifs, suivant des modalités à préciser). Les quatre types de configurations suivants sont distingués suivant la répétition de prise de boule (ou remise) et des considérations d'ordre.

1. Un k-tirage parmi n boules avec ordre et avec remise correspond à un *arrangement avec répétition de k objets parmi n*, soit un k-uplet $(x_1, \ldots, x_k)$ avec pour chaque coordonnée x_i un des n numéros de boule. Il y a n^k tels tirages : c'est le nombre d'applications d'un ensemble de cardinal k dans un ensemble de cardinal n.

   Par exemple, $(1,3,2,1)$ est un tel 4-arrangement issu d'un tirage simple répété 4 fois et basé sur un lot de $n = 3$ boules. Cet arrangement est distinct de $(1,3,1,2)$: il est possible d'écrire 3^4 4-uplets avec les chiffres $1,2,3$.

2. Un k-tirage parmi n boules avec ordre et sans remise correspond à un *arrangement sans répétition de k objets parmi n*. Il y en a $\mathrm{A}_n^k = n(n-1)\ldots(n-k+1)$ si $k \leq n$, il n'y en a pas si $k > n$. C'est le nombre d'injections d'un ensemble de cardinal k dans un ensemble de cardinal n. Si $k = n$, on obtient les bijections d'un ensemble de cardinal n.

   Un exemple d'un tel arrangement est $(1,3,2)$, arrangement distinct de $(3,1,2)$, $(3,3,1)$ n'en étant pas un.

3. Un k-tirage parmi n boules sans ordre ni remise correspond à une *combinaison de k objets parmi n*. Il y a en $\binom{n}{k}$ si $k \leq n$, il n'y en a pas si $k > n$.

   La partie $\{2,3\} = \{3,2\} = \{2,3,3\}$ est une telle combinaison de 2 objets parmi 3. Un tirage de loto (période 1976–2008) avec des planches à 49 cases consiste en un 6-tirage de jetons numérotés sans remise sans ordre : il y a $\binom{49}{6} = 13\,983\,816$ tels tirages.

4. Un k-tirage parmi n boules, avec remise et sans ordre, consiste à compter le nombre de fois que chaque boule de numéro j ($j = 1, \ldots, n$) est tirée au cours de k tirages simples sur ce lot de n boules. Combien de tels tirages existe-t-il? Le résultat d'un k-tirage consiste en k_j boules tirées de numéro j pour $j = 1, \ldots, n$ avec la somme $k = k_1 + \ldots + k_n$. Il est caractérisé par un et un seul M-uplet dont les coordonnées sont de deux types : soit un des entiers k_j ($j = 1, \ldots, n$) ordonnés suivant l'indice j, soit un séparateur $|$ utilisé $n-1$ fois et positionné entre k_j et k_{j+1} pour $j = 1, \ldots n-1$. Le k-tirage est caractérisé donc par un M-uplet avec $\mathrm{M} = 2n-1$ coordonnées (dont $n-1$ d'entre elles sont égales au séparateur, les autres étant les entiers k_j) :

   $$k_1 \,|\, k_2 \,|\, \ldots \,|\, k_{n-1} \,|\, k_n. \tag{3.1}$$

   On peut transformer ce M-uplet (bijectivement) en le N-uplet (où $\mathrm{N} = n-1+k$) avec deux types de coordonnées « 1, | »

   $$111\,|\,1111\,|\,\ldots\,|\,|\,11111\,|\,11 \tag{3.2}$$

où la coordonnée k_j dans (3.1) est remplacée par k_j coordonnées « 1 ». Pour la bijection inverse, on contracte chaque suite maximale de 1 (limitée par des séparateurs $\big|$) dans (3.2)o en un entier k_j suivant que cette suite est en j-ème position. L'ensemble des séparateurs constitue une combinaison de $n-1$ éléments parmi $n-1+k$ et, réciproquement, une telle combinaison de k éléments parmi $[\![1, n-1+k]\!]$ détermine un unique k-tirage (avec remise, sans ordre) parmi n.

PROPOSITION 3.7: *Soit un lot de n boules numérotées de 1 à n. Le nombre de k-tirages parmi n boules avec remise est égal à* $\mathrm{K}_n^k = \binom{n-1+k}{n-1} = \binom{n-1+k}{k}$.

Par exemple, on considère un lot de $n = 5$ boules sur lequel on effectue un 14-tirage avec remise d'où il ressort les nombres de boules tirées : $k_1 = 3, k_2 = 4, k_3 = 0, k_4 = 5, k_5 = 2$. Les M-uplet ($\mathrm{M} = 4+5 = 9$) et N-uplet ($\mathrm{N} = 4+14 = 18$) associés à ce 14-tirage sont

$$3\,\big|\,4\,\big|\,0\,\big|\,5\,\big|\,2, \qquad 111\,\big|\,1111\,\big|\,\big|\,11111\,\big|\,11, \tag{3.3}$$

Ce 14-tirage avec remise est un parmi $\binom{14+5-1}{5-1} = \binom{18}{4} = 3\,060$ 14-tirages sur un lot de 5 boules numérotées.

Un autre exemple est fourni par le décompte des types de dominos. Un domino est un petit rectangle constitué de 2 carrés numérotés de 0 à 6. Le nombre de types de dominos est donc celui de combinaisons de 2 parmi 7 avec répétition, soit $\mathrm{K}_7^2 = \binom{7-1+2}{2} = \binom{8}{2} = 8\cdot 7/2 = 28$ types. Vérifions ce calcul : il y a 7 dominos uni-chiffre et $\binom{7}{2} = 21$ dominos avec deux chiffres distincts, soit les 28 dominos vus comme 2 parmi 7 avec répétition.

Terminons avec le décompte d'applications croissantes (entre intervalles d'entiers munis de leur ordre naturel). À la combinaison de k boules de numéros dans $[\![1, n]\!]$ où la boule de numéro $j \in [\![1, n]\!]$ est répétée φ_j fois avec au total $\sum_{j=1}^n \varphi_j = k$ est associée l'application croissante

$$f : [\![1, k]\!] \to [\![1, n]\!] : (1, \ldots, 1, 2, \ldots, 2, \ldots, \ldots, n, \ldots, n)$$

où l'image 1 est répétée $\varphi_1 = \left|f^{-1}(\{1\})\right|$ fois, où 2 ($3, \ldots, n$ resp.) est répétée $\varphi_2 = \left|f^{-1}(\{2\})\right|$ fois ($\varphi_3, \ldots, \varphi_n$ fois resp.), certains de ces φ_j ($j = 1, \ldots, n$) étant éventuellement nuls.

Cette correspondance entre les listes de k éléments parmi n avec répétition et les applications croissantes f de $[\![1, k]\!]$ dans $[\![1, n]\!]$ est une bijection. On peut aussi associer à une telle f croissante l'application $\mathrm{F} : [\![1, k]\!] \to [\![1, n+k-1]\!]$ strictement croissante telle que

$$\mathrm{F}(\ell) = f(\ell) + \ell - 1, \quad \ell = 1, \ldots, k,$$

cette correspondance $f \leftrightarrow \mathrm{F}$ étant aussi bijective.

3.4 Principe des tiroirs

Le principe des tiroirs [11], attribué à Dirichlet [12], est le suivant :

11. Dans la tradition anglo-saxonne, on parle de principe du pigeonnier, où les chaussettes sont remplacées par des pigeons et les tiroirs par des perchoirs (cases ou boulins).

12. Johann P. G. Lejeune Dirichlet, 13 février 1805, Düren – 5 mai 1859, Göttingen.

PRINCIPE DES TIROIRS : Étant donnés m tiroirs et n objets rangés dans ces tiroirs, si $n > m$, alors il existe au moins un tiroir qui compte 2 objets ou plus.

Sinon, on aurait 0 ou 1 objet dans chaque tiroir, ainsi m_1 tiroirs avec 1 objet, m_0 tiroirs vides d'objets : l'égalité $m = m_0 + m_1$ induit $n = m_1 \leq m$, ce qui est contradictoire avec l'hypothèse $n > m$.

Ce principe des tiroirs se traduit en termes d'ensembles et de fonctions de la manière suivante : on a E un ensemble de $n = |\mathrm{E}|$ objets, une fonction $f : \mathrm{E} \to \mathrm{F}$ qui d'une part détermine une famille de $m = |\mathrm{F}|$ tiroirs $f^{-1}(y)$ avec $y \in \mathrm{F}$ (y est l'étiquette du du tiroir $f^{-1}(y)$), d'autre part attribue à chaque objet $e \in \mathrm{E}$ un tiroir de rangement $f^{-1}(f(e))$. S'il y a strictement plus d'objets que de tiroirs (*i. e.* $|\mathrm{E}| > |\mathrm{F}|$), alors il y a au moins un tiroir contenant au moins 2 objets.

THÉORÈME 3.2 (Principe des tiroirs): *Soient* E *et* F *deux ensembles finis et une application* $f : \mathrm{E} \to \mathrm{F}$. *Si* $|\mathrm{E}| > |\mathrm{F}|$, *alors il existe un élément de* F *ayant deux antécédents par* f *ou plus.*

DÉMONSTRATION. Raisonnons par l'absurde en supposant que tout $y \in \mathrm{F}$ a 0 ou 1 antécédent. Vu que $\mathrm{E} \subset \cup_{y \in f(\mathrm{E})} f^{-1}(y)$ avec les parties $f^{-1}(y)$ de cardinal 1 (car non vide), on a $|\mathrm{E}| \leq |\mathrm{F}|$, ce qui est contraire à l'hypothèse $|\mathrm{E}| > |\mathrm{F}|$. □

En termes mathématiques, on a des variantes

— Soit E un ensemble, $\mathrm{E} = \mathrm{A}_1 \sqcup \mathrm{A}_2 \sqcup \cdots \sqcup \mathrm{A}_n$ une partition [13] de E et P une partie de E avec $|\mathrm{P}| > n$. Alors il existe au moins un atome A_j contenant deux éléments distincts de P. Sinon, en mettant chaque élément de P dans un des atomes, on remplirait chaque atome de la partition par un élément de P, ou aucun, obtenant la majoration $|\mathrm{P}| \leq n$, ce qui est contradictoire avec l'hypothèse.

— Soient deux ensembles E, F et une application $f : \mathrm{E} \to \mathrm{F}$. On considère comme tiroirs les parties $f^{-1}(y)$ (non vides) paramétrées par y dans l'image de f. Si $|\mathrm{E}| > |\mathrm{F}|$, alors il existe $y \in \mathrm{F}$ avec au moins deux antécédents dans E. Ainsi l'application f est nécessairement non injective. Dans sa forme élémentaire, le principe des tiroirs énonce la non injectivité d'une fonction $f : \mathrm{E} \to \mathrm{F}$ sous la seule l'hypothèse $|\mathrm{E}| > |\mathrm{F}|$. Le principe des tiroirs étendu ci-après peut plus difficilement s'exprimer en termes d'injectivité.

On a des raffinements de ce principe des tiroirs :

PROPOSITION 3.8: *Soit une application* $f : \mathrm{E} \to \mathrm{F}$ *avec* E, F *finis.*

S'il existe un entier k *tel que* $|\mathrm{E}| > k|\mathrm{F}|$, *alors il existe un* $y \in \mathrm{F}$ *avec* $\left|f^{-1}(y)\right| \geq k+1$.

En particulier si $k+1$ *est* [14] *le plus petit entier majorant* $|\mathrm{E}|/|\mathrm{F}|$, i. e. *tel que* $k+1 \geq |\mathrm{E}|/|\mathrm{F}| > k$, *alors, il existe un* $y \in \mathrm{F}$ *tel que* $f^{-1}(y)$ *contienne au moins à* $k+1$ *éléments.*

13. Les A_i sont des parties de E, dites *atomes*, non vides, deux à deux disjointes et d'union égale à l'espace E, cf. définition 1.11.

14. $k+1 = \lceil |\mathrm{E}|/|\mathrm{F}| \rceil$ où $\lceil x \rceil$ est l'entier plafond de x, *i. e.* le plus petit entier ℓ majorant x : $\ell - 1 < x \leq \ell$.

DÉMONSTRATION. Montrons la première assertion par l'absurde, en supposant un rangement tel que chaque tiroir contient au plus k objets. On a $\mathrm{E} = \cup_{y\in f(\mathrm{E})} f^{-1}(y)$ d'où $|\mathrm{E}| \leq \sum_{y\in f(\mathrm{E})} \left|f^{-1}(y)\right| \leq k|\mathrm{F}|$, ce qui contredit l'hypothèse $|\mathrm{E}| > k|\mathrm{F}|$.

La dernière assertion donne des indications pour le k optimal auquel s'applique la première partie de cette proposition. □

Donnons quelques exemples d'utilisation du principe des tiroirs

▷ EXEMPLES 3.5:

3.5.1 Dans un groupe avec 367 personnes [15], il y a au moins deux personnes qui ont la même date d'anniversaire.

3.5.2 Soit un triangle T d'aire égale à 1. Si l'on choisit 9 points à l'intérieur de celui-ci, alors on peut en trouver 3 d'entre eux qui déterminent un triangle d'aire inférieure à $1/4$. En effet, pour chaque sommet s du triangle T, on peut considérer l'homothétique T_s de T par une homothétie centrée en s et de rapport $1/2$: ces trois triangles sont d'aire $1/4$ et leur complémentaire dans T est un triangle d'aire $1-3\frac{1}{4} = 1/4$ aussi. On considère les 4 triangles comme incarnant un tiroir, les 9 points étant rangés dans ces tiroirs. Vu $9/4 = 2.25 > 2$, le principe des tiroirs étendu assure de l'existence d'un tiroir/triangle parmi les 4 triangles contenant 3 des 9 objets/points, : le triangle déterminé par ces 3 points, contenus dans un triangle d'aire $1/4$, est d'aire au plus $1/4$.

3.5.3 Dans un groupe avec 241 personnes, il y a au moins 21 personnes qui sont nées le même mois. En effet, soit $f : [\![1,241]\!] \to [\![1,12]\!]$ l'application qui associe à un membre du groupe son mois de naissance. On a $241 > 20\cdot 12$ (en fait $241/12 = 20.08$). Il existe donc un mois tel que $\left|f^{-1}(m)\right| \geq 21$ *i. e.* un mois m tel que 21 personnes y sont nées.

3.5.4 Soit $n > 1$ et E un ensemble de $n+1$ entiers naturels distincts. Il existe deux nombres distincts dans E dont la différence est divisibe par n. En effet, si f est l'application naturelle $f : \mathrm{E} \to \mathbb{Z}/n\mathbb{Z}$, il existe deux nombres distincts x, x' de E qui sont envoyés par f sur le même élément de $\mathbb{Z}/n\mathbb{Z}$: la différence $x - x'$ est divisible par n.

3.5.5 Soit $a_1, \ldots, a_{2n}$ un ensemble de $2n$ naturels non nuls dont la somme est majorée par $3n$. Alors il existe $i < j$ tels que $a_{i+1} + \cdots + a_j = n-1$. En effet, posons $s_i = a_1 + \cdots + a_i$ et $t_i = s_i + n - 1$ pour $i = 1, \ldots, 2n$. Alors d'une part $0 < s_1 < \ldots < s_{2n} \leq 3n$, d'autre part $n-1 < t_1 < \cdots < t_{2n} < 4n$. Il y a $4n$ nombres dans $\{s_j, t_k | j,k \in [\![1,2n]\!]\}$ qui sont inclus dans $[\![1,4n-1]\!]$: deux sont donc égaux : les s_j (resp. t_k) sont distincts deux à deux, ainsi l'égalité vaut pour un s_j et un t_i, soit $s_j = s_i + n - 1$ avec $i < j$ ou encore $a_{i+1} + \cdots + a_j = n-1$ avec $i < j$ pour $i < j$.

3.5.6 Soit $\mathrm{E}_n = [\![1,2n]\!]$. Alors, pour toute partie A de E_n à $n+1$ éléments, il existe dans A deux nombres différents premiers entre eux. En effet, appliquons le principe des tiroirs avec les n tiroirs $[\![2k+1, 2k+2]\!]$ où $k = 0, \ldots, n-1$:

[[1,2]],[[3,4]],... [[2n-3,2n-2]],[[2n-1,2n]].

Il existe deux éléments a_1, a_2 de A distincts qui sont dans un même tiroir $[\![2k+1, 2k+2]\!]$ et diffèrent d'une unité : les nombres a_1 et a_2 sont donc pre-

15. 366 suffisent en 2019 qui n'est pas bissextile.

miers entre eux.

Ce résutat n'est plus valables si on considère des parties de cardinal n. Il suffit de considérer la partie $A_n = \{2, 4, \ldots, 2n\}$ dont tout élément est un entier pair.

3.5.7 Soit $E_n = [\![1, 2n]\!]$. Alors, pour toute partie B de E_n à $n+1$ éléments, il existe dans B deux nombres différents dont l'un divise l'autre.

En effet, écrivons chaque entier naturel $x \in E_n$ suivant $x = 2^k(2m+1)$ où $1 \leq 2m+1 \leq 2n$: un tiroir T_{2m+1} dans E_n est caractérisé comme la partie des entiers ayant $2m+1$ comme facteur impair maximal. Il y a n (comme le nombre d'entiers impairs entre 1 et $2n-1$) tels tiroirs recouvrant E_n. Vu que la partie B est de cardinal $n+1$, le principe des tiroirs affirme l'existence de deux entiers distincts $x = 2^k(2m+1), x' = 2^{k'}(2m'+1)$ de B dans le même tiroir, et donc ayant le même facteur maximal impair $2m+1$: ainsi, soit $k < k'$ et l'entier x divise x' comme 2^k divise $2^{k'}$, soit $k' < k$ et l'entier x' divise x.

Ce résutat n'est plus valables si on considère des parties de cardinal n : considérons la partie $B_n = \{n+1, n+2, \ldots, 2n\}$ où $n+k$ (avec $1 \leq k < n$) ne divise aucun $n+\ell$ (avec $k < \ell \leq n$) : sinon, pour certains k, ℓ tels que $1 \leq k < \ell \leq n$, l'entier $n+k$ diviserait $n+\ell = n+k+\ell-k$ et par suite $\ell-k$, et donc $n+k \leq \ell-k$, soit $n+2k \leq \ell$, ce qui n'est pas vu les conditions $1 \leq k < \ell \leq n$. ◁

Le principe des tiroirs apparaît comme tel dans les études de Dirichlet sur l'approximation d'un nombre réel par les rationnels. Soit a irrationnel et Q entier non nul. En recouvrant $\mathbb{R}$ par des intervalles $[p/Q, (p+1)/Q]$ où $p \in \mathbb{Z}$, il existe p_1 tel que l'intervalle $[p_1/Q, (p_1+1)/Q]$ contienne a : une de ses extrémités est au plus à distance $1/(2Q)$ de a. Autrement dit, on peut approcher a par un rationnel p/Q à $1/(2Q)$ près. Le théorème d'approximation de Dirichlet donne une approximation à $1/Q^2$ près pour une infinité de Q, bien meilleure que l'approximation à $1/(2Q)$ près valable pour tout Q, ou autrement dit, pour une approximation ε donnée le recours à une infinité de rationnels r/s avec des $s \simeq \varepsilon^{-1/2}$ moins grands que les $Q \simeq (2\varepsilon)^{-1}$ de la première méthode d'approximation.

PROPOSITION 3.9: *Soit a irrationnel. Il existe une infinité de rationnels $\dfrac{p}{q}$ tels que $\left|a - \dfrac{p}{q}\right| < \dfrac{1}{q^2}$.*

DÉMONSTRATION. Soit a irrationnel positif. Soit $Q > 0$ un entier. Considérons les parties fractionnaires

$$\{0\}, \{a\}, \{2a\}, \ldots, \{ka\} = ka - \lfloor ka \rfloor, \ldots, \{Qa\}$$

des $(Q+1)$ premiers multiples de a. Par le principe des tiroirs, deux parmi ces $(Q+1)$ nombres tombent dans l'un des Q intervalles

$$[0, 1/Q), [1/Q, 2/Q), \ldots, [(Q-1)/Q, 1).$$

Autrement dit, il existe des entiers s, q_1, q_2 tel que $\{q_1 a\}, \{q_2 a\}$ sont dans l'intervalle $[s/Q, (s+1)/Q)$. Prenant $q = |q_1 - q_2|$, on obtient pour l'entier p (égal au signe près à $\lfloor q_1 a \rfloor - \lfloor q_2 a \rfloor$) l'estimation $|qa - p| < \dfrac{1}{Q}$, soit en divisant par q

$$\left|a - \frac{p}{q}\right| < \frac{1}{Qq} \leq \frac{1}{q^2}, \tag{3.4}$$

vu que par définition $0 < q \leq Q$. On a donc associé à tout entier $Q > 0$ un rationnel $r = \dfrac{p}{q}$ qui vérifie (3.4).

Il reste à montrer que la partie de telles paires (p, q) est infini. Supposons qu'il n'y en ait qu'un nombre fini N :

$$\left|a - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}, \quad i = 1, \ldots, N.$$

Puisqu'aucune des différences n'est nulle vu l'irationnalité de a, il existe un entier Q_0 tel que $|a - p_i/q_i| > 1/Q_0$ pour tous les $i = 1,\ldots,N$. En appliquant l'argument ci-dessus à ce Q_0, nous obtenons un couple (p_0, q_0) tel que $|a - p_0/q_0| < 1/(Q_0 q_0) \leq 1/Q_0$. Ainsi, ce p_0/q_0 ne peut être un des $p_i/q_i, i = 1,\ldots,N$. Par ailleurs, comme précédemment, $|a - p_0/q_0| < q_0^{-2}$, cette inégalité pour (p_0, q_0) contredisant notre hypothèse que ces rationnels $r_i = p_i/q_i, i = 1,\ldots,N$ sont les *seuls* avec cette propriété. L'hypothèse de finitude des (r_i, q_i) amène à une contradiction, ceci achève la démonstration. □

Le caractère ultimement périodique du développement décimal d'un rationnel est démontré par application du principe des tiroirs :

PROPOSITION 3.10: *Soit le rationnel $x = p/q$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$. Alors le développement décimal de x est périodique, à un nombre fini de décimales près.*

La démonstration de cette proposition est basée sur l'analyse du développement d'un rationnel décrite dans le théorème suivant.

DÉMONSTRATION. Pour la division euclidienne par q, il y a q valeurs possibles pour le reste. Ainsi dans la suite $(r_n)_{n\geq 0}$ construite dans la démonstration du théorème ci-après, d'après le principe des tiroirs, il existe $s < t$ tels que $r_s = r_t$ et par suite $r_{s+k} = r_{t+k}$ pour $k \geq 0$, soit $r_K = r_{K+T}$ avec $K = s + k \geq s$ et $T = t - s$ et donc aussi $d_K = d_{K+T}$ pour $K \geq s$: la suite $(d_n)_{n\geq 0}$ est périodique à partir d'un K. □

THÉORÈME 3.3: *Soit $x = p/q \in \mathbb{Q}$ avec p, q premiers entre eux et $q > 0$. Il existe une suite $(d_n)_{n\geq 0}$ avec $d_0 \in \mathbb{Z}$ et $d_n \in \{0,\ldots,9\}$ pour $n \geq 1$ avec*

$$d_0 + \frac{d_1}{10} + \ldots + \frac{d_n}{10^n} \leq x < d_0 + \frac{d_1}{10} + \ldots + \frac{d_n}{10^n} + \frac{1}{10^n}, \quad n \geq 1.$$

DÉMONSTRATION. À partir du rationnel x, on construit deux suites (d_n), (r_n) avec $0 \leq r_n < q$ et $d_n \in \{0, 1, \ldots, 9\}$ si ≥ 1 par des divisions euclidiennes successives par q

$$p = qd_0 + r_0, \quad 10r_n = qd_{n+1} + r_{n+1}, \quad n \geq 0.$$

Si $n \geq 0$, on a

$$qd_{n+1} \leq 10r_n, \tag{3.5}$$

soit $d_{n+1} \leq 10r_n/q < 10$: l'entier d_{n+1} est donc dans $\{0, 1, \ldots, 9\}$.

Vérifions par récurrence que r_n est le reste de la division euclidienne de $10^n p$ par q et que le quotient de cette division est l'entier $D_n = \sum_{j=0}^{n} d_j 10^{n-j}$. C'est en effet vrai pour $n = 0$. Supposons le au rang n, ce qui signifie $10^n p = D_n q + r_n$, ce qui donne combiné avec la définition de r_{n+1}

$$10^{n+1} p = 10(10^n p) = 10(qD_n + r_n) = q10D_n + qd_{n+1} + r_{n+1} = q(10D_n + d_{n+1}) + r_{n+1}$$

avec

$$D_{n+1} = 10D_n + d_{n+1} = 10\sum_{j=0}^{n} d_j 10^{n-j} + d_{n+1} = \sum_{j=0}^{n} d_j 10^{n+1-j} + d_{n+1} = \sum_{j=0}^{n+1} d_j 10^{n+1-j}$$

ce qui assure la validité de la propriété de récurrence au rang $n+1$. De plus, vu que $r_n \in [[0, q-1]]$, on a $d_n \in [[0, 9]]$ grâce à (3.5). On a donc

$$10^n p = q\left[\sum_{j=0}^{n} d_j 10^{n-j}\right] + r_n, \quad 0 \leq r_n < q.$$

soit

$$0 \leq r_n = 10^n p - q\left[\sum_{j=0}^{n} d_j 10^{n-j}\right] < q$$

et après division par $10^n q$

$$0 \leq \frac{p}{q} - \left[\sum_{j=0}^{n} \frac{d_j}{10^j}\right] < \frac{1}{10^n}$$

ce qui achève la démonstration. □

3.5 Crible

La formule du crible permet d'effectuer le décompte d'ensembles définis comme union de parties, parties ayant des intersections non vides.

THÉORÈME 3.4 (Crible, principe d'inclusion/exclusion): *Soit* E *un ensemble fini et une famille de parties* $A_1,\dots,A_n$ *de l'ensemble* E. *Alors :*

$$|E| - \left|\cap_{i=1}^n \overline{A_i}\right| = \left|\cup_{i=1}^n A_i\right| = \sum_{k=1}^n (-1)^{k+1} \sum_{1\le i_1<\cdots<i_k\le n} \left|\cap_{j=1}^k A_{i_j}\right|. \tag{3.6}$$

△ REMARQUE 3.7: On a donc

$$\left|\cup_{i=1}^n A_i\right| = \sum_{i=1}^n |A_i| + \cdots + (-1)^{k+1} \sum_{1\le i_1<\cdots<i_k\le n} \left|\cap_{j=1}^k A_{i_j}\right| + \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|$$

Pour $n=2$ parties de E, la formule énonce

$$\boxed{|A\cup B| = |A| + |B| - |A\cap B|}$$

et pour $n=3$ parties

$$\boxed{|A\cup B\cup C| = |A|+|B|+|C|-|A\cap B|-|B\cap C|-|C\cap A|+|A\cap B\cap C|.}$$ ▽

DÉMONSTRATION. Une première démonstration emprunte la voie d'une récurrence sur le nombre n de parties (une seconde plus fonctionnelle est donnée ci-dessous dans la remarque 3.8). Pour $n=2$, on a clairement (avec un diagramme de Venn [16]

$$|A_1\cup A_2| = |A_1| + |A_2| - |A_1\cap A_2|.$$

Pour 3 parties, on obtient la formule en appliquant la formule pour 2 parties plusieurs fois :

$$\begin{aligned}
|A\cup B\cup C| &= |A\cup B| + |C| - |(A\cup B)\cap C| \\
&= |A| + |B| - |A\cap B| + |C| - |(A\cap C)\cup(B\cap C)| \\
&= |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |(A\cap C)\cap(B\cap C| \\
&= |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap B\cap C|
\end{aligned}$$

En général, supposons la formule du crible établie pour n (au moins égal à 2) parties et considérons $n+1$ parties $A_1,\dots,A_{n+1}$. En appliquant la formule du crible pour les $n=2$ parties $\cup_{i=1}^n A_i$ et A_{n+1}, on obtient

$$\left|\cup_{i=1}^{n+1} A_i\right| = \left|\cup_{i=1}^n A_i \cup A_{n+1}\right| = \left|\cup_{i=1}^n A_i\right| + |A_{n+1}| - \left|\left(\cup_{i=1}^n A_i\right)\cap A_{n+1}\right|$$

16. John Venn, 4 août 1834, Kingston-upon-Hull, RU – 4 avril 1923, Cambridge, RU.

et par suite

$$\left|\cup_{i=1}^{n+1} A_i\right| = \left|\cup_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\cup_{i=1}^{n} (A_i \cap A_{n+1})\right|$$

puis en faisant appel à l'hypothèse de récurrence pour les premier et dernier termes du membre de droite

$$\begin{aligned}
\left|\cup_{i=1}^{n+1} A_i\right| &= \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} \left|A_i \cap A_j\right| + \ldots + (-1)^{k+1} \sum_{1\le i_1<\ldots<i_k\le n} \left|A_{i_1} \cap \ldots \cap A_{i_k}\right| + \ldots \\
&\quad + (-1)^{n+1} |A_1 \cap \ldots \cap A_n| + |A_{n+1}| \\
&\quad - \sum_{1\le i\le n} |A_i \cap A_{n+1}| + \ldots + (-1)^{k+1} \sum_{1\le i_1<\ldots<i_k\le n} \left|A_{i_1} \cap \ldots \cap A_{i_k} \cap A_{n+1}\right| + \ldots \\
&\quad + (-1)^{n+2} |A_1 \cap \ldots \cap A_n \cap A_{n+1}| \\
&= \sum_{i=1}^{n+1} |A_i| - \sum_{1\le i<j\le n+1} \left|A_i \cap A_j\right| + \ldots + (-1)^{k+1} \sum_{1\le i_1<\ldots<i_k\le n+1} \left|A_{i_1} \cap \ldots \cap A_{i_k}\right| + \ldots \\
&\quad + (-1)^{n+2} |A_1 \cap \ldots \cap A_{n+1}|,
\end{aligned}$$

ce qui est la formule du crible pour $n+1$ parties. □

▷ EXEMPLES 3.6:

3.6.1 Soit $E = [[1,60]]$. Combien de nombres de E sont-ils pairs ou divisibles par 3 ? Soit A_d la partie des nombres de E divisibles par d : si p et q sont premiers entre eux, alors $A_p \cap A_q = A_{pq}$. Ainsi, $|A_2| = 30$, $|A_3| = 20$ et $|A_2 \cap A_3| = |A_6| = 10$. La formule du crible donne

$$|A_2 \cup A_3| = |A_2| + |A_3| - |A_6| = 30 + 20 - 10 = 40$$

Ainsi il y a 40 entiers divisibles par 2 ou par 3.

3.6.2 Soit $E = [[0,300]]$. Quel cardinal pour la partie des éléments de E qui ne sont ni multiples de 2 ni de 3 ni de 7 ? Notant encore par A_d la partie de E des nombres divisibles par d, l'application de la formule du crible donne

$$\begin{aligned}
\left|\overline{A}_2 \cap \overline{A}_3 \cap \overline{A}_7\right| &= \left|\overline{A_2 \cup A_3 \cup A_7}\right| = 301 - |A_2 \cup A_3 \cup A_7| \\
&= 301 - |A_2| - |A_3| - |A_7| + |A_2 \cap A_3| + |A_2 \cap A_7| + |A_3 \cap A_7| \\
&\qquad - |A_2 \cap A_3 \cap A_7| \\
&= 301 - |A_2| - |A_3| - |A_7| + |A_6| + |A_{14}| + |A_{21}| - |A_{42}| \\
&= 301 - 151 - 101 - 43 + 51 + 22 + 15 - 8 = 88.
\end{aligned}$$

3.6.3 Parmi 20 étudiants, 10 étudient les mathématiques, 11 étudient la physique, et 4 étudient les deux. Combien y a-t-il d'étudiants qui n'étudient ni les mathématiques ni la physique ? On considère M_- la partie des 10 qui n'étudient pas les mathématiques, P_- celle des 9 qui n'étudient pas la physique et $N_- = M_- \cup P_-$ celle des 16 qui n'étudient pas la physique ou les mathématiques. Alors, le cardinal de ceux qui n'étudient ni les math ni la physique est

$$|M_- \cap P_-| = |M_-| + |P_-| - |N_- = M_- \cup P_-| = 10 + 9 - 16 = 3$$

3.6.4 Le crible d'Ératosthène[17] permet de trouver les nombres premiers inférieurs à n en éliminant tous les multiples des nombres premiers inférieurs à $\sqrt{n}$, ces derniers étant supposés connus. Il est basé sur l'équivalence suivante : l'entier naturel k vérifiant $k \leq n$ est un nombre premier si et seulement si k n'est divisible par aucun nombre premier $p \leq \sqrt{n}$. Il donne une procédure pour trouver par élimination (ou criblage) les nombres premiers inférieurs à n connaissant ceux qui sont inférieurs à $\sqrt{n}$.
La formule du crible permet de calculer le nombre de ces nouveaux nombres premiers ainsi déterminés.
Pour x réel, on note par $\mathrm{P}(x)$ l'ensemble des entiers premiers inférieurs ou égaux à x, $\pi(x) = |\mathrm{P}(x)|$ son cardinal et $\mathscr{P}(k,x)$ l'ensemble des parties à k éléments de $\mathrm{P}(x)$. L'ensemble $[\![2,n]\!]$ est l'union disjointe des entiers premiers dans $]\sqrt{n},n]$ et de l'ensemble $\mathrm{R}(n)$ des multiples aq $(a \geq 1)$ de produits q d'entiers premiers dans $[\![2,\sqrt{n}]\!]$. Le cardinal $|\mathrm{R}(n)| = n-1-(\pi(n)-\pi(\sqrt{n}))$ peut être évalué par la formule du crible en considérant l'ensemble $[\![2,n]\!]$ et ses parties A_p constituées des multiples du nombre premier p pour $p \in \mathrm{P}(n)$. Pour une partie Q de $\mathrm{P}(\infty)$, l'intersection $\cap_{p\in\mathrm{Q}}\mathrm{A}_p$ est égal à la partie $([\prod_{p\in\mathrm{Q}} p]\mathbb{N}) \cap [\![2,n]\!]$ des multiples entiers du produit $\prod_{p\in\mathrm{Q}}$, de cardinal la partie entière $\lfloor n/(\prod_{p\in\mathrm{Q}} p)\rfloor$. La formule du crible (3.6) donne alors :

$$|\mathrm{R}| = \sum_{p\in\mathrm{P}(\sqrt{n})} \left\lfloor \frac{n}{p} \right\rfloor - \sum_{\mathrm{P}\in\mathscr{P}(\sqrt{n},2)} \left\lfloor \frac{n}{\prod_{p\in\mathrm{P}} p} \right\rfloor + \ldots + (-1)^{\pi(\sqrt{n})} \sum_{\mathrm{P}\in\mathscr{P}(\sqrt{n},\pi(\sqrt{n}))} \left\lfloor \frac{n}{\prod_{p\in\mathrm{P}} p} \right\rfloor$$

et donc

$$\pi(n) - \pi(\sqrt{n}) = n - 1 + \sum_{j=1}^{\pi(\sqrt{n})} (-1)^j \sum_{\mathrm{P}\in\mathscr{P}(\sqrt{n},j)} \left\lfloor \frac{n}{\prod_{p\in\mathrm{P}} p} \right\rfloor$$

Cette formule permet théoriquement le calcul de $\pi(n)$ si l'on connaît tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$.
Par exemple, on peut déterminer $\pi(120)$ sachant que les nombres premiers inférieurs à $\sqrt{120}$ sont 2, 3, 5 et 7 (puisque $121 = 11^2$) : $\pi\left(\sqrt{120}\right) = 4$ et

$$\begin{aligned}
|\mathrm{R}(120)| &= 119 - (\pi(120) - \pi(\sqrt{120})) \\
&= \left[\left\lfloor \frac{120}{2} \right\rfloor + \left\lfloor \frac{120}{3} \right\rfloor + \left\lfloor \frac{120}{5} \right\rfloor + \left\lfloor \frac{120}{7} \right\rfloor\right] \\
&\quad - \left[\left\lfloor \frac{120}{6} \right\rfloor + \left\lfloor \frac{120}{10} \right\rfloor + \left\lfloor \frac{120}{14} \right\rfloor + \left\lfloor \frac{120}{15} \right\rfloor + \left\lfloor \frac{120}{21} \right\rfloor + \left\lfloor \frac{120}{35} \right\rfloor\right] \\
&\quad \left[\left\lfloor \frac{120}{30} \right\rfloor + \left\lfloor \frac{120}{42} \right\rfloor + \left\lfloor \frac{120}{70} \right\rfloor + \left\lfloor \frac{120}{105} \right\rfloor\right] + \left\lfloor \frac{120}{210} \right\rfloor \\
&= 119 - (60+40+24+17) + (20+12+8+8+5+3) \\
&\quad - (4+2+1+1) + 0 = 119 - 141 + 56 - 8 = 26
\end{aligned}$$

donc il y a 26 nombres premiers entre 10 et 120, d'où $\pi(120) = 30$ nombres premiers inférieurs à 120 :

$$\begin{aligned}
&11,13,17,19,23,29,31,37,41,43,47,53,59,61,\\
&67,71,73,79,83,89,97,101,103,107,109,113
\end{aligned}$$

Bien sûr la formule ne donne pas les 26 nombres premiers qui suivent 2, 3, 5 et 7 ; on peut les trouver, par exemple, à l'aide de la méthode du crible d'Ératosthène. ◁

△ REMARQUES 3.8:

17. Ératosthène, v. -276, Cyrène -– v. -194, Alexandrie, Égypte.

1. En termes de fonctions caractéristiques [18], on a

$$\mathbf{1}_{A\cap B} = \mathbf{1}_A\mathbf{1}_B, \quad \mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_{A\cap B}, \quad \mathbf{1}_{\overline{A}} = \mathbf{1} - \mathbf{1}_A$$

d'où

$$\begin{aligned}\mathbf{1}_{\cup_{i=1}^n A_i} = \mathbf{1} - \mathbf{1}_{\cap_{i=1}^n \overline{A_i}} &= \mathbf{1} - \prod_{i=1}^n \mathbf{1}_{\overline{A_i}} = \mathbf{1} - \prod_{i=1}^n (\mathbf{1} - \mathbf{1}_{A_i}) \\ &= \sum_{k=1}^n (-1)^{k+1} \sum_{1\le i_1<\ldots<i_k\le n} \mathbf{1}_{A_{i_1}} \ldots \mathbf{1}_{A_{i_k}} \\ &= \sum_{k=1}^n (-1)^{k+1} \sum_{1\le i_1<\ldots<i_k\le n} \mathbf{1}_{\cap_{i=1}^k A_{i_1}}\end{aligned}$$

et en considérant pour A partie de E l'identité $|A| = \sum_{x\in E} \mathbf{1}_A(x)$

$$\left|\cup_{i=1}^n A_i\right| = \sum_{k=1}^n (-1)^{k+1} \sum_{1\le i_1<\ldots<i_k\le n} \left|\cap_{i=1}^k A_{i_i}\right|.$$

2. La formule du crible est souvent dénommée *Principe d'inclusion/exclusion*. On cherche à calculer le cardinal de $A = \cup_1^n A_i$: comme première approximation, on constate l'inclusion de A dans l'union des A_i, d'où résulte la première estimation de |A| par une majoration

$$|\cup A_i| \le \textstyle\sum_i |A_i|,$$

par excès si au moins un élément se trouve dans deux des A_i, *i. e.* dans l'intersection $A_i \cap A_j$. Par exclusion des intersections doubles $A_i \cap A_j$ $(i < j)$, on diminue le décompte, donnant une minoration à |A|

$$|\cup_i A_i| \ge \textstyle\sum_i |A_i| - \sum_{i<j} \left|A_i \cap A_j\right|$$

mais les éléments des intersections ternaires $A_i \cap A_j \cap A_k$ $(i < j < k$ ne sont plus décomptés : on les inclut en rajoutant les termes donnant à nouveau une majoration de |A| :

$$|\cup A_i| \le \sum_i |A_i| - \sum_{i<j} \left|A_i \cap A_j\right| + \sum_{i<j<k} \left|A_i \cap A_j \cap A_k\right|.$$

Ce balancement entre inclusion et exclusion donne à la méthode du crible l'appellation de *Méthode d'inclusion/exclusion*. ▽

Le décompte d'applications $f : E \to F$ avec cardinaux $|E| = n$, $|F| = p$ a été réalisé par des expressions simples : p^n pour le nombre de toutes les applications de E vers F, A_n^p pour les injections si $n \le p$ avec le cas particulier des $n!$ permutations de E). Le crible permet d'établir une formule pour le nombre des surjections si $n > p$.

18. On dit parfois *fonctions indicatrices*.

PROPOSITION 3.11: *Soient des entiers n, p avec $n \geq p$ et $\mathscr{S}_{n,p}$ l'ensemble des surjections de $[\![1,n]\!]$ sur $[\![1,p]\!]$. Alors*

$$\left|\mathscr{S}_{n,p}\right| = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n.$$

DÉMONSTRATION. Il y a p^n applications de $[\![1,n]\!]$ dans $[\![1,p]\!]$. Pour $i = 1,\ldots,p$, soit A_i la partie des applications $f : [\![1,n]\!] \to [\![1,p]\!]$ n'ayant pas i dans leur image. Le complémentaire dans $[\![1,p]\!]^{[\![1,n]\!]}$ de la partie des surjections est égal à l'union des parties A_i, ainsi

$$[\![1,p]\!]^{[\![1,n]\!]} \setminus \mathscr{S}_{n,p} = \cup_{i=1}^{p} \mathrm{A}_i.$$

L'ensemble $\mathrm{E}_i(n,p)$ des applications de $[\![1,n]\!]$ dans $[\![1,p]\!] \setminus \{i\}$ est en bijection avec la partie A_i. En effet, soit J_i l'inclusion naturelle $[\![1,p]\!] \setminus \{i\} \to [\![1,p]\!]$. À $\psi \in \mathrm{E}_i(n,p)$ on associe l'application $\mathrm{J}_i \circ \psi$ qui est une application de A_i :

$$\psi : [\![1,n]\!] \to [\![1,p]\!] \setminus \{i\}, \qquad \mathrm{J}_i : [\![1,p]\!] \setminus \{i\} \to [\![1,p]\!].$$

La transformation $\psi \in \mathrm{E}_i(n,p) \to \mathrm{J}_i \circ \psi \in \mathrm{A}_i$ a comme application réciproque celle qui associe à $\varphi \in \mathrm{A}_i$ l'unique application $\widetilde{\varphi} \in \mathrm{E}_i(n,p)$ telle que $\widetilde{\varphi}(x) = \varphi(x)$ pour $x \in [\![1,n]\!]$. Ainsi le cardinal de A_i est égal à celui de $\mathrm{E}_i(n,p)$, soit $|\mathrm{A}_i| = (p-1)^n$.

Plus généralement, pour $k \geq 2$, la partie $\mathrm{A}_{i_1} \cap \ldots \cap \mathrm{A}_{i_k}$ est constituée des applications n'atteignant pas $i_1,\ldots,i_k$: comme précédemment on peut mettre en bijection l'intersection $\mathrm{A}_{i_1} \cap \ldots \cap \mathrm{A}_{i_k}$ avec l'ensemble $\mathrm{E}_{i_1,\ldots,i_k}(n,p)$ des applications de $[\![1,n]\!]$ dans $[\![1,p]\!] \setminus \{i_1,\ldots,i_k\}$: de telles parties pour $1 \leq i_1 < i_2 < \ldots < i_k \leq p$ ont même cardinal, soit $(p-k)^n$. Par ailleurs, ces parties sont au nombre de $\binom{p}{k}$ comme le nombre de combinaisons $1 \leq i_1 < i_2 < \ldots < i_k \leq p$ parmi p. La formule du crible donne donc

$$\left|\cup_{i=1}^{p} \mathrm{A}_i\right| = \sum_{k=1}^{p} (-1)^{k+1} \binom{p}{k} (p-k)^n$$

et donc

$$\begin{aligned}
\left|\mathscr{S}_{n,p}\right| &= p^n - \left|\cup_{i=1}^{p} \mathrm{A}_i\right| \\
&= p^n - \sum_{k=1}^{p} (-1)^{k+1} \binom{p}{k} (p-k)^n \\
&= \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n.
\end{aligned}$$

□

▷ EXEMPLE 3.7: Pour $n = 3$ et $p = 2$, on a 8 applications de $[\![1,3]\!]$ dans $[\![1,2]\!]$. Le résultat de la proposition précédente donne 6 surjections

$$\sum_{k=0}^{2} (-1)^k \binom{2}{k} (2-k)^3 = \binom{2}{0}(2-0)^3 - \binom{2}{1}(2-1)^3 + \binom{2}{2}(2-2)^3 = 8-2+0 = 6.$$

qu'on peut expliciter : $112, 121, 211, 122, 212, 221$ où abc désigne l'application φ telle que $\varphi(1) = a, \varphi(2) = b$ et $\varphi(3) = c$. Les 2 autres applications (non surjectives) sont $111, 222$. ◁

Pour $p \leq n$, il n'y a pas de formule plus simple pour le nombre $S_{n,p}$ de surjections de $E = [\![1, n]\!]$ dans $F = [\![1, p]\!]$, en dépit ce la proposition précédente. Néanmoins on peut donner des relations entre ces nombres permettant leur calcul.

Une surjection de E sur F est caractérisée par la donnée d'une partition $\mathscr{P}$ de E constituée de p parties $E_1, \ldots, E_p$ non vides disjointes, puis d'une bijection qui associe à chaque atome E_a un élément $y(a) \in F$. Notons par $S(n, p)$ le nombre de partitions de E constituées de p parties non vides et par $S_{n,p}$ le nombres de surjections de E dans F. Par la règle du produit, on a $S_{n,p} = S(n, p)p!$. Par ailleurs, on a

$$S(n, 1) = 1, \quad S(n, n) = 1, \quad S(n + 1, p) = S(n, p - 1) + pS(n, p)$$

où les deux premières égalités correspondent à l'unique partition mono-atomique et l'unique partition de $[\![1, n]\!]$ avec n singletons resp. Pour la dernière relation, on choisit l'élément $x = n + 1$ de $E = [\![1, n + 1]\!]$, puis on considère les partitions de E où x est dans un singleton (l'oubliant, on obtient n'importe quelle partition à $p - 1$ atomes sur un espace à n éléments) ou bien x appartient à un atome d'au moins 2 éléments (l'oubliant, on obtient n'importe quelle partition à p atomes sur un espace de n éléments, chaque partition répétée p fois pour accrochage de x à un des p atomes) : on a alors la relation annoncée.

Cette relation sur les nombres $S(n, p)$ dits de Stirling de deuxième espèce, permet le calcul de proche en proche de ces nombres et donc celui du nombre des surjections entre ensembles finis.

	$p = 1$	2	3	4	5	6
$n = 1$	1					
2	1	1				
3	1	3	1			
4	1	7	6	1		
5	1	15	25	10	1	
6	1	31	90	65	15	1

TABLE III.5 – Un début de table des nombres de Stirling $S(n, p)$ de seconde espèce.

Une autre application du crible concerne le comptage de certaines permutations, dites dérangements, sur n objets.

DÉFINITION 3.5: *On appelle dérangement d'un ensemble fini* E *toute permutation de* E *sans point fixe (*i. e. *toute bijection s de* E *dans* E *telle que, si x est dans* E*, $s(x)$ est différent de x).*

PROPOSITION 3.12: *Soit* E *un ensemble fini de cardinal n. Alors* E *a* $D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ *dérangements.*

DÉMONSTRATION. On note $E = \{1, \ldots, n\}$, et A_i l'ensemble des permutations qui laisse i invariant. Le cardinal recherché est :

$$\left|\overline{A_1} \cap \ldots \cap \overline{A_n}\right| = n! - |A_1 \cup \ldots \cup A_n|$$

On va appliquer la formule du crible pour calculer ce cardinal. On a :

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} S_k$$

où

$$S_k = \sum_{1 \leq i_1 \leq \ldots i_k \leq n} \left|A_{i_1} \cap \ldots \cap A_{i_k}\right|$$

Maintenant, toute permutation qui laisse fixe les k éléments $i_1,\dots,i_k$ agit comme elle veut sur les autres. Il y a donc autant de permutations de E qui fixent $i_1,\dots,i_k$ que de permutations d'un ensemble à $n-k$ éléments. On a donc :

$$\left|\mathrm{A}_{i_1}\cap\ldots\cap\mathrm{A}_{i_k}\right| = (n-k)!.$$

Par conséquent : $\mathrm{S}_k = \binom{n}{k}(n-k)! = n!/k!$. On en déduit que le nombre de dérangements vaut :

$$\mathrm{D}_n = n!\sum_{k=1}^{n}\frac{(-1)^k}{k!}.$$ □

△ REMARQUE 3.9: On a la formule de récurrence $\mathrm{D}_n = n\mathrm{D}_{n-1}+(-1)^n$ pour $n>0$. En effet

$$\mathrm{D}_n = n!\sum_{k=1}^{n}\frac{(-1)^k}{k!} = n(n-1)!\left[\sum_{k=1}^{n-1}\frac{(-1)^k}{k!}+\frac{(-1)^n}{n!}\right] = n\mathrm{D}_{n-1}+(-1)^n$$

Par ailleurs, vu que $\mathrm{e}^{-1} = \sum_{k=0}^{\infty}(-1)^k/k!$, on a

$$\mathrm{D}_n = n!\left[\mathrm{e}^{-1}-\sum_{k=n+1}^{\infty}\frac{(-1)^k}{k!}\right]$$

La série donnant e^{-1} a des termes de signes alternés et de valeurs absolues décroissantes, donc la somme est majorée par le module du premier terme $1/n+1<1/2$. Ainsi D_n est le plus proche entier de $n!\mathrm{e}^{-1}$

Notons que la proportion de dérangements parmi les $n!$ permutations d'un ensemble à n éléments est égal à la somme $\sum_{j=0}^{n}\frac{(-1)^j}{j!}$ qui converge vers la somme $e^{-1}=\frac{1}{e}$ de la série convergente $\sum_{j=0}^{+\infty}\frac{(-1)^j}{j!}$. Ainsi la proportion de dérangements d'un ensemble fini de "grand" cardinal est proche de $e^{-1}\approx 0,3679 = 36,79\%$. ▽

3.6 Figures géométriques

Dans cette section nous donnons trois exemples de dénombrement de figures géométriques.

1. Pour deux entiers m,n non nuls, soit une grille rectangulaire de longueur m et de hauteur n, avec le point origine O = (0,0) et le point final F = (m,n). Un chemin tracé sur la grille est l'union de segments entiers horizontaux et verticaux. On considère les chemins joignant l'origine O et le point final F de longueur minimale $m+n$ (*i. e.* chaque pas unitaire le long de ce chemin est dirigé horizontalement vers la droite ou verticalement vers le haut). Combien y-a-t-il de tels chemins?

   Le nombre de chemins de longueur minimale entre O et F est égal à

   $$\binom{m+n}{m} = \binom{m+n}{n}.$$

   Un chemin minimal est de longueur $m+n$: en projetant sur les côtés horizontaux et verticaux, il est constaté qu'un tel chemin a m segments horizontaux et n segments verticaux. Un chemin correspond au choix de ces m segments (ou des n segments unitaires verticaux, en complémentaire des segments unitaires horizontaux), *i. e.* une partie de m segments unitaires horizontaux de l'ensemble des $m+n$ pas unitaires (soit en horizontale, soit en vertical) constituant le chemin. Autrement dit, un chemin est caractérisé par un mot HVVHHHHVHVHV en les lettres H et V contenant m (resp. n) fois la lettre H (V resp.) : le choix de la position des m lettres H dans ce mot est quelconque, il y a donc $\binom{m+n}{m}$ tels mots : c'est nombre de chemins!

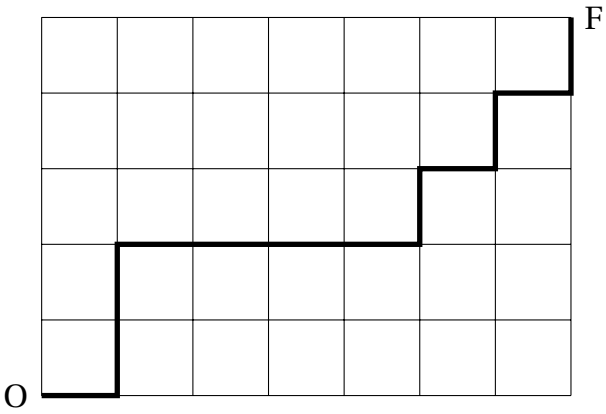

FIGURE III.1 – Un chemin de longueur minimale entre les deux sommets opposés O et F d'une grille rectangulaire $(7,5)$.

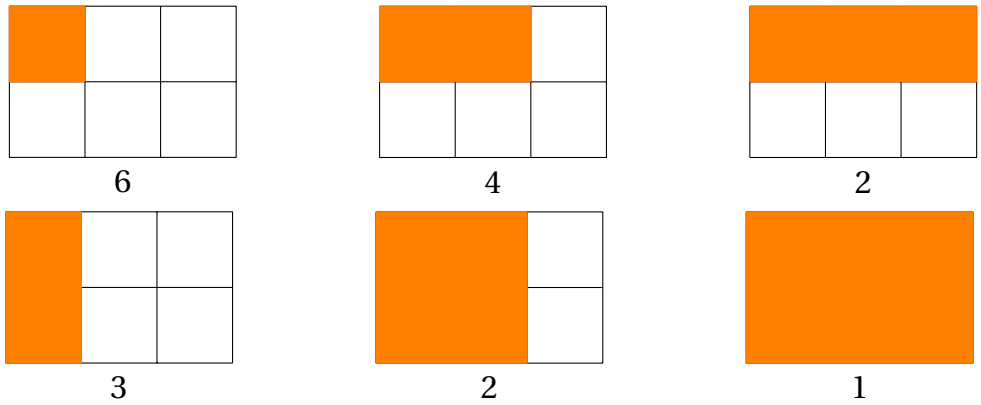

FIGURE III.2 – Rectangles de différents types inclus dans une grille $(3,2)$: il y en a $\binom{4}{3}\binom{3}{2} = \frac{3\cdot4}{2}\frac{2\cdot3}{2} = 18$ au total.

2. Pour deux entiers m,n non nuls, soit une grille rectangulaire de longueur m et de hauteur n. On considère les rectangles d'aire non nulle tracés sur cette grille : combien y-en-a-t-il?
   Le nombre de rectangles inscrits dans une grille de taille (m,n) est
   $$\frac{m(m+1)n(n+1)}{4} = \binom{m+1}{2}\binom{n+1}{2}.$$
   Il suffit de remarquer qu'un rectangle est caractérisé par ses deux projections sur un côté horizontal de la grille, *i. e.* deux nombres $m_1 < m_2$, soit une partie à deux éléments de $[\![1,m]\!]$ et de même $n_1 > n_2$ pour les côtés verticaux. De telles projections (aux directions horizontales et verticales indépendantes) sur le côté vertical sont au nombre de $\binom{n}{2}$, $\binom{m}{2}$ sur le côté horizontal, d'où le résultat.
3. Soit le polygone P_n régulier à $n+2$ sommets numérotés (le problème vaut de manière équivalente pour un polygone convexe). En rajoutant des cordes (*i. e.* des segments entre les sommets distincts) sans autre intersection qu'aux sommets et un nombre maximal $n-1$, on obtient une triangulation du polygone P_n. Combien de telles triangulations existe-t-il?
   Il y a
   $$\mathrm{C}_n = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1} = \frac{(2n)!}{(n+1)!n!} = \prod_{k=2}^{n}\frac{n+k}{k}, \quad n \geq 0.$$

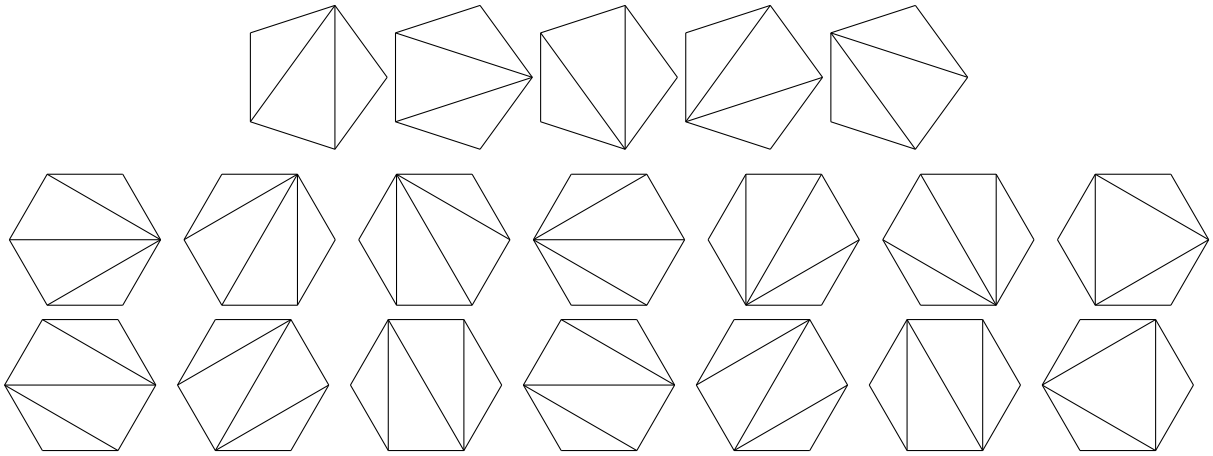

FIGURE III.3 – Les 5 triangulations du pentagone, suivies des 14 triangulations de l'hexagone.

triangulations distinctes dans un polygone convexe à $n+2$ sommets. La deuxième formule assure que C_n est un entier (ce qui n'est pas immédiat pour les autres expressions). La suite (C_n) des 10 premiers nombres de Catalan [19] est

$$1, 1, 2, 5, 14, 42, 132, 429, 1\,430, 4\,862$$

où il a été convenu $C_0 = 1$ pour la bonne validité des formules. Soit sur le polygone P_n un côté c d'extrémités a, b. Considérons une triangulation $\mathcal{T}$ de P_n. Il existe un sommet s de P_n (différent de a et b) tel que le coté c fasse partie d'un triangle $T_s = (a, b, s)$ de la triangulation $\mathcal{T}$. Si on retire ce triangle du polygone P_n (en ôtant l'intérieur du triangle, puis le côté c), on obtient deux polygones convexes triangulés avec $p+2$ sommets et $q+2$ sommets resp. tels que $p+q = n-1$ et $p, q \geq 0$: on a donc C_pC_q triangulations du polygone P_n contenant le triangle T_s. Faisant varier s parmi les sommets de P_n en dehors des sommets a et b, on obtient la relation de récurrence

$$C_n = \sum_{\substack{p,q\geq 0 \\ p+q=n-1}} C_pC_q = \sum_{k=0}^{n-1} C_kC_{n-1-k}, \quad n \geq 0,$$

avec $C_0 = 1$ (les termes extrêmes de la somme précédente sont bien justifiés). Cette relation de récurrence induit pour la fonction génératrice $C(X) = \sum_{n\geq 0} C_nX^n$ la relation fonctionnelle $C(X) = 1 + XC(X)^2$ qui, avec la condition $C_0 = 1$, se résout simplement en

$$C(X) = \frac{1-(1-4X)^{1/2}}{2X}$$

et dont le développement donne les nombres de Catalan

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Les nombres de Catalan interviennent dans le comptage de très nombreux problèmes combinatoires (arbres binaires ou enracinés, parenthésages cohérents,...).

19. Eugène Charles Catalan, 30 mai 1814, Bruges, Belgique – 14 février 1894, Liège, Belgique.

Bibliographie

[1] Martin Aigner, Günter M. Ziegler, *Raisonnements divins, quelques démonstrations mathématiques particulièrement élégantes*, Springer, 2013.

[2] Jeremy Avigad, *Mathematics and language*. In : Davis E., Davis P. (eds) Mathematics, Substance and Surmise. Springer, Cham, 2015.

[3] Olivier Bailleux, *Logique propositionnelle : un cours introductif*, YouTube (dernière consultation en janvier 2019).

[4] Nicolas Bourbaki, *Théorie des ensembles*, Springer, 2007.

[5] Alain Connes, *La conversation scientifique*, France Culture, 17 février 2018.

[6] Patrick Dehornoy, *La théorie des ensembles*, Paris, 2017.

[7] Roger Godement, *Algèbre*, Hermann, 1963.

[8] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Mathématiques concrètes : fondations pour l'informatique*, 2013.

[9] Internet, 2018.

[10] Wikipedia (en, de), 2019.

[11] Bernard Ycart, *M@ths en ligne* (dernière consultation en janvier 2019).