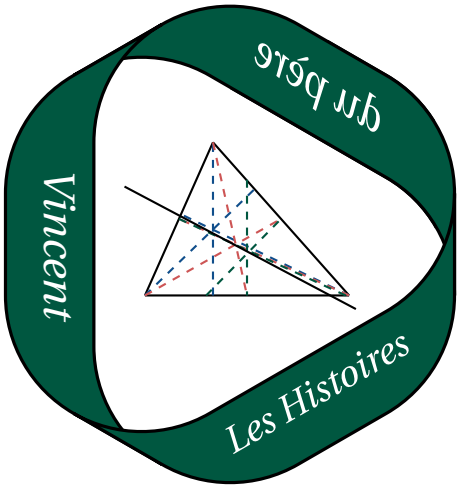


Méthodologie pour les mathématiques
Licence 1

Yannick VINCENT
Université Gustave Eiffel

www.yannickvincent.fr

Table des matières

Quelques conseils pour progresser

Si chacun a ses propres habitudes en ce qui concerne les apprentissages, il existe néanmoins des méthodes plus efficaces que d'autres. Les éléments ci-dessous constitue une liste non-exhaustive de conseils qui peuvent être utiles et que chacun pourra s'approprier à sa façon.

En Cours et en TDs

- **Être attentif** est une condition indispensable pour comprendre. Cela signifie notamment le fait de toujours écouter les explications données par le professeur. Cela inclus y compris le fait de ne pas demander des explications à son voisin sur une notion que le professeur est justement en train d'expliquer. Il y a des temps prévus pour le travail en groupe (parfois en TD par exemple) et d'autres où il est nécessaire d'écouter. Ne pas respecter ces différents moments apportera de la confusion et ne vous permettra pas de progresser.

- **L'écoute en cours doit être active**. Lorsque l'on écoute un cours, il faut toujours se poser les questions suivantes :

  1. Est-ce que j'ai compris exactement ce que dit le professeur ?
  2. Est-ce que je sais identifier précisément quelle proposition ou quelle définition on utilise dans le raisonnement ?
  3. Est-ce que je comprend globalement pourquoi on est en train de faire ce que l'on fait ? (à quoi cela sert)

  Cette dernière question étant d'ordre plus général, il est parfois nécessaire de la mettre provisoirement de côté afin de se concentrer dans un premier temps sur les aspects plus techniques. Cependant, il est toujours important d'y revenir par la suite car c'est cela qui vous permettra de vous approprier pleinement les notions et et de leur donner un sens.

- **Poser des questions**. Le fait de poser des questions lorsque l'on ne comprend pas (en demandant simplement au professeur de reexpliquer) est ce qui permettra au professeur de se mettre à votre niveau et d'adapter au mieux son cours. Cela rendra les choses plus faciles pour tout le monde et vous permettra de mieux comprendre la suite. S'il n'est pas toujours facile de poser une question en amphithéâtre, les Travaux Dirigés sont en revanche un lieu privilégié pour le faire.

- **Noter les passages pas clairs** (en faisant une petite croix dans la marge par exemple) est une astuce à retenir pour pouvoir revenir dessus après le cours. Dans le cas où vous êtes un peu perdu, il est inutile de paniquer mais il faut faire l'effort de s'accrocher. Il y a en fait pleins d'occasions de reprendre le fil : lorsque l'on termine une démonstration compliquée et que l'on passe à un autre théorème par exemple.

- **Lors des Travaux Dirigés**, il est nécessaire de ne pas attendre la correction mais de chercher activement les exercices. C'est notamment un moment privilégié pour revenir sur une méthode classique vue en cours afin de l'assimiler. Lorsque l'on ne sait pas faire un exercice, une erreur classique est de se tourner tout de suite vers un camarade pour demander des explications. Si la collaboration est quelque chose d'important, il est néanmoins tout aussi important de commencer à chercher un exercice seul. Ce n'est qu'après avoir bien cerné et identifié vos propres difficultés face à cet exercice que vous pourrez poser une questions plus précise à un camarade. Là aussi, il s'agit finalement de toujours être actif face aux apprentissages.

- Le point précédent ne doit pas masquer toute **l'importance de s'entraider entre camarades**. L'entraide est d'ailleurs tout aussi importante pour celui qui se fait aider que pour celui qui aide. Expliquer quelque chose permet en effet de s'assurer que l'on a bien compris soi-même. La collaboration entre étudiants est donc tout à fait importante. Il y a simplement un moment pour le faire.

À la maison

- **Travailler régulièrement** en revoyant systématiquement son cours avant le cours suivant et en faisant des exercices est indispensable. Travailler avec des camarades en allant par exemple à la Bibliothèque peut d'ailleurs être un bon moyen de se motiver.

- **Faire les devoirs demandés**, que ce soit les exercices donnés d'une séance à l'autre, ou les Devoirs maisons éventuels. En ce qui concerne les Devoirs maisons, il est important de passer du temps à les chercher seul. Ce n'est qu'après avoir cherché longtemps seul qu'il peut être utile de se faire aider. Quoi qu'il en soit, et même si vous vous faites aider par un ami, un professeur particulier ou que vous allez chercher des réponses sur internet, il est important que vous preniez le temps de rédiger seul votre Devoir. C'est en faisant ce travail de rédaction seul, sans recopier sur un autre étudiant ou sur un document trouvé sur internet, que vous verrez si vous avez vraiment compris ce qu'on vous avait expliqué.

- **Revoir le cours** ne signifie pas simplement le lire. Pour revoir le cours efficacement, il est possible de procéder en plusieurs étapes. La première étape consiste à relire rapidement le cours, en ne lisant pas les démonstrations et les points de détails par exemple mais en se concentrant sur la structure du cours, les définitions et les propositions importantes, *etc.* L'objectif est de faire de premiers liens entre les idées présentées dans le cours. Dans une deuxième étape, il s'agit de relire le cours de manière beaucoup plus approfondie afin de le comprendre en détails. Cette étape nécessite non seulement de lire mais aussi de refaire les démonstrations, les exemples, *etc.* **Revoir un cours de mathématiques se fait donc nécessairement un crayon à la main.** Dans une dernière étape, vous pouvez apprendre le cours en tant que tel : il faut connaître les définitions et les propositions de manière précise, sans oublier aucune hypothèse, et savoir les réciter. Cela ne doit pas être approximatif car c'est en connaissant bien le contenu de votre cours que vous pourrez résoudre des exercices sans vous tromper.

- **Faire et refaire des exercices**. Étant donné que les évaluations consistent majoritairement à résoudre des exercices, il est clair qu'il est important de s'entraîner à cela. Là aussi, il ne faut pas se contenter de relire les exercices vus en classe mais s'assurer que l'on est capable de les refaire, crayon en main. Tant que l'on est pas capable de refaire l'exercice sans aide du corrigé, il faut considérer que les notions ne sont pas complètement acquises et qu'il faudra donc refaire les exercices en questions le lendemain ou quelques jours plus tard.

- Il est important de savoir **trouver un équilibre entre l'apprentissage du cours et la résolution d'exercices**. Parfois, certains étudiants pensent que le fait de connaître précisément le cours est inutile car ce n'est pas ce qui sera directement évalué. C'est une erreur car c'est justement la connaissance du cours qui vous permettra de savoir si vous avez le droit d'utiliser un théorème ou non, et vous évitera de tomber dans les pièges classiques. A contrario, apprendre son cours sans faire d'exercices n'est pas une stratégie efficace. Il faut donc apprendre à gérer son planning de révisions afin de travailler à la fois le cours et les exercices.

- **Faire des fiches de révisions** peut s'avérer être une aide précieuse. Il existe différents types de fiches :
  — les **fiches de synthèse du cours** qui récapitulent les points important (définitions, propositions). Cela peut être utile dans un objectif de mémorisation du cours même s'il faut veiller à ne pas considérer qu'il y aurait des éléments du cours à retenir (ceux que l'on met dans ses fiches) et d'autres qui seraient accessoires (ceux que l'on n'a pas retenu). Tout ce qui est dans le cours doit être considéré comme étant important.
  — les **fiches méthodes** qui listent les différentes techniques ou astuces vues dans les exercices. Cela permet d'éviter les confusions entre les différentes méthodes vues en cours. De plus, certaines méthodes sont présentées dans le cours et peuvent être considérées comme des applications directes mais auront simplement été vues dans le cadre d'exercices. Faire une « fiche méthode » permettra ainsi de faire une synthèse de toutes ces méthodes. Concrètement, il s'agit de passer en revue la liste de tous les exercices faits dans le chapitre et de se poser la question suivante : « Quelle méthode ou idée puis-je retenir de cet exercice ? ». La réponse est individuelle et assez subjective mais l'important est surtout de vous poser la question, d'y apporter une réponse, et de mémoriser ces idées. Faire une fiche méthode, la relire et la réciter très régulièrement vous per-

mettra d'être au clair sur toutes les techniques que vous avez vues. Ce genre de « fiches méthodes » n'est pas forcément très courante chez les étudiants. Elle vous permettra néanmoins d'avoir des idées lorsque vous voudrez résoudre des exercices plus difficiles car vous pourrez alors vous inspirez des méthodes que vous connaissez. Cela n'est pas très long à faire (seulement quelques minutes par exercices) mais permet réellement de progresser.

- **S'entrainer à bien rédiger** n'est pas facultatif. Cela permet d'éviter la confusion et d'exprimer le plus clairement possible ses idées. Pour cela, vous pouvez prendre modèle sur les exemples du cours et sur les exercices corrigés en classe.

- N'hésitez pas à **faire des exercices supplémentaires** car plus vous en ferez, plus les méthodes deviendront des automatismes et moins vous ferez d'erreurs. Essayer par ailleurs d'inventer vos propres exercices est une activité très formatrice qui peut se faire à plusieurs (vous créez chacun un exercice et vous résolvez ensuite celui de l'autre).

Structuration du document

Ce document comporte essentiellement cinq chapitres ainsi que deux chapitres d'annexes. Les cinq chapitres suivants seront traités en Cours et en Travaux Dirigés tout au long du semestre de Méthodologie :

1. Logique et ensembles
2. Arithmétique
3. Applications
4. Polynômes
5. Groupes

Le chapitre A de l'annexe traite des sommes et sera traité dans le cadre d'heures de cours « à part ». Le chapitre B de l'annexe ne sera en revanche pas traité en cours et ne sera donc pas exigible aux examens. Il peut cependant apporter des compléments intéressants permettant de mieux comprendre le chapitre sur les groupes et le lien avec l'arithmétique. Les résultats de ce chapitre seront vus dans la suite de votre cursus.

Dans chaque chapitre, le cours présente une série de définitions (en bleu) et de propositions/théorèmes (en vert). Les démonstrations ne figurent pas sur le document papier. Elles seront faites en cours et les prendre en notes de manière exhaustive est bien entendu indispensable pour progresser. Quelques démonstrations seront d'ailleurs demandées aux examens. Les exemples sont corrigés dans la version en ligne à l'inverse des exercices. L'ensemble des exemples seront traités en cours ainsi que quelques exercices. Là aussi, une prise de notes précise est indispensable. Les exercices non traités en cours pourra par ailleurs fournir une base de questions permettant de s'exercer.

Vocabulaire mathématique

Les points « Étymologie » sont extraits de *Les mots et les maths, dictionnaire historique et étymologique du vocabulaire mathématique*, Bertrand Hauchecorne, 2014, ellipses.

Mathématiques

Étymologie : Le mot *mathématique* nous vient du grec *mathema* ou plutôt de son pluriel *mathemata*. ce mot désignait aussi bien le fait d'apprendre que son résultat : la connaissance, la science. Sous l'influence de Platon et d'Aristote pour qui les mathématiques sont un avoir fondamental, le mot se spécialise dans ce que nous appelons les mathématiques, au sens le plus large.
L'usage du pluriel *mathématiques* est un hériage de l'époque antique et médiévale où le *quadrivium* regroupait les quatre *ars mathematica* : l'arithmétique, la géométrie, l'astronomie et la musique.
Plus tard, au XVIII^{e} siècle, on parle des mathématiques sans doute avec l'idée que cette matière englobe des disciplines devenues différentes comme la géométrie, l'algèbre ou même des branches classerait de nos jours en physique. L'utilisation du pluriel semblait en tout cas tout à fait correspondre avec cette pluralité.
Au XX^{e} siècle, à la suite de Bourbaki (Jean Dieudonné en particulier), certains mathématicien-ne-s privilégient l'utilisation du singulier *mathématique* afin d'insister sur l'unité qui existe entre les différentes parties des mathématiques.

Définition

Une définition est acceptée sans démonstration puisqu'elle donne simplement la signification d'un terme à l'aide de concepts déjà définis antèrieurement. La nouvelle notion doit touefois être définie sans ambiguité, ce qui explique que l'on puisse trouver des éléments de preuve sous une définition mathématique. Pour ainsi dire, c'est comme si la définition pouvait se diviser en deux parties : une première partie énoncant une proposition (assurant une existence ou une unicité par exemple) et une seconde partie constituant la définition à proprement parler.
Étymologie : Les mathématiques utilisent de nos jours des concepts définis avec soin afin d'établir des théorèmes précis. Il faut cependant attendre le XVI^{e} siècle, avec le souci de rigueur insufflé à la Renaissance, pour que ce besoin se fasse sentir. Le mot *définition* est un calque du latin *definitio*. Ce dernier désigne une indication précise. On y sent encore l'idée étymologique de marquer une limite. *Définition* n'est d'abord utilisé que pour donner le sens d'un mot. Il faut attendre le XVI^{e} siècle pour que sons sens s'étende à la définition d'un concept.

Proposition

En logique, il s'agit d'une phrase qui ne peut être que vraie ou fausse (principe du tiers exclu).
En mathématiques, il s'agit d'un énoncé qui est vrai. Dans un cours de mathématiques, une proposition est toujours démontrée. Énoncée sous une forme « Si A alors B », on dit que A constitue les hypothèses et que B est la conclusion de la proposition.
Étymologie : Proposer, c'est *poser en avant*. Déjà dans l'Antiquité, *propositio* s'utilise en logique. Repris au XIII^{e} siècle en français, *proposition* désigne un énoncé soumis au consentement des autres.

Théorème

En mathématiques, il est d'usage de réserver le terme *théorème* aux propositions considérées comme particulièrement intéressantes ou importantes. D'un point de vue purement logique, rien ne distingue *théorème* et *proposition*. La différence est plutôt d'ordre subjectif.
Étymologie : Le mot *théorème* est construit sur deux racines grecques. la première *thea* désigne le spectacle, on la reconnait dans *théâtre* et *théorie*. La seconde signifie *observer* ou *contempler*. On la retrouve elle aussi dans *théorie* mais aussi dans *panorama*. *Theorema* désignait à la fois la fête, la méditation et l'objet d'étude. Au début, la pensée mathématique grecque était basée sur l'observation. La rupture fondamentale de ce peuple est de s'être ensuite soucié de justifier un résultat plutôt que de se contenter de l'établir. Le sens du mot *theorema* évolue parallèlement. À l'époque tardive puis chez les Romains il signifie *proposition démontrable*. Bien sûr, la notion de preuve n'était pas celle que nous connaissons de nos jours. Cependant, on peut dire que le mot avait déjà pris le sens actuel. À la Renaissance le souci de démonstration réapparaît en mathématiques. Le mot *théorème* est repris et francisé en 1539.

Axiome

En mathématiques, le mot axiome désignait une proposition qui est évidente en soi dans la tradition mathématique des Éléments d'Euclide. L'axiome est utilisé désormais, en mathématique, pour désigner une vérité première, à l'intérieur d'une théorie. De ce fait, un axiome est accepté sans démonstration. L'ensemble des axiomes d'une théorie doit être non contradictoire.
Étymologie : Dans son sens premier *axiôma* désignait pour les Grecs *prix, valeur* puis par extension ce qui paraît juste, convenable. L'adjectif *axiômatikos* désignait ce qui a un air de dignité ou d'autorité. Le mot est repris en latin puis en français à la Renaissance, époque à laquelle il est utilisé en chirurgie. Il faut attendre le siècle suivant pour voir les mathématiciens puis les philosophes l'employer. Le développement de la logique mathématique donne ensuite une place importante à l'adjectif *axiomatique*.

Postulat

Étymologie : Ce mot est introduit au XVIII^{e} siècle par des mathématiciens travaillant sur Euclide et son cinquième postulat. Il est forgé sur le verbe latin *postulare, demander, souhaiter*. Il désignait une proposition, non nécessairement évidente, que l'on supposait sans pouvoir la démontrer. Il se différenciait à l'époque d'un axiome, vérité évidente en soi mais qu'on ne pouvait démontrer. De nos jours, cette différence n'a plus de sens. Une théorie est basée sur des axiomes : ils sont le principe de base. Leur évidence est fonction de ce qu'elle est censée représenter et n'est plus du domaine de la théorie elle même.

Lemme

C'est une proposition technique, parfois difficile, mais qui n'a pas d'autre application que de permettre la démonstration d'un théorème. Il arrive qu'avec le temps, ce qui semblait un résultat intermédiaire apparaisse comme une proposition fondamentale et devienne un théorème. Parfois, pour des raisons historiques, le nom de *lemme* lui reste accolé. C'est par exemple le cas du lemme de Gauss en arithmétique.
Étymologie : Dans l'Antiquité, *lemme* était un terme de logique. Il désignait la majeure du syllogisme, c'est-à-dire la première assertion. Ainsi, dans la dialectique grecque, le lemme, le prolemme et l'épiphore sont les trois parties de l'argument. Par extension, le mot désigne ensuite en mathématiques l'un des arguments de la preuve sans en être le fondement.

Corollaire

C'est une proposition qui découle clairement (donc sans démonstration ou presque) d'un théorème établi.
Étymologie : Du latin *corolla* qui signifie petite couronne. *Corollaire* désigne quelque chose d'aucune valeur, de gratuit. Il apparaît puis se spécialise dans son sens mathématique au XVII^{e} siècle.

Conjecture

Il s'agit d'une proposition non démontrée et que les mathématicien-ne-s cherchent à démontrer. poser une conjecture est un processus fondamental dans la recherche en mathématiques. Les conjectures les plus célèbres qui ont été démontrées récemment sont, sans doute, le grand théorème de Fermat et la conjecture de Poincaré.
Étymologie : du latin *conjectura*, dérivé de *cum* et *jacio* (littéralement jeté avec).

Chapitre 1

Logique et ensembles

Introduction

Exemples d'introduction : Vrai ou faux?
$2 \in \mathbb{N}$? $2 \in \mathbb{Z}$? $2 \in \mathbb{D}$? $2 \in \mathbb{Q}$? $2 \in \mathbb{R}$? $2 \in \mathbb{C}$?
Idem pour -2, $\frac{1}{3}$, $\frac{\sqrt{2}}{2}$.
$\{-2, \sqrt{2}, \frac{1}{3}\} \subset \mathbb{N}$? $\subset \mathbb{Q}$? $\subset \mathbb{R}$?
Pour démontrer qu'un élément est dans un ensemble, on peut utiliser les propriétés classiques ci-dessous. Ces propriétés seront utilisées tout au long du semestre et doivent être connues.

Proposition 1.1

Les règles de calculs suivantes sont valables pour des nombres appartenant à $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Les premières sont également vraies sur $\mathbb{C}$. Attention! Les relations d'ordre n'ont en revanche pas de sens dans $\mathbb{C}$.

	Addition	Multiplication
Associativité	(n+m)+k =n+(m+k)	(nm)k=n(mk)
Commutativité	$n+m=m+n$	nm=mn
Distributivité	$n(m+k)=nm+nk$	
Élément neutre	$n+0=0+n=n$	$n\times 1=1\times n=n$
Simplification	Si $n+k=m+k$, alors $n=m$	Si ($k\neq 0$ et $nk=mk$), alors $n=m$
Somme nulle	Si ($n\geqslant 0$, $m\geqslant 0$ et $n+m=0$), alors $n=0$ et $m=0$	
Produit nul		Si $nm=0$, alors $n=0$ ou $m=0$
Monotonie	$n\leqslant m$ ssi $n+k\leqslant m+k$	Pour tout $k>0$, $n\leqslant m$ ssi $nk\leqslant mk$
Réflexivité	$n\leqslant n$	
Transitivité	Si $n\leqslant m$ et $m\leqslant k$, alors $n\leqslant k$	
Antisymétrie	Si $n\leqslant m$ et $m\leqslant n$, alors $n=m$	

I. Premiers éléments de logique

1. « Négation », « et », « ou »

Remarque. *En logique classique, une phrase ne peut être que vraie ou fausse (c'est le principe du tiers exclu).*

Définition 1.1

La **négation** de la proposition A, notée non(A), est la proposition qui est fausse quand A est vraie et vraie quand A est fausse.

Remarque. *non(non(A))=A.*

Définition 1.2

- On dit que la proposition « A et B » est vraie lorsque A et B sont toutes les deux vraies. Elle est fausse sinon.
- On dit que la proposition « A ou B » est vraie si au moins l'une des deux assertions est vraie. Elle est fausse si A et B sont toutes les deux fausses.

Proposition 1.2

- La négation de « P et Q » est « non(P) ou non(Q) ».
- La négation de « P ou Q » est « non(P) et non(Q) ».

Exemple 1. *La négation de « toutes les personnes du groupe sont majeures et vaccinées » est « toutes les personnes du groupe ne sont pas majeures ou toutes les personnes du groupe ne sont pas vaccinées ».*

2. L'implication logique

Définition 1.3 – Implication

L'implication « A $\Longrightarrow$ B » n'est fausse que dans le cas où A est vraie et B est fausse.

Remarque.

- *Affirmer que l'implication «* A $\Longrightarrow$ B *» est vraie ne signifie pas que* A *et* B *soient vraies. Cela signifie simplement que, ou bien* A *et* B *sont simultanément vraies, ou bien* A *est fausse (et on ne sait alors rien dire de* B*).*
- *En pratique, on pensera l'implication «* A $\Longrightarrow$ B *» comme étant « Si* A *est vraie, alors* B *est vraie ».*
- *En mathématiques, lorsqu'on énonce une proposition sous la forme* A $\Longrightarrow$ B*, on dit que* A *correspond aux hypothèses et* B *à la conclusion. On dit aussi que* A *est une condition suffisante à* B *et que* B *est une condition nécessaire à* B*.*

Exemple 2. *On considère l'implication « Si une personne est en licence, alors elle a eu son baccalauréat ». Cette phrase est vraie. Cela ne signifie pas que, lorsqu'on croise une personne dans la rue, elle soit forcément en licence et qu'elle ait eu son baccalauréat. En revanche, cela signifie que :*

- *soit elle est en licence, et on peut être sûr qu'elle a eu son baccalauréat.*
- *soit elle n'est pas en licence, et on ne peut pas savoir si elle a eu son baccalauréat.*

Exemple 3. *L'implication « S'il existe un être humain de plus de 30m, alors 0=1 » est vraie car la condition « il existe un être humain de plus de 30m » n'est jamais réalisée.*

Exemple 4. *Dans la proposition : « Si* ABCD *est un carré, alors* AB = BC = CD = AD *», la proposition «* ABCD *est un carré » est une condition suffisante à «* AB = BC = CD = AD *». En revanche, la proposition «* AB = BC = CD = AD *» est une condition nécessaire à «* ABCD *est un carré ».*

Proposition 1.3

La **négation** de l'implication « A $\Longrightarrow$ B » est « A et non(B) ».

Remarque.

- *Cela signifie que pour montrer qu'une implication soit fausse, il faut trouver un cas dans lequel* A *est vraie et (mais)* B *est fausse. Par exemple «* $x > 0 \Longrightarrow x > 1$ *» est fausse car on peut trouver un nombre réel* x *tel que* $x > 0$ *est vraie et tel que* $x > 1$ *est fausse. Il suffit par exemple de prendre* $x = \frac{1}{2}$*.*
- *On notera bien que la négation d'une implication n'est pas une implication.*

Exemple 5. *La négation de « s'il pleut, alors je reste chez moi » est « il pleut et je ne reste pas chez moi ».*

Proposition 1.4

La **réciproque** de l'implication « A $\Longrightarrow$ B » est « B $\Longrightarrow$ A ». On dit que A et B sont équivalentes, et on note A $\Longleftrightarrow$ B, si « A $\Longrightarrow$ B » et « B $\Longrightarrow$ A ».

Remarque.

- *Attention, ce n'est pas parce que* A $\Longrightarrow$ B *est vraie que sa réciproque est vraie. Par exemple, la proposition « Si* $x \geqslant 1$*, alors* $x \geqslant 0$ *» est vraie mais sa réciproque est fausse.*
- *Lorsque* A $\Longleftrightarrow$ B*, on dit que «* A *est vraie, si et seulement si,* B *est vraie ».*

Exercice 1. *On considère la proposition* (P) *: « s'il pleut, alors je reste chez moi ».*

1. *Écrire la réciproque de la proposition* P
2. *Si* P *est vraie, sa réciproque est-elle vraie ?*

Proposition 1.5

L'implication « A $\Longrightarrow$ B » est équivalente à « non(B) $\Longrightarrow$ non(A) »

Démonstration. Supposons que l'implication « A $\Longrightarrow$ B »est vraie.
Supposons que non(B) est vraie. C'est donc que A est fausse car sinon, d'après l'implication, on en déduirait que B est vraie. On a bien « non(B) $\Longrightarrow$ non(A) ».
Réciproquement, supposons que l'implication « non(B) $\Longrightarrow$ non(A) » est vraie.
Supposons que A est vraie. C'est donc que B est vraie, car si B était fausse, on pourrait en déduire que non(A) est vraie, c'est-à-dire que A est fausse. □

Définition 1.4

L'implication « non(B) $\Longrightarrow$ non(A) » est appelée la contraposée de « A $\Longrightarrow$ B ».

Exemple 6. *Quelle est la contraposée de « s'il pleut, alors je reste chez moi » ?*

Solution : « Si je ne reste pas chez moi, alors il ne pleut pas ». Clairement, cette implication est équivalente à l'implication « s'il pleut, alors je reste chez moi ».

II. Propositions et quantificateurs

1. Quantificateurs

En logique, il existe deux quantificateurs :

- le quantificateur existentiel $\exists$ (il existe au moins un)
- le quantificateur universel $\forall$ (pour tout).

Les quantificateurs n'ont leur place que dans des formules symboliques et pas au milieu des phrases écrites en français.

Dans une démonstration, pour montrer qu'une proposition est vraie pour tout $x \in$ A, on commencera par considérer un élément x en écrivant « Soit $x \in$ A ».
En revanche, si l'on écrit « $\forall x \in$ A », on considère ici que la variable est muette : elle n'est définie que dans la ligne correspondante. Elle ne pourra donc pas être réutilisée ensuite sans être redéfinie.

De la même manière, l'écriture $\exists x$ rend la variable x muette. Pour démontrer une existence en définissant une variable que l'on réutilisera dans la suite de la preuve, on a en revanche deux possibilités :

- « Il existe $x \in \ldots$ » : on l'utilise lorsque l'on sait qu'un élément existe sans savoir nécessairement l'exhiber.
  Exemple : d'après le théorème des valeurs intermédiaires, il existe $x_0 \in [0,10]$ …
- « On pose $x = \ldots$ » : on l'utilise afin de définir un élément de manière explicite. À noter que la définition de x peut faire intervenir d'autres variables déjà définies dans la démonstration (des variables parlantes).
  Exemple : montrer qu'il existe $x \in \mathbb{R}$ tel que $x^2 > 10$.

Solution : On pose $x = 4$. On a $x^2 = 16$ donc $x^2 > 10$.

Remarque. *De manière générale, on veillera à ce que toute variable utilisée dans une copie soit bien définie au préalable.*

Exemple 7. *Montrer la proposition suivante : si n est un entier naturel pair, alors n^2 est pair.*
Rappel : un entier $n \in \mathbb{N}$ est pair s'il existe $k \in \mathbb{N}$ tel que $n = 2k$.

Solution : Soit $n \in \mathbb{N}$ un entier naturel pair.
Il existe $k \in \mathbb{N}$ tel que $n = 2k$.
Ainsi, $n^2 = (2k)^2 = 4k^2 = 2 \times 2k^2$.
On pose $k' = 2k^2$.
Par conséquent, $n^2 = 2k'$, ce qui signifie que n^2 est pair.

Exemple 8. *Montrer la proposition suivante : $\forall x \in \mathbb{Q}^*, \exists y \in \mathbb{Q}$ tel que $xy = 1$.*

Solution : Soit $x \in \mathbb{Q}^*$.
Il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}$ tel que $x = \dfrac{p}{q}$.
De plus, comme $x \neq 0$, on sait que $p \neq 0$.
On pose $y = \dfrac{q}{p}$ (cela est possible car $p \neq 0$).
Ainsi,

$$xy = \frac{p}{q} \times \frac{q}{p} = 1.$$

Remarque. *On rencontre aussi la notation $\exists! x$ pour signifier « il existe un unique x ».*

2. Négation

Proposition 1.6

La négation de « $\forall x$, P(x) est vraie » est « $\exists x$, tel que P(x) est fausse ».
La négation de « $\exists x$, P(x) est vraie », est « $\forall x$, P(x) est fausse ».

Exemple 9. *Soit* A *un ensemble de nombres.*
La négation de « $\exists x \in$ A tel que $x > 0$ » est « $\forall x \in$ A, $x \leqslant 0$ ».
La négation de « $\forall x \in$ A, $x \geqslant 0$ » est « $\exists x \in$ A tel que $x < 0$ ».

Exemple 10. *Soient* A *et* B *deux points du plan et soit $\mathscr{D}$ une droite. Écrire la négation de la proposition suivante : Pour tout point* $M \in \mathscr{D}$, AM = BM.

Solution : Il existe un point $M \in \mathscr{D}$ *tel que* $AM \neq BM$.

3. Commutativité des quantificateurs identiques

La phrase $\forall x, \forall y, \ldots$ a la même signification que $\forall y, \forall x, \ldots$
La phrase $\exists x, \exists y, \ldots$ a la même signification que $\exists y, \exists x, \ldots$

4. Non-commutativité des quantificateurs différents

Lorsqu'on écrit plusieurs quantificateurs différents à la suite, le sens de la proposition dépend de l'ordre des quantificateurs.

Exercice 2. *Les propositions suivantes sont-elles vraies ou fausses ?*
- $\forall x \in \mathbb{R}^*, \exists y \in \mathbb{R}^*$ *tel que* $xy = 1$
- $\exists y \in \mathbb{R}^*$ *tel que* $\forall x \in \mathbb{R}^*, xy = 1$

III. Techniques de raisonnements

1. Raisonnement par implications successives

On suppose A et on prouve la proposition B en déduisant un certain nombre de propositions intermédiaires.

Exemple 11. *Montrer que :*

$$\forall x>1, \forall y>1, \left(\frac{x}{1+x^2}=\frac{y}{1+y^2} \Longrightarrow x=y\right).$$

Solution : Soit $x>1$, soit $y>1$.
Supposons que $\frac{x}{1+x^2}=\frac{y}{1+y^2}$. Alors, $x(1+y^2)=y(1+x^2)$
Donc $x+xy^2=y+yx^2$
Donc $x+xy^2-y-yx^2=0$
Donc $x-y-xy(x-y)=0$
Donc $(x-y)(1-xy)=0$
Donc, d'après la règle du produit nul : $x=y$ ou $xy=1$. Or, l'égalité $xy=1$ est impossible car $x>1$ et $y>1$ donc $xy>1$.
Ainsi, on en déduit que $x=y$.

2. Raisonnement par équivalences successives

On montre que A est équivalente à B en établissant une suite d'équivalences intermédiaires.
Attention! L'utilisation systématique du symbole $\Longleftrightarrow$ est à proscrire. Il pousse souvent à écrire des choses fausses ou inutiles. On l'utilisera en revanche dans le cadre de résolutions d'équations.

Exemple 12. *Résoudre le système suivant dans $\mathbb{R}^2$:* $\begin{cases} 2x_1 + x_2 = 1 \\ x_1 - x_2 = 4 \end{cases}$

Solution : Soit $(x_1,x_2)\in\mathbb{R}^2$,

$$\begin{aligned}
&\begin{cases} 2x_1 + x_2 = 1 \\ x_1 - x_2 = 4 \end{cases} \\
\underset{L_1\leftrightarrow L_2}{\Longleftrightarrow} &\begin{cases} x_1 - x_2 = 4 \\ 2x_1 + x_2 = 1 \end{cases} \\
\underset{L_2\leftarrow L_2-2L1}{\Longleftrightarrow} &\begin{cases} x_1 - x_2 = 4 \\ 3x_2 = -7 \end{cases} \\
\Longleftrightarrow &\begin{cases} x_1 = \frac{5}{3} \\ x_2 = -\frac{7}{3} \end{cases}
\end{aligned}$$

3. Raisonnement par disjonction de cas

On peut, par exemple, séparer les cas selon la valeur d'une des variables de l'énoncé à démontrer. Il faut néanmoins veiller à bien traiter tous les cas.

Exemple 13. *Montrer que pour tout $n\in\mathbb{N}$, $\frac{n(n+1)}{2}\in\mathbb{N}$.*

Solution : Soit $n\in\mathbb{N}$.

- *Si n est pair :*
  Il existe $k\in\mathbb{N}$ tel que $n=2k$.
  Donc $\frac{n(n+1)}{2}=\frac{2k(2k+1)}{2}=2k+1\in\mathbb{N}$

- *Si n est impair :*
  Il existe $k \in \mathbb{N}$ tel que $n = 2k+1$.
  Donc $\dfrac{n(n+1)}{2} = \dfrac{(2k+1)(2k+2)}{2} = (2k+1)(k+1) \in \mathbb{N}$.

Ainsi, dans tous les cas, $\dfrac{n(n+1)}{2}$ *est un entier naturel.*

4. Raisonnement par contraposée

Pour montrer A $\Longrightarrow$ B, on suppose non(B) et on montre que non(A) est vraie.

Exemple 14. *Soit $n \in \mathbb{N}$. Montrer que si n^2 est pair, alors n est pair.*

Solution :
On va montrer que si n n'est pas pair, alors n^2 n'est pas pair.
Autrement dit, on va montrer que si n est impair, alors n^2 est impair.
Soit $n \in \mathbb{N}$ un entier impair.
Il existe $k \in \mathbb{N}$ tel que $n = 2k+1$.
Ainsi, $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$.
On pose $k' = 2k^2+2k$.
On a donc $n^2 = 2k'+1$, ce qui prouve bien que n^2 est impair.

5. Raisonnement par l'absurde

Pour montrer qu'une proposition A est vraie, on suppose qu'elle est fausse et on montre alors que cela mène à une contradiction.

Exemple 15. *Montrer que $\sqrt{2} \notin \mathbb{Q}$.*

Solution : supposons par l'absurde que $\sqrt{2} \in \mathbb{Q}$.
Ainsi, il existerait deux entiers premiers entre eux $p \in \mathbb{N}$ et $q \in \mathbb{N}$ tels que $\sqrt{2} = \dfrac{p}{q}$.
Donc on aurait $2 = \dfrac{p^2}{q^2}$.
Donc $2q^2 = p^2$ *(*)*
On en déduit que p^2 serait pair et donc que p serait pair (voir exemple précédent).
Ainsi, il existerait $k \in \mathbb{N}$ tel que $p = 2k$.
Donc, en remplaçant dans (*), on aurait $2q^2 = (2k)^2$
Donc $q^2 = 2k^2$.
Ainsi, q^2 serait pair donc q serait pair.
Au final, p et q seraient pairs, ce qui est absurde car on les a supposé premiers entre eux.

Exercice 3. *L'ensemble des nombres décimaux est défini comme l'ensemble des nombres de la forme* $\dfrac{a}{10^n}$ *avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$. Montrer que* $\dfrac{1}{3} \notin \mathbb{D}$

6. Raisonnement par récurrence « faible »

Pour montrer qu'une propriété $\mathscr{P}(n)$ est vraie pour tout entier n supérieur ou égal à un entier n_0 (en général 0 ou 1), on procède de la manière suivante :

- Initialisation : on montre que $\mathscr{P}(n_0)$ est vraie.
- Hérédité : on montre que si $\mathscr{P}(n)$ est vraie pour un certain entier $n \geqslant n_0$, alors $\mathscr{P}(n+1)$ est vraie.

Une fois cela établi, on en conclut que cette propriété est vraie pour tous les nombres entiers naturels supérieurs ou égaux à n_0.

Exemple 16. *Montrer que pour tout $n \in \mathbb{N}$, $2^n \leqslant (n+1)!$.*

Solution : Montrons par récurrence que la proposition $\mathscr{P}(n)$: « $2^n \leqslant (n+1)!$ » est vraie pour tout $n \in \mathbb{N}$.

- *Initialisation : Pour $n = 0$, $2^0 = 1$ et $(0+1)! = 1$ donc on a bien $2^0 \leqslant (0+1)!$.*

- *Hérédité : Supposons que $\mathscr{P}(n)$ est vraie pour un certain entier $n \in \mathbb{N}$. On va montrer qu'alors $\mathscr{P}(n+1)$ est vraie.*
  On a
  $$2^{n+1} = 2 \times 2^n$$
  Or, par hypothèse de récurrence, $2^n \leqslant (n+1)!$. On en déduit donc que $2^{n+1} \leqslant 2 \times (n+1)!$.
  De plus, comme $2 \leqslant (n+2)$, on en déduit :
  $$2^{n+1} \leqslant (n+2) \times (n+1)! \leqslant (n+2)!$$
  Par conséquent $\mathscr{P}(n+1)$ est vraie.

Étymologie – Récurrence

Le verbe latin *recurrere, courir en arrière* a pour participe présent *recurrens*. C'est lui qui nomme notre raisonnement par récurrence apparu au milieu du XIX^{e} siècle. Le r intérieur est redoublé, comme en latin et l'on ne doit pas confondre cette racine avec *curare, prendre soin* que l'on retrouve dans *curé*, celui qui prend soin des âmes, *cure* qui prend soin de la santé et *récurer*, acte de prendre soin des casseroles ! Ceux-ci n'ont qu'un r.

7. Raisonnement par récurrence « double »

Pour l'hérédité, plutôt que de simplement supposer que $\mathscr{P}(n)$ est vraie, on peut supposer que $\mathscr{P}(n)$ et $\mathscr{P}(n-1)$ est vraie. En conséquence, dans l'initialisation, on a besoin de montrer que $\mathscr{P}(n_0)$ et $\mathscr{P}(n_0+1)$ sont vraies.

Exemple 17. *Soit (u_n) la suite définie par $u_0 = 1$, $u_1 = 3$ et $\forall n \in \mathbb{N}$, $u_{n+2} = 3u_{n+1} - 2u_n$.*
Montrer que : $\forall n \in \mathbb{N}$, $u_n = 2^{n+1} - 1$.

Solution : Montrons par récurrence double que la proposition $\mathscr{P}(n)$: « $u_n = 2^{n+1} - 1$ » est vraie pour tout $n \in \mathbb{N}$.

- *Initialisation : Pour $n = 0$: $2^{0+1} - 1 = 1 = u_0$ donc $\mathscr{P}(0)$ est vraie.*
  Pour $n = 1$: $2^{1+1} - 1 = 3 = u_1$ donc $\mathscr{P}(1)$ est vraie.
- *Hérédité : Supposons que $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ soient vraie pour un certain entier $n \in \mathbb{N}$. On va montrer qu'alors $\mathscr{P}(n+2)$ est vraie.*

$$\begin{aligned} u_{n+2} &= 3u_{n+1} - 2u_n \\ &= 3\left(2^{n+2} - 1\right) - 2\left(2^{n+1} - 1\right) && \text{d'après les hypothèses de récurrence} \\ &= 3 \times 2^{n+2} - 3 - 2^{n+2} + 2 \\ &= 2 \times 2^{n+2} - 1 \\ &= 2^{n+3} - 1 \end{aligned}$$

Donc $\mathscr{P}(n+2)$ est vraie.

8. Raisonnement par récurrence « forte »

Pour l'hérédité, plutôt que de simplement supposer que $\mathscr{P}(n)$ est vraie, on peut supposer que $\mathscr{P}(k)$ est vraie pour tout $k \in \{1, \ldots, n\}$.

Exemple 18. *Montrer que tout entier naturel $n \geqslant 2$ admet un diviseur premier. (On rappelle que, par définition, un nombre premier est un nombre entier admettant exactement deux diviseurs : 1 et lui-même).*

Solution : Montrons par récurrence forte que $\mathscr{P}(n)$: « n admet un diviseur premier » est vraie pour tout entier $n \geqslant 2$.

- *Initialisation : $\mathscr{P}(2)$ est vraie car 2 est divisible par le nombre premier 2.*

- *Hérédité : Supposons que, pour un certain $n \geqslant 2$, les propriétés $\mathscr{P}(k)$ sont vraies pour tout $1 \leqslant k \leqslant n$. Montrons qu'alors $\mathscr{P}(n+1)$ est vraie.*
  — *Si $n+1$ est premier, alors $n+1$ est bien divisible par un entier premier (lui-même)*

— *Sinon, il existe un entier k divisant $n+1$ tel que $1 < k < n+1$. En appliquant l'hypothèse de récurrence pour k, on sait qu'il existe un entier premier p divisant k.*
Ainsi, p divise k et k divise $n+1$.
On en déduit que p divise $n+1$ (la preuve est laissée au lecteur).
Au final, $\mathscr{P}(n+1)$ est vraie.

9. Raisonnement par analyse-synthèse

Un raisonnement par analyse-synthèse permet en général de montrer qu'il existe une solution a un problème. Le raisonnement se déroule en deux étapes :

- **l'analyse** : on suppose qu'une solution existe. Par une suite d'implications on en déduit la ou les valeurs possibles pour les solutions.
- **la synthèse** : pour chacune des valeurs obtenues, on vérifie qu'elles sont bien solutions.

Exemple 19. *Montrer la proposition suivante :*

$$\forall z \in \mathbb{C}^*, \exists z' \in \mathbb{C} \text{ tel que } zz' = 1.$$

Solution : Soit $z \in \mathbb{C}^*$.
Il existe $a, b \in \mathbb{R}$ tels que $z = a + ib$.
Dans le cas où $b = 0$, $z \in \mathbb{R}$ et la propriété est évidente. On peut donc supposer que $b \neq 0$.
Analyse : Supposons qu'il existe $z' \in \mathbb{C}$ tel que $zz' = 1$.
Il existe $c, d \in \mathbb{R}$ tels que $z' = c + id$. Ainsi, $(a+ib)(c+id) = 1$
Donc $(ac - bd) + i(ad + bc) = 1$

$$\text{Donc} \begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases}$$

$$\text{Donc} \begin{cases} ac - bd = 1 \\ c = -\frac{ad}{b} \end{cases} \quad (\text{car } b \neq 0)$$

$$\text{Donc} \begin{cases} a \times (-\dfrac{ad}{b}) - bd = 1 \\ c = -\frac{ad}{b} \end{cases}$$

$$\text{Donc} \begin{cases} -\frac{d}{b} \times (a^2 + b^2) = 1 \\ c = -\frac{ad}{b} \end{cases}$$

$$\text{Donc} \begin{cases} d = -\frac{b}{a^2+b^2} \\ c = -\frac{ad}{b} \end{cases} \quad (\text{car } a^2 + b^2 \neq 0)$$

$$\text{Donc} \begin{cases} d = -\frac{b}{a^2+b^2} \\ c = \frac{a}{a^2+b^2} \end{cases}$$

Ainsi, $z' = \dfrac{a}{a^2+b^2} - \dfrac{ib}{a^2+b^2}$.
Cela prouve donc que si z' existe, alors il est unique.

Synthèse : Soit $z = a + ib \in \mathbb{C}^*$ (avec $(a, b \in \mathbb{R})$.
On pose $z' = \dfrac{a}{a^2+b^2} - \dfrac{ib}{a^2+b^2}$ (ce qui est possible car $a^2 + b^2 \neq 0$).
On a alors $z \times z' = (a+ib)\left(\dfrac{a}{a^2+b^2} - \dfrac{ib}{a^2+b^2}\right) = \ldots = 1$.
Cela prouve donc l'existence de z'.

Remarque. *Considérons les premières lignes suivantes de la démonstration :*

> *« Soit $z \in \mathbb{C}^*$.*
> *Il existe $a, b \in \mathbb{R}$ tels que $z = a + ib$. »*

On pourrait les remplacer par « Soit $z = a + ib$ (avec $a, b \in \mathbb{R}$) » qui signifie implicitement la même chose.

Remarque. *Condition nécessaire/suffisante.*
Dans l'analyse, on a montré que, pour que l'inverse existe il est nécessaire que cet inverse soit $\dfrac{a}{a^2+b^2} - \dfrac{ib}{a^2+b^2}$.
Dans la synthèse, on montre qu'il suffit de prendre $\dfrac{a}{a^2+b^2} - \dfrac{ib}{a^2+b^2}$ pour trouver un inverse.

Exercice 4. *Soit une fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$. Montrer qu'il existe une unique fonction p paire et une unique fonction i impaire telles que $f = p + i$.*

IV. Ensemble et description d'un ensemble

1. Généralités

Définition 1.5

Un **ensemble** est une collection d'objets tous définis et tous distincts (par exemple, en mathématiques, des nombres, des fonctions, des points, etc.). En général, on note les ensembles avec une majuscule A, B, ….
Les objets constituants un ensemble sont appelés les éléments (notés en générale avec une minuscule a, x, …).
On écrit $a \in A$ pour dire que « a est un élément de l'ensemble A ».

Afin de décrire un ensemble on utilise des accolades.
Exemples :

- $A = \{1,2\}$. C'est le même ensemble que $\{2,1\}$ ou que $\{1,1,2\}$.
- $\{2\}$: on l'appelle le **singleton** 2 qui est différent du nombre 2.

Étymologie – Ensemble

Ensemble reprend au XI^{e} siècle le latin impérial *insimul*, mot de la même famille que *simultané*. *insimul* signifiait *en même temps*. Le français médiéval y ajoute l'idée d'action conjuguée. Le mot *ensemble* désigne une action faite en même temps par plusieurs personnes. De nos jours, la connotation temporelle a disparu.
Le mot se substantive à la fin du XVII^{e} siècle et désigne alors les éléments d'un tout.
Inspiré par les travaux de Cantor, Dedekind introduit en 1883 la notion d'ensemble en mathématiques et l'appelle *Menge*. Le mot est traduit peu après en français par *ensemble*.

Étymologie – Élément

Le latin *elementa* désignait les lettres de l'alphabet grec et par extension les principes ou les rudiments d'une science. C'est en ce sens qu'il faut comprendre *Les Éléments* d'Euclide. Le mot désigne au Moyen Âge les principes constitutifs. Ceci explique son utilisation pour parler des quatres éléments : eau, terre, feu, air.
Le mot prend le sens de la partie élémentaire d'un tout. Il est d'abord utilisé en mathématiques de manière informelle puis prend un sens précis avec la théorie des ensembles.
On le retrouve dans la *décomposition en éléments simples* notamment.

Étymologie – Singleton

Le mot *singleton* est issu d'un anglicisme. Il a été introduit vers 1960 dans le vocabulaire de la théorie des ensembles, quand, par souci de précision, on a voulu distinguer un élément et l'ensemble contenant cet élément.
Single vient du latin *signularis, seul*, par l'intermédiaire de l'ancien français. cet adjectif latin a donné en français *singulier* mais aussi *sanglier* car cet animal vit souvent isolé. Le suffixe *ton* indique une séparation. On le trouve dans l'anglais *town* mais aussi dans la racine celtique *dun* qui a servi à construire des noms de villes (Lugdunum par exemple pour Lyon).
Singleton était en fait apparu dans le langage des jeux de cartes dès 1650 en anglais et deux siècles plus tard en français pour désigner une carte qui est seule dans sa couleur.

Les ensembles peuvent être décrits :

- **en extension** : on énumère les éléments.
  Exemple : $A = \{0,2,4,6\}$

- **en compréhension** : on demande qu'en plus de faire partie d'un ensemble connu, les éléments satisfassent une ou plusieurs propriétés.
  Exemple : $A = \{n \in \mathbb{N} \mid n \text{ est pair}\}$.
  — Ici, l'ensemble $\mathbb{N}$ est appelé **l'ensemble de référence**
  — La barre | se lit « tel que ».
  — La barre | est suivie de propriété(s) portant sur la variable (ici n est pair).
  Autre exemple :
  $$\{x \in \mathbb{R} \mid |x| \leqslant 2\} = [-2;2]$$
  ‘
- **sous forme paramétrique** : on se donne une variable décrite à l'aide d'un ou plusieurs paramètres.
  Exemple : $I = \{2n \mid n \in \mathbb{N}\}$.
  Le paramètre est n et il parcourt l'ensemble $\mathbb{N}$.
  Les éléments de l'ensemble I ($2n$) sont exprimés en fonction du paramètre n. Autre exemple :
  $$\{a^2 \mid a \in \mathbb{Q}\}$$

Exemples plus élaborés (couples, suites, fonctions) :
- $\left\{(a,b) \in \mathbb{R}^2 \mid |a|+|b| \leqslant 1\right\}$ (écriture en compréhension)
- $\left\{(2n^2, 3p+1) \mid n \in \mathbb{N}, p \in \mathbb{N}, n > p\right\}$ (écriture paramétrique)
- $\left\{(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N}\, u_n \leqslant u_{n+1}\right\}$

Exercice 5.
- *Justifier que* $4 \in \{2n \mid n \in \mathbb{N}\}$
- *Justifier que* $5 \in \{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, n = 2k+1\}$
- *Justifier que* $5 \notin \{2n \mid n \in \mathbb{N}\}$

Remarque. *Les éléments d'un ensemble peuvent être eux-mêmes des ensembles. Par exemple, si* $E = \{\{1\},\{2\},\{2,3\}\}$, *alors* $\{1\} \in E$ *mais* $1 \notin E$.

2. L'ensemble vide

Définition 1.6

L'ensemble vide est l'ensemble ne contenant aucun élément. On le note $\emptyset$.

Exemple 20. $\{n \in 2\mathbb{N} \mid n > 2 \text{ et } n \text{ premier}\} = \emptyset$.

3. Parties d'un ensemble

Définition 1.7

Soient A et B deux ensembles. On dit que B est une **partie** ou un **sous-ensemble** de A si, et seulement si, tous les éléments de B sont des éléments de A. On note $B \subset A$. On dit que B est inclus dans A.
Par convention, pour tout ensemble A, $\emptyset \subset A$.

Définition 1.8

Soit A un ensemble. L'ensemble des parties d'un ensemble, noté $\mathscr{P}(A)$ est l'ensemble constitué par tous les sous-ensembles de A.

Exemple 21. *Si* $A = \{1,2,3\}$, *on a* $\mathscr{P}(A) = \left\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\right\}$

Étymologie – Partie

L'ancien français avait deux verbes *partir*. Nous n'en connaissons plus qu'un seul. Le second a été éliminé par *partager* pour éviter l'homonymie. Il ne subsiste plus que dans l'expression *avoir maille à partir*. La maille était la plus petite pièce de monnaie donc impossible à partager.
Formé sur ce dernier verbe, *partie* désigne dès le Moyen Âge ce qui est inclus dans un tout. On parle ainsi des parties du monde, des parties du corps avec en particulier les parties honteuses qui ont depuis perdu leur qualificatif. Tout naturellement, au XX^{e} siècle, la théorie des ensembles a employé ce mot pour parler des sous-ensembles d'un ensemble.

4. Égalité d'ensembles

Définition 1.9

Deux ensembles A et B sont **égaux** (on note A = B) si, et seulement si, chaque élément de A est aussi dans B et chaque élément de B est aussi dans A. Autrement dit, A = B si, et seulement si, A ⊂ B et B ⊂ A.

Exercice 6. *Montrer que* $\{2p+4q \mid p \in \mathbb{N}, q \in \mathbb{N}\} = \{2n \mid n \in \mathbb{N}\}$.

5. Réunion

Définition 1.10

La **réunion** A ∪ B de deux ensembles A et B est l'ensemble

$$A \cup B = \{x, \mid x \in A \text{ ou } x \in B\}.$$

Exemple 22. *Si* $A = \{1,2,3\}$ *et* $B = \{2,7\}$, *alors* $A \cup B = \{1,2,3,7\}$.

Proposition 1.7

Soit A, B, C des ensembles. Alors,

- A ∪ B = B ∪ A (commutativité)
- (A ∪ B) ∪ C = A ∪ (B ∪ C) (associativité)
- A ∪ ∅ = A
- A ⊂ A ∪ B

Remarque. *Il est possible de prouver formellement la Proposition 1.7 à partir de la définition 1.10. Il est cependant important de retrouver très rapidement ce genre de résultats (voir également la Proposition 1.8) en faisant un diagramme.*

Remarque. *La définition de la réunion se généralise à plus de deux ensembles :*

- *Soient* $A_1, \ldots, A_n$ *des ensembles. On définit,*

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

- *On définit également l'**union quelconque** d'ensembles. Si* I *est un ensemble (fini ou infini) et* $(A_i)_{i \in I}$ *une famille d'ensembles,*

$$\bigcup_{i \in I} A_i = \{x \in E \mid \exists i \in I \text{ tel que } x \in A_i\}.$$

Ici, la variable i *est muette : on peut par exemple la remplacer* i *par* j. *Ainsi,* $\bigcup_{i \in I} A_i = \bigcup_{j \in I} A_j$.

6. Intersection

Définition 1.11

L'**intersection** A ∩ B de deux ensembles A et B est l'ensemble

$$A \cap B = \{x \mid x \in A \text{ et } x \in B\}.$$

Exemple 23. *Si* $A = \{1,2,3\}$ *et* $B = \{2,7\}$, *alors* $A \cap B = \{2\}$.

Exercice 7. *Écrire une proposition similaire à la proposition 1.7 pour l'intersection.*

Remarque. *La définition de la réunion se généralise à plus de deux ensembles :*

- *Soient* $A_1, \ldots, A_n$ *des ensembles. On définit,*

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

- *On définit également l'**intersection quelconque** d'ensembles. Si* I *est un ensemble (fini ou infini),*

$$\bigcap_{i\in I} A_i = \{x \in E \mid \exists i \in I \text{ tel que } x \in A_i\}.$$

Ici aussi, la variable i est muette : on peut par exemple la remplacer i par j. Ainsi, $\bigcap_{i\in I} A_i = \bigcap_{j\in I} A_j$.

Proposition 1.8

Soit A, B, C des ensembles. Alors,
- $(A \cup B) \cap C = (A \cap B) \cup (B \cap C)$
- $(A \cap B) \cup C = (A \cup B) \cap (B \cup C)$

Remarque. *La proposition précédente s'interprète comme une « distributivité » de $\cap$ sur $\cup$ et inversement.*

Définition 1.12

Deux ensembles A et B sont disjoints si $A \cap B = \emptyset$

7. Différence et complémentaire

Définition 1.13

La **différence** $A \setminus B$ de deux ensembles est l'ensemble

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Exemple 24. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Définition 1.14

Si $A \subset X$, l'ensemble $X \setminus A$ s'appelle le **complémentaire** de A dans X. Il est aussi noté $\complement_X A$.
Ainsi, pour tout $x \in X$, $x \in \complement_X A$ si, et seulement si, $x \notin A$.
Lorsqu'il n'y a pas d'ambiguïté sur l'ensemble X, on note $\complement A$ ou A^c.

Proposition 1.9

Soit X un ensemble. Soit $A \subset X$ et $B \subset X$.
- $(A^c)^c = A$
- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

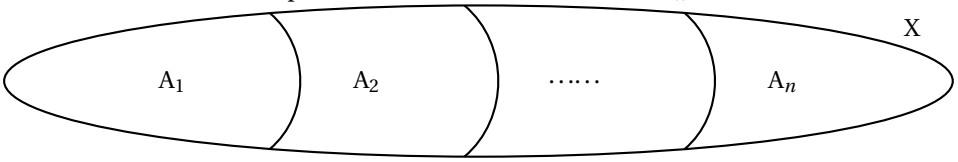
Exemple 25. *L'ensemble* I *des entiers impairs est le complémentaire dans* N *des entiers pairs :* $I = \{2n \mid n \in \mathbb{Z}\}^c$.

8. Partition d'un ensemble

Définition 1.15

Soit X un ensemble non vide et $\mathscr{R} \subset \mathscr{P}(X)$ ($\mathscr{R}$ est un ensemble de parties de X). On dit que $\mathscr{R}$ est une **partition** de X si :
- Pour tout $A \in \mathscr{R}$, $A \neq \emptyset$
- $\bigcup_{A\in\mathscr{R}} A = X$
- Pour tous $A \in \mathscr{R}$ et $B \in \mathscr{R}$ tels que $A \neq B$, $A \cap B = \emptyset$ (les parties sont deux à deux disjointes).

Représentation avec $\mathscr{R} = \{A_1, A_2, \ldots, A_n\}$



Exemple 26. *Soit* $X = \{1,2,3,4,5,6\}$ *et* $\mathscr{R} = \Big\{\{1,3,5\},\{2,4\},\{6\}\Big\}$. *$\mathscr{R}$ est une partition de* X.

Exercice 8. *Donner plusieurs partitions de $\mathbb{Z}$.*

Remarque. *La loi des probabilités totales vue au lycée fait par exemple intervenir la notion de partition.*

9. Produit cartésien d'ensembles

Définition 1.16

Soient A et B deux ensembles. Le produit cartésien de A et B est l'ensemble, noté A × B constitué des couples $(x\,;y)$ où $x \in$ A et $y \in$ B. On a ainsi :

$$\mathrm{A} \times \mathrm{B} = \left\{(x\,;y) \,|\, x \in \mathrm{A}, y \in \mathrm{B}\right\}.$$

Exemple 27. *Si* $A = \{a\,;b\}$ *et* $B = \{5\,;6\,;7\}$, *alors* $A \times B = \Big\{(a\,;5);\,(a\,;6);\,(a\,;7);\,(b\,;5);\,(b\,;6);\,(b\,;7)\Big\}$.

On généralise la définition du produit cartésien à un produit de plus de deux ensembles avec la définition suivante.

Définition 1.17

Soit $n \geqslant 2$ un entier. Soient $\mathrm{A}_1, \mathrm{A}_2, \ldots \mathrm{A}_n$ des ensembles non vides. On définit le produit cartésien des ensembles $\mathrm{A}_1, \mathrm{A}_2, \ldots \mathrm{A}_n$ par :

$$\mathrm{A}_1 \times \mathrm{A}_2 \times \ldots \times \mathrm{A}_n = \Big\{(x_1\,;x_2\,;\ldots\,;x_n) \,|\, \forall 1 \leqslant i \leqslant n, x_i \in \mathrm{A}_i\Big\}$$

Si A est un ensemble, on note A^n le produit de A avec lui-même n fois. Par exemple, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.
On appelle n-uplet un élément de A^n.

Chapitre 2

Arithmétique

I. Relation de divisibilité dans $\mathbb{Z}$

1. Définition et premières propriétés

Définition 2.1

Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On dit aussi que a est un **diviseur** de b et que b est un **multiple** de a. On note $a|b$.

Exemple 1. $3|15$ *car* $15 = 3 \times 5$.

Proposition 2.1

Soit b un entier non nul.

- Si $a|b$ alors $|a| \leqslant |b|$.
- L'entier b admet donc un nombre fini de diviseurs.

Proposition 2.2

Soient $a, b \in \mathbb{Z}$. Alors,

$$a|b \iff -a|b \iff a|-b \iff -a|-b.$$

Démonstration. Montrons que si $a|b$ alors $-a|b$.
Supposons que $a|b$. Par définition, il existe $k \in \mathbb{Z}$ tel que $b = ak$.
Ainsi, $b = (-a) \times (-k)$ et on en déduit donc que $-a|b$.
La réciproque et les autres équivalences se montrent d'une manière similaire. □

2. Propriétés de la divisibilité

Proposition 2.3 – Transitivité

Soient $a, b, c \in \mathbb{Z}$.
Si $a|b$ et $b|c$, alors $a|c$.

Démonstration. Supposons que $a|b$ et $b|c$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $b = ak$. De même, il existe $k' \in \mathbb{Z}$ tel que $c = bk'$.
Finalement, on en déduit que $c = akk'$ et donc que $a|c$. □

Exemple 2. $3|9$ *et* $9|45$ *donc* $3|45$.

Proposition 2.4

Soient $a, b, c \in \mathbb{Z}$ tels que $a|b$ et $a|c$.
- Pour tous $m, n \in \mathrm{Z}$, $a|(mb+nc)$.
- En particulier, $a|(b+c)$ et $a|(b-c)$.

Démonstration. $a|b$ et $a|c$ donc il existe $k \in \mathbb{Z}$ tel que $b = ak$ et il existe $k' \in \mathbb{Z}$ tel que $c = ak'$. Ainsi,

$$mb + nc = mak + nak' = a(mk + nk')$$

et on en déduit donc que $a|(mb+nc)$. □

Exemple 3. $3|60$ *et* $3|27$ *donc* $3|87$

Remarque. *Attention! La proposition « Si* $a|c$ *et si* $b|c$ *alors* $a+b|c$ *» est fausse.*
Par exemple $2|6$ *et* $3|6$ *mais* 5 *ne divise pas* 6.

3. Division euclidienne

Proposition 2.5 – Division euclidienne dans $\mathbb{N}$

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$.
Il existe un unique couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < b$. L'entier q est appelé le quotient de la division de a par b et r le reste.

Remarque. *Pour démontrer cette proposition, on utilisera le fait que tout ensemble* A *inclus dans* $\mathbb{N}$ *et non vide admet un minimum (c'est-à-dire qu'il existe* $m \in$ A *tel que pour tout* $n \in$ A, $m \leqslant n$*).*

Démonstration. Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$.
- Montrons tout d'abord l'existence des entiers q et r.
  On définit l'ensemble $\mathrm{A} = \{a - bn,\ n \in \mathbb{N}\} \bigcap \mathbb{N}$. Alors A est inclus dans $\mathbb{N}$ et est non vide (pour $n = 0$, on voit que $a \in$ A).
  Ainsi, on en déduit que A admet un élément minimum que l'on note r.
  Comme $r \in$ A, par définition de A, il existe $q \in \mathbb{N}$ tel que $a - bq = r$.
  Finalement, on a prouvé qu'il existe des entiers a et r tels que $a = bq + r$. De plus, supposons par l'absurde que $r \geqslant b$. En posant $q' = q + 1$, on aurait $a = bq' + r - b$ et par conséquent, $r - b \in$ A. Cela est absurde car r est l'élément minimum de A.
- Montrons l'unicité du couple (q, r).
  On suppose qu'il existe deux couples (q_1, r_1) et (q_2, r_2) vérifiant les conditions de la propriété.
  Ainsi, $a = bq_1 + r_1 = bq_2 + r_2$.
  On en déduit que $b(q_1 - q_2) = r_2 - r_1$ et donc que $b|r_2 - r_1$. Par ailleurs, on sait que $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$. Par conséquent, $-b < r_2 - r_1 < b$. Comme on a montré par ailleurs que $b|r_2 - r_1$, on en déduit que $r_2 - r_1 = 0$, c'est-à-dire que $r_2 = r_1$. Par suite, on obtient aussi que $q_2 = q_1$ ce qui prouve l'unicté.

□

Proposition 2.6 – Division euclidienne dans $\mathbb{Z}$ (admise)

Soient $a, \in \mathbb{Z}$ et $b, \in \mathbb{Z} \setminus \{0\}$.
Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < |b|$.

Exemple 4.
- *La division euclidienne de* 35 *par* 6 *est* $35 = 6 \times 4 + 3$.
- *La division euclidienne de* -15 *par* 4 *est* $-15 = 4 \times (-4) + 1$.

Histoire – Division euclidienne

On parle de « division euclidienne » en référence au mathématicien grec **Euclide (300 av. J.C.)**. La division était néanmoins connue bien avant lui et utilisée par exemple par les égyptiens. Le nom « euclidien » s'explique plutôt par le fait qu'Euclide a utilisé un algorithme basé sur la division euclidienne (voir chapitre suivant). Il le présente dans un ouvrage célèbre intitulé *Les Éléments*. Avec plus de mille éditions différentes depuis l'antiquité, il s'agit, juste après la Bible, de l'ouvrage le plus imprimé dans l'histoire de l'humanité.

II. Congruences

1. Définition

Définition 2.2

Soit $m \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.
On dit que a et b sont **congrus modulo m** s'ils ont le même reste dans la division euclidienne par m.
On note $a \equiv b\,[m]$ ou $a \equiv b \mod m$.

Exemple 5. *Le reste de la division de 16 par 5 est 1. De même, le reste de la division de 31 par 5 est 1. Ainsi,* $16 \equiv 31\,[5]$.

Proposition 2.7

Soit $m \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.

$$a \equiv b\,[m] \iff m|(b-a)$$

Démonstration. Soit $m \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.

- Supposons que $a \equiv b\,[m]$. Cela signifie que a et b ont le même reste dans la division euclidienne par m. Autrement dit, il existe $p, q, r \in \mathbb{Z}$ tels que $a = mp + r$ et $b = mq + r$ avec $0 \leqslant r < |m|$.
  Ainsi, $b - a = (mq + r) - (mp + r) = m \times (q - p)$.
  Cela montre bien que m divise $b - a$.

- Réciproquement, supposons que $m|(b-a)$.
  On effectue alors les divisions euclidiennes de a et b par m.
  D'une part, il existe $q, r \in \mathbb{Z}$ tels que $a = mq + r$ avec $0 \leqslant r < |m|$.
  D'autre part, il existe $q', r' \in \mathrm{Z}$ tels que $b = mq' + r'$ avec $0 \leqslant r' < |m|$.
  L'objectif est de démontrer alors que $r = r'$.
  En fait, $b - a = (mq' + r') - (mq + r) = m(q' - q) + (r' - r)$.
  Or, les inégalités vérifiées par r et r' impliquent nécessairement que $(r' - r) \leqslant |m|$.
  Ainsi, si $r' - r \geqslant 0$, l'égalité 1 correspond à la division euclidienne de $b - a$ par m.
  Mais comme on sait que $m|(b-a)$, on en déduit que le reste $r' - r$ est nul, c'est-à-dire, $r' = r$.
  Autrement dit, a et b ont même reste dans la division par m et sont donc congrus modulo m.
  Dans le cas où $r' - r < 0$, il suffit de raisonner de même avec $a - b$ au lieu de $b - a$.

□

Histoire – Congruences

Carl Friedrich Gauß (1777-1855) est originaire d'une famille pauvre de la principauté de Brunswick. Dès l'école primaire, l'instituteur et son assistant décèlent ses talents et lui transmettent leur passion pour les mathématiques. Gauß publie ses premiers résultats à 19 ans et à 24 ans, il introduit la notion de congruences dans un ouvrage célèbre intitulé *Disquisitiones Arithmeticae*. Dès 28 ans, il dirigea l'observatoire astronomique de Göttingen. Alors qu'il n'aimait pas vraiment enseigner, cela lui permettait justement de se consacrer à ses recherches mathématiques.

2. Congruences et opérations

Proposition 2.8 – Transitivité

Soit $m \in \mathbb{N}^*$ et $a, b, c \in \mathbb{Z}$.

Si $a \equiv b\,[m]$ et $b \equiv c\,[m]$ alors $a \equiv c\,[m]$

Démonstration. Évident en revenant à la définition d'une congruence. □

Proposition 2.9

Soit $m \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$.

- **Compatibilité avec l'addition :**
  Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a + c \equiv b + d\,[m]$
- **Compatibilité avec la multiplication :**
  Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a \times c \equiv b \times d\,[m]$
- **Compatibilité avec les puissances :**
  Si $a \equiv b\,[m]$, alors pour tout $p \in \mathbb{N}^*$, $a^p \equiv b^p\,[m]$

Démonstration. Soient $a \equiv b\,[m]$ et $c \equiv d\,[m]$.
Cela signifie qu'il existe $k \in \mathbb{Z}$ tel que $a - b = mk$ et il existe $k' \in \mathbb{Z}$ tel que $c - d = mk'$.
Autrement dit, $a = b + mk$ et $c = d + mk'$.
En sommant les deux égalités, on obtient : $a + c = b + d + m(k + k')$, ce qui signifie exactement que $a + c \equiv b + d\,[m]$.
De la même manière, en multipliant les deux égalités, $a \times c = (b + mk) \times (d + mk') = b \times d + m(dk + bk')$.
On en déduit que $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a \times c \equiv b \times d\,[m]$.
Finalement, la dernière propriété s'obtient par récurrence comme conséquence de la seconde.

□

Exemple 6. *Montrer que pour tout entier* $n \in \mathbb{Z}$, $2n(n+1)(n+5)$ *est divisible par* 3.

Solution :
On distingue les cas modulo 3 *:*

n	0	1	2
$2n$	0	2	1
$n+1$	1	2	0
$n+5$	2	0	1
$2n(n+1)(n+5)$	0	0	0

Ainsi, dans tous les cas, $2n(n+1)(n+5) \equiv 0\,[3]$ *ce qui signifie exactement que* $2n(n+1)(n+5)$ *est divisible par* 3.

3. Inverse modulo m

Définition 2.3

Soient $m \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$.
On dit que a est **inversible** modulo m lorsqu'il existe un entier b tel que $a \times b \equiv 1\,[m]$. De plus, l'entier b est appelé **inverse de a modulo m** .

Exemple 7. 8 *est inversible modulo* 3 *car* $8 \times 2 \equiv 1[3]$. *Son inverse est* 2 *modulo* 3.

Proposition 2.10 – Unicité de l'inverse

Soient $m \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$.
Si a est inversible modulo m alors l'inverse est unique modulo m.

Démonstration. Supposons qu'il existe deux inverse de a, notés b_1 et b_2. On va montrer que $b_1 \equiv b_2\,[m]$.
En fait, $a \times b_1 \equiv 1\,[m]$ (car b_1 est un inverse).
Ainsi, en multipliant par b_2, il vient :

$b_2 \times a \times b_1 \equiv b_2 \times 1\,[m]$
donc $1 \times b_1 \equiv b_2\,[m]$
donc $b_1 \equiv b_2\,[m]$
Cela prouve donc l'unicité, modulo m de l'inverse. □

Exemple 8.

1. *Montrer que* 7 *est inversible modulo* 9.
2. *Montrer que* 4 *n'est pas inversible modulo* 6.

Solution :

1.

$n \equiv \ldots [9]$	0	1	2	3	4	5	6	7	8
$7n \equiv \ldots [9]$	0	7	5	3	1	…	…	…	…

Ainsi, $7 \times 4 \equiv 1\,[9]$ *donc* 7 *est inversible modulo* 9.

2.

$n \equiv \ldots [6]$	0	1	2	3	4	5
$4n \equiv \ldots [6]$	0	4	2	0	4	2

Ainsi, pour tout entier n, $4n \not\equiv 1\,[6]$, *ce qui signifie que* 4 *n'est pas inversible modulo* 6.

III. PGCD

1. Définitions et premières propriétés

Définition 2.4

Soient $a, b \in \mathbb{Z}$ tels que $(a;b) \neq (0,0)$.
L'ensemble des diviseurs communs à a et à b admet un plus grand élément appelé **Plus Grand Commun Diviseur de a et b**, noté $\text{PGCD}(a;b)$.

Démonstration. L'ensemble des diviseurs communs à a et à b admet un plus grand élément car cet ensemble est inclus dans $\mathbb{Z}$, est non vide (il contient 1) et est majoré par $\max(|a|;|b|)$. □

Exemple 9.

- $PGCD(6;10) = 2$
- *Pour tout* $a \in \mathbb{N}$, $PGCD(a;1) = 1$ *et* $PGCD(a;0) = a$.

Proposition 2.11

Soient $a, b \in \mathbb{Z}$ tels que $(a;b) \neq (0;0)$.

$$\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|).$$

Proposition 2.12

Soient $a, b \in \mathbb{N}$ tels que $a \neq 0$.

- $\text{PGCD}(a;b) \geqslant 1$;
- $a|b \iff \text{PGCD}(a;b) = a$;

2. Algorithme d'Euclide

Proposition 2.13

Soient $a, b \in \mathbb{N}^*$ tels que $a > b$. On note q et r le quotient et le reste de la division euclidienne de a par b. Alors,

$$\text{PGCD}(a;b) = \text{PGCD}(b;r).$$

Démonstration. On note E_1 l'ensemble des diviseurs communs à a et à b et E_2 l'ensemble des diviseurs communs à b et à r. On va montrer que $E_1 = E_2$.

- Supposons que $d \in E_1$, c'est-à-dire que d divise a et b.
  On sait que $a = bq + r$ donc $r = a - bq$.
  Ainsi, l'entier r est une combinaison linéaire de a et b donc r est divisible par d. Finalement, d est un diviseur de b et de r donc $d \in E_2$.
- Supposons que $d \in E_2$, c'est-à-dire que d divise b et r.
  On sait que $a = bq + r$.
  Ainsi, l'entier a est une combinaison linéaire de b et r donc a est divisible par d. Finalement, d est un diviseur de a et de b donc $d \in E_1$.

Au final, on a montré que $E_1 = E_2$. Ces deux ensembles étant égaux, ils ont nécessairement le même plus grand élément d'où $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$. □

Exemple 10. *PGCD*(512 ; 20) = *PGCD*(20 ; 12) = 4 *car le reste de la division de* 512 *par* 20 *est* 12.

Proposition 2.14

Soient $a, b \in \mathbb{N}^*$ tels que $a > b$.
On définit par récurrence la suite d'entiers naturels $(r_n)_{n\in\mathbb{N}}$ tels que :

- r_0 est le reste de la division euclidienne de a par b.
- → Si $r_0 = 0$, on pose $r_1 = 0$;
  → Sinon r_1 est le reste de la division euclidienne de b par r_0.
- pour tout $n \geqslant 1$:
  → Si $r_n = 0$, on pose $r_{n+1} = 0$.
  → Sinon, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.

Alors, cette suite d'entiers est nulle à partir d'un certain rang et la dernière valeur non nulle prise par cette suite est le PGCD de a et b.

Démonstration.

- On va montrer que la suite s'annule à partir d'un certain (il est clair qu'elle sera ensuite nulle pour les rangs suivants).
  Supposons par l'absurde que pour tout n, $r_n \neq 0$. Comme pour tout $n \geqslant 1$, r_{n+1} est défini comme le reste de la division de r_{n-1} par r_n, on sait que $r_{n+1} < r_n$ et donc la suite $(r_n)_{n\in\mathbb{N}}$ est strictement décroissante. Comme il s'agit d'une suite d'entiers naturels, on en déduit qu'elle s'annule à partir d'un certain rang, ce qui est impossible par hypothèse.
  Ainsi, on a montré qu'il existe un entier n_0 tel que pour tout $n \geqslant n_0$, $r_{n_0} = 0$.
- La propriété 2. justifie que :

$$\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r_0) = \text{PGCD}(r_0\,;r_1) = \ldots = \text{PGCD}(r_{n_0-1}\,;r_{n_0})$$

$$= \text{PGCD}(r_{n_0-1}\,;0) = r_{n_0-1} \text{ (qui est la dernière valeur non nulle de la suite).}$$

□

Exemple 11. *Déterminer le PGCD de 896 et 259.*

Solution :

$$\begin{aligned} 896 &= 259 \times 3 + 119 \\ 259 &= 119 \times 2 + 21 \\ 119 &= 21 \times 5 + 14 \\ 21 &= 14 \times 1 + 7 \\ 14 &= 7 \times 2 + 0 \end{aligned}$$

Ainsi, on a PGCD(896 ; 259) = 7.

Histoire – Algorithme d'Euclide

L'algorithme d'Euclide a été présenté dans *Les Éléments* vers l'an 300 av. J.-C. Il est présenté d'une part sous forme arithmétique mais également géométrique en cherchant à construire une unité de mesure commune à deux longueurs. A la différence de l'algorithme arithmétique, le procédé géométrique ne s'arrête pas nécessairement. Il faut en fait que le rapport des deux longueurs soit rationnel pour que l'on soit sûr que le procédé s'arrête.

3. Corollaires de l'algorithme d'Euclide

Proposition 2.15

Pour tous $a, b \in \mathbb{N}^*$ et $d \in \mathbb{N}$:

$$d|a \text{ et } d|b \iff d|\text{PGCD}(a;b).$$

Démonstration. Soient $a, b \in \mathbb{N}^*$.
Dans l'algorithme d'Euclide, r_0 est reste de la division euclidienne de a par b. D'après démonstration de la propriété 2., on sait que l'ensemble des diviseurs communs à a et à b est égale à l'ensemble des diviseurs communs à b et à r_0. On note E cet ensemble.
Comme r_1 est le reste de la division de r_0 par b, on en déduit que E est aussi l'ensemble des diviseurs communs de r_0 et r_1.
En procédant par récurrence, on montre finalement que E est l'ensemble des diviseurs communs de $r_{n_0-1} = \text{PGCD}(a;b)$ (le dernier reste non nul) et de 0, ce qui correspond à l'ensemble des diviseurs de $\text{PGCD}(a;b)$. □

Proposition 2.16

Pour tous $a, b \in \mathbb{N}$ et $k \in \mathbb{N}$,

$$\text{PGCD}(ka;kb) = k \times \text{PGCD}(a;b).$$

Démonstration. Pour calculer $\text{PGCD}(ka;kb)$, toutes les étapes de l'algorithme d'Euclide seront les mêmes que pour calculer $\text{PGCD}(a;b)$ à un facteur multiplicatif k près. □

Définition 2.5

Soient $a, b \in \mathbb{N}$ et $k \in \mathbb{Z}^*$.
On dit que a et b sont premiers entre eux lorsque $\text{PGCD}(a;b) = 1$.

Proposition 2.17

Soient $a, b \in \mathbb{N}^*$ et avec $d = \text{PGCD}(a;b)$.
Il existe des entiers premiers entre eux a' et b' tels que $\begin{cases} a = da' \\ b = db' \end{cases}$

Démonstration. Soient $a, b \in \mathbb{N}^*$ et $k \in \mathbb{Z}^*$ avec $d = \text{PGCD}(a;b)$. Comme d est un diviseur commun de a et b, il existe a' et b' des entiers tels que $a = da'$ et $b = db'$. Il suffit donc de montrer que a' et b' sont premiers entre eux. Or, on a :

$$\begin{aligned} \text{PGCD}(a;b) &= \text{PGCD}(da';db') \\ &= d \times \text{PGCD}(a';b') \end{aligned}$$

Ainsi, $d = d \times \text{PGCD}(a';b')$ et comme $d \neq 0$ (a et b sont non nuls simultanément), on en déduit que $\text{PGCD}(a';b') = 1$. □

4. Identité et théorème de Bézout

Proposition 2.18 – Identité de Bézout

Soient $a, b \in \mathbb{N}^*$.
Il existe des entiers relatifs u et v tels que

$$au + bv = \text{PGCD}(a;b).$$

Démonstration. On considère la suite des divisions de l'algorithme d'Euclide (où r_{n_0-1} est le dernier reste non nul, c'est-à-dire $r_{n_0-1} = \text{PGCD}(a;b)$) :

$$\begin{aligned}
a &= bq_0 + r_0 \\
b &= r_0 q_1 + r_1 \\
&\vdots \qquad \vdots \\
r_{k-1} &= r_k q_{k+1} + r_{k+1} \\
&\vdots \qquad \vdots \\
r_{n_0-4} &= r_{n_0-3} q_{n_0-2} + r_{n_0-2} \\
r_{n_0-3} &= r_{n_0-2} q_{n_0-1} + r_{n_0-1} \\
r_{n_0-2} &= r_{n_0-1} q_{n_0} + 0
\end{aligned}$$

L'avant dernière égalité donne :

$$\text{PGCD}(a;b) = r_{n_0-1} = r_{n_0-3} - r_{n_0-2} q_{n_0-1} \quad (*)$$

Cela signifie que $\text{PGCD}(a;b)$ est une combinaison linéaire de r_{n_0-3} et r_{n_0-2}. En exprimant r_{n_0-2} dans la ligne du dessus et en la réinjectant dans l'égalité (*), on obtient ensuite :

$$\begin{aligned}
\text{PGCD}(a;b) &= r_{n_0-3} - (r_{n_0-4} - r_{n_0-3} q_{n_0-2}) q_{n_0-1} \\
&= r_{n_0-3}(1 + q_{n_0-2}) - r_{n_0-4}
\end{aligned}$$

Cela signifie que $\text{PGCD}(a;b)$ est une combinaison linéaire de r_{n_0-4} et r_{n_0-3}. De proche en proche, on pourra finalement écrire $\text{PGCD}(a;b)$ comme une combinaison linéaire de a et b. □

Exemple 12. *On sait que PGCD*$(896;259) = 7$. *Déterminer des entiers relatifs u et v tels que* $896u + 259v = 7$.

Solution :
On écrit les différentes étapes de l'algorithme d'Euclide :

$$\begin{aligned}
896 &= 259 \times 3 + 119 \\
259 &= 119 \times 2 + 21 \\
119 &= 21 \times 5 + 14 \\
21 &= 14 \times 1 + 7
\end{aligned}$$

En remontant l'algorithme, on obtient :

$$\begin{aligned}
7 &= 21 - 14 \times 1 \\
&= 21 - (119 - 21 \times 5) \times 1 \\
&= 6 \times 21 - 119 \\
&= 6 \times (259 - 119 \times 2) - 119 \\
&= 6 \times 259 - 13 \times 119 \\
&= 6 \times 259 - 13 \times (896 - 259 \times 3) \\
&= -13 \times 896 + 45 \times 259
\end{aligned}$$

Ainsi, $896u + 259v = 7$ *avec* $u = -13$ *et* $v = 45$.

Histoire – Identité de Bézout

L'identité de Bézout porte le nom du mathématicien français **Étienne Bézout** (1730-1783). Ce résultat avait cependant déjà été découvert et démontré par **Claude Gaspard Bachet de Méziriac** (1581-1638). Bézout a en fait généralisé un résultat similaire pour les polynômes. Pour cette raison, l'identité de Bézout prend parfois le nom de « théorème de Bachet-Bézout ».

Proposition 2.19 – Théorème de Bézout

Soient $a, b \in \mathbb{Z}^*$. Les entiers a et b sont premiers entre eux si, et seulement si, il existe des entiers relatifs u et v tels que

$$au + bv = 1.$$

Démonstration.

- Supposons que $\text{PGCD}(a;b) = 1$. D'après l'identité de Bézout, il est immédiat de voir qu'il existe des entiers relatifs u et v tels que $au + bv = \text{PGCD}(a;b) = 1$.
- Réciproquement, supposons qu'il existe des entiers relatifs u et v tels que $au + bv = 1$.
  Soit d un diviseur commun de a et b. On en déduit que d divise la combinaison linéaire $au+bv$ donc d divise 1. Ainsi, on en déduit que $d = 1$ qui est le seul diviseur commun de a et b.
  Par conséquent, $\text{PGCD}(a;b) = 1$.

□

Remarque.

- *L'équivalence n'est vraie que si* $PGCD(a;b) = 1$.
  Dans le cas général, seule l'identité de Bézout est vraie.
- *Le couple* $(u;v)$ *de l'identité de Bézout n'est pas unique.*

IV. Lemme de Gauss et corollaire

Lemme 2.20 – Gauss

Soient $a, b, c \in \mathbb{Z}^*$.
Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Démonstration. Soient $a, b, c \in \mathbb{Z}^*$ tels que $a|bc$ et tels que a et b sont premiers entre eux.
a et b sont premiers entre eux donc, d'après le théorème de Bézout, il existe des entiers u et v tels que $au + bv = 1$. Ainsi, en multipliant par c, on obtient :

$$auc + bvc = c.$$

Comme $a|a$ et $a|bc$, on en déduit que a divise la combinaison linéaire $auc + bcv$, c'est-à-dire $a|c$. □

Remarque. *La condition « a et b sont premiers entre eux » est indispensable.*
En effet, 9 *divise* $6 \times 15 = 90$ *et pourtant* 9 *ne divise ni* 6, *ni* 15.

Histoire – Théorème de Gauss

Carl Friedrich Gauß (1777-1855) est l'un des mathématiciens les plus célèbres du XIX^{e} siècle. On le surnomme « le prince des mathématiques » et il existe un nombre important de résultats qui portent son nom. Il a démontré le théorème ci-dessus en 1801 dans un ouvrage intitulé *Diquisitiones arithmeticae*. C'est d'ailleurs la même année qu'il a déterminé la trajectoire de la planète naine *Cérès* en utilisant notamment la méthode des moindres carrés.

Corollaire 2.21

Soient $a, b, c \in \mathbb{Z}^*$ tels que $b|a$, $c|a$ et tels que $\text{PGCD}(b;c) = 1$, alors $bc|a$.

Démonstration. Soient $a, b, c \in \mathbb{Z}^*$ tels que $b|a$, $c|a$ et tels que $\text{PGCD}(b;c) = 1$.
Comme $b|a$ et $c|a$, il existe des entiers k et l tels que $a = bk = cl$. Ainsi, $c|bk$.
Mais comme b et c sont premiers entre eux, on en déduit d'après le lemme de Gauss que $c|k$.
Donc il existe un entier k' tel que $k = ck'$.
Finalement, on obtient $a = b(ck') = bck'$ donc $bc|a$. □

La propriété précédente se reformule à l'aide de congruences de la façon suivante :

Corollaire 2.22

Soient $a, b, c \in \mathbb{Z}^*$.

$$\begin{cases} a \equiv 0\,[b] \\ a \equiv 0\,[c] \\ \text{PGCD}(b;c) = 1 \end{cases} \implies a \equiv 0\,[bc]\,.$$

V. Nombres premiers

1. L'ensemble des nombres premiers

Définition 2.6

Un entier naturel est un **nombre premier** s'il admet exactement deux diviseurs positifs : 1 et lui même.

Exemple 13. *La liste des nombres premiers inférieurs à 30 est la suivante : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29.*

Remarque. *L'entier 1 n'est pas un nombre premier car il n'admet qu'un seul diviseur.*

Proposition 2.23

Tout entier naturel supérieur ou égal à 2 est divisible par un nombre premier.

Démonstration. Voir chapitre 1 (récurrence forte). □

Proposition 2.24

Soit $n \geqslant 2$. Il y a deux possibilités :
- Soit n est un nombre premier ;
- Soit n est divisible par un nombre premier compris entre 2 et $\sqrt{n}$.

Démonstration. Soit $n \geqslant 2$. Supposons que n ne soit pas premier.
Cela signifie qu'il existe des entiers a et b, avec $a > 1$ et $b > 1$ tels que $n = ab$.
L'un des deux entiers a, ou b est inférieur ou égal à $\sqrt{n}$ car sinon, on aurait $ab > n$.
Supposons par exemple, que $a \leqslant \sqrt{n}$ (le cas $b \leqslant \sqrt{n}$ se traite de la même manière).
D'après la propriété 1, a est divisible par un nombre premier p. Comme $p|a$ et $a|n$, on en déduit, par transitivité que $p|n$. De plus, on a bien $p \leqslant \sqrt{n}$. □

Exercice 1. *Montrer que* 71 *est premier.*

Proposition 2.25

Il existe une infinité de nombres premiers.

Démonstration. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombre premiers.
On note $p_1, p_2, \ldots, p_n$ ces nombres premiers. On considère alors l'entier $N = p_1 \times p_2 \times \ldots \times p_n + 1$.
D'après la propriété 1, N est divisible par l'un des nombres premiers.
Autrement dit, il existe $1 \leqslant i \leqslant n$ tel que p_i divise N.
On a donc $N \equiv 0 \left[p_i\right]$
Or, $N \equiv p_1 \times p_2 \times \ldots \times p_n + 1 \equiv 1 \left[p_i\right]$, ce qui est absurde. □

Histoire – Infinité des nombres premiers

L'infinité de l'ensemble des nombres premiers est énoncé et démontré dans les *Éléments* d'**Euclide**. Plus tard, les mathématiciens continuèrent d'étudier la répartition des nombres premiers. Par exemple, en utilisant les congruences, l'allemand **Gustav Lejeune Dirichlet (1805-1859)** a pu établir le théorème de progression arithmétique : si a et b sont premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$.

2. Décomposition en produit de facteurs premiers

Proposition 2.26

Pour tout entier $n \geqslant 2$, il existe des nombres premiers distincts $p_1, p_2, \ldots, p_k$ et des entiers $\alpha_1, \alpha_2, \ldots, \alpha_k$ tels que $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$.
De plus, cette décomposition est unique à l'ordre des facteurs près.

Démonstration.
Démontration de l'existence : On va montrer par récurrence que la propriété $\mathscr{P}(n)$:« Pour entier naturel k compris entre 2 et n, k se décompose en produit de nombres premiers » est vraie pour tout entier $n \geqslant 2$.
Initialisation : Il est clair que $\mathscr{P}(2)$ est vraie.
Hérédité : Supposons que $\mathscr{P}(n)$ soit vraie pour un certain entier $n \geqslant 2$ et montrons qu'alors $\mathscr{P}(n+1)$ est vraie.
Pour montrer que $\mathscr{P}(n+1)$ est vraie, il suffit de montrer que $n+1$ admet une décomposition en produit de nombres premiers.
Si $n+1$ est un nombre premier, alors $\mathscr{P}(n+1)$ est vraie.
Sinon, d'après la propriété 1, $n+1$ admet un diviseur premier p. Par conséquent, il existe un entier k tel que $n+1 = kp$ (avec $2 \leqslant k \leqslant n$).
D'après l'hypothèse $\mathscr{P}(n)$, k se décompose en produit de nombres premiers et par conséquent, $n+1$ aussi.
Ainsi, on a montré que $\mathscr{P}(n+1)$ est vraie.

Démonstration de l'unicité : Soit $n \geqslant 2$. On suppose par l'absurde qu'un certain nombre premier p apparaît avec l'exposant α dans une décomposition de n et avec l'exposant β dans une autre décomposition de n (avec éventuellement $\beta = 0$ si p n'apparaît pas dans la deuxième décomposition).
Ainsi, il existe des entiers a et b premiers avec p tels que $n = p^\alpha a$ et $n = p^\beta b$.
Si $\alpha > \beta$, alors $a = p^{\alpha-\beta} b$. Par conséquent, $p|a$, ce qui est impossible.
De même si $\beta > \alpha$, alors $b = p^{\beta-\alpha} a$. Par conséquent, $p|b$, ce qui est impossible.
Finalement, on a montré que $\alpha = \beta$, ce qui prouve l'unicité de la décomposition. □

Proposition 2.27 – Corollaire

Soit $n \geqslant 2$ un entier dont la décomposition en produit de nombres premiers est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$. Alors,

- les diviseurs de n sont les nombres de la forme :
$$n = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k} \quad (\text{avec } 0 \leqslant \beta_i \leqslant \alpha_i, \text{ pour tout } i).$$
- le nombre de diviseurs de n est $(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1)$.

Chapitre 3

Applications

I. Définitions

Définition 3.1

Soient E et F deux ensembles. Une **application** f de E dans F, notée $f : \mathrm{E} \longrightarrow \mathrm{F}$ associe à chaque élément x de E un et un seul élément de F noté $f(x)$. E est **l'ensemble de départ** et F **l'ensemble d'arrivée**. On dit que $f(x)$ est **l'image** de x et que x est un **antécédent** de $y = f(x)$. On écrit :

$$f : \left\{ \begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{F} \\ x & \longmapsto & f(x) \end{array} \right.$$

Étymologie – Application

Issu du latin *applicare*, appliquer apparaît au XIII^e siècle avec le sens d'appliquer un objet contre quelque chose et celui d'appliquer son esprit à quelque chose. *Application* le suit au siècle suivant. La notion d'application n'apparaît qu'avec la théorie des ensembles. Il remplace souvent le mot *fonction*. On comprend cependant aisément que ces deux mots proviennent de connotations différentes. La fonction semble tisser un lien objectif entre deux éléments en transformant le premier en le second. L'application a un rôle plus neutre. Elle se contente de faire correspondre, sans état d'âme, les éléments de l'ensemble de départ sur ceux de l'ensemble d'arrivée.

Remarque. *Un élément de* E *ne possède qu'une seule image par* f. *En revanche, un élément de* F *peut n'avoir aucun antécédent, un antécédent ou plusieurs.*

Exemple 1. *L'application* ***identité*** *d'un ensemble* E, *notée* Id_E *est l'application*

$$\mathrm{Id}_\mathrm{E} : \left\{ \begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{E} \\ x & \longmapsto & x \end{array} \right.$$

Exemple 2. *Soit* E *un ensemble et* $\mathrm{A} \subset \mathrm{E}$. *L'application* ***indicatrice*** *de* A *est définie par*

$$\mathbf{1}_\mathrm{A} : \left\{ \begin{array}{ccc} \mathrm{E} & \longrightarrow & \{0,1\} \\ x & \longmapsto & \left\{ \begin{array}{ll} 1 & si\ x \in \mathrm{A} \\ 0 & sinon \end{array} \right. \end{array} \right.$$

Exemple 3. *Soit* E *un ensemble,* $a \in \mathrm{E}$ *et* $b \in \mathrm{E}$. *La* ***transposition*** *de* a *et* b *est l'application*

$$t_{a,b} : \left\{ \begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{E} \\ x & \longmapsto & \left\{ \begin{array}{ll} a & si\ x = b \\ b & si\ x = a \\ x & si\ x \notin \{a,b\} \end{array} \right. \end{array} \right.$$

Définition 3.2 – Ensemble des applications de E dans F

On note F^E l'ensemble des applications de E dans F. On a $F^E = \{f : E \longrightarrow F\}$.

Remarque. $\mathbb{R}^{\mathbb{N}}$ *(l'ensemble des applications de* $\mathbb{N}$ *dans* $\mathbb{R}$*) est l'ensemble des suites réelles.*

II. Opérations sur les applications

Définition 3.3 – Égalité d'applications

Deux applications $f : E \longrightarrow F$ et $g : E' \longrightarrow G'$ sont égales si $E = E'$, $F = F'$ et si pour tout $x \in E$, $f(x) = g(x)$.

Exemple 4. *Les fonctions suivantes ne sont pas égales (leur ensemble d'arrivée ne sont pas les mêmes).*

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \right. \qquad g : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array} \right.$$

Exemple 5. *Soit* E *un ensemble,* $a \in E$ *et* $b \in E$*. Montrer que* $t_{a,b} = t_{b,a}$ *et que* $t_{a,a} = Id_E$.

Solution : Il suffit de montrer que pour tout $x \in E$, $t_{a,b}(x) = t_{b,a}(x)$.
Or $t_{a,b}(b) = a$ *et* $t_{b,a}(b) = a$.
De même, $t_{a,b}(a) = b$ *et* $t_{b,a}(a) = b$.
Enfin, si $x \in E \setminus \{a; b\}$, $t_{a,b}(x) = x$ *et* $t_{b,a}(x) = x$.
La preuve du fait que $t_{a,a} = Id_E$ *est similaire et laissée au lecteur.*

Définition 3.4 – Restriction

Soit $f : E \longrightarrow F$ et $A \subset E$ une partie non vide de E. La restriction de f à A, notée $f_{|A}$ est l'application de A dans F telle que pour tout $x \in A$, $f_{|A}(x) = f(x)$.

Exemple 6.

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \right. \qquad g : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \right.$$

g est la restriction de f à $[0,1]$.

Définition 3.5 – Corestriction

Soit $f : E \longrightarrow F$ et $B \subset F$ une partie non vide de F. La corestriction de f à B ne peut être définie que si, pour tout $x \in E$, $f(x) \in B$. C'est alors l'application $\tilde{f}$ de E dans B telle que pour tout $x \in E$, $\tilde{f}(x) = f(x)$.

Exercice 1. *Soit* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *définie par* $f(x) = x^2$*. Est-il possible de restreindre* f *à* $[0,3]$ *et de la corestreindre à* $[0,6]$ *?*

Définition 3.6 – Prolongement

Soit $f : E \longrightarrow F$. Soit E' un ensemble tel que $E \subset E'$. Une application $g : E' \longrightarrow F$ est un prolongement de f à E' si l'on a $g_{|E} = f$.

Remarque. *Si* $A \subset E \subset E'$*, il y a une seule restriction de* f *à* A *mais de nombreux prolongements de* f *à* E'.

Exercice 2.

$$f : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \right.$$

Construire au moins trois prolongements de f *à* $\mathbb{R}$.

Définition 3.7 – Composition d'applications

Soient E, F, G trois ensembles, $f : E \longrightarrow F$ et $g : F \longrightarrow G$. La composée de f et g est l'application

$$g \circ f : \left\{ \begin{array}{ccc} E & \longrightarrow & G \\ x & \longmapsto & g(f(x)) \end{array} \right.$$

Proposition 3.1

La loi de composition est associative : soient E, F, G, H des ensembles et $f : E \longrightarrow F$, $g : F \longrightarrow G$, $h : G \longrightarrow H$ des applications. Alors $(h \circ g) \circ f = h \circ (g \circ f)$.

Exemple 7. *Pour toute application* $f : E \longrightarrow E$, *montrer que* $f \circ Id_E = Id_E \circ f = f$.

Solution : Soit $x \in E$.
$f \circ Id_E(x) = f(Id_E(x)) = f(x)$
et $Id_E \circ f(x) = Id_E(f(x)) = f(x)$, *d'où le résultat.*

Exercice 3. *Soient* E *un ensemble possédant au moins trois éléments distincts* a, b *et* c. *Déterminer* $t_{a,b} \circ t_{b,c}(c)$ *et* $t_{b,c} \circ t_{a,b}(c)$. *La loi de composition est-elle commutative ?*

III. Image directe et image réciproque

Définition 3.8 – Image directe

Soient E et F deux ensembles et soit $f : E \longrightarrow F$ une application. Soit $A \subset E$ L'image directe de A par f, notée $f(A)$ est l'ensemble des images par f, c'est-à-dire :

$$f(A) = \{f(a) | a \in A\}.$$

Exemple 8. *Soit* $f : x \in \mathbb{R} \longmapsto x^2 \in \mathbb{R}$. *Le tableau de variations de* f *permet d'établir que* $f([-2,1]) = [0,4]$.

Exercice 4. $f : n \in \mathbb{N} \longrightarrow 2n \in \mathbb{N}$ *Déterminer l'image directe de* $\mathbb{N}$ *et de* $\{2n+1 \mid n \in \mathbb{N}\}$.

Exercice 5.

- *Si* A *est non vide,* $f(A)$ *peut-il être vide ?*
- *Si* A *possède deux éléments, combien* $f(A)$ *peut posséder d'éléments ?*

Proposition 3.2

Soit $f : E \longrightarrow F$ une application. Soient $A \subset E$ et $B \subset E$.

- Si $A \subset B$, alors $f(A) \subset f(B)$
- $f(A \cup B) = f(A) \cup f(B)$
- $f(A \cap B) \subset f(A) \cap f(B)$.

Démonstration. Soit $f : E \longrightarrow F$ une application. Soient $A \subset E$ et $B \subset E$

- Supposons que $A \subset B$. Montrons que $f(A) \subset f(B)$.
  Soit $y \in f(A)$. Il existe $a \in A$ tel que $y = f(a)$.
  Or, $A \subset B$ donc $a \in B$.
  Ainsi, $y = f(a) \in f(B)$.

- Montrons que $f(A \cup B) = f(A) \cup f(B)$ par double inclusion.
  Soit $y \in f(A \cup B)$. Il existe $x \in A \cup B$ tel que $y = f(x)$.
  Si $x \in A$, alors $y \in f(A)$.
  Si $x \in B$, alors $y \in f(B)$.
  Ainsi, dans tous les cas, $y \in f(A) \cup f(B)$.
  Inversement, considérons $y \in f(A) \cup f(B)$. Alors $y \in f(A)$ ou $y \in f(B)$.
  Si $y \in f(A)$, il existe $x \in A$ tel que $y = f(x)$. Comme $x \in A$, on a aussi $x \in A \cup B$ et donc $y = f(x) \in f(A \cup B)$.
  De la même manière, si $y \in f(B)$, on montre que $y \in f(A \cup B)$, ce qui permet de conclure.

- Montrons que $f(A\cap B)\subset f(A)\cap f(B)$. Soit $y\in f(A\cap B)$. Il existe $x\in A\cap B$ tel que $y=f(x)$.
Ainsi, comme $x\in A$, $y\in f(A)$ et comme $x\in B$, $y\in f(B)$.
Au final, $y\in f(A)$ et $y\in f(B)$ donc $y\in f(A)\cap f(B)$.

□

Exercice 6. *Donner un exemple d'application et de parties* A *et* B *telles que* $f(A\cap B)\neq f(A)\cap f(B)$.

Définition 3.9 – Image réciproque

Soient E et F deux ensembles et soit $f:E\longrightarrow F$ une application. Soit $B\subset F$ L'image réciproque de B par f, notée $f^{-1}(B)$ est l'ensemble des antécédents par f des éléments de B, c'est-à-dire :

$$f^{-1}(B)=\left\{x\in E\mid f(x)\in B\right\}.$$

Exercice 7. *Soit* $f:x\in\mathbb{R}\longmapsto x^2\in\mathbb{R}$. *Montrer que* $f^{-1}\left([-1,3]\right)=\left[-\sqrt{3},\sqrt{3}\right]$.

Exercice 8. *Quelle est l'image directe et réciproque de* $\mathbb{R}$, $\mathbb{R}^+$ *et de* $[0,1]$ *par la fonction exponentielle ?*

Exercice 9. *Si* B *est non vide,* $f^{-1}(B)$ *peut-il être vide ?*

Proposition 3.3

Soit $f:E\longrightarrow F$ une application. Soit $A\subset F$ et $B\subset F$.
- $f^{-1}(A\cup B)=f^{-1}(A)\cup f^{-1}(B)$
- $f^{-1}(A\cap B)=f^{-1}(A)\cap f^{-1}(B)$
- $f^{-1}(A^c)=\left(f^{-1}(A)\right)^c$

Démonstration. Soit $f:E\longrightarrow F$ une application. Soit $A\subset F$ et $B\subset F$.

- Montrons que $f^{-1}(A\cup B)=f^{-1}(A)\cup f^{-1}(B)$ par double inclusion.
Montrons d'abord que $f^{-1}(A\cup B)\subset f^{-1}(A)\cup f^{-1}(B)$.
Soit $x\in f^{-1}(A\cup B)$. Par définition de l'image réciproque, $f(x)\in A\cup B$ donc $f(x)\in A$ ou $f(x)\in B$.
Si $f(x)\in A$, alors $x\in f^{-1}(A)$ et donc $x\in f^{-1}(A)\cup f^{-1}(B)$.
De même, si $f(x)\in B$, alors $x\in f^{-1}(B)$ donc $x\in f^{-1}(A)\cup f^{-1}(B)$.
Ainsi, dans tous les cas, $x\in f^{-1}(A)\cup f^{-1}(B)$.
Inversement, montrons que $f^{-1}(A)\cup f^{-1}(B)\subset f^{-1}(A\cup B)$.
Soit $x\in f^{-1}(A)\cup f^{-1}(B)$.
On sait que $x\in f^{-1}(A)$ ou $x\in f^{-1}(B)$.
Si $x\in f^{-1}(A)$, $f(x)\in A$. Par conséquent, $f(x)\in A\cup B$ et donc $x\in f^{-1}(A\cup B)$.
De même, si $x\in f^{-1}(B)$, on montre que $x\in f^{-1}(A\cup B)$.
Ainsi, dans tous les cas, on a bien $x\in f^{-1}(A\cup B)$.

- Montrons que $f^{-1}(A\cap B)=f^{-1}(A)\cap f^{-1}(B)$ par double inclusion.
Montrons d'abord que $f^{-1}(A\cap B)\subset f^{-1}(A)\cap f^{-1}(B)$.
Soit $x\in f^{-1}(A\cap B)$. On a $f(x)\in A\cap B$, donc $f(x)\in A$ et $f(x)\in B$.
Comme $f(x)\in A$, on en déduit que $x\in f^{-1}(A)$ et comme $f(x)\in B$, on en déduit que $x\in f^{-1}(B)$.
Au final, $x\in f^{-1}(A)\cap f^{-1}(B)$. Inversement, montrons que $f^{-1}(A)\cap f^{-1}(B)\subset f^{-1}(A\cap B)$.
Soit $x\in f^{-1}(A)\cap f^{-1}(B)$.
Alors $x\in f^{-1}(A)$ et $x\in f^{-1}(B)$,
Donc $f(x)\in A$ et $f(x)\in B$
Donc $f(x)\in A\cap B$
Donc $x\in f^{-1}(A\cap B)$.

- Montrons que $f^{-1}(A^c)=\left(f^{-1}(A)\right)^c$ par double inclusion.
Montrons d'abord que $f^{-1}(A^c)\subset\left(f^{-1}(A)\right)^c$.
Soit $x\in f^{-1}(A^c)$.
On a donc $f(x)\in A^c$, c'est-à-dire $f(x)\notin A$. Supposons par l'absurde que $x\in f^{-1}(A)$.
On aurait $f(x)\in A$, ce qui est contradictoire.
Ainsi, on a donc $x\in\left(f^{-1}(A)\right)^c$.
Inversement, montrons que $\left(f^{-1}(A)\right)^c\subset f^{-1}(A^c)$.
Soit $x\in\left(f^{-1}(A)\right)^c$.

Alors $x \notin f^{-1}(A)$
Donc $f(x) \notin A$
Donc $f(x) \in A^c$
Donc $x \in f^{-1}(A^c)$.

□

Remarque. *Attention, f^{-1} n'est pas une fonction !*

Exercice 10. *Soit $f : n \in \mathbb{N} \longmapsto n^2 \in \mathbb{N}$. Déterminer l'image réciproque de $\{0,1,2,3\}$ et de $\mathbb{N}$. Déterminer ensuite l'image réciproque de $\{n \in \mathbb{N} \mid 0 \leqslant n \leqslant 40\}$, de $\mathbb{N}$ et de $\{50\}$.*

IV. Injectivité, surjectivité, bijectivité

Définition 3.10 – Injectivité

Soit $f : E \longrightarrow F$ une application. On dit que f est injective si chaque élément de F a au plus un antécédent. On peut caractériser l'injectivité de la façon suivante :

- f est injective si, et seulement si, pour tous $x, y \in E$ tels que $x \neq y$, on a $f(x) \neq f(y)$.
- f est injective si, et seulement si, pour tous $x, y \in E$, si $f(x) = f(y)$, alors $x = y$.

Remarque. *Les deux caractérisations de la définition d'injectivité sont simplement la contraposée l'une de l'autre. Elles sont donc équivalentes.*

Exemple 9. *La fonction* $\exp : \mathbb{R} \longrightarrow \mathbb{R}$ *est injective car elle est strictement croissante.*

Exemple 10. *Montrer que la fonction $f : x \in \mathbb{R} \longmapsto e^{-3x+2} + 7 \in \mathbb{R}$ est injective.*

Solution : Soient $x_1, x_2 \in \mathbb{R}$ tels que $f(x_1) = f(x_2)$.
On a : $e^{-3x_1+2} + 7 = e^{-3x_2+2} + 7$
Donc $e^{-3x_1+2} = e^{-3x_2+2}$
Donc $-3x_1 + 2 = -3x_2 + 2$ (car l'exponentielle est injective)
Donc $-3x_1 = -3x_2$
Donc $x_1 = x_2$.
Cela prouve bien que f est injective.

Exemple 11. *Montrer que la fonction $f : (x, y) \in \mathbb{R}^2 \longmapsto (x - 2y, y) \in \mathbb{R}^2$ est injective.*

Solution : Soient $(x_1, y_1) \in \mathbb{R}^2$ et $(x_2, y_2) \in \mathbb{R}^2$ tels que $f(x_1, y_1) = f(x_2, y_2)$.

$$\text{On a : } \begin{cases} x_1 - 2y_1 = x_2 - 2y_2 \\ \text{et} \\ y_1 = y_2 \end{cases}$$

Donc $y_1 = y_2$ et $x_1 = x_2$.
Ainsi, $(x_1, y_1) = (x_2, y_2)$ et f est bien injective.

Étymologie – Injection

Injection est formé de la particule latine *in-* signifiant *dans* et de *-jection* du latin *jacere, jeter*. *Injecter* signifie en quelque sorte mettre à l'intérieur. *Injection* apparaît en français à la fin du XIV^{e} siècle dans le domaine médical. Il s'y cantonne jusqu'au XIX^{e} siècle. il s'étend alors au langage courant pour signifier *introduction*, mais ce sens disparaît rapidement.
Le développement de la théorie des ensembles au début du XX^{e} siècle nécessite la création d'un vocabulaire nouveau. Dans les années 1930, le groupe Bourbaki introduit en mathématiques le mot *injection*. Il sous-tend l'idée que l'ensemble de départ A se retrouve injecté à l'intérieur de l'ensemble d'arrivée B puisque les points différents de A le restent dans B après l'action de l'application. Bourbaki construit sur le même modèle les mots bijection et surjection.
Le concept était parfois utilisé antérieurement sans être isolé en lui-même ce qui explique une absence de nom jusqu'à cette date récente.

Définition 3.11 – Surjectivité

Soit $f : E \longrightarrow F$ une application. On dit que f est surjective si chaque élément de F a au moins un antécédent par f. On peut caractériser la surjectivité de la façon suivante :

f est surjective si, et seulement si, pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$.

Remarque. *En terme d'image directe, une application $f : E \longrightarrow F$ est surjective si, et seulement si, $f(E) = F$.*

Exemple 12. *La fonction $f : x \in \mathbb{R} \longrightarrow x^2 \in \mathbb{R}^+$ est surjective.*

Exercice 11. *Pour tout $n \in \mathbb{N}$, on pose $g(n) = \dfrac{n}{2}$ si n est pair et $g(n) = 0$ si n est impair. La fonction $g : \mathbb{N} \longrightarrow \mathbb{N}$ est-elle surjective ?*

Définition 3.12 – bijectivité

Soit $f : E \longrightarrow F$ une application. On dit que f est bijective si chaque élément de F a exactement un antécédent par f. On peut caractériser la bijectivité de la façon suivante :

f est bijective si, et seulement si, f est injective et surjective.

Étymologie – Bijection

Le développement de la théorie des ensembles au début du XX^e siècle nécessita la création d'un vocabulaire nouveau. Jusque là, le concept sous-tendu par ce mot se nomme *biunivoque*. Le groupe Bourbaki créa le mot *bijection* sur le modèle d'*injection*. La particule *bi-* indique la réversibilité du concept.

Exercice 12. *Soit $f : E \longrightarrow F$ une application. Que peut-on dire de la corestriction de f à $f(E)$? Que peut-on dire de plus si f est injective ?*

Exercice 13. *La fonction $\exp : \mathbb{R} \longrightarrow \mathbb{R}_*^+$ est bijective.*

Exemple 13. *L'application $f : n \in \mathbb{N} \longmapsto n^2 \in \mathbb{N}$ est injective mais non surjective.*

Proposition 3.4

Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- Si f et g sont injectives, alors $g \circ f$ est injective.
- Si f et g sont surjectives, alors $g \circ f$ est surjective.
- Si f et g sont bijectives, alors $g \circ f$ est bijective.

Démonstration. Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- Supposons que f et g sont injectives.
  Soient $x_1, x_2 \in E$ tels que $g \circ f(x_1) = g \circ f(x_2)$.
  Donc $g(f(x_1)) = g(f(x_2))$
  Donc $f(x_1) = f(x_2)$ (car g est injective)
  Donc $x_1 = x_2$ (car f est injective) On a donc montré que $g \circ f$ est injective.

- Supposons maintenant que f et g sont surjectives.
  Soit $z \in G$. Il existe $y \in F$ tel que $z = g(y)$.
  De plus, il existe $x \in E$ tel que $y = f(x)$.
  Par conséquent,
  $$z = g(y) = g(f(x)) = g \circ f(x)$$
  ce qui prouve que $g \circ f$ est surjective.

- Le troisième point est une conséquence immédiate des deux premiers, en utilisant le fait qu'une application bijective est une application qui est injective et surjective.

□

Proposition 3.5

Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- Si $g \circ f$ est injective alors f est injective.
- Si $g \circ f$ est surjective alors g est surjective.

Démonstration. Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- Supposons que $g \circ f$ est injective.
  Montrons que f est injective.
  Soient $x_1, x_2 \in E$ tels que $f(x_1) = f(x_2)$.
  En appliquant g, on a :
  $g(f(x_1)) = g(f(x_2))$
  Donc $g \circ f(x_1) = g \circ f(x_2)$
  Donc $x_1 = x_2$ (car $g \circ f$ est injective).

- Supposons que $g \circ f$ est surjective.
  Soit $z \in G$. Il existe $x \in E$ tel que $z = g \circ f(x)$.
  On pose $y = f(x)$.
  On a $z = g(y)$, ce qui prouve que g est surjective.

□

Théorème 3.6

Une application $f : E \longrightarrow F$ est bijective si, et seulement si, il existe une application $g : F \longrightarrow E$ telle que $g \circ f = Id_E$ et $f \circ g = Id_F$.
De plus, l'application g est unique. On l'appelle la bijection réciproque de f, et on la note f^{-1}.

Démonstration. Soit $f : E \longrightarrow F$ une application.

- Supposons que f est bijective. On définit l'application $g : F \longrightarrow E$ de la façon suivante :
  Pour tout $y \in F$, $g(y)$ est l'unique antécédent de y par f.
  g est bien défini car cet antécédent appartient à E.
  Montrons maintenant que $g \circ f = Id_E$.
  Soit $x \in E$,
  $g \circ f(x) = g(f(x))$.
  Or, x est un antécédent de $f(x)$ par f (c'est le seul car f est bijective) donc, par définition de g, on a $g \circ f(x)$.
  De même, montrons que $f \circ g = Id_F$.
  Soit $y \in F$,
  $f \circ g(y) = f(g(y))$.
  Or, par définition de y, $g(y)$ est l'unique antécédent de y par f. Son image par f est donc y et on a bien $f \circ g(y) = y$.

- Réciproquement, supposons qu'il existe $g : F \longrightarrow E$ telle que $g \circ f = Id_E$ et telle que $f \circ g = Id_F$.
  Comme l'identité est bijective, on sait donc que $g \circ f$ est injective et donc, d'après la proposition **??**, que f est injective.
  De même, $f \circ g$ est surjective et on en déduit que f est surjective.
  Ainsi, f étant injective et surjective, elle est bijective.

- Montrons enfin que l'application g est unique. Supposons qu'il existe deux applications g_1 et g_2 telles que $g_1 \circ f = Id_E$ et $f \circ g_1 = Id_F$ d'une part et $g_2 \circ f = Id_E$ et telle que $f \circ g_2 = Id_F$ d'autre part.
  Supposons par l'absurde que $g_1 \neq g_2$.
  Il existe $y \in F$ tel que $g_1(y) \neq g_2(y)$.
  Par conséquent, $f(g_1(y)) \neq f(g_2(y))$ car f est injective.
  Donc $Id_F(y) \neq Id_F(y)$, ce qui implique que $y \neq y$, ce qui est absurde.

□

Remarque. *Il ne faut pas confondre l'image réciproque d'un ensemble* B *notée* $f^{-1}(B)$ *(qui existe toujours) et la bijection réciproque de* f*, notée* f^{-1} *(qui n'existe que si* f *est bijective). Dans le cas où* f *est bijective, l'image directe d'un ensemble* B *par l'application* f^{-1} *coïncide avec l'image réciproque de* B *par* f*. En revanche, cela n'aurait aucun sens si* f *n'était pas bijective.*

Exemple 14. *Soit* $f : z \in \mathbb{C} \setminus \{3\} \longmapsto \dfrac{iz - i}{z + 3} \in \mathbb{C} \setminus \{i\}$. *Montrer que* f *est bijective et déterminer sa bijection réciproque.*

Solution : Soit $z \in \mathbb{C} \setminus \{3\}$ et $z' \in \mathbb{C} \setminus \{i\}$.

$$\begin{aligned}
& z' = f(z) \\
\iff \quad & z' = \frac{iz - i}{z + 3} \\
\iff \quad & z'(z+3) = iz - i \quad (car\ z \neq -3) \\
\iff \quad & z(z' - i) = -3z' - i \\
\iff \quad & z = \frac{-3z' - i}{z' - i} \quad (car\ z' \neq i)
\end{aligned}$$

Cela prouve donc que f est bijective et que sa bijection réciproque est $f^{-1} : z \in \mathbb{C} \setminus \{i\} \longmapsto \dfrac{-3z - i}{z - i} \in \mathbb{C} \setminus \{3\}$

Exemple 15. *Soit $f : (x, y) \in \mathbb{R}^2 \longmapsto (x + y, x - y) \in \mathbb{R}^2$. Montrer que f est bijective et déterminer sa bijection réciproque.*

Solution : Soit $(x, y) \in \mathbb{R}^2$ et soit $(x', y') \in \mathbb{R}^2$.

$$\begin{aligned}
& (x', y') = f((x, y)) \\
\iff \quad & (x', y') = (x + y, x - y) \\
\iff \quad & \begin{cases} x' = x + y \\ y' = x - y \end{cases} \\
\iff \quad & \begin{cases} x' + y' = 2x \\ x' - y' = 2y \end{cases} \\
\iff \quad & (x, y) = \left(\frac{x' + y'}{2}, \frac{x - y}{2} \right)
\end{aligned}$$

Cela prouve donc que f est bijective et que sa bijection réciproque est $f^{-1} : (x, y) \in \mathbb{R}^2 \longmapsto \left(\frac{x+y}{2}, \frac{x-y}{2}\right)$.

Exercice 14. *Soit $f : (n, p) \in \mathbb{N}^2 \longmapsto 2^p(2n + 1) \in \mathbb{N}$. Montrer que f est bijective et déterminer sa bijection réciproque.*

Chapitre 4

Polynômes

I. Définition de l'ensemble des polynômes

1. Définition formelle

Dans tout ce chapitre, $\mathbb{K}$ désigne l'ensemble $\mathbb{R}$ ou $\mathbb{C}$. On note $\mathbb{K}^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathbb{K}$, c'est-à-dire l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{K}$.

Définition 4.1

Un polynôme sur $\mathbb{K}$ est une suite $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ dont les coefficients sont tous nuls à partir d'un certain rang, c'est à dire telle que :

$$\exists N \in \mathbb{N} \text{ tel que } \forall k > N,\ a_k = 0$$

On note $\mathbb{K}[X]$ l'ensemble des polynômes sur $\mathbb{K}$.

Définition 4.2

Soit $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ (avec P non identiquement nulle). L'indice du dernier coefficient non nul de P est appelé degré de P et est noté deg(P).
Si $N = \deg(P)$, on a donc $a_N \neq 0$ et $\forall k > N,\ a_k + 0$.

Remarque. *Par convention, si* P *est la suite nulle, on pose* $\deg(P) = -\infty$.

Exemple 1. $P = (2,0,1,-6,0,0,0,0,0,\ldots) \in \mathbb{R}[X]$. *De plus,* $\deg(P) = 3$. *Donc* $P \in \mathbb{R}_3[X]$. *On a aussi* $P \in R_4[X]$ *mais* $P \notin \mathbb{R}_2[X]$.

Remarque. *Comme* $\mathbb{R} \subset \mathbb{C}$, *on a* $\mathbb{R}[X] \subset \mathbb{C}[X]$. *Autrement dit, un polynôme à coefficients réels peut toujours être considéré comme un polynôme à coefficients complexes. La réciproque est en revanche fausse.*

Définition 4.3

Soient $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On définit :

- $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$
- $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$
- $P \times Q = (c_n)_{n\in\mathbb{N}}$ où, pour tout $n \in \mathbb{N}$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Remarque. *Ainsi définis, on a* $P + Q \in \mathbb{K}[X]$, $\lambda P \in \mathbb{K}[X]$ *et* $P \times Q \in \mathbb{K}[X]$. *Pour le justifier, il suffit de vérifier que ces suites sont bien identiquement nulles à partir d'un certain rang (preuve laissée au lecteur).*

Remarque. *La définition du produit de deux polynômes et celle de la multiplication par un scalaire (nombre) semble naturelle. Celle du produit de deux polynômes peut paraître étrange. On va cependant voir qu'elle correspond à la notion de « multiplication de fonction polynomiales ».*

Proposition 4.1

Si $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$, alors :
- $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$
- $\deg(PQ) = \deg(P) + \deg(Q)$.

Définition 4.4

On définit la suite $X = (0,1,0,0,0,0,\ldots)$.

Exercice 1. *Soit $k \in \mathbb{N}^*$. Déterminer $X^k = X \times X \times \ldots \times X$ (on pourra raisonner par récurrence).*

Proposition 4.2

Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ de degré N. On a

$$P = \sum_{k=0}^{N} a_k X^k$$

où l'on a posé, par convention, $X^0 = (1,0,0,0,0,\ldots)$.

Démonstration. Laissée au lecteur. □

Exemple 2. *Si* $P = (2,0,1,-6,0,0,0,0,0,\ldots)$, *on a* $P = 2 \times X^0 + 0X + 1X^2 + (-6)X^3$

2. Définition des fonctions polynomiales

Définition 4.5

Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ de degré N. La fonction $\tilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$ et définie par $\tilde{P}(x) = \sum_{k=0}^{n} a_k x^k$ est appelée fonction polynomiale associée à P.

Remarque.

Si l'on note $\mathscr{F}$ l'ensemble des fonctions polynomiales, il est possible de montrer que l'application suivante est bijective (elle est clairement bijective, par définition de $\mathscr{F}$) :

$$\left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathscr{F} \\ P & \longmapsto & \tilde{P} \end{array} \right.$$

En pratique, on ne distinguera pas les deux ensembles.

L'intérêt théorique de distinguer $\mathbb{K}[X]$ et $\mathscr{F}$ apparaît lorsque $\mathbb{K}$ est différent de $\mathbb{R}$ ou $\mathbb{C}$.

Dans le cadre de ce cours, par abus de notation, on notera souvent P l'application polynomiale associée à P, sans faire de distinction entre P et $\tilde{P}$.

Exercice 2. *Il est désormais possible de voir que la définition formelle que nous avons donné du produit de deux polynômes (Définition 4.3) correspond bien au produit de fonctions polynomiales. Par exemple, si $P = a_0 + a_1X + a_2X^2$ et $Q = b_0 + b_1X + b_2X^2 + b_3X^3$, calculer $P \times Q$ et $\tilde{P} \times \tilde{Q}$.*

II. Relation de divisibilité entre polynômes

1. Définition et premières propriétés

Définition 4.6

Soient $P, Q \in \mathbb{K}[X]$. On dit que P **divise** Q dans $\mathbb{K}[X]$ lorsqu'il existe $S \in \mathbb{K}[X]$ tel que $Q = PS$. On dit aussi que P est un **diviseur** de Q et que Q est un **multiple** de P. On note P|Q.

Exemple 3. *Si* $P = X - 1$ *et* $Q = X^2 - 1$ *alors* P *divise* Q *car* $X^2 - 1 = (X-1)(X+1)$

Proposition 4.3

Soient P, Q, R ∈ 𝕂[X].
Si P|Q et Q|R, alors P|R.

Proposition 4.4

Soient P, Q, R ∈ 𝕂[X] tels que P|Q et P|R.
- Pour tous m, $n \in K$, P|(mQ + nR).
- En particulier, P|(Q + R) et P|(Q − R).

Démonstration. La preuve de ces résultats est identique à celle des propriétés établies dans ℤ. □

2. Division euclidienne de polynômes

Proposition 4.5 – (admise)

Soient A ∈ 𝕂[X] et B ∈ 𝕂[X] \ {$0_{\mathbb{K}[X]}$}.
Il existe un unique couple (Q, R) ∈ 𝕂[X] × 𝕂[X] tels que :

$$\begin{cases} A = BQ + R \\ \text{et} \\ \deg(R) < \deg(B) \end{cases}$$

Remarque. *La condition* B ∈ 𝕂[X] \ {0} *signifie que* B *n'est pas le polynôme nul.*

Exemple 4. *Effectuer la division euclidienne de* A *par* B *dans les cas suivants :*

1. $A(x) = x^4 + 3x^3 + x^2 - 5x + 3$ *et* $B(x) = x$
2. $A(x) = x^4 + 3x^3 + x^2 - 5x + 3$ *et* $B(x) = x^2$
3. $A(x) = x^4 + 3x^3 + x^2 - 5x + 3$ *et* $B(x) = x^2 + x + 1$

Solution :

1. $A(x) = x(x^3 + 3x^2 + x - 5) + 3$.
   Ainsi $Q(x) = x^3 + 3x^2 + x - 5$ *et* $R(x) = 3$ *(avec* deg(R) < deg(B)*).*
2. $A(x) = x^2(x^2 + 3x + 1) - 5x + 3$.
   Ainsi $Q(x) = x^2 + 3x + 1$ *et* $R(x) = -5x + 3$ *(avec* deg(R) < deg(B)*).*
3. *On pose la division euclidienne comme ci-dessous, en ordonnant les polynômes selon les puissances décroissantes de* x*.*

$$\begin{array}{rl|l} & x^4 + 3x^3 + x^2 - 5x + 3 & x^2 + x + 1 \\ \cline{3-3} - & x^4 + x^3 + x^2 & x^2 + 2x - 2 \\ \cline{1-2} & 2x^3 - 5x + 3 & \\ - & 2x^3 + 2x^2 + 2x & \\ \cline{1-2} & -2x^2 - 7x + 3 & \\ - & -2x^2 - 2x - 2 & \\ \cline{1-2} & -5x + 5 & \end{array}$$

   Ainsi, on a $A(x) = (x^2 + x + 1)(x^2 + 2x - 2) + (-5x + 5)$.
   Par conséquent, $Q(x) = x^2 + 2x - 2$ *et* $R(x) = -5x + 5$ *(avec* deg(R) < deg(B)*).*

III. Application à l'étude des racines

1. Racines d'un polynôme

Définition 4.7

Soit $P \in \mathbb{K}[X]$ et soit $a \in \mathbb{C}$. On dit que a est une racine de P si $\tilde{P}(a) = 0$.

Remarque. *Même si* $P \in \mathbb{R}[X]$, P *peut admettre des racines complexes non réelles. C'est par exemple le cas de polynômes du second degré lorsque* $\Delta < 0$.

Proposition 4.6

Soit $P \in \mathbb{R}[X]$ et soit $z \in \mathbb{C}$. z est une racine de P si, et seulement si, $\overline{z}$ est une racine de P.

Démonstration. Soit $P = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[X]$ et soit $z \in \mathbb{C}$. Alors,

$$\begin{aligned}
P(z) = 0 &\iff \sum_{k=0}^{n} a_k z^k = 0 \\
&\iff \overline{\sum_{k=0}^{n} a_k z^k} = 0 \\
&\iff \sum_{k=0}^{n} \overline{a_k z^k} = 0 \\
&\iff \sum_{k=0}^{n} \overline{a_k}\,\overline{z}^k = 0 \\
&\iff \sum_{k=0}^{n} a_k \overline{z}^k = 0 \qquad (\text{car } \forall k,\ a_k \in \mathbb{R}) \\
&\iff P(\overline{z}) = 0
\end{aligned}$$

□

Remarque. *La condition* $P \in \mathbb{R}[X]$ *est essentielle. La Proposition devient fausse si* $P \in \mathbb{C}[X]$.
Il suffit de considérer par exemple le polynôme $P(X) = (X - i)(X - 1)$.

2. Existence de racines et nombre de racines

Proposition 4.7 – Théorème de D'Alembert-Gauss (admis)

Tout polynôme $P \in \mathbb{K}[X]$ non constant admet au moins une racine complexe.

Histoire – Théorème de d'Alembert-Gauss

Au XVIII^{e} siècle, l'existence de racines complexes était globalement admise mais cela n'a été démontrée rigoureusement qu'au début du XIX^{e} siècle. Ce théorème est également connu sous le nom de « théorème fondamental de l'algèbre ». Il s'agit là d'une situation que l'on peut aujourd'hui estimer paradoxale car toutes les démonstrations connues utilisent des arguments analytiques (d'analyse complexe par exemple). Cependant, le paradoxe n'est qu'apparent car le nom de « théorème fondamental de l'algèbre » est apparu à une époque où l'algèbre désignait la théorie des équations. De nos jours, ce terme désigne plutôt la discipline qui s'intéresse aux structures et aux opérations sur les ensembles.

Proposition 4.8

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors

$$P(a) = 0 \iff \text{Il existe } Q \in \mathbb{K}[X] \text{ tel que, } P = (X - a)Q$$

Démonstration.

- $\Longleftarrow$ Supposons qu'il existe $Q \in \mathbb{K}[X]$ tel que, pour tout $x \in \mathbb{K}$, $P = (X-a)Q$.
  Alors, $P(a) = (a-a)Q(a) = 0$.
- $\Longrightarrow$ Réciproquement, supposons que $P(a) = 0$.
  On effectue la division euclidienne de P par $X - a$.
  Ainsi, il existe des polynômes Q et R tels que

$$\begin{cases} P = (X-a)Q + R \ (\star) \\ \text{et} \\ \deg(R) < 1 \end{cases}$$

  Par conséquent, R est un polynôme constant. On note c cette constante.
  En évaluant l'égalité $(\star)$ pour $x = a$, on obtient

$$\begin{aligned} & P(a) = (X-a)Q(a) + c \\ \Longleftrightarrow\ & 0 = 0 + c \\ \Longleftrightarrow\ & 0 = c \end{aligned}$$

  Finalement, $R = 0$ et donc $P = (X-a)Q$.

□

Exemple 5. *On considère le polynôme* $P(x) = x^3 - 1$.
Montrer que $(X-1)$ *divise* P *puis établir la factorisation de* P *par* $X-1$.

Solution :
$P(1) = 1^3 - 1 = 0$. *Ainsi,* 1 *est une racine de* P *donc* $x-1$ *divise* P.
On effectue la division euclidienne de P *par* $X-1$ *et on trouve :*

$$P = (X-1)(X^2 + X + 1).$$

Proposition 4.9

Pour tout $n \geqslant 1$, pour tout polynôme $P \in \mathbb{K}[X]$ de degré n, P admet au plus n racines.

Démonstration. On démontre par récurrence que la propriété $\mathscr{H}(n)$: « Pour tout $P \in \mathbb{K}[X]$ de degré n, P admet au plus n racines » est vraie pour tout entier $n \geqslant 1$.

- Initialisation : Si P est un polynôme de degré 1, $P(x) = aX + b \quad (\text{avec } a \neq 0)$.
  Par conséquent, $-\dfrac{b}{a}$ est l'unique racine de P et donc $\mathscr{H}(1)$ est vraie.
- Hérédité : Supposons que $\mathscr{H}(n)$ soit vraie pour un certain entier $n \geqslant 1$. Montrons qu'alors $\mathscr{H}(n+1)$ est vraie.
  Soit $P \in \mathbb{K}[X]$ de degré $n+1$. On va montrer que P admet au plus $n+1$ racines.
  En fait, on peut supposer que P admet une racine (car sinon il n'y alors rien à démontrer). On note a cette racine.
  D'après la Proposition 7, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q$.
  En utilisant la règle du produit nul, on voit que l'ensemble des racines de P est constitué de l'ensemble des racines de Q auquel on ajoute a.
  On a de plus $\deg(Q) = n$ et donc, d'après $\mathscr{H}(n)$, Q admet au plus n racines.
  Finalement, on en déduit que P admet au plus $n+1$ racines et donc que $\mathscr{H}(n+1)$ est vraie.

□

IV. Factorisation de polynômes

1. Factorisation dans $\mathbb{C}[X]$

Proposition 4.10

Soit $P \in \mathbb{C}[X]$. Il existe $x_1, x_2, \dots, x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que

$$P = a \prod_{k=1}^{n} (X - x_k).$$

Remarque.

- *a est le coefficient dominant de* P.
- *Les nombres x_k ne sont pas nécessairement deux à deux distincts.*
- *On peut aussi utiliser ce résultat si* $P \in \mathbb{R}[X]$ *car* $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Démonstration. On démontre par récurrence que la propriété $\mathscr{H}(n)$: « Pour tout $P \in \mathbb{C}[X]$ de degré n, il existe $x_1, x_2, \dots, x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que, $P = a \prod_{k=1}^{n} (X - x_k)$ » est vraie pour tout entier $n \geqslant 1$.

- Initialisation : Si P est un polynôme de degré 1, $P(x) = aX + b$ (avec $a \neq 0$).
  En posant $x_1 = -\dfrac{b}{a}$, on a $P = a(X - x_1)$ et donc $\mathscr{H}(1)$ est vraie.
- Hérédité : Supposons que $\mathscr{H}(n)$ soit vraie pour un certain entier $n \geqslant 1$.
  Montrons qu'alors $\mathscr{H}(n+1)$ est vraie.
  Soit $P \in \mathbb{K}[X]$ de degré $n+1$.
  D'après le théorème de D'Alembert-Gauss, P admet une racine complexe (on la note x_{n+1}). De plus, d'après la Proposition 4.8, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - x_{n+1})Q$.
  D'après l'hypothèse de récurrence, comme $\deg(Q) = n$, il existe $x_1, \dots x_n \in \mathbb{C}$ et $a \in \mathbb{C}$
  tels que $Q = a \prod_{k=1}^{n} (X - x_k)$.
  Par conséquent, on a

$$\begin{aligned} P &= (X - x_{n+1})Q \\ &= (X - x_{n+1}) \times a \prod_{k=1}^{n} (X - x_k) \\ &= a \prod_{k=1}^{n+1} (X - x_k) \end{aligned}$$

  Ainsi, on a montré que $\mathscr{H}(n+1)$ est vraie.

□

2. Factorisation dans $\mathbb{R}[X]$

Proposition 4.11

Soit $P \in \mathbb{R}[X]$. Il existe $x_1, x_2, \dots, x_r \in \mathbb{R}$, il existe $s_1, t_1, s_2, t_2, \dots s_l, t_l \in \mathbb{R}$ et $a \in \mathbb{R}$ tels que pour tout x, $P(x) = a \prod_{k=1}^{r} (x - x_k) \times \prod_{k=1}^{l} (x^2 + s_k x + t_k)$ où les polynômes $x^2 + s_k x + t_k$ sont sans racines réelles, c'est-à-dire que $s_k^2 - 4t_k < 0$.

Démonstration. On sait, d'après la Proposition 4.10 qu'il existe $x_1, x_2, \dots, x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que :

$$P = a \prod_{k=1}^{n} (X - x_k).$$

Quitte à permuter les x_i, on peut supposer que $x_1, x_2, \dots, x_r \in \mathbb{R}$ et que $x_{r+1}, \dots, x_n \in \mathbb{C} \setminus \mathbb{R}$.
Par conséquent, on a $P = a \prod_{k=1}^{r} (X - x_k) \times Q$ où Q admet pour racines $x_{r+1}, \dots, x_n \in \mathbb{C} \setminus \mathbb{R}$ et, *a priori*, $Q \in \mathbb{C}[X]$.

En fait, comme les polynômes $a\prod_{k=1}^{r}(X-x_k)$ et P sont à coefficients réels, il en est de même pour Q (cela découle directement de l'unicité de la division euclidienne dans $\mathbb{R}[X]$).

Par ailleurs, d'après la Proposition 5, comme x_{r+1} est une racine de Q, $\overline{x_{r+1}}$ est également une racine de Q. Sachant que $x_{r+1} \neq \overline{x_{r+1}}$, Q est donc divisible par $(X-x_{r+1})(X-\overline{x_{r+1}})$.
Or,

$$\begin{aligned}(X-x_{r+1})(X-\overline{x_{r+1}}) &= X^2-(x_{r+1}+\overline{x_{r+1}})X+x_{r+1}\overline{x_{r+1}}\\ &= X^2-2\mathrm{Re}(x_{r+1})X+(\mathrm{Re}(x_{r+1}))^2+(\mathrm{Im}(x_{r+1}))^2\end{aligned}$$

Cela prouve donc que $(X-x_{r+1})(X-\overline{x_{r+1}})$ est un polynôme à coefficient réel. Il existe donc des réels s_1 et t_1 tels que, pour tout $x\in\mathbb{R}$, $(X-x_{r+1})(X-\overline{x_{r+1}}) = X^2+s_1X+t_1$
Ainsi, il existe $Q'\in\mathbb{R}[X]$ tel que, $Q = (X^2+s_1X+t_1)Q'$ et les racines de Q' sont les racines de Q auxquelles on a enlevé x_{r+1} et $\overline{x_{r+1}}$.
En répétant le procédé avec Q', on voit que l'on pourra factoriser Q en produit de polynômes réels du second degré.
Finalement, on obtiendra une factorisation de P de la forme suivante :

$$P = a\prod_{k=1}^{r}(X-x_k)\times\prod_{k=1}^{l}(X^2+s_kX+t_k)$$

□

Exemple 6. *Factoriser dans* $\mathbb{R}[X]$ *et dans* $\mathbb{C}[X]$ *le polynôme* $P = X^4-1$.

Solution :
P *admet les quatre racines suivantes :* $1, -1, i, -i$.
Ainsi, $P = (X-1)(X+1)(X-i)(X+i)$ *(factorisation dans* $\mathbb{C}[X]$*)*
Par conséquent, $P = (X-1)(X+1)(X^2+1)$ *(factorisation dans* $\mathbb{R}[X]$*).*

Chapitre 5

Groupes

I. Groupes

1. Définitions

Définition 5.1

Soit E un ensemble. Une loi de composition interne sur E est une application $\star : E \times E \longrightarrow E$. Pour désigner l'image d'un couple (x, y), plutôt que d'utiliser la notation $\star(x, y)$, on note $x \star y$.

Exemple 1. *La multiplication, notée* $\times$*, dans* $\mathbb{R}$ *est une loi de composition interne sur* $\mathbb{R}$.

Définition 5.2

Soit G un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un groupe lorsque les trois conditions suivantes sont vérifiées :

1. $\forall x, y, z \in G,\ (x \star y) \star z = x \star (y \star z)$ (associativité)
2. $\exists e \in G, \forall x \in G,\ x \star e = e \star x = x$ (existence d'un élément neutre)
3. $\forall x \in G, \exists y \in G,\ x \star y = y \star x = e$ (existence d'un inverse)

Étymologie – Groupe

Le mot *groupe* vient de l'italien *gruppo, noeud, assemblage*, lui-même issu de la racine germanique *kruppa* (l'anglais *crop, récolte* est de la même racine). Il apparaît en françaisau XVII^{e} siècle et donne bientôt de nombreux dérivés.
Évariste Galois utilise le mot groupe pour désigner les permutations qui agissent sur les racines d'une équation. Il s'intéresse surout à la structure obtenue en composant ces permutations.
À partir des années 1850, des mathématiciens utilisent de manière d'abord informelle l'expression *groupe de permutations* pour désigner les actions de transformations sur des ensembles. Le besoin d'une formalisation puis d'une axiomatisation de cette notion se fait sentir tout au long du XIX^{e} siècle. Les premières définitions sont dues à Arthur Cayley, camille Jordan, Leopold kronecker, Walter Dyck. La définition actuelle est donnée par Heinrich Weber en 1893.

Étymologie – Neutre

Le mot *neutre* est formé sur le latin *ne uter* qui signifie *aucun des deux*. Il est apparu en français au XVI^{e} siècle et signifiait celui qui ne prend pas partie. L'élément neutre est introduit avec la théorie des groupes vers 1900.

Exemple 2. $(\mathbb{R}^*, \times)$ *est un groupe mais* $(\mathbb{R}, \times)$ *n'est pas un groupe.*

2. Premières propriétés

Proposition 5.1

Soit $(G, \star)$ un groupe.
- L'élément neutre est unique.
- Chaque élément $x \in G$ possède un unique inverse (appelé aussi symétrique). On le note x^{-1}.
- Pour tout $x \in G$, $\left(x^{-1}\right)^{-1} = x$

Démonstration. Soit $(G, \star)$ un groupe.
- Soient e et e' deux éléments neutre de G.
  Comme e est un élément neutre, on a $e \star e' = e'$.
  De plus, comme e' est un élément neutre, on a $e \star e' = e$
  Par conséquent, $e' = e$ et l'élément neutre est donc unique.
- Soit $x \in G$. Supposons qu'il existe deux inverses y et y'.
  D'une part $yxy' = ey' = y'$ car y est un inverse de x.
  D'autre part, $yxy' = ye = y$ car y' est un inverse de x.
  On en déduit que $y = y'$ et donc que l'inverse est unique.
- Par définition de x^{-1}, $xx^{-1} = x^{-1}x = e$ donc x^{-1} est inversible et son inverse est x, ce qui s'écrit aussi $\left(x^{-1}\right)^{-1} = x$.

□

Dans la suite du cours, et sauf mention du contraire, on utilise la notation multiplicative, donc $a \star b$ sera noté simplement ab.

Proposition 5.2

Soit $(G, .)$ un groupe. Alors pour tous éléments $a, b, x \in G$:
1. Si $ax = bx$, alors $a = b$ (simplification à droite)
2. Si $xa = xb$, alors $a = b$ (simplification à gauche)
3. Le symétrique de ab est $b^{-1}a^{-1}$.

Démonstration. Pour les points 1 et 2, il suffit de multiplier par x^{-1} à droite dans le premier cas et à gauche dans le second.
Pour le point 3, il suffit de voir que

$$(ab)\left(b^{-1}a^{-1}\right) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$$

De même,

$$\left(b^{-1}a^{-1}\right)(ab) = e$$

Cela prouve bien que l'inverse de ab est $b^{-1}a^{-1}$. □

Définition 5.3 – Puissance

Soit $(G, .)$ un groupe et soit $n \in \mathbb{N}^*$.
- Pour tout $x \in G$, on note $x^n = \underbrace{x \times x \times \ldots \times x}_{n \text{ facteurs}}$.
- Par convention, pour tout $x \in G$, $x^0 = e$.
- Pour tout $x \in G$, $(x^{-1})^n = (x^n)^{-1}$. Cet élément est noté x^{-n}.

Définition 5.4

Un groupe est dit commutatif (on dit aussi abélien) si :

$$\forall x, y \in G,\ x \star y = y \star x.$$

Étymologie – Abélien

L'adjéctif *abélien* vient du nom du mathématicien norvégien Niels Abel. Camille Jordan trouve dans les écrits de Galois la réponse à la question posée par Abel : une équation polynomiale est résoluble par radicaux si, et seulement si, son groupe de Galois est résoluble. Ceci ammène à étudier les groupes commutatifs qu'il nomme groupe abéliens. Ce terme apparaît dans *Traité des substitutions et des équations algébriques* publiés en 1870.

Exemple 3. $(\mathbb{Z},+)$ *est un groupe commutatif.*

Remarque. *Dans le cas d'un groupe commutatif, on privilégie souvent la notation additive* $+$*. On note alors* 0 *l'élément neutre et* $-x$ *l'inverse de* x*. De plus, on écrit* nx *au lieu de* x^n*.*

Exemple 4 (Groupes concernant les ensembles de nombres usuels)**.**

- $(\mathbb{N},+)$ *n'est pas un groupe (*2 *n'admet pas d'inverse).*
- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ *sont des groupes d'élément neutre* 0.
- $(\mathbb{Z}^*,\times)$ *n'est pas un groupe (*2 *n'admet pas d'inverse).*
- $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$ *sont des groupes d'élément neutre* 1.

Définition 5.5 – Ordre d'un groupe

L'ordre d'un groupe (G,.) est le cardinal de G.

Définition 5.6 – Groupes produits

Soient $(G,\star)$ et (H,Δ) deux groupes d'éléments neutres respectifs e_G et e_H. On munit le produit cartésien $G\times H$ de la loi de composition interne $\wedge$ définie pour tout $(a,b),(c,d)\in G$ par $(a,b)\wedge(c,d)=(a\star c, b\Delta d)$. Alors $(G\times H,\wedge)$ est un groupe d'élément neutre (e_G,e_H). On l'appelle le groupe produit de G et de H.

II. Sous-groupes

1. Définition et premiers exemples

Définition 5.7 – Sous-groupe

Soit (G,.) un groupe. On dit qu'un sous-ensemble H de G est un **sous-groupe** de G lorsque les trois conditions suivantes sont vérifiées :

1. L'ensemble H n'est pas vide.
2. Pour tous $x,y\in H$, $\quad xy\in H$
3. Pour tous $x\in H$, $\quad x^{-1}\in H$

Pour vérifier qu'un ensemble est un sous-groupe on peut rassembler les conditions 2 et 3 dans une seule condition :

Proposition 5.3

Soit (G,.) un groupe et $H\subset G$. H est un sous-groupe de G si, et seulement si, les deux conditions suivantes sont vérifiées :

1. H contient l'élément neutre
2. $\forall x,y\in H,\ xy^{-1}\in H$

Démonstration. Laissée en exercice. □

Exemple 5.

- *Si* G *est un groupe,* $\{e\}$ *et* G *sont des sous-groupes de* G.
- *Dans* $(\mathbb{Z},+)$*, une partie de la forme* $n\mathbb{Z}$ *(avec* $n\in\mathbb{N}$*) est un sous-groupe.*
  En effet,

— $1 \in n\mathbb{Z}$
— *Si* $x \in n\mathbb{Z}$ *et* $y \in n\mathbb{Z}$, *alors* $x+y \in n\mathbb{Z}$
— *Si* $x \in n\mathbb{Z}$, *alors* $-x \in n\mathbb{Z}$.

Remarque. *Les deux derniers points peuvent être remplacés par : pour tout* $x \in n\mathbb{Z}$ *et tout* $y \in n\mathbb{Z}$, $x-y \in n\mathbb{Z}$.

Théorème 5.4

Soit (G,.) un groupe et H un sous groupe de G. La restriction à H de la loi de composition sur G fait de (H,.) un groupe.

Remarque. *On utilise souvent ce théorème pour montrer qu'un ensemble est un groupe. Par exemple,* $(n\mathbb{Z},+)$ *est un groupe car c'est un sous-groupe de* $(\mathbb{Z},+)$. *Cela évite d'avoir à redémontrer l'associativité notamment.*

Proposition 5.5

Soit (G,.) un groupe et H_1 et H_2 deux sous-groupes de G. Alors $H_1 \cap H_2$ est un sous-groupe de G.

Démonstration. Soit G un groupe et H_1 et H_2 deux sous groupes.
- $e \in H_1$ et $e \in H_2$ donc $e \in H_1 \cap H_2$
- Soit $x \in H_1 \cap H_2$ et $y \in H_1 \cap H_2$.
  Alors $xy^{-1} \in H_1$ car H_1 est un sous-groupe de G.
  De même, $xy^{-1} \in H_2$ car H_2 est un sous-groupe de G.
  Ainsi, $xy^{-1} \in H_1 \cap H_2$

Finalement, on a montré que $H_1 \cap H_2$ est un sous-groupe de G. □

Corollaire 5.6

Soit (G,.) un groupe d'ordre fini n et d'élément neutre e. Pour tout $a \in G$, $a^n = e$.

Démonstration. Soit (G,.) un groupe d'ordre fini m et d'élément neutre e. Soit $a \in G$.
On pose $H =< a >$ et on note m l'ordre de a dans G. Alors $H = \{e, a, a^2, \dots, a^{m-1}\}$ d'après la proposition **??** et $\text{Card}(H) = m$.
Ainsi, on a m divise n donc il existe $k \in \mathbb{N}$ tel que $n = mk$.
Finalement,

$$a^n = a^{mk} = (a^m)^k = e^k = e$$

□

III. Exemples fondamentaux de groupes

1. Le groupe $(\mathbb{Z},+)$

Théorème 5.7

Soit $H \subset \mathbb{Z}$. H est un sous-groupe de $\mathbb{Z}$ ssi il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. De plus, l'entier n est unique.

Remarque. *On dit que tous les sous groupes de* $\mathbb{Z}$ *sont monogènes.*

Démonstration. On a déjà vu que les ensembles de la forme $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.
Réciproquement, soit H un sous-groupe de $\mathbb{Z}$.
Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
Sinon, $H \cap \mathbb{N}^* \neq \emptyset$.
On pose $n_0 = \min(H \cap N^*)$
On va montrer que $H = n_0\mathbb{Z}$.
Comme $n_0 \in H$ et que H est stable par addition et passage à l'opposé, il est clair que $n_0\mathbb{Z} \subset H$.
Montrons l'inclusion inverse :
Soit $m \in n_0\mathbb{Z}$. On fait la division euclidienne de m par n_0.
Il existe ainsi deux entiers r et q tels que $m = n_0 q + r$ et $0 \leqslant r < n_0$.
Supposons par l'absurde que $r \neq 0$,

On aurait $r = m - n_0 q \in \mathrm{H}$ (car $m \in \mathrm{H}$ et $n_0 q \in \mathrm{H}$).
Ainsi, $r \in \mathrm{H} \cap \mathrm{N}^*$ et $r < n_0$.
Cela est absurde par définition de n_0. Finalement, on a bien montré que $\mathrm{H} \subset n_0\mathbb{Z}$ et donc que $\mathrm{H} = n_0\mathbb{Z}$. □

2. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z})^*, \times)$

Soit $n \in \mathbb{N}^*$. On définit sur $\mathbb{Z}$ la relation de congruence modulo n par :

$$a \equiv b \, mod(n) \qquad \text{ssi } n \text{ divise } (b-a).$$

Définition 5.8

$\mathbb{Z}/n\mathbb{Z}$ est défini comme l'ensemble $\{0, 1, \ldots, n-1\}$ muni de l'addition modulo n (notée $+$) et de la multiplication modulo n (notée $\times$).

Proposition 5.8

- $\mathrm{Card}(\mathbb{Z}/n\mathbb{Z}) = n$
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif d'élément neutre $\overline{0}$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique ($\overline{1}$ est un générateur).
- La loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative, commutative, d'élément neutre $\overline{1}$.

Définition 5.9

L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\times$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$.

Proposition 5.9

$((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe commutatif d'élément neutre 1.

Remarque.

- *L'inverse de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ n'existe pas nécessairement. De plus, écrire que l'inverse est $\overline{\frac{1}{x}}$ n'a en général pas de sens car $\frac{1}{x}$ n'est pas entier. Par exemple, l'inverse de $\overline{2}$ dans $\mathbb{Z}/5\mathbb{Z}$ est $\overline{3}$.*
- *La règle de simplification*
$$\text{Pour tout } \overline{a} \neq \overline{0}, \quad \overline{a}\,\overline{b} = \overline{a}\,\overline{c} \Longrightarrow \overline{b} = \overline{c}$$
n'est pas valide en général. On peut néanmoins simplifier si $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

3. Le cercle unité et le groupe des racines n^e dans $\mathbb{C}$

Définition 5.10

On appelle **cercle unité** et on note $\mathbb{U}$, l'ensemble des nombres complexes de module 1. On a donc :

$$\mathbb{U} = \{z \in \mathbb{C} \,/\, |z| = 1\}.$$

Géométriquement, $\mathbb{U}$ correspond au cercle de centre O et de rayon 1.

Proposition 5.10

$(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Démonstration. Laissée en exercice. □

Remarque. $(\mathbb{U}, +)$ *n'est pas un groupe car il ne contient pas d'élément neutre et $\mathbb{U}$ n'est pas stable par addition.*

Définition 5.11

Pour $n \in \mathbb{N}^*$, on appelle **racine n^e de l'unité** et on note $\mathbb{U}_n$ l'ensemble des solutions de l'équation $z^n = 1$.

Proposition 5.11

Pour tout $n \in \mathbb{N}^*$,

- $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.
- $\text{Card}(\mathbb{U}_n) = n$.
- $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\} = < e^{\frac{2i\pi}{n}} >$.

Démonstration. Soit $n \in \mathbb{N}^*$.

- Montrons que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$. Déjà, il est clair que $\mathrm{U}_n \subset \mathbb{U}$. En effet, si $z \in \mathbb{U}_n$, alors $z^n = 1$ donc $|z^n| = 1$ donc $|z|^n = 1$.
  Étant donné que $|z| \in \mathbb{R}^+$, on en déduit que $|z| = 1$ et on a bien $z \in \mathbb{U}$.
  On montre désormais $\mathbb{U}_n$ contient le neutre, et qu'il est stable par multiplication et passage à l'inverse.
  — Neutre : $1\mathbb{U}_n$
  — Soient $z \in \mathbb{U}_n$ et $z' \in \mathbb{U}_n$.
  Alors, $\left(zz'^{-1}\right)^n = \left(\frac{z}{z'}\right)^n = \frac{z^n}{z'^n} = 1$
- On va montrer les points 2 et 3 conjointement. Soit $z \in \mathbb{C}^*$. On pose $z = \rho e^{i\theta}$

$$\begin{aligned} z^n = 1 &\Longleftrightarrow \rho^n e^{in\theta} = 1 \\ &\Longleftrightarrow \begin{cases} \rho^n = 1 \\ n\theta = 2k\pi \ \ (k \in \mathbb{Z}) \end{cases} \\ &\Longleftrightarrow \begin{cases} \rho = 1 \\ n\theta = \dfrac{2k\pi}{n} \ \ (k \in \mathbb{Z}) \end{cases} \end{aligned}$$

  Ainsi, $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in \mathbb{Z} \right\} = < e^{\frac{2i\pi}{n}} >$.

  Montrons de plus que $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$.
  L'inclusion $\left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\} \subset \mathbb{U}_n$ est évidente.
  Réciproquement, soit $k \in \mathbb{Z}$. En faisant la division euclidiennde de k par n, il existe deux entiers p et q tels que $k = nq + r$ avec $0 \leqslant r < n$.
  Ainsi,

$$e^{\frac{2ik\pi}{n}} = e^{\frac{2i(nq+r)\pi}{n}} = e^{2iq\pi} e^{\frac{2ir\pi}{n}} = e^{\frac{2ir\pi}{n}}$$

  Donc on a bien $e^{\frac{2ik\pi}{n}} \in \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$.

  Enfin, on va montrer que l'ensemble $\left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$ possède exactement n éléments. Pour cela, on va montrer que si k et k' sont deux entiers distincts, alors $e^{\frac{2ik\pi}{n}} \neq e^{\frac{2ik'\pi}{n}}$.
  Par contraposée, supposons que k et k' soient des entiers tels que $e^{\frac{2ik\pi}{n}} = e^{\frac{2ik'\pi}{n}}$.
  Alors $\dfrac{e^{\frac{2ik\pi}{n}}}{e^{\frac{2ik'\pi}{n}}} = 1$ et on a donc $e^{2i(k-k')\pi n} = 1$
  Donc n divise $k - k'$.
  Comme $|k - k'| \leqslant n-1$, on en déduit que $k - k' = 0$, c'est-à-dire $k = k'$.
  Ainsi, on a bien montré que l'ensemble $\left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$ possède exactement n éléments.

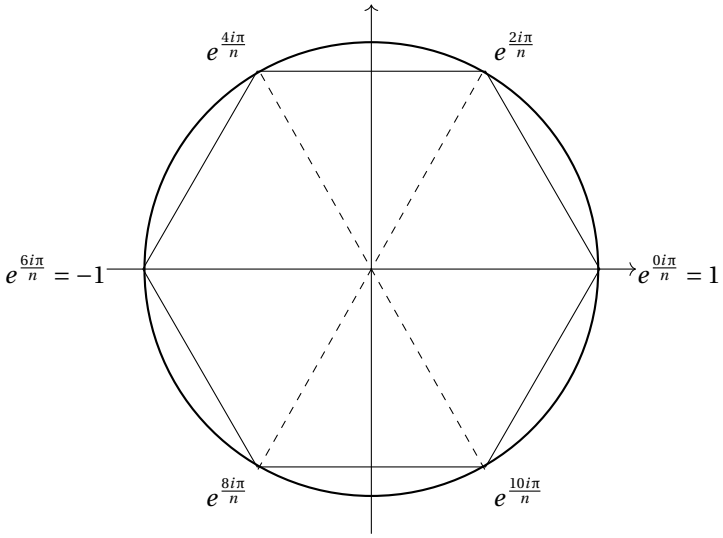
□

Remarque. *En utilisant le vocabulaire de la théorie des groupes, on aurait pu montrer que $e^{\frac{2i\pi}{n}}$ est d'ordre n dans $\mathbb{U}_n$ et appliquer la Proposition B.8*

Exemple 6.

- $\mathbb{U}_2 = \{1; -1\}$
- $\mathbb{U}_3 = \{1; j; j^2\}$ *avec* $j = e^{\frac{2i\pi}{3}}$
- $\mathbb{U}_4 = \{1; i; -1; -i\}$

Remarque. *Si $n \geqslant 3$, alors les points dont les affixes sont des racines n^e de l'unité forment un polygône régulier à n côtés. Par exemple, le dessin ci-dessous représente les racines de l'unité pour $n = 6$.*



4. Le groupe des permutations

Définition 5.12

Soit E un ensemble. L'ensemble $\mathscr{S}(E)$ des bijections de E dans E est un groupe pour la loi de composition $\circ$. Son élément neutre est l'application Id_E. Le groupe $(\mathfrak{S}(E), \circ)$ est appelé **groupe symétrique de** E. Les éléments de $\mathfrak{S}(E)$ sont appelés des permutations.

Remarque.

- *Dans le cas où* $E = \{1, \dots, n\}$, *on note* $\mathfrak{S}_n = \mathfrak{S}(E)$. *Le groupe* $\mathfrak{S}_n$ *est appelé le groupe symétrique d'ordre* n.
- $Card(\mathfrak{S}_n) = n!$.
- *Rappel : l'identité* $Id_{\{1,\dots,n\}}$ *et les transpositions* $t_{a,b}$ *sont des permutations.*
- *Pour* $n \geqslant 3$, $\mathfrak{S}_n$ *est un groupe non commutatif.*
  En effet, si on choisit trois éléments distincts $a, b, c \in \{1, \dots, n\}$, *on a :*

$$t_{a,b} \circ t_{b,c} \neq t_{b,c} \circ t_{a,b}.$$

- *Dans* $\mathfrak{S}_5$, *une permutation se note par exemple* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$. *On la note aussi* (15423). *Avec cette notation la composée des transpositions* $t_{1,2} \circ t_{4,5}$ *se note* $(12) \circ (45)$.

Étymologie – Permutation

En latin, *permutare* signifiait *échange* et *permutatio* désignait un changement, une modification. Au Moyen Âge, la permutation était le troc ou le change. Vers le XV^{e} siècle, son sens se spécialise dans le fait d'échanger deux éléments, Leibniz appelait variation ce que nous appelons de nos jours permutation.
Au début du XIX^{e} siècle, se rapprochant du sens latin, on appelle *permutation* en mathématique la modification de l'ordre de n lettres. Certains l'utilisent cependant dans le sens d'arrangement. On rencontre souvent *permutation* chez Lagrange, Cauchy et Galois lorsqu'ils travaillent sur les racines d'une équation polynomiale. cauchy distingue curieusement une permutation dans le sens que nous venons de voir et une substitution qui représente à ses yeux réellement une bijection, c'est-à-dire le passage d'un ordre à un autre. De nos jours, les deux mots sont synonymes.

Annexes

Chapitre A

Calculs de sommes

I. Sommes simples

Définition A.1

Soient a et b des entiers et soit $(x_i)_{a\leqslant i\leqslant b}$ une famille de nombres (réels ou complexes). On note $\sum_{i=a}^{b} x_i$ la **somme des** x_i.

Remarque.

- *En général, on considérera des sommes où l'indice i va de 1 à n ou de 0 à n.*
- *Il pourra être utile de noter, au brouillon la somme avec des pointillés ($\sum_{i=1}^{n} a_i = a_1 + a2 + \ldots + a_n$. Cependant, afin de rédiger une démonstration rigoureuse, il est attendu d'utiliser le symbole $\sum$.*

1. Sommes de référence

Proposition A.1 – Somme d'une constante

Si $a \leqslant b$ sont des entiers et $\lambda \in \mathbb{R}$ une constante, alors :

$$\sum_{k=a}^{b} \lambda = \lambda(b-a+1)$$

.

Proposition A.2 – Somme géométrique

(Par convention, $x^0 = 1$ même si x est nul)
Pour tout $x \neq 1$,

$$\sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}.$$

Exemple 1.

$$\sum_{k=0}^{9} 2^k = \frac{1-2^{10}}{1-2} = 2^{10} - 1 = 1023$$

Remarque. *De manière générale, on peut retenir que la somme des termes d'une suite géométrique (u_n) est donnée par :*

$$\sum u_k = (\textit{premier terme}) \times \frac{1-(\textit{raison})^{\textit{nombre de termes}}}{1-(\textit{raison})}$$

Proposition A.3 – Somme des entiers, des carrés, des cubes

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \qquad \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad \sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

Démonstration. Laissée en exercice, par récurrence sur n. □

2. Opérations sur les sommes

a. Linéarité

- $\sum_{k=a}^{b} u_k + v_k = \sum_{k=a}^{b} u_k + \sum_{k=a}^{b} v_k$
- $\sum_{k=a}^{b} \lambda u_k = \lambda \left(\sum_{k=a}^{b} u_k \right)$

En revanche, en général, $\sum_{k=a}^{b} u_k \times v_k \neq \left(\sum_{k=a}^{b} u_k \right) \times \left(\sum_{k=a}^{b} v_k \right)$

Étymologie – Distributivité

Dans le produit $(a_1 + a_2 + \ldots + a_n)b$ on peut distribuer b à chaque a_i comme on distribue un carré de chocolat à chaque enfant d'un groupe. cette analogie a amené vers 1950 à forger le mot distributivité sur l'adjectif *ditributif*, lui-même utilisé pour qualifier les lois de composition internes ayant cette propriété.

Exemple 2. *Calculer* $\mathrm{S} = \sum_{k=0}^{n} 3^{2k}(5^k - 3^k)$.

Solution :

$$\begin{aligned}
\mathrm{S} &= \sum_{k=0}^{n} 3^{2k} \times 5^k - 3^{2k} \times 3^k \\
&= \sum_{k=0}^{n} 9^k \times 5^k - 3^{3k} \\
&= \sum_{k=0}^{n} 45^k - 27^k \\
&= \sum_{k=0}^{n} 45^k - \sum_{k=0}^{n} 27^k \\
&= \frac{1-45^{n+1}}{1-45} - \frac{1-27^{n+1}}{1-27} \\
&= \frac{45^{n+1}-1}{44} - \frac{27^{n+1}-1}{26}
\end{aligned}$$

‘

b. Relation de Chasles

Si $a \leqslant b < c$ sont des entiers,

$$\sum_{k=a}^{b} u_k + \sum_{k=b+1}^{c} u_k = \sum_{k=a}^{c} u_k.$$

Exemple 3. *Calculer* $\mathrm{S} = \sum_{k=0}^{2n} |n-k|$.

Solution :

$$\begin{aligned}
\mathrm{S} &= \sum_{k=0}^{2n} |n-k| \\
&= \sum_{k=0}^{n} |n-k| + \sum_{k=n+1}^{2n} |n-k| \\
&= \sum_{k=0}^{n} (n-k) + \sum_{k=n+1}^{2n} -(n-k) \\
&= \sum_{k=0}^{n} n - \sum_{k=0}^{n} k - \sum_{k=n+1}^{2n} n + \sum_{k=n+1}^{2n} k \\
&= \sum_{k=0}^{n} n - \sum_{k=0}^{n} k - \sum_{k=n+1}^{2n} n + \left(\sum_{k=0}^{2n} k - \sum_{k=0}^{n} k \right) \\
&= (n+1)n - \frac{n(n+1)}{2} - n^2 + \left((n+1)n - \frac{n(n+1)}{2} \right) \\
&= n
\end{aligned}$$

c. Changement d'indice

On peut faire un changement de variable dans une somme. **Il faut alors bien penser à changer les bornes de la somme.**

Exemple 4. *Calculer* $\mathrm{S} = \sum_{k=0}^{n} (k+2)^3$.

Solution :
Dans la somme, on pose $j = k+2$. *Lorsque* k *va de* 0 *à* n, j *va de* 2 *à* $n+2$.

$$\begin{aligned}
\mathrm{S}_1 &= \sum_{j=2}^{n+2} j^3 \\
&= \left(\sum_{j=0}^{n+2} j^3 \right) - 0^3 - 1^3 \\
&= \frac{(n+2)^2 \times (n+3)^2}{4} - 1
\end{aligned}$$

Exemple 5. *Calculer* $\mathrm{S} = \sum_{k=0}^{n} k$ *à l'aide du changement d'indice* $j = n-k$.

Solution :
Dans la somme, on pose $j = n-k$. *Lorsque* v *va de* 0 *à* n, j *va de* n *à* 0. *On a* $k = n-j$

$$\begin{aligned}
\mathrm{S}_2 &= \sum_{j=0}^{n} (n-j) \\
&= \sum_{j=0}^{n} n - \sum_{j=0}^{n} j \\
&= n(n+1) - \mathrm{S}_2
\end{aligned}$$

Donc $2\mathrm{S}_2 = n(n+1)$
Donc $\mathrm{S}_2 = \dfrac{n(n+1)}{2}$

d. Téléscopage

$$\sum_{k=a}^{b} (u_{k+1} - u_k) = u_b - u_a.$$

Exemple 6. *Calculer* $S = \sum_{k=1}^{n} \frac{1}{k(k+1)}$.

Solution :
On remarque que pour tout $k \neq 0$,

$$\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}.$$

$$\begin{aligned} S &= \sum_{k=1}^{n} \frac{1}{k(k+1)} \\ &= \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k+1} \\ &= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \ldots + \left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= 1 - \frac{1}{n+1} \end{aligned}$$

3. Formule du binôme de Newton

La formule du binôme de Newton va nécessiter de revenir sur la notion de coefficient binomial et de démontrer la formule dite « formule de Pascal ».
Tirage de k éléments sans remise (où l'ordre de tirage ne compte pas) parmi un ensemble à n éléments.
Soit $E = \{x_1, \ldots, x_n\}$ un ensemble.
Une combinaison de k éléments parmi les n éléments de E est une sous-partie de E de cardinal k.
L'ensemble des partis à k éléments de E se note $\mathscr{P}_k(E)$. On note $\text{Card}(\mathscr{P}_k(E)) = \binom{n}{k}$.
On a alors :

$$\binom{n}{k} = \frac{A_k^n}{k!} = \frac{n!}{k!(n-k)!}.$$

Exemple 7.

$$\binom{n}{n} = 1; \qquad \binom{n}{1} = n; \qquad \binom{n}{0} = 1.$$

Proposition A.4

Pour tout $n \in \mathbb{N}^*$ et $0 \leqslant k \leqslant n$: $\binom{n}{n-k} = \binom{n}{k}$.

Démonstration.

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

‘ □

Proposition A.5 – formule de Pascal

Pour tout $n \in \mathbb{N}^*$ et $0 \leqslant k \leqslant n$:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Démonstration.
Soit E un ensemble à $n+1$ éléments. On considère un élément fixé que l'on note x_1.
Il y a $\binom{n+1}{k+1}$ sous-ensembles de E ayant $k+1$ éléments.
On va calculer ce nombre de sous-ensembles d'une autre façon afin d'établir la formule annoncée.
Pour choisir un sous ensemble de E ayant $k+1$ éléments, on peut commencer par choisir si x_1 appartient à ce sous ensemble.
Si x_1 appartient au sous-ensemble, il reste alors à choisir k éléments parmi les n restants. Il y a $\binom{n}{k}$ possibilités.

Si x_1 n'appartient pas au sous-ensemble, il reste à choisir $k+1$ éléments parmi les n restants. Il y a $\binom{n}{k+1}$ possibilités.

Au total, le nombre de sous-ensembles possibles est $\binom{n}{k}+\binom{n}{k+1}$, d'où le résultat. □

Remarque. *La formule de Pascal est une relation de récurrence. Elle nécessite de calculer tous les coefficients binomiaux précédents mais permet d'éviter le calcul des factorielles. Elle permet de construire le tableau suivant appelé* ***triangle de Pascal****.*
Chaque coefficient s'obtient en ajoutant le coefficient au dessus de lui et celui à gauche de ce dernier.

n \ k	0	1	2	3	4	5	…
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	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

D'après le tableau, on sait par exemple que $\binom{4}{2}=6$.

Proposition A.6 – Binôme de Newton

Pour tout $n\in\mathbb{N}^*$, pour tous $a,b\in\mathbb{C}$:

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

Démonstration.

On montre par récurrence que la propriété $\mathscr{P}(n)$: « Pour tous $a,b\in\mathbb{C}$, $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ » est vraie pour tout $n\in\mathbb{N}^*$.

Initialisation : Pour $n=1$,
$(a+b)^1=a+b$ et $\sum_{k=0}^{1}\binom{1}{k}a^k b^{n-k}=\binom{1}{0}a^0b^1+\binom{1}{1}a^1b^0=a+b.$
Ainsi, $\mathscr{P}(1)$ est vraie.

Hérédité : Supposons que $\mathscr{P}(n)$ est vraie pour un certain $n\in\mathbb{N}^*$.

Montrons qu'alors $\mathscr{P}(n+1)$ est vraie, c'est-à-dire que $(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$. On a :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b) \times \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \text{ (par hypothèse de récurrence)} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&\quad \text{On pose } j = k+1 \text{ dans la première somme. Quand } k \text{ va de 0 à } n,\ j \text{ va de 1 à } n+1 \text{ et } k = j-1. \\
&= \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n-(j-1)} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \left(\sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n-k+1} \right) + a^{n+1} + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \right) + b^{n+1} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} \text{ (d'après la formule de Pascal)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}$$

Donc $\mathscr{P}(n+1)$ est vraie. □

Étymologie – Binôme

On trouve déjà le terme *binomium* dans la traduction latine d'un texte de mathématiques par Gérard de Crémone au XII^e siècle. Il désigne une quantité algébrique à deux termes.
Cependant, l'étymologie de ce mot est contestée. La particule *bi-* marque la duplication. Certains font dériver la fin du mot grec *nomos* qui signifie *part* ou *partie*. En Grèce actuelle, c'est toujours le nom de l'équivalent de nos départements. D'autres penchent pour le mot grec *onoma*, nom que l'on trouve dans le mot français *onomatopée*. Plus simplement, la terminaison de binôme proviendrait du latin *nomen, nom, dénomination* de même racine indo-européenne que *onoma*. Quelle que soit la réelle étymologie, l'accent circonflexe sur le o ne se justifie pas car il s'utilise pour transcrire la lettre grecque oméga.
Binôme apparaît dans notre langue vers 1550 suivi bientôt par d'autres dérivées en *-nôme*. Cependant, contrairement à ceux-ci, binôme se spécialise pour désigner avant tous les coefficients du binôme de Newton $(a+b)^n$: il y a deux parties a et b. Il s'oppose en cela à *multinôme* de création tardive et non à *polynôme*. L'adjectif *binomial* s'utilise pour désigner les coefficients du binôme et par extension la loi de probabilités qui les utilise.

4. Exercices : calculs de sommes simples

Exercice 1. *Calculer* $\sum_{k=0}^{n} \frac{3k(k^2-5k)}{2}$

Exercice 2. *Calculer* $\sum_{k=0}^{n} 2^k + 3k^2 - 2$.

Exercice 3. *Calculer* $\sum_{k=1}^{n} 2^{2k+1}(1-3^k)$

Exercice 4. *Calculer* $\sum_{k=1}^{n} (-1)^k$

Exercice 5. *Calculer* $\sum_{k=1}^{n} \frac{1}{\sqrt{k+1}-\sqrt{k}}$.

Exercice 6. *Calculer* $\sum_{k=2}^{n} \frac{k^3-1}{k-1}$.

Exercice 7. *Calculer* $\sum_{k=0}^{n} \binom{n}{k}$

Exercice 8. *Montrer que pour tout* $n \in \mathbb{N}^*$, $\sum_{k=0}^{n} k! \leqslant (n+1)!$.

Exercice 9. *Calculer* $\sum_{k=0}^{n} \frac{1}{(k+1)(k+3)}$.

Exercice 10. *Calculer* $\sum_{k=0}^{n} k2^k$.

Exercice 11. *Soit* $n \geqslant j \geqslant 0$. *Montrer que* $\sum_{i=j}^{n} \binom{i}{j} = \binom{n+1}{j+1}$.

Exercice 12. *Calculer* $\sum_{k=0}^{n} (-1)^k \binom{n}{k}$

Exercice 13. *Calculer* $\sum_{k=0}^{n} k \binom{n}{k}$

Exercice 14. *Calculer* $\sum_{k=0}^{n} \frac{1}{k+1} \binom{n}{k}$

Exercice 15. *Calculer* $\sum_{k=0}^{n} \binom{n}{k}$

Exercice 16. *Calculer* $\sum_{k=0}^{n} \binom{n}{k} \cos(x)$

Exercice 17. *Montrer que* $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

Exercice 18. *Calculer* $\sum_{k=1}^{n} (-1)^k k$

Exercice 19. *Déterminer un polynôme* P *de degré* 2 *tel que pour tout entier* k, $\mathrm{P}(k+1) - \mathrm{P}(k) = k$. *En déduire alors* $\sum_{k=0}^{n} k$ *en utilisant un téléscopage.*

Utiliser cette méthode pour trouver calculer $\sum_{k=0}^{n} k^4$

II. Sommes doubles

1. Somme sur un rectangle

Dans une somme $\mathrm{S} = \sum_{i=1}^{n} x_i$, chaque élément x_i peut être défini lui-même par une somme. On parle dans ce cas de somme double. Naturellement, on utilisera un indice différent dans les deux sommes.

Exemple 8. *Calculer* $\sum_{i=1}^{3}\left(\sum_{j=1}^{5} ij\right)$.

Solution :

$$\begin{aligned}\sum_{i=1}^{3}\left(\sum_{j=1}^{5} ij\right) &= \sum_{i=1}^{3}(1i+2i+3i+4i+5i)\\ &= (1\times1+2\times1+3\times1+4\times1+5\times1)+(1\times2+2\times2+3\times2+4\times2+5\times2)+(1\times3+2\times3+3\times3+4\times3+5\times3)\\ &= 90\end{aligned}$$

Lorsque l'on calcule une somme double de la forme $\sum_{i=1}^{n}\left(\sum_{j=1}^{m} x_{i,j}\right)$, les deux sommes peuvent se permuter et ne change pas la somme calculée. On a

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} x_{i,j}\right)=\sum_{j=1}^{m}\left(\sum_{i=1}^{n} x_{i,j}\right)$$

Cela s'explique par le fait que, lorsque i va de 1 à n et que j va de 1 à m, l'ensemble des couples (i,j) forment un rectangle de taille $n\times m$.
On retiendra donc que l'ordre n'importe pas. De plus, les parenthèses entre les deux sommes seront toujours implicites et il n'est donc pas nécessaire de les écrire.

Exemple 9. *Calculer* $\mathrm{S}=\sum_{j=0}^{n}\sum_{i=0}^{n} i2^j$

Solution :

$$\begin{aligned}\mathrm{S} &= \sum_{j=0}^{n}\sum_{i=0}^{n} i2^j\\ &= \sum_{j=0}^{n} i\sum_{i=0}^{n} 2^j \qquad \textit{(par distributivité)}\\ &= \sum_{j=0}^{n} i\times\frac{1-2^{n+1}}{1-2}\\ &= (2^{n+1}-1)\times\sum_{j=0}^{n} i \qquad \textit{(par distributivité)}\\ &= \frac{(2^{n+1}-1)n(n+1)}{2}\end{aligned}$$

Exemple 10. *Calculer* $\mathrm{S}=\sum_{j=1}^{n}\sum_{i=1}^{m}\ln(i)\ln(j)$.

Solution :

$$\begin{aligned}\mathrm{S} &= \sum_{j=1}^{n}\sum_{i=1}^{m}\ln(i)\ln(j)\\ &= \sum_{j=1}^{n}\ln(j)\sum_{i=1}^{m}\ln(i)\\ &= \sum_{j=1}^{n}\ln(j)\times ln(m!)\\ &= \ln(m!)\times\sum_{j=1}^{n}\ln(j) \qquad \textit{(par distributivité)}\\ &= \ln(m!)\times\ln(n!)\end{aligned}$$

2. Somme sur un triangle

Dans certains cas, dans la somme $\mathrm{S}=\sum_{i=1}^{n} x_i$, le terme x_i est défini lui-même par une somme indexée par un entier j qui va de 1 à i.

Exemple 11. *Calculer* $\mathrm{S} = \sum_{i=1}^{n} \sum_{j=1}^{i} i$.

Solution :

$$\begin{aligned}
\mathrm{S} &= \sum_{i=1}^{n} \sum_{j=1}^{i} i \\
&= \sum_{i=1}^{n} i \sum_{j=1}^{i} 1 \qquad \textit{(par distributivité)} \\
&= \sum_{i=1}^{n} i \times i \\
&= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

Dans le cas d'une telle somme, permuter les sommes sans rien changer n'aurait alors aucun sens. On peut toutefois les permuter en représentant l'ensemble des couples (i, j) considérés (l'ensemble de ces couples forment un triangle).

Exemple 12. *Calculer* $\mathrm{S} = \sum_{i=1}^{n} \sum_{j=i}^{n} ij$.

Solution :

$$\begin{aligned}
\mathrm{S} &= \sum_{i=1}^{n} \sum_{j=i}^{n} ij \\
&= \sum_{j=1}^{n} \sum_{i=1}^{j} ij \\
&= \sum_{j=1}^{n} j \sum_{i=1}^{j} j \\
&= \sum_{j=1}^{n} j \times \frac{j(j+1)}{2} \\
&= \frac{1}{2}\left(\sum_{j=1}^{n} j^3 + \sum_{j=1}^{n} j^2 \right) \\
&= \frac{n(n+1)(3n^2+7n+2)}{12}
\end{aligned}$$

Exemple 13. *Calculer* $\mathrm{S} = \sum_{i=1}^{n} \sum_{j=1}^{n} \min(i, j)$.

Solution : Pour i fixé entre 1 *et n, on note* $\mathrm{S}_i = \sum_{j=1}^{n} \min(i, j)$.
Pour tout $1 \leqslant i \leqslant n$,

$$\begin{aligned}
\mathrm{S}_i &= \sum_{j=1}^{i} j + \sum_{j=i+1}^{n} i \\
&= \frac{i(i+1)}{2} + (n-i)i \\
&= \left(n + \frac{1}{2}\right) i - \frac{i^2}{2}
\end{aligned}$$

On peut maintenant calculer S.

$$\begin{aligned}
\mathrm{S} &= \sum_{i=1}^{n} \mathrm{S}_i \\
&= \sum_{i=1}^{n} \left(n + \frac{1}{2}\right) i - \frac{i^2}{2} \\
&= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

Exemple 14. *Calculer* $\mathrm{S} = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j}$.

Solution :

$$\begin{aligned}
\mathrm{S} &= \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} \\
&= \sum_{j=0}^{n} \sum_{i=j}^{n} \binom{i}{j} \\
&= \sum_{j=0}^{n} \binom{n+1}{j+1} \qquad (*) \\
&= \sum_{j=1}^{n+1} \binom{n+1}{j} \\
&= 2^{n+1} - 1
\end{aligned}$$

L'égalité $(*)$ *provient en fait d'une égalité générale qui fait l'objet de l'exemple 11.*

3. Exercices : calculs de sommes doubles

Exercice 20. *Calculer* $\sum_{i=1}^{n} \sum_{j=1}^{n} i^2$

Exercice 21. *Calculer* $\sum_{i=0}^{n} \sum_{j=0}^{i} 2$.

Exercice 22. *Calculer* $\sum_{k=1}^{n} \sum_{i=1}^{k} (k^2 - i^2)$

Exercice 23. *Calculer* $\sum_{k=1}^{n} \sum_{j=1}^{k} \frac{j^2}{k}$

Exercice 24. *Calculer* $\sum_{k=1}^{n} \sum_{j=k}^{n} \frac{k}{j}$.

Exercice 25. *Calculer* $\sum_{i=1}^{n} \sum_{j=1}^{n} |j - i|$

Chapitre B

Complément d'arithmétique et de théorie des groupes

Ce chapitre présente un résultat classique d'arithmétique le petit théorème de Fermat. La deuxième partie aborde la question des sous groupes, en partant de la définition et en montrant une propriété importante des sous-groupes d'un groupe fini : le théorème de Lagrange. Si ces deux parties semblent *a priori* bien différentes, on verra pourtant que le petit théorème de Fermat est un cas particulier du théorème de Lagrange. La troisième partie présente enfin la notion de morphismes de groupes, centrale dans la théorie des groupes.

I. Petit théorème de Fermat

Proposition B.1 – Lemme

Si p est un nombre premier et k un entier tel que $1 \leqslant k \leqslant p-1$, alors p divise $\binom{p}{k}$.

Démonstration. Soit p un nombre premier et k un entier tel que $1 \leqslant k \leqslant p-1$. On a $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$.

Par conséquent, $k!\binom{p}{k} = \dfrac{p!}{(p-k)!}$.

Comme $k \geqslant 1$, on voit que p divise $\dfrac{p!}{(p-k)!}$.

Cela signifie que p divise $k!\binom{p}{k}$.

Or, comme $k \leqslant p-1$, $k!$ et p sont premiers entre eux.

D'après le théorème de Gauss, on en déduit donc que p divise $\binom{p}{k}$. □

Proposition B.2

Si p est un nombre premier alors pour tout entier a, $a^p \equiv a\,[p]$.

Démonstration. Soit p un nombre premier.
Montrons par récurrence que la propriété $\mathscr{P}(a)$:« $a^p \equiv a\,[p]$ » est vraie pour tout entier $a \geqslant 0$.
Initialisation : Il est clair que $\mathscr{P}(0)$ est vraie.
Hérédité : Supposons que $\mathscr{P}(a)$ soit vraie pour un certain entier $a \geqslant 0$ et montrons qu'alors $\mathscr{P}(a+1)$ est

vraie.
On a :

$$\begin{aligned}(a+1)^p &= \sum_{k=0}^{p}\binom{p}{k}a^k \\ &= 1+\left(\sum_{k=1}^{p-1}\binom{p}{k}a^k\right)+a^p \\ &\equiv 1+a^p\,[p] \quad \left(\text{car pour tout } 1\leqslant k\leqslant p-1,\ p \text{ divise } \binom{p}{k}\right) \\ &\equiv 1+a\,[p] \quad \text{(d'après l'hypothèse } \mathscr{P}(a)\text{)}\end{aligned}$$

Ainsi, on a montré que $(a+1)^p = a+1$ donc $\mathscr{P}(a)+1$ est vraie.

□

Proposition B.3 – Petit théorème de Fermat

Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} \equiv 1\,[p]$.

Remarque. *Dans le cas où a est divisible par p, on a $a^{p-1} \equiv 0\,[p]$.*

Démonstration. Soit p un nombre premier et a un entier non divisible par p.
D'après la propriété précédente, $a^p \equiv a\,[p]$ $\quad(\star)$.
Or, comme p est premier et ne divise pas a, p est donc premier avec a.
Par conséquent, a est inversible modulo p.
En multipliant l'égalité $(\star)$ par l'inverse de a, on obtient $a^{p-1} \equiv 1\,[p]$. □

Exemple 1. *29 est un nombre premier et 250 n'est pas divisible par 29. On a donc* $250^{28} \equiv 1\,[29]$.

Histoire – Grand théorème de Fermat

Le petit théorème de Fermat est à distinguer du grand théorème de Fermat, beaucoup plus difficile à démontrer. Ce théorème indique que l'équation $x^n + y^n = z^n$ (où n est un entier supérieur ou égal à 3) admet aucune solution entière et non nulle. Dans un ouvrage publié au XVII^{e} siècle, **Pierre de Fermat** avait énoncé ce résultat en ajoutant : « j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir ». Il s'était vraisemblablement trompé et de nombreux mathématiciens ont cherché à démontré ce résultat depuis. En particulier, au XIX^{e} siècle, **Sophie Germain (1776-1831)** a démontré le théorème pour une certaine classe d'exposants (les nombres premiers dits de Sophie Germain). Finalement, ce n'est qu'en 1994, plus de 350 ans après que Fermat ait énoncé le théorème, que le britannique **Andrew Wiles** parvient à une démonstration complète.

II. Sous-groupes

1. Définition et premiers exemples

Définition B.1 – Sous-groupe

Soit (G, .) un groupe. On dit qu'un sous-ensemble H de G est un **sous-groupe** de G lorsque les trois conditions suivantes sont vérifiées :

1. L'ensemble H n'est pas vide.
2. Pour tous $x, y \in \mathrm{H}$, $\quad xy \in \mathrm{H}$
3. Pour tous $x \in \mathrm{H}$, $\quad x^{-1} \in \mathrm{H}$

Pour vérifier qu'un ensemble est un sous-groupe on peut rassembler les conditions 2 et 3 dans une seule condition :

Proposition B.4

Soit (G,.) un groupe et H ⊂ G. H est un sous-groupe de G si, et seulement si, les deux conditions suivantes sont vérifiées :

1. H contient l'élément neutre
2. $\forall x, y \in H,\ xy^{-1} \in H$

Démonstration. Laissée en exercice. □

Exemple 2.

- *Si* G *est un groupe,* $\{e\}$ *et* G *sont des sous-groupes de* G.
- *Dans* $(\mathbb{Z},+)$*, une partie de la forme* $n\mathbb{Z}$ *(avec* $n \in \mathbb{N}$*) est un sous-groupe.*
  En effet,
  — $1 \in n\mathbb{Z}$
  — *Si* $x \in n\mathbb{Z}$ *et* $y \in n\mathbb{Z}$*, alors* $x+y \in n\mathbb{Z}$
  — *Si* $x \in n\mathbb{Z}$*, alors* $-x \in n\mathbb{Z}$.

Remarque. *Les deux derniers points peuvent être remplacés par : pour tout* $x \in n\mathbb{Z}$ *et tout* $y \in n\mathbb{Z}$*,* $x-y \in n\mathbb{Z}$.

Théorème B.5

Soit (G,.) un groupe et H un sous groupe de G. La restriction à H de la loi de composition sur G fait de (H,.) un groupe.

Remarque. *On utilise souvent ce théorème pour montrer qu'un ensemble est un groupe. Par exemple,* $(n\mathbb{Z},+)$ *est un groupe car c'est un sous-groupe de* $(\mathbb{Z},+)$*. Cela évite d'avoir à redémontrer l'associativité notamment.*

Proposition B.6

Soit (G,.) un groupe etH_1 et H_2 deux sous-groupes de G. Alors $H_1 \cap H_2$ est un sous-groupe de G.

Démonstration. Soit G un groupe et H_1 et H_2 deux sous groupes.

- $e \in H_1$ et $e \in H_2$ donc $e \in H_1 \cap H_2$
- Soit $x \in H_1 \cap H_2$ et $y \in H_1 \cap H_2$.
  Alors $xy^{-1} \in H_1$ car H_1 est un sous-groupe de G.
  De même, $xy^{-1} \in H_2$ car H_2 est un sous-groupe de G.
  Ainsi, $xy^{-1} \in H_1 \cap H_2$

Finalement, on a montré que $H_1 \cap H_2$ est un sous-groupe de G. □

Proposition B.7

Soit (G,.) un groupe et $\mathscr{H}$ un ensemble non vide de sous-groupes de G. L'intersection $\bigcap_{H \in \mathscr{H}} H$ est un sous-groupe de G.

Démonstration. Soit G un groupe et $\mathscr{H}$ un ensemble de sous-groupes de G.

- Pour tout $H \in \mathscr{H}$, $e \in H$. Par conséquent, $e \in \bigcap_{H \in \mathscr{H}} H$
- Soit $x \in \bigcap_{H \in \mathscr{H}} H$ et $y \in \bigcap_{H \in \mathscr{H}} H$.
  Alors, pour tout $H \in \mathscr{H}$, $xy^1 \in H$ (car H est un sous-groupe de G)
  Donc $xy^{-1} \in \bigcap_{H \in \mathscr{H}} H$.

Finalement, on a montré que $\bigcap_{H \in \mathscr{H}} H$ est un sous-groupe de G. □

2. Sous groupe engendré

Définition B.2

Soit (G,.) un groupe et A $\subset$ G une partie non vide. On note $\mathscr{H}_A$ l'ensemble des sous groupes de G contenant A ($\mathscr{H}_A \neq \emptyset$ car il contient G). On appelle **sous-groupe engendré** par A le sous groupe $< A >= \bigcap_{H \in H_A} H$.

Remarque.

- $< A >$ *est bien un groupe d'après la proposition B.7. C'est le plus petit sous-groupe de* G *contenant* A *(au sens de l'inclusion).*
  En effet, si L *est un sous-groupe de* G *contenant* A*, alors* $L \in \mathscr{H}_A$*. On a donc* $< A > \subset \bigcap_{H \in H_A} H \subset L$
- *Si* $A = a$ *est un singleton, le sous-groupe engendré par* A *est*

$$< a >= \left\{ a^k \mid k \in \mathbb{Z} \right\}.$$

  Preuve : il est clair que $\{a^k \mid k \in \mathbb{Z}\}$ *est un sous-groupe (il contient e, il est stable par multiplication et par passage à l'inverse).*
  De plus, c'est le plus petit sous-groupe contenant a.
  En effet, si H *est un sous groupe contenant a, il contient toutes les puissances de a et toutes les puissances de* a^{-1} *donc il contient tous les éléments de la forme* a^k *(*$k \in \mathbb{Z}$*).*

- *Si* $G =< \{a\} >$ *est engendré par un singleton (par abus de notation, on note* $G =< a >$*), on dit que* G *est* ***monogène*** *et que a est un générateur de* G*. Si de plus* G *est un groupe fini (de cardinal fini), on dit que* G *est* ***cyclique****.*

Étymologie – Monogène

Ce mot est formé avec le préfixe d'origine grecque *mono-, seul* et par une racine grecque que l'on retrouve dans *engendrer* et dans *gènes*. Le terme *monogène* apparaît en théorie des groupes dans le courant du XX^e siècle.

3. Ordre d'un élément et ordre d'un sous-groupe

Définition B.3

Soit (G,.) un groupe d'élément neutre e et $a \in G$.

- S'il existe $m \in \mathbb{N}^*$ tel que $a^m = e$, on dit que a est d'ordre fini égal à $n = \min\{m \in \mathbb{N}^* \mid a^m = e\}$.
- Sinon, on dit que a est d'ordre infini.

Proposition B.8

Soit (G,.) un groupe d'élément neutre e et $a \in G$ d'ordre fini n. Alors

$$< a >= \left\{ e, a, \ldots, a^{n-1} \right\}.$$

Démonstration. Soit a d'ordre fini n. Alors $a^n = e$.
On a vu que $< a >= \left\{ a^k \mid k \in \mathbb{Z} \right\}$.
Il est clair que $\{e, a, \ldots, a^{n-1}\} \subset \left\{ a^k \mid k \in \mathbb{Z} \right\}$.
Montrons l'inclusion réciproque.
Soit $x \in \left\{ a^k \mid k \in \mathbb{Z} \right\}$. Alors il existe $k \in \mathbb{Z}$ tel que $x = a^k$.
On fait la division euclidienne de k par n.
Il existe q et r entiers tels que $k = nq + r$ avec $0 \leqslant r < n$.
Ainsi, $x = a^{nq+r} = (a^n)^q \, a^r = e a^r = a^r$ car $a^n = e$. □

4. Théorème de Lagrange

Théorème B.9 – Lagrange

Soit G un groupe fini et H un sous groupe de G. Alors Card(H) divise Card(G).
Autrement dit, l'ordre de H divise l'ordre de G.

Démonstration. Soit G un groupe fini et soit H un sous-groupe de G. On va construire un algorithme permettant de comprendre le résultat.

- Si H = G, alors Card(H) = Card(G) et le résultat est vérifié.
- Sinon, il existe $a_1 \in G \setminus H$.
  L'ensemble $a_1H = \{a_1 h | h \in H\}$ (attention ce n'est pas nécessairement un groupe) est en bijection avec H.
  En effet, l'application suivante est bijective :

$$\Phi : \begin{cases} H & \longrightarrow aH \\ h & \longmapsto a_1 h \end{cases}$$

  son application réciproque étant simplement

$$\begin{cases} a_1H & \longrightarrow H \\ x & \longmapsto {a_1}^{-1} x \end{cases}$$

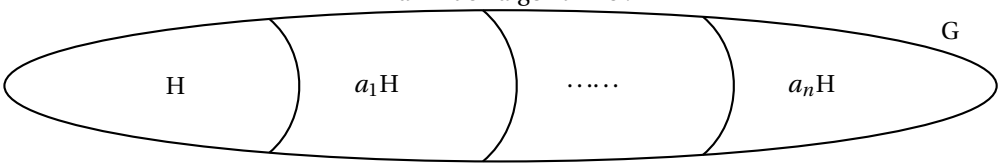
  On en déduit que $Card(a_1H) = Card(H)$.
  Par ailleurs, $a_1H \cap H = \emptyset$. En effet, supposons qu'il existe $x \in a_1H \cap H$.
  Alors il existe $h \in H$ tel que $x = a_1 h$.
  On aurait donc $a_1 = xh^{-1} \in H$ ce qui est absurde par définition de a_1. À ce stade, si $G = H \cup a_1H$, alors $G = Card(a_1H) + Card(H) = 2Card(H)$ donc Card(H) divise Card(G).
- Sinon, il existe $a_2 \in G \setminus (H \cup a_1H)$.
  On aura alors $Card(a_2H) = Card(H)$ (même preuve que précédemment)
  De plus H, a_1H et a_2H seront deux à deux disjoints.
- En itérant, le procédé, on obtient une suite d'éléments $a_1, \ldots, a_n$ telle que $G = H \cup a_1H \cup \cdots \cup a_nH$, telle que $Card(H) = Card(a_1H) = \ldots = Card(a_nH)$ et telle que les ensembles H, a_1H, $\ldots a_nH$ sont deux à deux disjoints. L'algoriothme s'arrête forcément étant donné que G est un ensemble fini.
  Autrement dit, les ensembles H, a_1H, …, a_nH forment une partition de G tous de même cardinal.
  On aura donc

$$Card(G) = Card(H) + Card(a_1H) + \ldots + Card(a_nH) = (n+1)Card(H)$$

  et on a bien montré que Card(H) divise Card(G)

□

À la fin de l'algorithme :



Corollaire B.10

Soit (G, .) un groupe d'ordre fini n et d'élément neutre e. Pour tout $a \in G$, $a^n = e$.

Démonstration. Soit (G, .) un groupe d'ordre fini m et d'élément neutre e. Soit $a \in G$.
On pose $H = < a >$ et on note m l'ordre de a dans G. Alors $H = \{e, a, a^2, \ldots, a^{m-1}\}$ d'après la proposition **??** et $Card(H) = m$.
Ainsi, on a m divise n donc il existe $k \in \mathbb{N}$ tel que $n = mk$.
Finalement,

$$a^n = a^{mk} = (a^m)^k = e^k = e$$

□

Remarque. *Le Corollaire B.10 est une généralisation du petit théorème de Fermat. En effet, si p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est de cardinal $p-1$. Dans le cas d'un entier naturel n (non nécessairement premier), le Corollaire B.10 exprime que pour tout entier a premier avec n, $a^{\phi(n)} = 1\,[n]$.*
$\phi(n)$ est alors le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ et correspond au nombre d'entier compris entre 1 et n et qui sont premiers avec n.

III. Morphismes de groupes

Exemple d'introduction : Avec $G_1 = \mathbb{Z}/4\mathbb{Z}$, $G_2 = \mathbb{U}_4$ et $G_3 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Il est possible de définir un bijection entre G_1 et G_2 qui respecte la structure des opérations des groupes : effectuer les opérations dans le groupe de départ avant de calculer l'image donne le même résultat que de commencer par calculer les images puis d'effectuer les opérations dans le groupe d'arrivée. On dit que G_1 et G_2 sont isomorphes.

En notant $\omega = e^{\frac{2i\pi}{4}}$, on a $\mathbb{U}_4 = \{1, \omega, \omega^2, \omega^3\}$ et la bijection en question est :

$$\Phi : \left\{ \begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{U}_4 \\ 0 & \longmapsto & 1 \\ 1 & \longmapsto & w \\ 2 & \longmapsto & w^2 \\ 3 & \longmapsto & w^3 \end{array} \right.$$

Les structures sont « identiques » : sommer dans $\mathbb{Z}/4\mathbb{Z}$ ou multiplier dans $\mathbb{U}_4$ revient pour ainsi dire au même. On a par exemple

$$w^2 \times w^3 = w^5 = w \qquad \text{et} \qquad 2+3 \equiv 5 \equiv 1 \mathrm{mod}(4)$$

En revanche, définir une telle bijection entre G_1 et G_3 est impossible. En effet, pour tout $x \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $x + x = 0$, ce qui n'est pas le cas dans $\mathbb{Z}/4\mathbb{Z}$.
On dit que G_1 et G_3 ne sont pas isomorphes.

Définition B.4 – Morphisme

Soient $(G_1, \star)$ et (G_2, Δ) deux groupes. Une application $f : G_1 \longrightarrow G_2$ est un **morphisme de groupes** si pour tous $x, y \in G_1$,

$$f(x \star y) = f(x) \Delta f(y).$$

Étymologie – Morphisme

Morphisme et ses dérivés sont apparus avec le développement et l'étude des structures abstraires, tant topologiques qu'algébriques, au début du XX^{e} siècle. *Morphe* en grec désigne la forme. Il semble que *forme*, venu du latin, soit de même racine mais modifié par une métathèse (inversion du f et du m).
Le mot *morphisme* a d'abord été employé avec un préfixe (*homo, iso, auto, homéo*). son emploi isolé date du développement de la théorie des cathégorie vers 1950. Il tend maintenant à supplanter *homomorphisme*.

Dans toute la suite, on considère $(G_1, \star)$ et (G_2, Δ) deux groupes d'élements neutres respectifs e_1 et e_2. De plus, $f : G_1 \longrightarrow G_2$ désigne un morphisme de groupes.

Proposition B.11

- $f(e_1) = e_2$
- $\forall x \in G_1,\ f(x^{-1}) = f(x)^{-1}$.

Démonstration. Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.

- $e_1 \star e_1 = e_1$ donc $f(e_1 \star e_1) = f(e_1)$
  Comme f est un morphisme, on en déduit :

$$f(e_1) \Delta f(e_1) = f(e_1)$$

donc

$$f(e_1)\Delta f(e_1) = f(e_1)\Delta e_2$$

donc, en simplifiant par $f(e_1)$ (proposition 5.2), on a :

$$f(e_1) = e_2$$

- Soit $x \in G_1$. On a $x \star x^{-1} = e_1$
  Donc, en appliquant f :

$$f(x \star x^{-1}) = f(e_1)$$

Comme f est un morphisme,

$$f(x)\Delta f(x^{-1}) = e_2.$$

De même, on prouve que $f(x^{-1})\Delta f(x) = e_2$ et on en déduit donc que l'inverse de $f(x^{-1})$ est $f(x)$.

□

Définition B.5

On appelle **image** du morphisme $f : G_1 \longrightarrow G_2$ l'ensemble $Im(f) = f(G_1)$.

Définition B.6

On appelle **noyau** du morphisme $f : G_1 \longrightarrow G_2$ l'ensemble

$$\mathrm{Ker}(f) = f^{-1}(\{e_2\}) = \{x \in G_1 \,|\, f(x) = e_2\}.$$

Proposition B.12

Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
f est injectif si, et seulement si, $\mathrm{Ker}(f) = \{e_1\}$.

Démonstration. Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
Supposons que f est injective. Un antécédent de e_2 est e_1 d'après la proposition B.11. Comme f est injective, c'est le seul et on a bien $\mathrm{Ker}(f) = \{e_1\}$.

Réciproquement, supposons que $\mathrm{Ker}(f) = \{e_1\}$.
Soit $x, y \in G_1$ tels que $f(x) = f(y)$.
Alors $f(x)\Delta f(y)^{-1} = e_2$
Donc $f(x)\Delta f(y^{-1}) = e_2$ (d'après la proposition B.11)
Donc $f(xy^{-1}) = e_2$ (par définition d'un morphisme)
Donc $xy^{-1} \in \mathrm{Ker}(f)$
Donc $xy^{-1} = e_1$
Donc $x = y$. On a ainsi prouvé que f est injectif. □

Proposition B.13

Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
- Le noyau de f est un sous-groupe de G_1.
- L'image de f est un sous-groupe de G_2.

Démonstration. Laissée en exercice □

Définition B.7 – Isomorphisme

Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes. Si f est bijective, on dit que f est un isomorphisme de groupes et que les groupes G_1 et G_2 sont isomorphes.

Étymologie – Isomorphisme

Le terme *Isomorphisme* existe en chimie dès le début du *xix*^{e} siècle. Son utilisation en algèbre date de la fin de ce même siècle. Henri Poincaré l'introduit en topologie en 1905.

Théorème B.14

Pour $n \in \mathrm{N}^*$, $(\mathbb{U}_n, \times)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Démonstration. On pose $\omega = e^{\frac{2i\pi}{n}}$ Soit

$$\Phi : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ \overline{k} & \longmapsto & w^k \end{array} \right.$$

Φ est bien définie car si $k = k' \bmod(n)$, alors $w^k = w^{k'}$. Montrons que Φ est un morphisme :
Soient $\overline{k_1}, \overline{k_2} \in \mathbb{Z}/n\mathbb{Z}$.

$$\Phi(\overline{k_1} + \overline{k_2}) = \Phi(\overline{k_1 + k_2}) = w^{k_1+k_2} = w^{k_1} \times w^{k_2} = \Phi(\overline{k_1}) \times \Phi(\overline{k_2}).$$

De plus, Φ est injective car $\ker(\Phi) = \{\overline{0}\}$. En effet, soit $\overline{k} \in \ker(\Phi)$.
On a $\Phi(\overline{k}) = 1$
Donc $w^k = 1$
Donc $e^{\frac{2ki\pi}{n}} = 1$ Donc n divise k
Donc $\overline{k} = \overline{0} \bmod(n)$. On en déduit ainsi que $\ker(\Phi) = \{\overline{0}\}$.

Enfin, comme Φ est injective et que $\mathrm{Card}(\mathbb{Z}/n\mathbb{Z}) = \mathrm{Card}(\mathbb{U}_n)$, on en déduit que Φ est bijective.
Finalement, Φ est bien un isomorphisme.

□