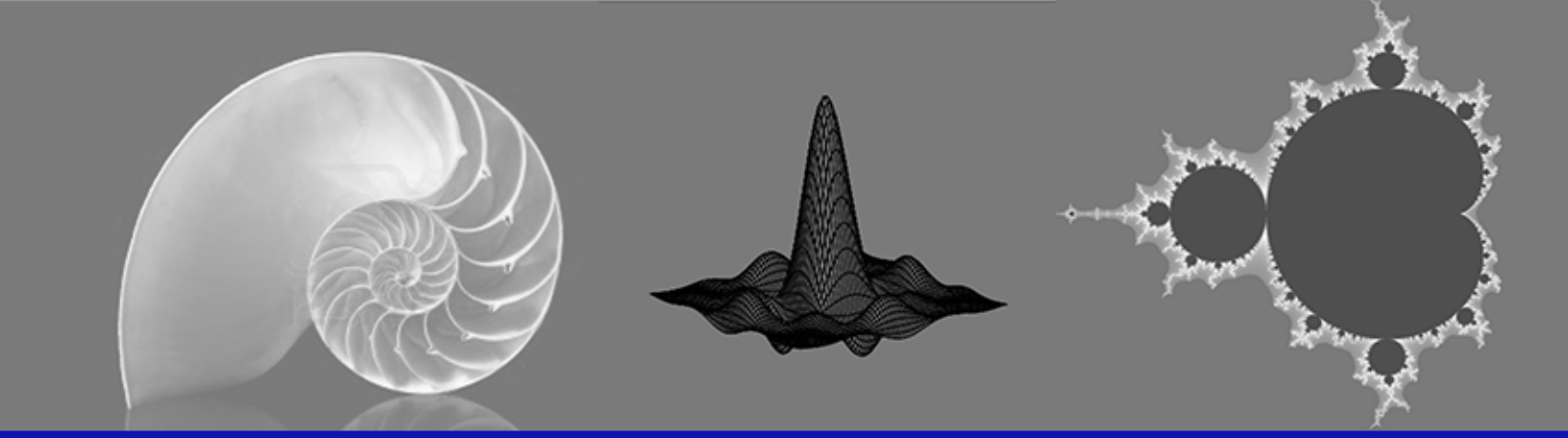


Mathématiques discrètes

Nicolas Bouffard

Automne 2019

Université de Saint-Boniface
Une éducation supérieure depuis 1818

Dernière mise à jour:
10 août 2019 à 10:10

Table des matières

1 La logique mathématiques **5**
- 1.1 Le calcul des propositions . . . 5
- 1.2 Équivalence des propositions . . . 7
- 1.3 Le calcul des prédicats . . . 10
- 1.4 Les règles d'inférence . . . 11
- 1.5 Les démonstrations . . . 14

2 La théorie des ensembles **19**
- 2.1 Introduction . . . 19
- 2.2 Sous-ensemble et égalité . . . 20
- 2.3 Opérations sur les ensembles . . . 21
- 2.4 Démonstrations en théorie des ensembles . . . 22
- 2.5 Les paradoxes . . . 25

3 Les fonctions et les relations **27**
- 3.1 Les relations . . . 27
- 3.2 Les relations d'ordre . . . 31
- 3.3 Les relations d'équivalence . . . 31
- 3.4 Les fonctions . . . 32
- 3.5 La composition des fonctions . . . 34
- 3.6 Les fonctions injectives . . . 35
- 3.7 Les fonctions surjectives . . . 36
- 3.8 Les fonctions bijectives . . . 38
- 3.9 L'inverse d'une fonction . . . 40

4 L'arithmétique **41**
- 4.1 La divisibilité . . . 41
- 4.2 La division euclidienne . . . 42
- 4.3 Le plus grand commun diviseur . . . 43
- 4.4 Le plus petit commun multiple . . . 47
- 4.5 Les nombres premiers . . . 49
- 4.6 La crible d'Ératosthène . . . 51

5 Les nombres modulos **53**
- 5.1 Introduction aux nombres modulos . . . 53
- 5.2 Derniers chiffres d'un expression . . . 55
- 5.3 Les critères de divisibilités . . . 57
- 5.4 Les théorèmes de Fermat, Euler et Wilson . . . 59
- 5.5 L'équation $ax = b$ en modulo . . . 61
- 5.6 La cryptographie RSA . . . 64

6 Quelques outils essentiels **69**
6.1 La notation sigma . . . 69
6.2 Les sommes arithmétiques et géométriques . . . 70
6.3 L'induction . . . 72
6.4 Le théorème du binôme . . . 76
6.5 Les nids de pigeons . . . 78

7 La combinatoire **81**
7.1 Introduction et méthodes élémentaires . . . 81
7.2 Principe du produit, de la somme et d'inclusion-d'exclusion . . . 82
7.3 Combinaison, arrangement et permutation . . . 84
7.4 Permutation d'objet indistingable . . . 86
7.5 Les relations de récurrence . . . 86
7.6 Les fonctions génératrices . . . 88

8 La théorie des graphes **93**
8.1 Les graphes et les arbres . . . 93
8.2 Les graphes biparties et le couplage . . . 96
8.3 Les graphes eulériens / hamiltoniens et la connexité . . . 99
8.4 Les graphes planaires . . . 101
8.5 Le problème du plus court trajet . . . 104
8.6 Les problèmes de coloriage . . . 106

Bibliographie **107**

Index **109**

Chapitre 1

La logique mathématiques

1.1 Le calcul des propositions

La logique est la science du raisonnement, un sujet à cheval entre les mathématiques et la philosophie. Il s'agit d'un language qui est à la base de toutes les mathématiques et sert de fondement aux mathématiques. Ses applications sont très nombreuses, entre autre dans des domaines tels que l'informatique et l'électronique. Elle est omniprésente dans tous les domaines des mathématiques.

Dans cette section, nous allons commencer par définir le concept de proposition logique, et puis nous allons voir les différentes opérations permettant de composer entre eux les propositions (les connecteurs logiques).

Definition 1.1.1. Une **proposition logique** est un énoncé qui est soit vrai ou faux, mais pas les deux en même temps.

Il existe de très nombreux exemples de proposition logique, que ce soit en mathématiques ou dans d'autre discipline. En voici quelques exemples.

Exemple 1.1.1. Les énoncés suivants sont des propositions logiques :

1. La pomme est rouge
2. Toronto est la capitale du Canada
3. $2 + 4 = 6$
4. Tous les entiers sont pair

La première proposition suppose que nous pouvons voir la pomme, et donc déterminer si l'énoncé est vrai ou faux. La proposition 3 est vraie, alors que les propositions 2 et 4 sont fausses.

Une proposition logique peut prendre la forme d'une simple phrase ou d'un énoncé mathématique. Ceci ne change rien au fait qu'il s'agit d'une proposition logique. Remarquez cependant qu'un énoncé de la forme :

$$2 + x = 5$$

ne peut pas être qualifié de proposition logique, car il n'est pas possible de déterminé s'il est vrai ou faux sans connaitre la valeur de x. Nous allons un peu plus loin appeler un tel énoncé un prédicat. Par contre, si on affirme que $x = 3$, alors l'énoncé $2 + x = 5$ devient alors une proposition logique (qui dans ce cas est vraie).

Nous allons maintenant regarder les différentes opérations sur les propositions logiques, c'est ce que nous appellons des connecteurs logiques. C'est ce qui va nous permettre de donner une définition formelle à des termes tel que "et", "ou", et "implique". Un connecteur logique sert à modifier la valeur d'une proposition logique ou d'en combiner plusieurs ensembles. Nous allons définir ces connecteurs à l'aide de tables de vérité. Une table de vérité est un tableau indiquant les différentes valeurs, un peu comme une table de valeur lorsque l'on étudie les fonctions. Par contre, comme une propositions logiques ne peut prendre que les valeurs vraie ou fausse, toute les possibilités sont représenter dans une table de valeurs.

Le premier connecteur logique est la négation et contrairement aux autres connecteurs logiques qui suivrons, la négation ne prend qu'une proposition logique comme entré. La négation représente la notion de "n'est pas" que l'on retrouve en français. Par exemple, la négation de la proposition logique "La pomme est rouge" serait donné par "La pomme n'est pas rouge". On dénote habituellement la négation par le symbol $\neg$ ou $\sim$. Dans le cours, seul le premier des deux symboles sera utilisé. Voici la table de vérité représentant la négation.

TABLE 1.1 – Table de vérité pour la négation

p	$\neg p$
V	F
F	V

Vient ensuite des connecteurs binaires, c'est à dire des connecteurs qui prennent deux valeurs comme entrées. Il en existe plusieurs. Parmi les plus important on notera entre autre :

1. La **disjonction** : On la représente habituellement par le symbole $\vee$. Elle représente la notion de "ou" que l'on retrouve en français. La disjonction est vraie, si l'une ou l'autre des propositions logiques est vraie et est fausse autrement. Ici il faut faire attention, car en français le "ou" peut avoir deux significations. Le "ou inclusif" ou le "ou exclusif". La disjonction fait référence au "ou inclusif", c'est à dire que si les deux propositions logiques sont vraie en même temps, alors la disjonction est vraie.
2. La **conjonction** : On la représente habituellement par le symbole $\wedge$. Elle représente la notion de "et" que l'on retrouve en français. La conjonction est vraie lorsque les deux propositions logiques sont vraie en même temps. Elle est fausse autrement.
3. L'**implication** : On la représente habituellement par le symbole $\rightarrow$. Elle représente la notion de "alors" que l'on retrouve en français. La proposition $p \rightarrow q$ est fausse si p est vrai et q est fausse, et est vraie autrement. Remarquer qu'il arrive occasionnelement qu'on écrive $q \leftarrow p$ pour représenter la même chose que $p \rightarrow q$.
4. L'**équivalence** : On la représente habituellement par le symbole $\leftrightarrow$. Elle représente la notion de si et seulement si, qui n'apparait pas nécessairement très souvent dans le language courant, mais qui est très commun en mathématiques. L'équivalence $p \leftrightarrow q$ est vrai si p et q ont la même valeur, et est fausse autrement.

Voici une table de vérité représentant les différentes valeurs des connecteurs logiques binaires :

TABLE 1.2 – Table de vérité pour les connecteurs binaires

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

Comme pour les opérations sur les nombres réels, il existe une **prioritée des opérations** avec les connecteurs logiques. L'ordre est le suivant :

1. On commence par évaluer les expressions à l'intérieur des parenthèses.
2. On évalue les négations ($\neg$).
3. On évalue les connecteurs de conjonction ($\wedge$) et de disjonction ($\vee$) dans l'ordre qu'ils apparaissent.
4. On évalue les connecteurs d'implication ($\rightarrow$) et d'équivalence ($\leftrightarrow$) dans l'ordre qu'ils apparaissent.

Exemple 1.1.2. On veut construire une table de vérités représentant l'expression $(p \to q) \wedge (p \to r)$. On a donc :

p	q	r	$p \to q$	$p \to r$	$(p \to q) \wedge (p \to r)$
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	F	V	F
V	F	F	F	F	F
F	V	V	V	V	V
F	V	F	V	V	V
F	F	V	V	V	V
F	F	F	V	V	V

Les trois premières colonnes représentes toutes les différentes combinaisons de valeurs que peuvent prendre les propositions p, q et r. Par la suite, on complète les autres colonnes. Notez que techniquement les colonnes 4 et 5 ne sont pas essentielles, mais sont utiles pour construire la dernière. il est commun d'inclure dans notre table de vérité une colonne pour chacune des opérations que nous souhaitons évaluer.

1.2 Équivalence des propositions

Considérons la table de vérité de l'expression $(p \vee q) \to (p \wedge q)$. On a donc :

p	q	$p \vee q$	$p \wedge q$	$(p \vee q) \to (p \wedge q)$
V	V	V	V	V
V	F	V	F	F
F	V	V	F	F
F	F	F	F	V

En regardant attentivement, on remarque qu'il s'agit en fait de la même table de vérité que celle de l'équivalence $p \leftrightarrow q$. C'est ce que nous allons appeler deux propositions équivalentes. Dans cette section, nous allons commencer par donner une définition formelle du concept d'équivalence des propositions, et nous allons regarder deux méthodes permettant d'établir que deux propositions sont équivalentes.

Definition 1.2.1. Une **tautologie** est une combinaison de proposition et de connecteur qui nous donne une expression qui est toujours vrai. Au contraire, une **contradiction** est une combinaison de proposition et de connecteur logique qui est toujours fausse.

Definition 1.2.2. Des propositions p et q sont dites équivalente si $p \leftrightarrow q$ est une tautologie. On dénote l'équivalence des propositions p et q par $p \Leftrightarrow q$.

Notez la différence entre le connecteur logique d'équivalence, et l'équivalence de deux propositions. Le connecteur $p \leftrightarrow q$ peut prendre les valeurs vraie ou fausse, alors que l'équivalence $p \Leftrightarrow q$ nous affirme que $p \leftrightarrow q$ est toujours vrai (et donc une tautologie).

Exemple 1.2.1. Voici quelques exemples de tautologie et de contradiction.

1. Si p est une proposition logique, alors $\neg(\neg p) \leftrightarrow p$ est une tautologie. On peut donc écrire $\neg(\neg p) \Leftrightarrow p$.
2. Si p et q sont des propositions logiques, alors $p \vee \neg p$ est une tautologie. On peut donc écrire $p \vee \neg p \Leftrightarrow V$.
3. Si p et q sont des propositions logiques, alors $p \wedge \neg p$ est une contradiction. On peut donc écrire $p \wedge \neg p \Leftrightarrow F$.

Exemple 1.2.2. On veut montrer que si p et q sont des propositions logiques, alors $p \to q \Leftrightarrow \neg q \to \neg p$. Pour ce faire, il s'agit de faire une table de vérité :

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

On remarque donc que les deux dernières colonnes sont identiques, ce qui confirme que $p \to q \Leftrightarrow \neg q \to \neg p$.

Exemple 1.2.3. On veut montrer que si p, q et r sont des proposition logique, alors $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$. Pour ce faire, on fait une table de vérité :

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
V	V	V	V	V	V	V	V
V	V	F	F	V	V	V	V
V	F	V	F	V	V	V	V
V	F	F	F	V	V	V	V
F	V	V	V	V	V	V	V
F	V	F	F	F	V	F	F
F	F	V	F	F	F	V	F
F	F	F	F	F	F	F	F

On remarque donc que les colonnes 5 et 8 sont identiques, ce qui confirme l'équivalence des deux propositions.

Exemple 1.2.4. On appelle "ou exclusif" le connecteur logique $\oplus$ définie par la table de vérité ci-dessous. Ce dernier représente l'idée d'une proposition qui est vrai si la première partie est vrai ou bien la deuxième, mais pas les deux en même temps. Réécrivez l'opération $p \oplus q$ en terme des connecteurs logiques que nous avons définie plus haut.

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

Pour ce faire, remarquons que la table de vérité du ou exclusif ressemble beaucoup à celui de l'équivalence, sauf que les valeurs logiques en sont inversé. On a donc l'équivalence suivante :

$$p \oplus q \Leftrightarrow \neg(p \leftrightarrow q)$$

Les équivalences logiques permettent de simplifier la démonstration de certaine équivalence. Pour le moment, la seule façon que nous avons de démontrer que deux propositions sont équivalentes était de faire une table de vérité, ce qui peut devenir particulièrement long. Par contre, en ayant une banque de proposition que nous savons équivalentes, on peut simplifier certaine expression sans avoir recours aux tables de vérités. Nous allons donc immédiatement donner une liste d'équivalence importante qui vont nous permettre de démontrer l'équivalence de certaine proposition sans avoir recours à nos tables de vérité. Notez cependant que chacune de ces équivalence a été démontré (pas nécessairement dans ce texte) premièrement en utilisant une table de vérité. Comme exercice, vous devriez démontrer toutes les équivalences du tableau qui n'ont pas été fait dans le texte ou en classe.

Équivalences logique

Équivalence	Nom
$p \wedge V \Leftrightarrow p$ $p \vee F \Leftrightarrow p$	Identité
$p \vee V \Leftrightarrow V$ $p \wedge F \Leftrightarrow F$	Domination
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Idempotence
$p \vee \neg p \Leftrightarrow V$ $p \wedge \neg p \Leftrightarrow F$	Loi des négations
$\neg(\neg p) \Leftrightarrow p$	Double négation
$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Commutativité
$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$	Associativité
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributivité
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	Loi de De Morgan
$p \to q \Leftrightarrow \neg p \vee q$ $p \to q \Leftrightarrow \neg q \to \neg p$	Équivalence avec le connecteur d'implication
$p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$ $p \leftrightarrow q \Leftrightarrow \neg p \leftrightarrow \neg q$	Équivalence avec le connecteur d'équivalence

Voici deux exemples permettant d'illustrer l'utilisation des équivalences du tableau précédent pour démontrer l'équivalence de certaine proposition logique.

Exemple 1.2.5. On veut utiliser les équivalences logiques pour démontrer l'équivalence suivante :

$$p \vee (q \wedge \neg p) \Leftrightarrow p \vee q$$

Pour ce faire, on a :

$$\begin{aligned} p \vee (q \wedge \neg p) &\Leftrightarrow (p \vee q) \wedge (p \vee \neg p) \quad \text{Distributivité} \\ &\Leftrightarrow (p \vee q) \wedge V \quad \text{Loi des négations} \\ &\Leftrightarrow p \vee q \quad \text{Identité} \end{aligned}$$

Notez que lorsque l'on fait une telle démonstration, chacune des équivalence doit être justifié.

Exemple 1.2.6. On peut maintenant utiliser les équivalences logiques que nous avons vu pour démontrer l'équivalence suivante :

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg q$$

Pour ce faire, on a :

$$\begin{aligned} \neg(p \vee (\neg p \wedge q)) &\Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)) \quad \text{Loi de De Morgan} \\ &\Leftrightarrow \neg p \wedge (\neg(\neg p) \vee \neg q) \quad \text{Loi de De Morgan} \\ &\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double négation} \\ &\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributivité} \\ &\Leftrightarrow F \vee (\neg p \wedge \neg q) \quad \text{Loi des négations} \\ &\Leftrightarrow \neg p \wedge \neg q \quad \text{Identité} \end{aligned}$$

1.3 Le calcul des prédicats

Dans l'état actuelle, notre étude de la logique mathématique est plutôt restrictive. Rappelons nous que dans les exemples de propositions logiques, nous avions noté qu'une expression de la forme $2 + x = 5$ ne pouvait pas être qualifié de proposition logique, car il est impossible de savoir si elle est vraie ou fausse sans connaitre la valeur du x. Pourtant ce type d'expression est très courant en mathématiques. Il est maintenant temps d'étudier ce type d'expression.

Definition 1.3.1. Un prédicat est un énoncé qui peut être vrai ou faux dépendant de la valeur des variables. C'est à dire qu'un prédicat est une proposition logique pour chacune des valeurs des variables.

Exemple 1.3.1. Si on dénote par $Q(x)$ l'énoncé $x+2<5$, alors $Q(x)$ est un prédicat. De plus, on remarque que $Q(1)$ est vrai, mais que $Q(7)$ est faux.

L'étude des prédicats nous amène à définir trois quantificateurs logiques que l'on retrouve un peu partout en mathématiques et permet de traduire des expressions de la forme pour tout, il existe, et il existe un unique.

Definition 1.3.2. On définit les trois quantificateurs comme suit :

1. On écrit $\forall x, Q(x)$ si le prédicat $Q(x)$ est vrai pour chacune des valeurs de x dans le domaine. Ce quantificateur se traduit par **pour tout** et est équivalent à écrire $Q(x_1) \wedge Q(x_2) \wedge Q(x_3) \wedge ....$
2. On écrit $\exists x, Q(x)$ s'il existe au moins une valeur de x dans le domaine tel que $Q(x)$ est vrai. Ce quantificateur se traduit par **il existe** et est équivalent à écrire $Q_(x_1) \vee Q(x_2) \vee Q(x_3) \vee ....$
3. On écrit $\exists! x, Q(x)$ s'il existe exactement une valeur de x dans le domaine tel que $Q(x)$ est vrai. On le traduit par **il existe un unique**.

Les énoncés $\forall x, P(x)$, $\exists x, P(x)$ et $\exists! x, P(x)$ peuvent donc être vrai ou faux, mais pas les deux en même temps. Il s'agit donc de propositions logiques. Il est donc possible de définir des propositions logiques à partir de prédicat, et en conséquence combiner les différents quantificateurs avec les connecteurs logiques que nous avons vu dans la première section. Notez aussi que chaque quantificateur fait référence à un domaine sur lequel il est définie. Le contexte doit donc permettre d'identifier clairement quel est ce domaine. Le tableau ci-dessous indique dans quel cas ces propositions sont vraies et dans quels cas elles sont fausses.

Énoncé	**Quand est-il vrai ?**	**Quand est-il faux ?**
$\forall x, P(x)$	$P(x)$ est vrai pour tout les x	Il existe un x pour lequel $P(x)$ est faux.
$\exists x, P(x)$	Il existe un x pour lequel $P(x)$ est vrai	$P(x)$ est faux pour tout les x.

En regardant attentivement le tableau, on remarque qu'il y a une forme de symétrie entre les deux quantificateurs, ceci nous amène donc aux lois de De Morgan pour les quantificateurs. Ceci est énoncé dans le théorème ci-dessous.

Théorème 1.3.1. **(Lois de De Morgan pour les quantificateurs)** Si $P(x)$ est un prédicat, alors on a les deux équivalences suivantes :

1. $\neg\exists x, P(x) \Leftrightarrow \forall x, \neg P(x)$.
2. $\neg\forall x, P(x) \Leftrightarrow \exists x, \neg P(x)$.

Le language des prédicats nous permet d'énoncé plusieurs théorèmes et axiomes des mathématiques. Voici quelques exemples de théorème que vous connaissez déjà écrit dans le language de la logique mathématiques.

Exemple 1.3.2. Voici la traduction de quelques énoncés en termes de logique mathématique :

1. Tout les nombres réels possède un inverse additif peut s'écrire sous la forme
$$\forall x \exists y (x + y = 0).$$
2. L'addition dans les nombres réels est commutative peut s'écrire sous la forme
$$\forall x \forall y (x + y = y + x).$$

3. Le produit de deux nombres négatif est toujours positif peut s'écrire sous la forme

$$\forall x \forall y((x < 0) \wedge (y < 0) \rightarrow (xy > 0)).$$

La logique mathématique servant de fondement aux mathématiques, il est donc important d'être capable de traduire des expressions écrites en français dans le language de la logique, et vice-versa. Notez cependant qu'il ne faut pas non plus abuser de ce symbolisme. Une sur-utilisation de la logique dans les définitions et démonstrations peut rendre des textes mathématiques complètement illisible. Il est donc considéré une bonne pratique d'agrémenter les textes mathématiques de texte écrit en français pour aider à la compréhension.

1.4 Les règles d'inférence

Les règles d'inférence pour les propositions logiques servent de prototype pour une démonstration mathématique. Il s'agit tout simplement d'une suite de proposition vrai, qui combiné ensemble permettent d'obtenir une conclusion qui sera aussi vrai. En voici un exemple. Il est facile de démontrer que la proposition

$$(p \wedge (p \rightarrow q)) \rightarrow q$$

est une tautologie. Ceci nous amène à la règle d'inférence appelé modus ponen qui peut s'énoncer comme suit :

$$\begin{array}{ll} & p \\ & p \rightarrow q \\ \hline \therefore & q \end{array}$$

Ceci signifie que si p est vrai et $p \rightarrow q$ est vrai, alors q doit être vrai. Le symbol $\therefore$ signifie "alors" et sert à identifier la conclusion. Notez que chacune des propositions peut être vrai soit par des hypothèses fournies dans le problème, ou bien par des règles provenant de l'équivalence des propositions.

Il existe plusieurs règles d'inférences. Les plus communes sont résumé dans le tableau 1.3.

Exemple 1.4.1. Est-ce que l'argument ci-dessous est valide ?

$$\begin{array}{ll} & q \\ & \neg p \rightarrow q \\ \hline \therefore & p \end{array}$$

Pour le savoir, on doit construire une table de vérité pour le proposition logique $(q \wedge (\neg p \rightarrow q)) \rightarrow p$, ce qui nous donne :

p	q	$\neg p$	$\neg p \rightarrow q$	$q \wedge (\neg p \rightarrow q)$	$(q \wedge (\neg p \rightarrow q)) \rightarrow p$
V	V	F	V	V	V
V	F	F	V	F	V
F	V	V	V	V	F
F	F	V	F	F	V

On remarque donc facilement (voir troisième ligne) qu'il ne s'agit pas d'une tautologie. L'argument n'est donc pas valide.

Remarquez que certaines des règles d'inférence peuvent aussi être appliqué aux quantificateurs logiques. Parmi celle-ci, on notera entre autre la règle de simplification qui peut facilement être appliqué dans le cas du quantificateur pour tout ($\forall$). L'exemple ci-dessous montre comment cette idée peut être appliqué.

Exemple 1.4.2. Parmi les argumentations suivantes, lesquelles sont valide ? Parmi celle qui sont valides, identifié quelle règle d'inférence a été utilisé.

1. Si Marc est un médecin et si tous les médecins ont étudié dans une école de médecine, alors Marc a étudié dans une école de médecine.

TABLE 1.3 – Les règles d'inférence

Nom	Règle d'inférence	Tautologie associé
Modus ponens	$\begin{array}{l} p \\ p \to q \\ \hline \therefore \quad q \end{array}$	$(p \wedge (p \to q)) \to q$
Modus tollens	$\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore \quad \neg p \end{array}$	$(\neg q \wedge (p \to q)) \to \neg p$
Syllogisme hypothétique	$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore \quad p \to r \end{array}$	$((p \to q) \wedge (q \to r)) \to (p \to r)$
Syllogisme disjontif	$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore \quad q \end{array}$	$((p \vee q) \wedge (\neg p)) \to q$
Addition	$\begin{array}{l} p \\ \hline \therefore \quad p \vee q \end{array}$	$p \to (p \vee q)$
Simplification	$\begin{array}{l} p \wedge q \\ \hline \therefore \quad p \end{array}$	$(p \wedge q) \to p$
Conjonction	$\begin{array}{l} p \\ q \\ \hline \therefore \quad p \wedge q \end{array}$	$(p \wedge q) \to (p \wedge q)$
Résolution	$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore \quad q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$

2. Si Marc n'est pas médecin et si tous les médecins ont étudié dans une école de médecine, alors Marc n'a pas étudié dans une école de médecine.
3. Si Marc a étudié dans une école de médecine, et si tous les médecins ont étudié dans une école de médecine, alors Marc est médecin.
4. Si Marc n'a pas étudié dans une école de médecine, et si tous les médecins ont étudié dans une école de médecine, alors Marc n'est pas médecin.

Nous allons donc regarder chaque exemple un par un. Dans chacun des cas, nous allons définir les propositions logiques élémentaires suivantes :

— $p(x)$ représente la proposition x est médecin.

— $q(x)$ représente la proposition x a été dans une école de médecine.

On a donc :

1. La proposition Marc est médecin peut s'écrire sous la forme $p(Marc)$, la proposition tous les médecins ont étudié dans une école de médecine peut elle s'écrire sous la forme $\forall x, p(x) \to q(x)$. On obtient donc l'argumentation suivante :

$$\begin{array}{ll} & p(Marc) & \text{Hypothèse du problème} \\ & \forall x, p(x) \to q(x) & \text{Hypothèse du problème} \\ & p(Marc) \to q(Marc) & \text{Règle de simplification appliqué à la 2e ligne} \\ \hline \therefore & q(Marc) & \text{Modus ponens avec les lignes 1 et 3.} \end{array}$$

   La conclusion $q(Marc)$ signifiant que Marc a été dans une école de médecine, on peut donc affirmer que l'argumentation est correcte basé sur les règle d'inférence de simplification et du Modus Ponens.

2. La proposition Marc n'est pas médecin peut s'écrire sous la forme $\neg p(Marc)$, la proposition tous les médecins ont étudié dans une école de médecine peut elle s'écrire sous la forme $\forall x, p(x) \to q(x)$. On obtient donc l'argumentation suivante :

	$\neg p(Marc)$	Hypothèse du problème
	$\forall x, p(x) \to q(x)$	Hypothèse du problème
	$p(Marc) \to q(Marc)$	Règle de simplification appliqué à la 2e ligne
$\therefore$	$\neg q(Marc)$	À vérifier

Faute d'avoir une règle d'inférence nous permettant de vérifier la conclusion, nous allons cette fois construire une table de vérité pour vérifier si la proposition

$$(\neg p(Marc) \wedge (p(Marc) \to q(Marc))) \to \neg q(Marc)$$

est une tautologie. Pour simplifier, nous allons écrire p à la place de $p(Marc)$ et q à la place de $q(Marc)$ dans le tableau ci-dessous. On a donc :

p	q	$\neg p$	$p \to q$	$\neg p \wedge (p \to q)$	$\neg q$	$(\neg p \wedge (p \to q)) \to \neg q$
V	V	F	V	F	F	V
V	F	F	F	F	V	V
F	V	V	V	V	F	F
F	F	V	V	V	V	V

Comme il ne s'agit pas d'une tautologie, la règle d'inférence est fausse. L'argumentation est donc incorrecte.

3. En se basant sur les deux premières partie, l'argumentation peut s'écrire sous la forme suivante :

	$q(Marc)$	Hypothèse du problème
	$\forall x, p(x) \to q(x)$	Hypothèse du problème
	$p(Marc) \to q(Marc)$	Règle de simplification appliqué à la 2e ligne
$\therefore$	$p(Marc)$	À vérifier

Encore une fois, nous allons construire une table de vérité pour vérifier si l'argumentation est correcte. On a donc :

p	q	$p \to q$	$q \wedge (p \to q)$	$(q \wedge (p \to q)) \to p$
V	V	V	V	V
V	F	F	F	V
F	V	V	V	F
F	F	V	F	V

Comme pour l'exemple précédent, il ne s'agit pas d'une tautologie. L'argument est donc incorrecte.

4. En se basant sur les parties précédentes, l'argumentation peut s'écrire sous la forme suivante :

	$\neg q(Marc)$	Hypothèse du problème
	$\forall x, p(x) \to q(x)$	Hypothèse du problème
	$p(Marc) \to q(Marc)$	Règle de simplification appliqué à la 2e ligne
$\therefore$	$\neg p(Marc)$	Modus tollens appliqué aux lignes 1 et 3.

Comme chacune des étapes a pu être justifié à l'aide d'une règle d'inférence, on peut donc affirmer que l'argumentation est correcte.

Exemple 1.4.3. On veut vérifier (ou justifier) à l'aide des règles d'inférence l'argumentation suivante. Jeanne est soit une étudiante en mathématique ou une étudiante en informatique. Tous les étudiants de mathématiques prennent leur cours dans l'édifice A. De plus, tous les étudiants d'informatique prennent leur cours dans l'édifice A. On peut donc conclure que Jeanne prend ses cours dans l'édifice A. Pour justifier l'argumentation, nous allons premièrement identifier les différentes propositions logiques présentent dans le texte. On a donc :

— $p(x)$: x est un étudiant de mathématiques

— $q(x)$: x est un étudiant d'informatique

— $r(x)$: x prend ses cours dans l'édifice A

Maintenant nous allons appliquer les règles d'inférence. On a donc :

	$p(Jeanne) \vee q(Jeanne)$	par hypothèse
	$\forall x, p(x) \to r(x)$	par hypothèse
	$\forall x, q(x) \to r(x)$	par hypothèse
	$p(Jeanne) \to r(Jeanne)$	Règle de simplification appliqué à la 2e ligne
	$q(Jeanne) \to r(Jeanne)$	Règle de simplification appliqué à la 3e ligne
	$(p(Jeanne) \to r(Jeanne)) \wedge (q(Jeanne) \to r(Jeanne))$	Conjonction appliqué aux lignes 4 et 5
	$(p(Jeanne) \vee q(Jeanne)) \to r(Jeanne)$	Équivalence logique de la ligne 6
$\therefore$	$r(Jeanne)$	Modus ponens appliqué aux lignes 1 et 7.

On peut donc affirmer que Jeanne prend ses cours dans l'édifice A.

1.5 Les démonstrations

À la base des mathématiques se trouve la logique mathématiques. La logique est à la fois un language, et un ensemble de règle permettant d'écrire une argumentation correcte. Pour obtenir une théorie mathématiques complètes, il est cependant nécessaire d'aller un peu plus loin. Une théorie mathématiques se fonde sur un ensemble de définitions et d'axiomes, ainsi que l'ensemble de tous les résultats qui leur en découle.

> Un **axiome** est un énoncé que l'on accepte comme étant vrai sans démonstration. Les axiomes servent de point de départ à une théorie mathématiques.

Les différents résultats d'une théorie est ce que l'on peut obtenir à partir des règles d'inférence. Ils portent différent nom selon le contexte : Théorème, lemme, corollaire ou proposition.

1. Un **théorème** est un résultat important et central d'une théorie obtenu à partir des axiomes de la théorie et les règles de l'inférence logique. Dans certain cas, un ou plusieurs lemmes sont utilisé dans la démonstration d'un théorème.
2. Un **lemme** est un résultat intermédiaire utilisé pour démontrer un théorème.
3. Un **corollaire** est un résultat découlant (facilement) d'un théorème.
4. Une **proposition** est un résultat généralement moins important qu'un théorème, mais intéressant par lui même. Généralement il n'y a pas de lemme ou de corollaire associé à une proposition.
5. Une **conjecture** est un résultat que l'on croit vrai, mais qui n'a pas encore été démontré ou réfuté. Notez qu'une conjecture ne fait pas encore partie d'une théorie mathématique étant donné que nous n'avons toujours pas réussi à vérifier s'y elle est correcte.

L'ensemble des règles d'inférence permettant d'obtenir le résultat est ce que l'on appelle une démonstration. Il existe plusieurs approche permettant de construire une démonstration correcte. Dans ce chapitre, nous allons regarder à l'aide d'exemple quelques méthodes parmi les plus importantes. Tous au long du cours, nous aurons l'occasion de voir d'autre approche importante.

Preuves directes

La première méthode de démonstration consiste à faire une **preuve directe**. Une preuve directe est une démonstration qui consiste à démontrer directement un résultat à partir des hypothèses du problème. Le plus souvent, il s'agit d'une application du modus ponens, souvent combiné avec des syllogismes hypothétiques. En voici un exemple.

Exemple 1.5.1. Un nombre impair est un nombre qui peut s'écrire sous la forme $2k+1$ où k est un entier. Si n est un nombre impair, on veut démontrer que n^2 est aussi un nombre impair. Pour ce faire, supposons que n est un nombre impair, alors il existe un entier k tel que $n = 2k+1$. On obtient donc :

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Si on pose $m = 2k^2 + 2k$, alors m est un entier et on a donc $n^2 = 2m + 1$. On peut donc affirmer que n^2 est aussi un nombre impair.

Preuve par contraposé

Bien que la méthode de preuve directe que nous venons de voir soit en théorie la plus simple, dans certain cas la méthode peut être très difficilement applicable. En utilisant les différentes règles d'inférence que nous avons vu, il est cependant facile de développer d'autres méthodes de démonstration. L'une d'entre elle consiste à faire une démonstration par contraposé. Une **preuve par contraposé** est une démonstration qui se base sur l'équivalence logique suivante :

$$(\neg q \to \neg p) \Leftrightarrow (p \to q)$$

Donc plutôt que de démontrer directement qu'une proposition p implique une proposition q, on démontre que la négation de l'énoncé q implique la négation de l'énoncé p. En voici un exemple.

Exemple 1.5.2. On veut démontrer que si p^2 est un nombre pair, alors p doit être pair. Pour ce faire, une preuve directe peut devenir particulièrement compliqué, par contre, la contraposé est relativement simple à démontrer. Supposons que p n'est pas un nombre pair, alors p doit être impair, c'est à dire qu'on peut l'écrire sous la forme $p = 2k + 1$ où k est un entier. On a donc :

$$p^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2m + 1, \quad (m = 2k^2 + 2k)$$

comme m est un entier, on peut donc affirmer que p^2 est impair. Ceci est exactement la contraposé de ce que nous voulions démontrer. On peut donc affirmer que si p^2 est pair, alors p est pair.

Preuve par contradiction

Une autre méthode très souvent rencontré en mathématiques consiste à faire une **démonstration par contradiction**. Il s'agit d'une méthode qui peut être exprimé par l'expression

$$\neg p \to F \Leftrightarrow p.$$

En terme simple, ceci reviens à dire que si on suppose la négation de ce que l'on veut démontrer et on obtient une contradiction, alors la proposition doit être vrai. En voici un exemple.

Exemple 1.5.3. On veut démontrer que $\sqrt{2}$ n'est pas un nombre rationnel. Pour ce faire, nous allons procéder par contradiction. Supposons donc que $\sqrt{2}$ est un nombre rationnel. On peut donc l'écrire sous forme d'une fraction. C'est à dire qu'il existe des entiers m et n tel que $\sqrt{2} = \dfrac{m}{n}$. Maintenant, comme toutes les fractions peuvent être transformer sous forme irréductible, on peut donc supposer que $\dfrac{m}{n}$ est irréductible (C'est à dire que le pgcd de m et n est 1). On obtient donc :

$$\sqrt{2} = \frac{m}{n} \quad \Rightarrow \quad 2 = \frac{m^2}{n^2} \quad \Rightarrow \quad 2n^2 = m^2$$

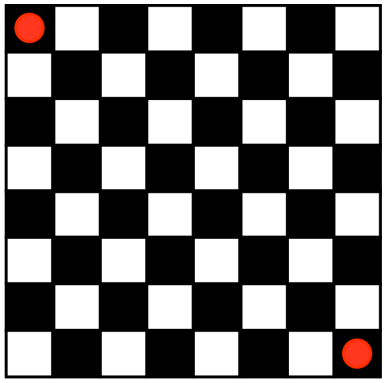
On peut donc déduire que m^2 est pair, c'est à dire que m doit être pair. On peut donc trouver un entier k tel que $m = 2k$. On obtient donc :

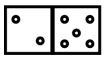
$$2n^2 = m^2 \quad \Rightarrow \quad 2n^2 = (2k)^2 = 4k^2 \quad \Rightarrow \quad n^2 = 2k^2$$

On peut donc déduire que n^2 est pair, et donc que n est pair. Comme m et n sont tous deux pairs, la fraction $\dfrac{m}{n}$ n'est donc pas réduite. On a donc obtenue une contradiction, car $\dfrac{m}{n}$ ne peut pas être à la fois réduite et ne pas être réduite. On peut donc conclure que $\sqrt{2}$ n'est pas un nombre rationnel.

Un autre exemple classique de démonstration par contradiction est le problème de l'échiquier énoncé dans l'exemple suivant.

Exemple 1.5.4. Un échiquier standard est formé de 64 cases organisé en 8 rangés et 8 colonnes. Si on suppose qu'un domino couvre exactement 2 cases (soit à l'horizontale ou à la verticale), et que les deux coins opposés de l'échiquier ont été bloqué par un objet, est-il possible de couvrir entièrement le reste de l'échiquier avec des dominos ? Il s'agit à nouveau d'une démonstration d'existence. On a donc deux options. Pour démontrer que c'est possible, tout ce que nous avons à faire est de trouver un exemple qui fonctionne, si au contraire on veut démontrer que c'est impossible, il faut démontrer qu'aucune configuration fonctionne. En essayant à plusieurs reprises, on remarque facilement que si c'est possible, trouver un exemple n'est absolument pas évident. On va donc essayer de démontrer au contraire que c'est impossible, cette fois en faisant une démonstration par contradiction. Supposons donc qu'il est possible de couvrir entièrement les cases restantes de l'échiquier avec des dominos, comme chaque domino couvre une case blanche et une case noire, il doit donc y avoir autant de case blanche que de case noire. Par contre, en comptant les cases restantes de l'échiquier, on remarque qu'il y a deux cases blanches de plus que de case noire. On a donc obtenu une contradiction. Il est donc impossible de couvrir entièrement les cases restantes de l'échiquier avec des dominos.





Preuve d'existence

Un point important à noter, dans l'exemple précédent est qu'il n'était pas suffisant de donner un exemple qui ne permettait pas de couvrir entièrement l'échiquier. Pour résoudre le problème de l'échiquier à l'aide d'exemple, il aurait fallu étudier tous les exemples de configuration de dominos, et montrer qu'aucune d'entre elles fonctionnent. Considérant le nombre très élevé de configuration possible, cette méthode n'aurait certainement pas été très efficace. Donc bien qu'un exemple n'aurait pas été suffisant pour résoudre le problème de l'échiquier, dans certain cas un exemple aurait bel et bien pu être suffisant. C'est le cas des **problèmes d'existence**. En voici deux exemples.

Exemple 1.5.5. On veut démontrer l'existence d'un entier x tel que $x^2 - 10x < -24$. Pour ce faire, nous allons essayer de procéder de manière constructive, c'est à dire chercher à construire un tel entier. En réécrivant l'équation on obtient :

$$x^2 - 10x + 24 < 0 \quad \Rightarrow \quad (x-4)(x-6) < 0$$

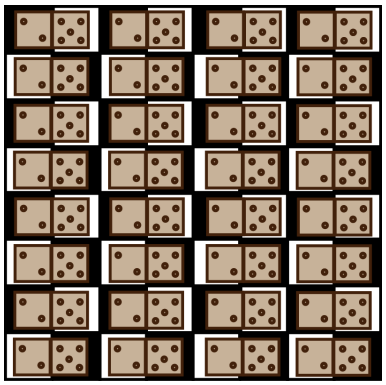
Pour que le produit soit négatif, on doit donc avoir l'un des termes positif et l'autre négatif. Comme $x-6 < x-4$, la seule façon pour que ce soit possible est que $x-6<0$ et $x-4>0$, c'est à dire que $x<6$ et $x>4$. On remarque donc que 5 est un entier satisfaisant c'est deux conditions. On a donc :

$$5^2 - 10(5) + 24 = 25 - 50 + 24 = -1 < 0$$

On a donc trouvé un entier qui satisfait l'inégalité.

Exemple 1.5.6. Un échiquier standard est formé de 64 cases organisé en 8 rangés et 8 colonnes. Si on suppose qu'un domino couvre exactement 2 cases (soit à l'horizontale ou à la verticale), démontrer qu'il est possible de couvrir entièrement l'échiquier avec des dominos. Pour ce faire, comme il s'agit d'une démonstration

d'existence, il suffit de trouver un exemple qui montre que c'est possible de couvrir entièrement l'échiquier. Il y a bien entendu plusieurs options, mais voici un exemple qui fonctionne.



Les deux exemples précédent illustrent une méthode constructive de faire une démonstration d'existence. Dans certain cas, construire un exemple satisfaisant les conditions peut cependant être particulièrement difficile. Dans certain cas, il est cependant possible de démontrer l'existence d'un élément satisfaisant certaine conditions, sans pour autant être capable d'en fournir un exemple. On parle alors de démonstration non-constructive. En voici un exemple.

Exemple 1.5.7. On veut démontrer qu'il existe un des nombres irrationnels x et y tel que x^y est un nombre rationnel. Pour ce faire, nous allons procéder de manière non-constructive. Supposons que $\sqrt{2}^{\sqrt{2}}$ est un nombre rationnel, alors on a trouvé un nombre satisfaisant la propriété. Si on contraire $\sqrt{2}^{\sqrt{2}}$ n'est pas un nombre rationnel, alors $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ est un nombre qui satisfait la propriété. Remarquez que notre démonstration ne nous permet pas de déterminer si le nombre satisfaisant propriété est $\sqrt{2}^{\sqrt{2}}$ ou $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$.

Chapitre 2

La théorie des ensembles

2.1 Introduction

Un ensemble est une collection d'objets. Les ensembles sont présent dans essentiellement toutes les branches des mathématiques, et vous en avez déjà rencontrer plusieurs durant vos études. On dénote habituellement un ensemble à l'aide d'une lettre majuscule, mais ce n'est pas une obligation. Pour dénoter les éléments d'une ensemble, on peut les énumérer en utilisant les accolades. Par exemple, on peut écrire :

$$A = \{1, 3, 8, 17\}$$

$$B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Pour les ensemble contenant seulement quelques éléments, cette notation est particulièrement pratique, par contre si on souhaite dénoter tout les entiers entre 1 et 100, la liste devient particulièrement longue. Dans ce cas, il est commun d'utiliser ... pour indiquer que le pattern continue de la même manière. L'ensemble B ci-dessus peut donc être réécrit sous la forme :

$$B = \{1, 2, 3, ..., 10\}$$

De la même manière les nombres pairs entre 2 et 100 pourront être écrit sous la forme :

$$\{2, 4, 6, 8, 10, ..., 100\}$$

Lorsqu'un ensemble a été définie, un peut alors s'intéressé à savoir si un élément fait parti de l'ensemble ou non. Pour ce faire, on utilise la notation $\in$ qui signifie l'appartenance, et $\notin$ qui signifie n'appartient pas.

Exemple 2.1.1. Voici deux exemples illustrant l'utilisation du symbol d'appartenance.

1. Définissons l'ensemble $A = \{2, 7, 12, 19\}$. Alors on peut écrire $12 \in A$ et $21 \notin A$.
2. Définissons l'ensemble B comme étant l'ensemble de tous les nombres pairs. On a donc $6 \in B$ et $13 \notin B$.

Une notation particulière est utilisé pour certain ensemble qui sont très souvent utilisé en mathématiques. On notera entre autre :

1. $\varnothing$ qui dénote l'ensemble vide, i.e. l'ensemble ne contenant aucun élément.
2. $\mathbb{N}$ l'ensemble des nombres naturels $\mathbb{N} = \{1, 2, 3, 4, ...\}$.
3. $\mathbb{Z}$ l'ensemble des nombres entiers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.
4. $\mathbb{Q}$ l'ensemble des nombres rationnels, c'est à dire l'ensemble de toutes les fractions d'entier.
5. $\mathbb{R}$ l'ensemble des nombres réels, c'est à dire l'ensemble de tous les nombres de la droite.
6. $\mathbb{C}$ l'ensemble des nombres complexes.

Dans bien des cas, un ensemble peut être définie à l'aide d'une certaine propriété. On utilise alors les deux points : ou la barre verticale | les deux signifiant tel que. On pourra par exemple définir l'ensemble des nombres pairs comme étant :

$$\{2x : x \in \mathbb{Z}\} \quad \text{ou} \quad \{2x | x \in \mathbb{Z}\}$$

Ceci peut nous permettre de définir correctement l'ensemble des nombres rationnels et l'ensemble des nombres complexes. Dans les deux cas, la notation ... n'était pas d'une grande utilité. On a donc :

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$$

Notez que nous n'avons pas indiquer ce qu'est exactement l'ensemble des nombres réels. Ce dernier est en fait beaucoup plus difficile que les autres à définir de manière formelle, et dépasse le contenu de notre cours. Sa définition repose sur l'axiome de complétude et est étudier normalement dans les cours d'analyse. Pour nous, il sera suffisant de définir les nombres réels comme étant la droite de nombres.

Definition 2.1.1. Si A est un ensemble, alors on appelle cardinalité de A, dénoté $|A|$, le nombre d'élément que contient l'ensemble A.

Exemple 2.1.2. Si $A = \{1, 4, 8, 13\}$, alors $|A| = 4$.

Il faut cependant noté un problème important. Quelle est la cardinalité des ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$? Dans chaque cas, ces ensembles contiennent un nombre infinie d'élément. Pourtant, l'ensemble $\mathbb{R}$ contient beaucoup plus d'élément que l'ensemble $\mathbb{N}$, il faudra donc plus tard dans le texte trouver une façon de comparer la cardinalité des ensembles contenant un nombre infinie d'élément. Ceci sera fait lorsque nous étudierons les fonctions bijectives.

2.2 Sous-ensemble et égalité

Il est maintenant temps de commencer à comparer deux ensembles donnés. Pour ce faire nous allons commencer par nous intéressé à l'inclusion. Par exemple, tout les nombres naturels sont des nombres entiers, et tous les nombres entiers sont des nombres rationnels.

Definition 2.2.1. Si A et B sont des ensembles, alors on dit que A est inclut dans B et on écrit $A \subseteq B$ si tout les éléments de A sont des éléments de B. De manière formelle, on écrira donc :

$$A \subseteq B \iff \forall x((x \in A) \to (x \in B))$$

Definition 2.2.2. Si A et B sont des ensembles, alors on dit que A est égal à B, et on écrit $A = B$, si A et B contiennent exactement les mêmes éléments. De manière formelle, on écrira

$$A = B \iff (A \subseteq B) \wedge (B \subseteq A)$$

Si A et B ne sont pas égal, on écrira alors $A \neq B$.

L'inclusion comme nous l'avons définie autorise donc deux ensembles à être égal. Pour signifier qu'un ensemble est inclut dans un autre, mais qu'ils ne sont pas égal, on utilisera la notation $\subset$. De manière formelle, on pourra donc écrire

$$A \subset B \iff (A \subseteq B) \wedge (A \neq B)$$

Exemple 2.2.1. Si on considère les trois ensembles suivant :

$$A = \{1, 2, 3, 4, 5, 6\} \qquad B = \{1, 3, 6\} \qquad C = \{1, 3, 7\}$$

alors on a :

1. $B \subset A$ car tous les éléments de B sont des éléments de A.
2. $C \not\subset A$ car le nombre 7 ne fait pas partie de A.

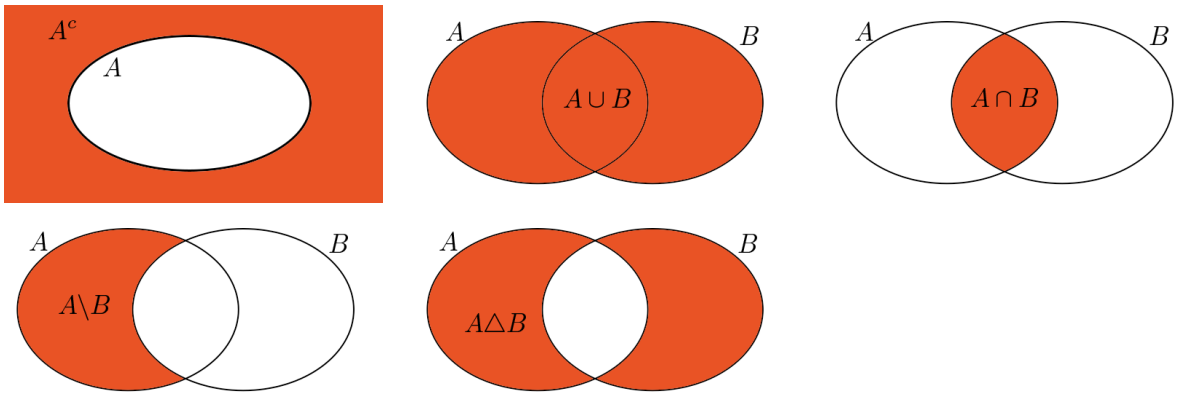
2.3 Opérations sur les ensembles

Comme pour les nombres, il existe plusieurs opérations importantes sur les ensembles. On notera entre autre le complément, l'union, l'intersection, la différence et la différence symétrique. Chacune de ces opérations peut être définie à partir du symbol d'appartenance $\in$, et des connecteurs logiques du premier chapitre.

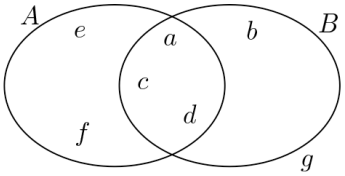
Definition 2.3.1. Les différentes opérations sur les ensembles sont définies comme suit :

1. Le complément d'un ensemble A, dénoté A^c ou $\overline{A}$, est l'ensemble des éléments qui ne sont pas dans A. On écrira donc
$$A^c = \{x : x \notin A\}$$
2. L'union d'un ensemble A avec un ensemble B, dénoté $A \cup B$, est l'ensemble des éléments qui sont dans A ou dans B. On écrira donc
$$A \cup B = \{x : (x \in A) \vee (x \in B)\}$$
3. L'intersection d'un ensemble A avec un ensemble B, dénoté $A \cap B$, est l'ensemble des éléments qui sont dans A et dans B. On écrira donc
$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}$$
4. La différence d'un ensemble A avec un ensemble B, dénoté $A \backslash B$ ou parfois $A - B$, est l'ensemble des éléments qui sont dans A mais pas dans B. On écrira donc
$$A \backslash B = \{x : (x \in A) \wedge (x \notin B)\}$$
5. La différence symétrique d'un ensemble A avec un ensemble B, dénoté $A \triangle B$, est l'ensemble des éléments qui sont dans A ou dans B, mais pas dans les deux. On écrira donc
$$A \triangle B = (A \backslash B) \cup (B \backslash A)$$

Les cinq opérations que nous venons de définir sont plus facilement visualisé à l'aide de schéma qui porte le nom de diagramme de Venn. On a donc :



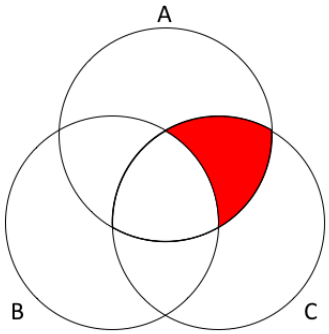
Exemple 2.3.1. En considérant le diagramme de Venn ci-dessous qui représente les ensembles A et B.



on obtient les ensembles suivant :

1. $A = \{a, c, d, e, f\}$
2. $B = \{a, b, c, d\}$
3. $A \cup B = \{a, b, c, d, e, f\}$
4. $A \cap B = \{a, c, d\}$
5. $A \triangle B = \{b, e, f\}$
6. $A \backslash B = \{e, f\}$
7. $B \backslash A = \{b\}$
8. $A^c = \{b, g\}$
9. $B^c = \{e, f, g\}$

Exemple 2.3.2. Considérons le diagramme ci-dessous. On veut trouver une expression permettant d'identifié la région en rouge.



Pour ce faire, il s'agit de remarquer que cette région fait à la fois partie de l'ensemble A et C, mais exclut les éléments de l'ensemble B. On peut donc écrire $(A \cap C) \backslash B$.

Il existe deux autres opérations sur les ensembles qui sont particulièrement importantes, Les deux étant très différentes des précédentes. Il s'agit du produit cartésien et de l'ensemble puissance. Vous avez déjà rencontrer au secondaire la première de ces opérations lorsque vous avez parler du plan cartésien $\mathbb{R}^2$, qui est en fait une notation abrégé pour signifier $\mathbb{R} \times \mathbb{R}$.

Definition 2.3.2. Le produit cartésien d'un ensemble A avec un ensemble B, dénoté $A \times B$, est l'ensemble de tous les couples qu'on peut formé où le premier élément est dans A et le second dans B. On écrira donc :

$$A \times B = \{(a, b) : (a \in A) \wedge (b \in B)\}$$

Donc à partir de la définition, on peut donc dire que $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ est l'ensemble de tous les couples formé de deux nombres réels.

Exemple 2.3.3. Si $A = \{1, 2, 3\}$ et $B = \{a, b\}$, quel est le produit cartésien $A \times B$? En utilisant la définition, on a donc :

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

En particulier, on remarque que $|A \times B| = |A| \cdot |B|$, ce qui sera toujours vrai.

Finalement, si A est un ensemble, on définit l'ensemble puissance $\mathcal{P}(A)$ comme étant l'ensemble des sous-ensembles de A. C'est ce que nous écrivons $\mathcal{P}(A) = \{B : B \subseteq A\}$. Notez ici qu'il faut faire attention de ne pas oublier l'ensemble vide qui est un sous-ensemble de n'importe quel ensemble.

Exemple 2.3.4. Si $A = \{1, 2, 3\}$, alors l'ensemble puissance est :

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

2.4 Démonstrations en théorie des ensembles

Dans cette section, nous voulons maintenant nous intéressé à deux problèmes particulièrement important dans la théorie des ensembles. Comment démontrer qu'un ensemble est inclut dans un autre, et comment démontrer l'égalité de deux ensembles. Dans les deux cas, ce sont les règles d'équivalence des propositions

logiques qui vont nous guider. Commençons par regarder la question de démontrer l'inclusion d'un ensemble dans un autre.

$$\begin{aligned} A \subseteq B &\Leftrightarrow \forall x\{(x \in A) \to (x \in B)\} \\ &\Leftrightarrow (x \in A) \to (x \in B) \text{ est une tautologie} \end{aligned}$$

C'est cette dernière équivalence qui va nous permettre de démontrer l'inclusion d'un ensemble dans un autre. Noter que le faut que cette dernière expression soit une tautologie peut être écrit sous la forme $(x \in A) \Rightarrow (x \in B)$. La flèche double signifiant qu'il s'agit d'une tautologie.

Exemple 2.4.1. On veut démontrer que pour tout ensemble A, B on a $A \subseteq A \cup B$. Pour ce faire, on doit démontrer que $(x \in A) \to (x \in A \cup B)$ est une tautologie. C'est ce que nous allons faire immédiatement :

$$\begin{aligned} (x \in A) \to (x \in A \cup B) &\Leftrightarrow (x \in A) \to ((x \in A) \vee (x \in B)) && \text{Définition de l'union} \\ &\Leftrightarrow \neg(x \in A) \vee ((x \in A) \vee (x \in B)) && \text{Équivalence avec le connecteur d'implication} \\ &\Leftrightarrow (\neg(x \in A) \vee (x \in A)) \vee (x \in B) && \text{Associativité} \\ &\Leftrightarrow V \vee (x \in B) \quad \text{car } \neg p \vee p \Leftrightarrow V \\ &\Leftrightarrow V \quad \text{Domination} \end{aligned}$$

Comme il s'agit d'une tautologie, on peut donc conclure que $A \subseteq (A \cup B)$.

Nous allons maintenant considérer le second problème, celui de démontrer l'égalité de deux ensembles. Il existe plusieurs façon de décrire le même ensemble, et en conséquence, pouvoir démontrer que deux ensembles sont égaux est particulièrement important. Il s'agit d'un sujet récurrent dans toutes les branches des mathématiques. Pour résoudre ce problème, il existe plusieurs méthodes. Parmi les plus courante on notera :

1. On peut démontrer que $A \subseteq B$ et $B \subseteq A$, c'est à dire démontrer que tous les éléments de A sont dans B et tous les éléments de B sont dans A.
2. On peut utiliser les règles d'équivalence logique
3. On peut faire un tableau semblable aux tables de vérités

La première méthode est sans aucun doute celle qui revient le plus souvent, mais pour les besoins de ce chapitre, ce sont les deux autres qui nous intéresserons. Utiliser les règles d'équivalence logique n'est certainement pas la méthode la plus simple, mais est particulièrement intéressante car nous permet d'utiliser directement la définition des différentes opérations sur les ensembles, en combinaison avec les règles de la logique mathématique que nous avons vu au chapitre 1. L'idée de la méthode est la suivante :

$$\begin{aligned} A = B &\Leftrightarrow (A \subseteq B) \wedge (B \subseteq A) && \text{Définition de l'égalité} \\ &\Leftrightarrow \forall x((x \in A) \to (x \in B)) \wedge \forall x((x \in B) \to (x \in A)) && \text{Définition d'un sous-ensemble} \\ &\Leftrightarrow \forall x(((x \in A) \to (x \in B)) \wedge ((x \in B) \to (x \in A))) && \text{Commutativité et définition de } \forall \\ &\Leftrightarrow \forall x((x \in A) \leftrightarrow (x \in B)) && \text{Équivalence avec le connecteur d'équivalence} \end{aligned}$$

Maintenant, pour que cette dernière équivalence soit vrai, on doit donc avoir que $(x \in A) \leftrightarrow (x \in B)$ est une tautologie. Par définition c'est ce que nous écrivons :

$$(x \in A) \Leftrightarrow (x \in B)$$

C'est donc ce que nous devons démontrer pour établir l'égalité de deux ensembles. Voici un exemple illustrant la méthode.

Exemple 2.4.2. Si A, B et C sont des ensembles, on veut démontrer l'égalité suivante :

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

En utilisant les règles de la logique, on a donc :

$$\begin{aligned}
x \in A \cup (B \cap C) &\Leftrightarrow (x \in A) \vee (x \in B \cap C) \quad \text{Définition de l'union} \\
&\Leftrightarrow (x \in A) \vee ((x \in B) \wedge (x \in C) \quad \text{Définition de l'intersection} \\
&\Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) \quad \text{Distributivité} \\
&\Leftrightarrow (x \in (A \cup B)) \wedge (x \in (A \cup C)) \quad \text{Définition de l'union} \\
&\Leftrightarrow x \in (A \cup B) \cap (A \cup C) \quad \text{Définition de l'intersection}
\end{aligned}$$

Ce qui confirme l'égalité des deux ensembles.

Nous allons maintenant démontrer une loi particulièrement importante de la théorie des ensembles : la loi de De Morgan (pour les ensembles). Dans un premier temps, nous allons utilisé la même méthode que l'exemple précédent. Pour la seconde partie, nous allons essayer une seconde méthode en utilisant cette fois un tableau.

Théorème 2.4.1. **(Loi de De Morgan pour les ensembles)** Si A et B sont des ensembles, alors on a les deux égalités suivantes :

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

Démonstration.

1. Dans un premier temps, nous allons utiliser les règles d'équivalence logique. On a donc :

$$\begin{aligned}
x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \quad \text{Définition du complément} \\
&\Leftrightarrow \neg(x \in A \cup B) \quad \text{Définition de } \notin \\
&\Leftrightarrow \neg((x \in A) \vee (x \in B)) \quad \text{Définition de l'union} \\
&\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \quad \text{Loi de De Morgan} \\
&\Leftrightarrow (x \notin A) \wedge (x \notin B) \quad \text{Définition de } \notin \\
&\Leftrightarrow (x \in A^c) \wedge (x \in B^c) \quad \text{Définition du complément} \\
&\Leftrightarrow x \in A^c \cap B^c \quad \text{Définition de l'intersection}
\end{aligned}$$

2. Pour la seconde partie, nous allons utiliser une méthode différente et faire un tableau. Dans ce dernier, le 0 signifie n'est pas élément, et le 1 signifie est élément. On a donc :

A	B	$A \cap B$	$(A \cap B)^c$	A^c	B^c	$A^c \cup B^c$
0	0	0	**1**	1	1	**1**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
1	1	1	**0**	0	0	**0**

On remarque donc que les colonnes correspondant à $(A \cap B)^c$ et $A^c \cup B^c$ sont identique, ce qui nous permet d'affirmer que $(A \cap B)^c = A^c \cup B^c$

□

Remarquer dans notre démonstration précédente, le choix de la méthode était arbitraire. Les deux méthodes auraient pu être appliquer à chacune des deux parties.

2.5 Les paradoxes

La théorie des ensembles que nous avons étudié dans ce chapitre est souvent appelé théorie naive des ensembles. La raison en est simple, bien que la plupart de ce que nous avons fait dans le chapitre ait comme base la logique mathématique, notre définition de ce qu'est un ensemble reste informelle (ou naive). La théorie tel que nous l'avons définie permet plusieurs paradoxes, l'un des plus connu et simple est celui de Russell qui considère l'ensemble :

$$A = \{x : x \notin A\}$$

Cet ensemble n'a pas de sens car si $y \in A$, alors par définition $y \notin A$. il existe plusieurs théorie permettant de remédier à ces paradoxes, l'une des plus importante est celle de Zermalo-Frankel. Cette théorie est cependant particulièrement compliqué, et est relégué à des cours plus avancé. La bonne nouvelle est que pour la plupart des mathématiques que vous rencontrerez au niveau du premier cycle universitaire, la théorie naive tel que nous l'avons étudié est amplement suffisant.

Chapitre 3

Les fonctions et les relations

3.1 Les relations

Au chapitre précédent, nous nous somme intéressé à la théorie des ensembles, dans ce chapitre, nous voulons aller un peut plus loin et étudier les relations. Une relation est en quelques sorte un lien entre certain élément de deux ensembles.

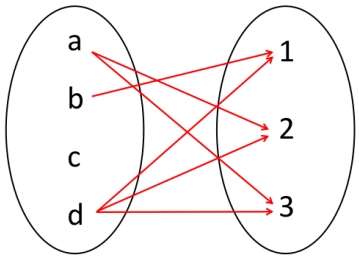
Definition 3.1.1. Si X et Y sont des ensembles, alors une relation R entre X et Y est un sous ensemble $R \subseteq X \times Y$. Dans ce cas on écrira

$$xRy \iff (x, y) \in R$$

Si $X = Y$ on dira que R est une relation sur X.

Une relation peut être définie de différente façon. Les plus courante sont à l'aide d'un diagramme de Venn, ou bien à l'aide d'une équation. Ceci est illustré dans les deux exemples suivant.

Exemple 3.1.1. Le diagramme ci-dessous représente une relation :



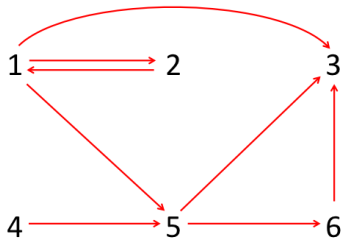
Les éléments de cette relation sont $R = \{(a, 2), (a, 3), (b, 1), (d, 1), (d, 2), (d, 3)\}$.

Exemple 3.1.2. Le cercle unité est une relation sur $\mathbb{R}$. On peut le définir comme étant

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

Comme le dernier exemple l'illustre, il est tout à fait acceptable de parler d'une relation d'un ensemble sur lui même. il est aussi courant de représenté une relation sous forme d'un graphe comme le montre l'exemple suivant.

Exemple 3.1.3. Le graphe suivant représente une relation sur un ensemble X. C'est à dire que l'ensemble de départ est le même que celui d'arriver.



Notez que la direction des flèches est importante de manière générale. Les éléments de cette relation sont donc :

$$R = \{(1,2),(1,3),(1,5),(2,1),(4,5),(5,3),(5,6),(6,3)\}$$

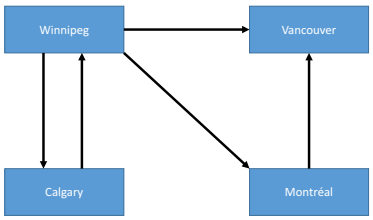
Les relations d'un ensemble sur lui même sont particulièrement courante en mathématiques, et plusieurs des exemples intéressant possèdent certaine propriétés supplémentaire que nous allons définir immédiatement.

Definition 3.1.2. Si R est une relation sur un ensemble A, alors on dit que :

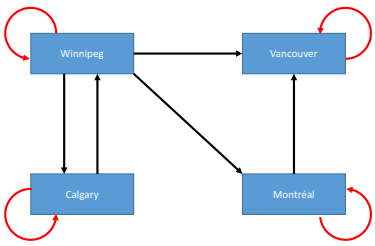
1. R est une relation réflexive si xRx pour tout $x \in A$.
2. R est une relation symétrique si pour tout $x, y \in A$ tel que xRy, alors yRx.
3. R est une relation antisymétrique si pour tout $x, y \in A$ tel que xRy et yRx, alors $x = y$.
4. R est une relation transitive si pour tout $x, y, z \in A$ tel que xRy et yRz, alors xRz.

Notez que lorsque qu'une relation est symétrique et représenté sous forme d'un graphe, on peut alors omettre d'indiquer la direction des flèches. Il sera alors compris de manière implicite que chaque lien représente une flèche allant dans chacune des deux directions. Ceci est cependant possible seulement si la relation est symétrique.

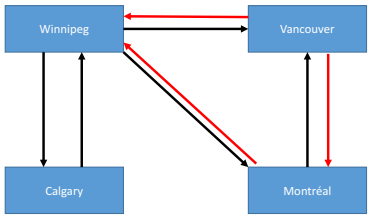
Exemple 3.1.4. Supposons que nous voulons démarrer notre compagnie aérienne. Notre compagnie desservira les villes de Winnipeg, Calgary, Vancouver et Montréal (i.e. notre ensemble A). Les différents vols que notre compagnie offrira sont illustrer sur le schéma ci-dessous (les liens représentent notre relation). Nous voulons maintenant déterminer si cette relation est réflexive, symétrique, antisymétrique et/ou transitive.



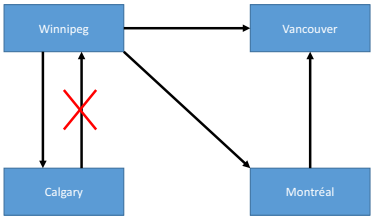
Concrètement, dans notre exemple, une relation qui est réflexive signifie qu'il existe toujours un vol permettant d'aller d'une ville vers elle même. Notre relation n'est évidement pas réflexive, car aucune ville n'offre de vol vers elle même. Pour rendre la relation réflexive, il faudrait des vols de Winnipeg à Winnipeg, de Calgary à Calgary, de Vancouver à Vancouver, et finalement de Montréal à Montréal. Ceci est illustré sur le graphe ci-dessous.



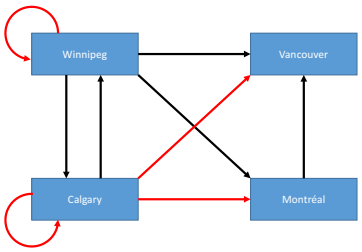
Revenons maintenant au graphe original. Nous voulons déterminer si notre relation est symétrique. Concrètement dans notre exemple la relation est symétrique si chaque fois qu'un vol est offert entre une ville A et une ville B, le vol de retour est aussi disponible. Notre relation (originale) n'est évidement pas symétrique car aucun vol de retour n'est disponible pour les liaisons Winnipeg-Vancouver, Winnipeg-Montréal et Montréal-Vancouver. Pour rendre la relation symétrique, il faudrait ajouter les liaisons en rouge illustré sur le graphe ci-dessous.



Revenons à nouveau au graphe original. Concrètement, la relation est antisymétrique si chaque fois qu'il y a un vol aller-retour offert entre deux villes, ces deux villes doivent en fait être la même. En d'autre mots, les seuls vols aller-retour qui sont permis sont les boucles (un vol allant d'une ville à elle même). Dans notre exemple, un vol aller-retour est offert entre Winnipeg et Calgary. Pourtant ces deux villes sont différentes (ce n'est pas une boucle), donc la relation n'est pas antisymétrique. Pour rendre la relation antisymétrique, il faut retirer la liaison Calgary-Winnipeg (ou le retour Winnipeg-Calgary), comme illustré ci-dessous.



Finalement, en revenant à nouveau à notre graphe original, on veut regarder la question de transitivité. Concrètement dans notre exemple, la transitivité signifie que chaque fois qu'il est possible d'aller d'un point A à un point B avec ou sans escale, il existe aussi un vol directe entre A et B. Dans notre exemple, il est possible d'aller de Calgary à Vancouver avec escale à Winnipeg, mais il n'existe aucun vol directe entre Calgary et Vancouver. La relation n'est donc pas transitive. Pour rendre la relation transitive, on doit donc ajouter cette liaison. On remarque aussi qu'il est possible d'aller de Winnipeg à Winnipeg via Calgary, et de Calgary à Calgary via Winnipeg. Il faut donc aussi ajouter une liaison de Winnipeg à Winnipeg et de Calgary à Calgary. Ceci est représenté dans le graphe ci-dessous.



Remarquez que notre exemple peut être représenté sous forme de relation formelle. Si

$$A = \{\text{Winnipeg}, \text{Vancouver}, \text{Calgary}, \text{Montreal}\},$$

alors on définit la relation $\mathcal{R}$ sur A comme étant :

$$\mathcal{R} = \{(\text{Win.}, \text{Cal.}), (\text{Cal.}, \text{Win.}), (\text{Win.}, \text{Mon.}), (\text{Mon.}, \text{Van.}), (\text{Win.}, \text{Van.})\}$$

Il s'agit alors d'exactement de la même relation, mais écrite de manière à ne pas avoir besoin d'un graphe pour la représenté.

Exemple 3.1.5. Considérez les relations suivantes qui sont définies sur l'ensemble $A = \{1, 2, 3\}$

$$R_1 = \{(1,1), (1,2), (2,2), (3,3)\}$$

$$R_2 = \{(1,2), (2,3), (3,1)\}$$

$$R_3 = \{(1,1), (1,2), (1,3), (2,1), (2,3), (3,1), (3,2), (3,3)\}$$

Lesquels de ces relations sont réflexives ? Pour ce faire, il suffit de vérifier si tout les couples de la forme (a, a) où $a \in A$ sont dans l'ensemble. On a donc :

1. La relation R_1 est réflexive car elle contient les couples $(1,1), (2,2), (3,3)$.
2. La relation R_2 n'est pas réflexive car aucun des éléments $(1,1), (2,2), (3,3)$ font partie de l'ensemble.
3. La relation R_3 n'est pas réflexive car $(2,2)$ ne fait pas partie de l'ensemble.

Exemple 3.1.6. Considérez les relations suivantes qui sont définies sur l'ensemble $A = \{1, 2, 3\}$

$$R_1 = \{(1,1), (1,2), (2,2), (3,3)\}$$

$$R_2 = \{(1,2), (2,3), (3,1)\}$$

$$R_3 = \{(1,1), (1,2), (1,3), (2,1), (2,3), (3,1), (3,2), (3,3)\}$$

Lesquels de ces relations sont symétriques ?

1. La relation R_1 n'est pas symétrique car $(1,2)$ fait partie de l'ensemble, mais pas $(2,1)$.
2. La relation R_2 n'est pas symétrique car $(1,2)$ fait partie de l'ensemble, mais pas $(2,1)$.
3. La relation R_3 est symétrique.

Exemple 3.1.7. Considérez les relations suivantes qui sont définies sur l'ensemble $A = \{1, 2, 3\}$

$$R_1 = \{(1,1), (1,2), (2,2), (3,3)\}$$

$$R_2 = \{(1,2), (2,3), (3,1)\}$$

$$R_3 = \{(1,1), (1,2), (1,3), (2,1), (2,3), (3,1), (3,2), (3,3)\}$$

Lesquels de ces relations sont antisymétriques ?

1. La relation R_1 est antisymétrique, car les seuls éléments pour lesquels (a, b) et (b, a) sont dans R_1 sont des éléments de la forme (a, a).
2. La relation R_2 est antisymétrique, car il n'existe aucun élément de R_2 pour lesquels (a, b) et (b, a) sont dans R_2.
3. La relation R_3 n'est pas antisymétrique, car $(1,2)$ et $(2,1)$ sont tous deux dans R_3, mais $1 \neq 2$.

Exemple 3.1.8. Considérez les relations suivantes qui sont définies sur l'ensemble $A = \{1, 2, 3\}$

$$R_1 = \{(1,2), (2,3), (1,3)\}$$

$$R_2 = \{(1,1), (1,2), (1,3), (2,1), (2,3), (3,1), (3,2), (3,3)\}$$

Lesquels de ces relations sont transitives ?

1. La relation R_1 est transitive.
2. La relation R_2 n'est pas transitive, car $(2,1)$ et $(1,2)$ sont dans R_2, mais $(2,2)$ n'en fait pas partie.

3.2 Les relations d'ordre

Une relation d'ordre ou d'ordre partielle est un type de relation particulièrement important en mathématiques. Il sert à généraliser l'idée de "est plus petit que" que l'on retrouve dans les nombres réels. Pour cette raison, il est commun d'utiliser le symbol $\preceq$ pour dénoter une relation d'ordre ou d'ordre partielle, mais ce n'est pas une obligation.

Definition 3.2.1. Une relation d'ordre partiel sur un ensemble A est une relation qui est réflexive, anti-symétrique et transitive. Une relation d'ordre sur un ensemble A est une relation d'ordre partiel pour laquelle pour tout $x, y \in A$, alors xRy ou yRx. C'est à dire qu'il s'agit d'une relation d'ordre partielle pour laquelle tous les éléments sont comparables.

Exemple 3.2.1. Il existe plusieurs relation d'ordre et d'ordre partielle qui vous sont déjà familier. Parmi celle-ci on notera :

1. Les relations $\leq$ et $\geq$ sont des relations d'ordre sur l'ensemble des nombres réels $\mathbb{R}$.
2. Si A est un ensemble, alors la relation $\subseteq$ est une relation d'ordre partielle sur l'ensemble puissance $\mathcal{P}(A)$, mais n'est pas une relation d'ordre.
3. Si a et b sont des nombres naturels, alors on dit que a divise b, et on écrit $a|b$ s'il existe un entier k tel que $ak = b$. La relation $|$ est une relation d'ordre partiel sur l'ensemble des nombres naturels $\mathbb{N}$ qui n'est pas une relation d'ordre.

Remarquez que la relation de divisibilité $|$ peut être étendu à l'ensemble des entiers. Si $a, b \in \mathbb{Z}$, alors on dit que a divise b et on écrit $a|b$ s'il existe un entier k tel que $ak = b$. Par contre, dans ce cas il ne s'agit pas d'une relation d'ordre partielle sur $\mathbb{Z}$ car $-1|1$ et $1|-1$, mais $1 \neq -1$.

Exemple 3.2.2. Il faut faire attention, certaine relation similaire à celles de l'exemple précédent ne sont pas des relations d'ordre ou d'ordre partielle. On notera entre autre :

1. Les relations $<$ et $>$ sur les réels ne sont pas de relation d'ordre, car elle ne sont pas réflexive.
2. Si A est un ensemble, la relation $\subset$ sur l'ensemble puissance $\mathcal{P}(A)$ n'est pas une relation d'ordre partielle, car elle n'est pas réflexive.

3.3 Les relations d'équivalence

Un autre type de relation particulièrement importante en mathématiques est la notion de relation d'équivalence qui sert à généraliser le concept d'égalité que l'on retrouve dans les nombres réels. Il est commun de dénoté une relation d'équivalence par le symbol $\sim$, mais ce n'est pas obligatoire. Dans certain cas particulier, le symbole $\equiv$ est aussi utilisé. Une relation d'équivalence sert à partitionner un ensemble en sous-ensemble contenant des éléments qui pour un contexte donner on considère équivalent. Vous pouvez par exemple imaginer un horloge, sur laquelle les nombres 1 et 13 se retrouve au même endroit, et donc peut être considéré comme équivalent.

Definition 3.3.1. Une relation d'équivalence sur un ensemble A est une relation qui est réflexive, symétrique et transitive.

Exemple 3.3.1. Il existe plusieurs exemple de relation d'équivalence qui vous sont déjà familière. En voici quelques exemples important :

1. La relation $=$ est une relation d'équivalence sur l'ensemble des nombres réels $\mathbb{R}$.
2. Si A est un ensemble, alors la relation $=$ est une relation d'équivalence sur l'ensemble puissance $\mathcal{P}(A)$.
3. Si n est un entier plus grand ou égal à 2, alors on définit la relation $\equiv_n$ sur l'ensemble des entiers comme étant
$$a \equiv_n b \iff n|(b-a)$$
dans ce cas, $\equiv_n$ forme une relation d'équivalence.

Exemple 3.3.2. On veut démontrer que la relation ci-dessous définie sur l'ensemble $\mathbb{N} \times \mathbb{N}$ est une relation d'équivalence.

$$(a,b)R(c,d) \quad \Leftrightarrow \quad a+d=b+c$$

Pour ce faire, on doit montrer que la relation est réflexive, symétrique et transitive.

1. **Réflexive :** Prenons $(a,b) \in \mathbb{N} \times \mathbb{N}$. On veut montrer que $(a,b)R(a,b)$. Pour ce faire, il suffit de remarquer que $a+b=b+a$, ce qui est évidement vrai. La relation est donc réflexive.
2. **Symétrique :** Prenons $(a,b),(c,d) \in \mathbb{N}\times\mathbb{N}$, et supposons que $(a,b)R(c,d)$. Par définition de la relation, on a donc $a+d=b+c$. En réarrangeant les termes, on obtient $c+b=d+a$, ce qui est équivalent à dire que $(c,d)R(a,b)$. La relation est donc symétrique.
3. **Transitive :** Prenons $(a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$, et supposons que $(a,b)R(c,d)$ et $(c,d)R(e,f)$. Par définition, on a donc $a+d=b+c$ et $c+f=d+e$. À partir de ces deux équations, on obtient donc :

   $$a+f=(b+c-d)+(d+e-c)=b+e$$

   ce qui est équivalent à dire $(a,b)R(e,f)$. La relation est donc transitive.

Comme la relation est réflexive, symétrique et transitive, on peut donc conclure qu'il s'agit d'une relation d'équivalence.

Notez que la relation de l'exemple précédent joue un rôle important pour construire l'ensemble des entiers à partir de celui des nombres naturels. Nous ne le ferons pas dans notre cours, mais il s'agit d'une façon de définir l'égalité sur les entiers à partir de l'égalité des nombres naturels. Vous pouvez consulter des livres sur les fondations des mathématiques pour plus de détails.

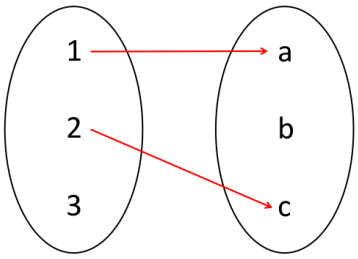
3.4 Les fonctions

Definition 3.4.1. Si A et B sont des ensembles, alors on définit une fonction $f : A \to B$ comme étant une relation R pour laquelle pour tout $x \in A$, il existe un et un seul $y \in B$ tel que xRy. Dans ce cas, on écrit $f(x)=y$ plutôt que xRy. L'ensemble A porte le nom de domaine de la fonction f, et l'ensemble B porte le nom de codomaine.

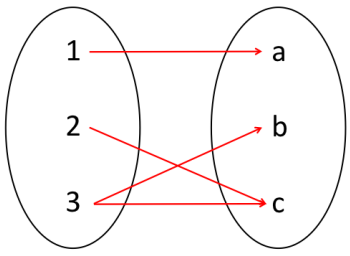
Lorsqu'une relation est définie à partir d'un diagramme de Venn, pour vérifier s'il s'agit d'une fonction il suffit de vérifier si chaque élément de l'ensemble de départ (le domaine) possède exactement une flèche.

Exemple 3.4.1. Parmi les 3 relations illustrés ci-dessous, lesquels sont des fonctions ?

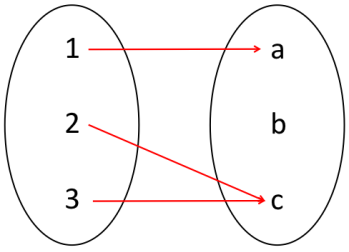
Relation 1



Relation 2



Relation 3

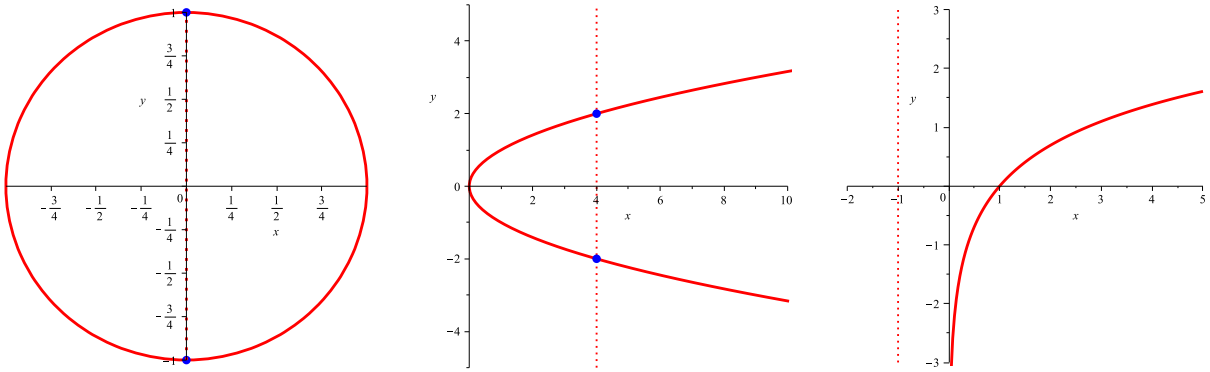


La relation un n'est pas une fonction, car aucune flèche commence au nombre 3. La relation 2 n'est pas n'ont plus une fonction, car deux flèches commencent au nombre 3. Par contre, on remarque que la relation 3 est bien une fonction.

Lorsqu'une relation est déterminé à partir de son graphique, il suffit de regarder que chaque droite verticale (Dans le domaine) rencontre la relation en exactement un point.

Exemple 3.4.2. Parmi les relations ci-dessous, lesquels sont des fonctions ?

$\mathcal{R}_1 = \{(x,y) \in [-1,1]^2 : x^2 + y^2 = 1\}$ $\mathcal{R}_2 = \{(x,y) \in [0,\infty) \times \mathbb{R} : x = y^2\}$ $\mathcal{R}_3 = \{(x,y) \in \mathbb{R}^2 : y = \ln(x)\}$

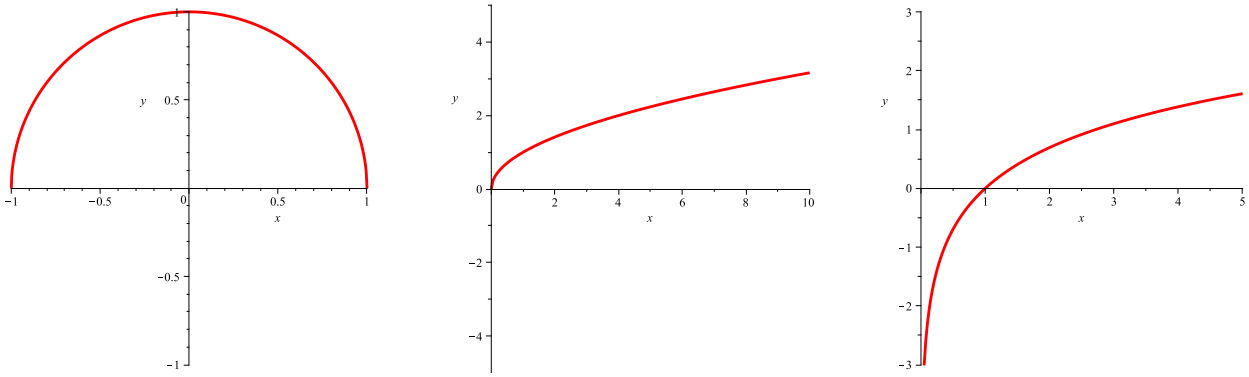


1. La relation $\mathcal{R}_1$ représente le cercle unité. Il s'agit d'une relation qui n'est pas une fonction, car $(0,1)$ et $(0,-1)$ font tout les deux parties de l'ensemble.
2. La relation $\mathcal{R}_2$ représente une parabole. Si on dessine une droite verticale à $x = 4$, on remarque que la droite croise la relation en exactement deux points : $(4,2)$ et $(4,-2)$. Elle ne satisfait donc pas la règle qui suppose que chaque droite verticale doit rencontrer exactement un point. Il ne s'agit donc pas d'une fonction.
3. La relation $\mathcal{R}_3$ n'est pas non plus une fonction, car $x = -1$ fait partie du domaine, mais la droite verticale $x = -1$ ne croise la relation en aucun point car $\ln(-1)$ n'est pas définie dans les nombres réels.

Remarquez que chacune des relations de l'exemple précédent peuvent devenir des fonctions si on considère seulement un sous-ensemble de la relation. C'est ce que nous allons faire dans l'exemple suivant :

Exemple 3.4.3. Les exemples suivant sont des fonctions. Dans chacun des cas, identifier le domaine et le codomaine.

$\mathcal{R}_1 = \{(x,y) \in [-1,1] \times \mathbb{R}^+ : x^2 + y^2 = 1\}$ $\mathcal{R}_2 = \{(x,y) \in [0,\infty)^2 : x = y^2\}$ $\mathcal{R}_3 = \{(x,y) \in (0,\infty) \times \mathbb{R} : y = \ln(x)\}$



1. La fonction définie par la relation $\mathcal{R}_1$ a comme domaine l'intervalle $[-1,1]$ et comme codomaine $\mathbb{R}^+$. On peut réécrire cette fonction sous la forme fonctionnelle $y(x) = \sqrt{1-x^2}$.
2. La fonction définie par la relation $\mathcal{R}_2$ a comme domaine l'intervalle $[0,\infty)$ et comme codomaine $[0,\infty)$. On peut réécrire cette fonction sous la forme fonctionnelle $y(x) = \sqrt{x}$.
3. La fonction définie par la relation $\mathcal{R}_3$ a comme domaine l'intervalle $(0,\infty)$ et comme codomaine $\mathbb{R}$. On peut réécrire cette fonction sous la forme fonctionnelle $y(x) = \ln(x)$.

Notez qu'il arrive souvent (en particulier dans les cours de calcul) de ne pas spécifier explicitement le domaine et le codomaine d'une fonction. Dans ce cas, on comprend que le domaine de la fonction est le plus grand ensemble pour laquelle la fonction est définie. Remarquez cependant que ceci n'est pas une bonne

pratique, car dans bien des cas cette approche peut créer de la confusion. Par exemple, dans un cours de calcul, si on vous demande le domaine de la fonction $f(x) = \sqrt{x}$, votre réponse sera l'intervalle $[0, \infty)$, pourtant dans un cours d'analyse complexe, la réponse serait l'ensemble des nombres complexes $\mathbb{C}$. La raison est simple, dans un cours de calcul, il est sous entendu que nous travaillons avec les nombres réels, alors que dans un cours d'analyse complexe, il est sous entendu que nous travaillons avec les nombres complexes.

Definition 3.4.2. Si $f : A \to B$ est une fonction, alors on appelle l'image de f l'ensemble :

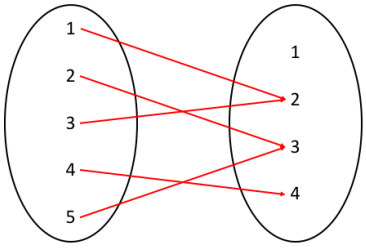
$$Im(f) = f(A) = \{f(x) : x \in A\}$$

Dans tous les cas $Im(f) \subseteq B$.

Remarquez que l'image d'une fonction n'est pas la même chose que le codomaine. De manière générale, l'image est un sous-ensemble du codomaine.

Exemple 3.4.4. Pour chacune des fonctions suivantes, identifier le domaine, le codomaine et l'image.

1. La fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. Dans ce cas, le domaine et le codomaine sont $\mathbb{R}$, mais l'image de la fonction est $[0, \infty)$.
2. La fonction définie à partir du diagramme ci-dessous a comme domaine l'ensemble $\{1, 2, 3, 4, 5\}$, comme codomaine l'ensemble $\{1, 2, 3, 4\}$ et comme image l'ensemble $\{2, 3, 4\}$.



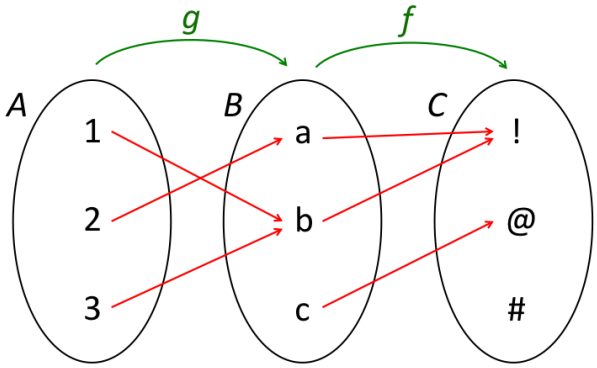
3.5 La composition des fonctions

Parmi les différentes opérations sur les fonctions que vous avez appris au secondaire, celle qui est sans doute la plus importante est la composition de fonction. Cette dernière a l'avantage de pouvoir être définie sur des ensembles quelconque, et non pas seulement sur un ensemble comme les réels.

Definition 3.5.1. Si A, B et C sont des ensembles, et $f : B \to C$, $g : A \to B$ sont des fonctions, alors on définit une nouvelle fonction appelé composition de f et g et dénoté $f \cdot g$ comme étant la fonction :

$$f \circ g : A \to C$$
$$(f \circ g)(x) = f(g(x))$$

Exemple 3.5.1. Voici un schéma illustrant des fonctions $f : B \to C$ et $g : A \to B$.



Dans ce cas, la composition $f \circ g$ sera une fonction de A à C qui prendra les valeurs suivantes :

$$(f \circ g)(1) =! \qquad (f \circ g)(2) =! \qquad (f \circ g)(3) =!$$

Il s'agit donc d'une fonction constante.

Remarquez que l'ordre dans laquelle on évalue la composition de fonction va de droite à gauche, ce qui est contraire à l'ordre dans lequel on lit habituellement un texte. La raison vient de l'écriture emboité $f(g(x))$ qui par la priorité des opérations signifie qu'on doit évaluer l'intérieur des parenthèses en premier.

Exemple 3.5.2. Considérez les deux fonctions suivantes :

$$\begin{array}{ll} f : \mathbb{R} \to [0, \infty) & g : [0, \infty) \to \mathbb{R} \\ f(x) = x^2 & g(x) = \sqrt{x} \end{array}$$

Donner une expression pour $f \circ g$ et $g \circ f$.

1. Premièrement, remarquons que $f \circ g$ est bien définie car le codomaine de g est le même ensemble que le domaine de f. Maintenant, remarquons que le domaine de $f \circ g$ est le même ensemble que le domaine de g, et le codomaine de $f \circ g$ est le même ensemble que le codomaine de f. On peut donc écrire :

   $$f \circ g : [0, \infty) \to [0, \infty)$$

   Ensuite, on a :

   $$(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x$$

2. Premièrement, remarquons que $g \circ f$ est bien définie car le codomaine de f est le même ensemble que le domaine de g. Maintenant, remarquons que le domaine de $g \circ f$ est le même ensemble que le domaine de f, et le codomaine de $g \circ f$ est le même ensemble que le codomaine de g. On peut donc écrire :

   $$g \circ f : \mathbb{R} \to \mathbb{R}$$

   Ensuite, on a :

   $$(g \circ f)(x) = g(f(x)) = g(x^2) = \sqrt{x^2} = x$$

On peut donc remarquez que $(f \circ g)(x) = x$ et $(g \circ f)(x) = x$, pourtant il ne s'agit pas de la même fonction, car elles n'ont pas le même domaine et codomaine.

La composition des fonctions fait son apparition à beaucoup d'endroit en mathématiques. Parfois de manière explicite, d'autre fois implicitement. On notera par exemple la règle de dérivation en chaîne (MATH 1501 - Intro. au calcul), la règle du changement de variable (MATH 1701 - Calcul II), la multiplication des matrices (MATH 1301 - Géométrie vectorielle et algèbre linéaire), les groupes de permutation (MATH 2021 - Algèbre 1).

3.6 Les fonctions injectives

Definition 3.6.1. Si $f : A \to B$ est une fonction, alors on dit que f est injective [1] si pour tout $x, y \in A$ tel que $f(x) = f(y)$, alors $x = y$. Certain auteurs écrivent $f : A \hookrightarrow B$ pour indiquer que la fonction est injective. De manière formelle, on écrit donc :

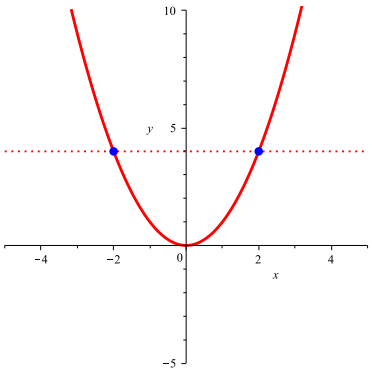
$$\forall x, y \in A, ((f(x) = f(y)) \to (x = y))$$

Il est facile de vérifier qu'une fonction est injective à partir de son graphique. Pour ce faire, il suffit de vérifier que chaque ligne horizontale coupe la fonction en au plus un point.

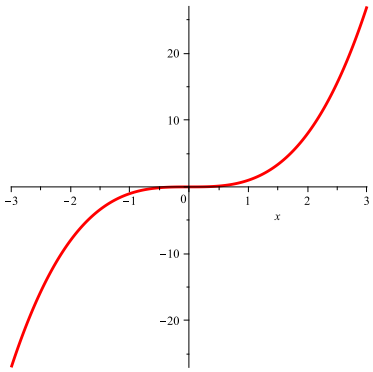
Exemple 3.6.1. Lesquels des fonctions suivantes sont injectives ?

1. En anglais, le terme fonction injective se traduit soit par injective function ou bien f is one-to-one. On verra aussi parfois la notation abrégé 1-1.

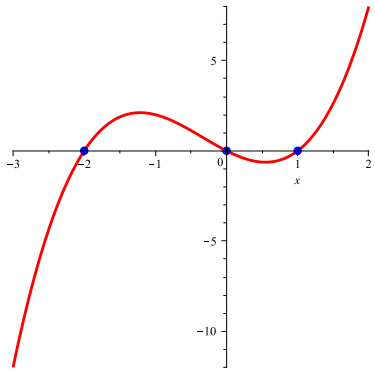
$f : \mathbb{R} \to \mathbb{R}$
$f(x) = x^2$



$g : \mathbb{R} \to \mathbb{R}$
$g(x) = x^3$

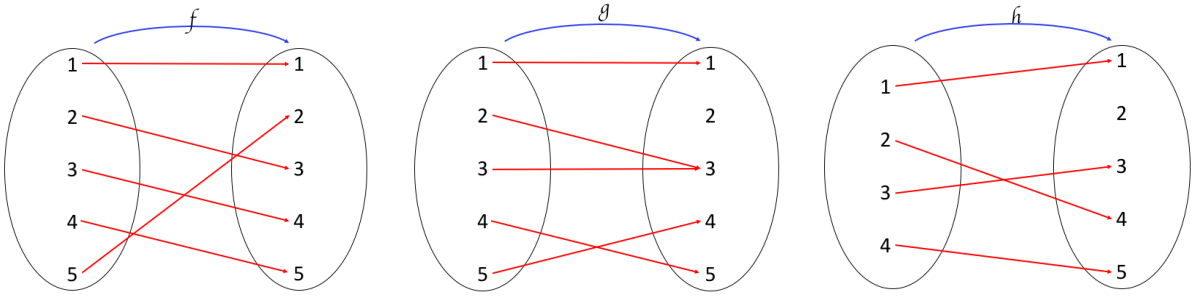


$h : \mathbb{R} \to \mathbb{R}$
$h(x) = x^3 + x^2 - 2x$



1. La fonction f n'est pas injective. Si on dessine une droite horizontale à $y = 4$, on remarque que la droite croise exactement deux points de la fonction. Une fonction injective ne peut cependant couper au plus une fois chacune des ligne horizontale. En utilisant la définition, on peut aussi affirmer que la fonction n'est pas injective car $f(-2) = f(2)$, mais $-2 \neq 2$.
2. La fonction g est injective. En effet, si $x^3 = y^3$, alors $x = y$. Ce qui peut être facilement observer à partir du graphique, car chaque droite horizontale croise la fonction en au plus un point.
3. La fonction h n'est pas injective. Si on factorise le polynome x^3+x^2-2x, on obtient $h(x) = x(x-1)(x+2)$. La fonction h a donc trois zéros (distincts). Par contre, une fonction injective ne peut pas avoir plus qu'un zéro.

Exemple 3.6.2. Lesquels des fonctions suivantes sont injectives ?



1. La fonction f est injective, car il n'y a jamais deux flèches qui pointent vers la même valeur.
2. La fonction g n'est pas injective, car $g(2) = g(3) = 3$.
3. La fonction h est injective, car il n'y a jamais deux flèches qui pointent vers la même valeur.

Théorème 3.6.1. Si A et B sont des ensembles contenant un nombre fini d'élément et $f : A \to B$ est une fonction injective, alors $|A| \leq |B|$.

Démonstration. Comme la fonction f est injective, tout les éléments de A doivent être associé à des éléments différents de B. Il doit donc y avoir au moins autant d'élément dans B que dans A. □

3.7 Les fonctions surjectives

Definition 3.7.1. Si $f : A \to B$ est une fonction, alors on dit que f est surjective [2] si pour tout élément y dans B, il existe un élément x dans A tel que $f(x) = y$. De manière abrégé on peut écrire que f est

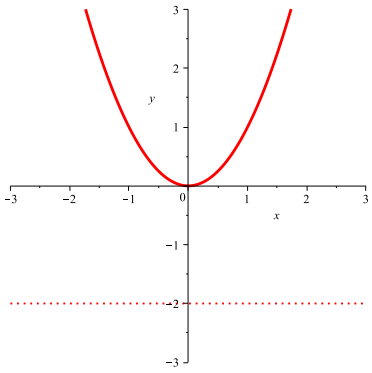
2. En anglais, on traduit habituellement le terme fonction surjective par surjective function, ou bien tout simplement f is onto.

surjective si $f(A) = B$, c'est à dire si l'image de f est égal à l'ensemble B au complet. Certain auteurs écrivent $f : A \twoheadrightarrow B$ pour indiquer que la fonction est surjective. De manière formelle, on peut définir la surjectivité par la proposition logique suivante :

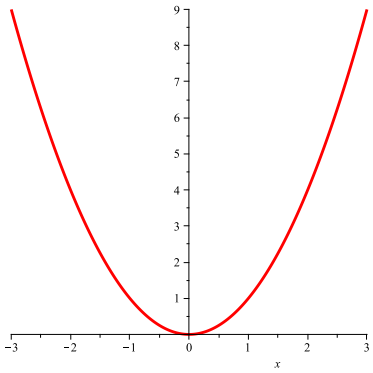
$$\forall y \in B, \exists x \in A, (f(x) = y)$$

Exemple 3.7.1. Lesquels des fonctions suivantes sont surjectives ?

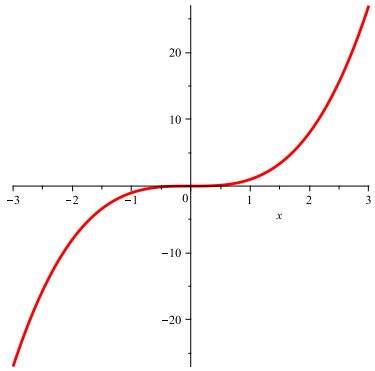
$f : \mathbb{R} \to \mathbb{R}$
$f(x) = x^2$



$g : \mathbb{R} \to [0, \infty)$
$g(x) = x^2$

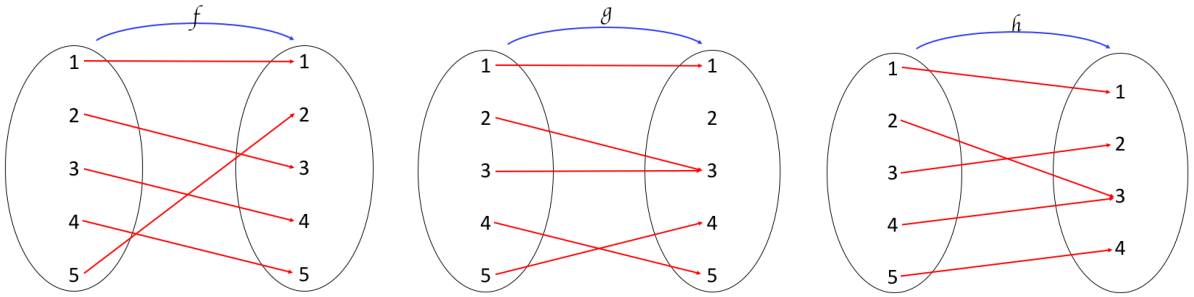


$h : \mathbb{R} \to \mathbb{R}$
$h(x) = x^3$



1. La fonction f n'est pas surjectve. La valeur -2 fait partie du codomaine, mais pas de l'image de la fonction car pour aucun $x \in \mathbb{R}$ on a $f(x) = -2$.
2. Bien que la fonction g soit très semblable à la fonction f, cette fois le codomaine est différent. Cette fonction est surjective.
3. Comme chaque droite verticale dans le codomaine croise la fonction h en au moins un point, la fonction h est surjective.

Exemple 3.7.2. Lesquels des fonctions suivantes sont surjectives ?



1. La fonction f est surjective, car pour chaque valeur du codomaine, il y a une flèche qui pointe vers cette valeur.
2. La fonction g n'est pas surjective, car aucune flèche ne pointe vers la valeur 2.
3. La fonction h est surjective, car pour chaque valeur du codomaine, il y a une flèche qui pointe vers cette valeur.

Théorème 3.7.1. Si A et B sont des ensembles contenant un nombre fini d'élément et $f : A \to B$ est une fonction surjective, alors $|A| \geq |B|$.

Démonstration. Comme la fonction f est surjective, pour chaque élément de B, il doit exister un élément de A qui lui est associé. Comme aucun élément de A ne peut être associé à plus d'un élément de B, on peut donc conclure que A possède au moins autant d'élément que B. □

3.8 Les fonctions bijectives

Definition 3.8.1. Si $f : A \to B$ est une fonction, alors on dit que f est bijective si elle est injective et surjective.

Théorème 3.8.1. Si A et B sont des ensembles contenant un nombre fini d'élément et $f : A \to B$ est une fonction bijective, alors $|A| = |B|$.

Démonstration. La démonstration est particulièrement simple. Comme une fonction bijective est par définition injective, alors $|A| \leq |B|$. De plus, comme une fonction bijective doit aussi être surjective, alors $|A| \geq |B|$. En combinant ces deux inégalités, on obtient donc $|A| = |B|$. □

Le théorème précédent illustre en fait une méthode pour comparer la cardinalité de deux ensembles. Il est facile de voir que si deux ensembles on exactement n éléments, alors il existe une fonction bijective entre les deux ensembles. Dans le cas des ensembles de cardinalité infinie, la question n'est pas aussi évidente. Nous allons donc l'utiliser comme définition.

Definition 3.8.2. On dit que deux ensembles ont la même cardinalité, s'il existe une fonction bijective entre ces deux ensembles.

Cette définition nous permet donc de comparer la cardinalité de deux ensembles, incluant le cas où les ensembles sont de cardinalité infinie. À noter que cette définition nous permet en même temps de montrer l'existence de plusieurs type d'infinie.

Exemple 3.8.1. On veut démontrer que les ensembles $[0, 1]$ et $[0, 5]$ ont la même cardinalité. Pour ce faire, nous devons trouver une fonction bijective $f : [0, 1] \to [0, 5]$. Pour ce faire, il est facile de remarquer que la fonction

$$f : [0, 1] \to [0, 5]$$
$$f(x) = 5x$$

Satisfait cette condition. Les deux ensembles ont donc la même cardinalité.

Exemple 3.8.2. On veut démontrer que les ensembles $\mathbb{N}$ et $\mathbb{Z}$ ont la même cardinalité. Pour ce faire, nous devons trouver une fonction bijective entre ces deux ensembles. Ceci peut être accomplie de la manière suivante :

$$\begin{array}{lccccccccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \mathbb{Z}: & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & \ldots \end{array}$$

Les deux ensembles ont donc la même cardinalité.

Exemple 3.8.3. On veut démontrer que les ensembles $\mathbb{Z}$ et $\mathbb{Q}$ ont la même cardinalité. Pour ce faire, nous devons trouver une fonction bijective entre ces deux ensembles. L'idée est de trouver premièrement une suite permettant d'énumérer tout les nombres rationnels positifs. Par le suite, il suffit d'appliquer le même truc que pour l'exemple précédent. Pour construire la suite, on va utiliser le diagramme suivant :

$$\begin{array}{ccccccccccccc} 0 & \to & 1 & \to & 2 & & 3 & \to & 4 & & 5 & \to & \ldots \\ & & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\ & & 1/2 & & 2/2 & & 3/2 & & 4/2 & & 5/2 & & \ldots \\ & & \downarrow & \nearrow & & \swarrow & & \nearrow & & & & & \\ & & 1/3 & & 2/3 & & 3/3 & & 4/3 & & 5/3 & & \ldots \\ & & & \swarrow & & \nearrow & & & & & & & \\ & & 1/4 & & 2/4 & & 3/4 & & 4/4 & & 5/4 & & \ldots \\ & & \downarrow & \nearrow & & & & & & & & & \\ & & 1/5 & & 2/5 & & 3/5 & & 4/5 & & 5/5 & & \ldots \\ & & & & & & & & & & & & \\ & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \end{array}$$

En suivant l'ordre des flèches et en prenant soins d'éliminer toutes les fractions de la liste qui ne sont pas réduite, on obtient donc la fonction bijective suivante :

$$\begin{array}{lccccccccccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \dots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \mathbb{Q}: & 0 & 1 & -1 & 2 & -2 & \frac{1}{2} & \frac{-1}{2} & \frac{1}{3} & \frac{-1}{3} & 3 & -3 & \dots \end{array}$$

Les nombres naturels et les nombres rationnels ont donc la même cardinalité.

Definition 3.8.3. On définit la cardinalité de l'ensemble des nombres naturels comme étant aleph 0, ce que l'on écrit $|\mathbb{N}| = \aleph_0$. Noter qu'aleph ($\aleph$) est un lettre de l'alphabet hébreux.

À partir des exemples que nous avons fait précedemment, on peut donc affirmer que $|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$. La question de savoir si les nombres réels ont eux aussi la même cardinalité est un peut plus délicate, et nous allons y répondre dans le théorème ci-dessous dû à Cantor.

Théorème 3.8.2. **(Théorème de Cantor)** Les nombres naturels et les nombres réels n'ont pas la même cardinalité.

Démonstration. Nous allons montrer qu'il n'existe aucune fonction surjective entre $\mathbb{N}$ et l'intervalle $(0,1)$. Comme l'intervalle $(0,1)$ est inclut dans les nombres réels, ceci nous permettra d'affirmer qu'il y a plus de nombre dans l'intervalle $(0,1)$ que de nombres naturels, et donc en conséquence qu'il y a plus de nombres réels que de nombres naturels. La démonstration se fait par contradiction. Supposons aux contraires qu'il existe une fonction bijective entre $\mathbb{N}$ et $(0,1)$. On peut donc énumérer tout les éléments de $(0,1)$ sous forme d'une suite :

$$\begin{aligned} 1 &\to 0, y_{11}y_{12}y_{13}y_{14}y_{15}y_{16}y_{17}y_{18}y_{19}\dots\dots \\ 2 &\to 0, y_{21}y_{22}y_{23}y_{24}y_{25}y_{26}y_{27}y_{28}y_{29}\dots\dots \\ 3 &\to 0, y_{31}y_{32}y_{33}y_{34}y_{35}y_{36}y_{37}y_{38}y_{39}\dots\dots \\ 4 &\to 0, y_{41}y_{42}y_{43}y_{44}y_{45}y_{46}y_{47}y_{48}y_{49}\dots\dots \\ 5 &\to 0, y_{51}y_{52}y_{53}y_{54}y_{55}y_{56}y_{57}y_{58}y_{59}\dots\dots \\ 6 &\to 0, y_{61}y_{62}y_{63}y_{64}y_{65}y_{66}y_{67}y_{68}y_{69}\dots\dots \\ 7 &\to 0, y_{71}y_{72}y_{73}y_{74}y_{75}y_{76}y_{77}y_{78}y_{79}\dots\dots \\ &\vdots \end{aligned}$$

Où les y_{ij} représentent les différentes décimales des nombres de l'intervalle $(0,1)$. Nous allons maintenant montrer qu'il y a au moins un nombre de $(0,1)$ qui ne fait pas parties de notre suite, contredisant notre hypothèse. Considérons le nombre :

$$z = w_1w_2w_3w_4w_5w_6w_7w_8w_9\dots.$$

avec

$$w_i = \begin{cases} 1 & \text{si } y_{ii} \neq 1 \\ 2 & \text{si } y_{ii} = 1 \end{cases} \tag{3.1}$$

Ce nombre ne fait pas parti de la suite, car la i-ième décimale de z est toujours différente de la i-ième du i-ième nombre de notre suite. Il n'existe donc pas de fonction bijective entre $\mathbb{N}$ et $(0,1)$. En conséquence, il n'y a pas non plus de fonction bijective entre $\mathbb{N}$ et $\mathbb{R}$. □

Le théorème de Cantor que nous venons d'énoncer signifie en quelques sorte qu'il y a beaucoup plus de nombres réels que de nombres rationnels. Beaucoup plus que ce que l'on peut imaginer.

Definition 3.8.4. On définit la cardinalité de l'ensemble des nombres réels comme étant $\mathfrak{c}$, pour continuum, écrit en style gothique.

Il existe un lien curieux entre les deux types d'infinie que nous venons de voir. Il est possible de démontrer que $\mathfrak{c} = 2^{\aleph_0}$. Nous ne démontrerons cependant pas ce résultat. Il est cependant important de comprendre qu'il existe différent type d'infinie. Ce domaine des mathématiques porte le nom d'étude des cardinaux transfinies. L'une des grandes questions des mathématiques du XX^e siècle fut de déterminer s'il existe un cardinal entre $\aleph_0$ et $\mathfrak{c}$. Ce n'est qu'en 1963 que Paul Cohen détermina qu'il est impossible de répondre à cette question en utilisant les axiomes habituels des mathématiques. Ce problème porte aujourd'hui le nom d'hypothèse du continue.

Hypothèse du continue : Il n'existe aucun ensemble A tel que $\aleph_0 < |A| < \mathfrak{c}$.

Comme il est impossible de démontrer si cette hypothèse est vraie ou fausse, il s'agit donc d'un axiome que l'on peut choisir d'accepter ou non sans introduire de nouveaux paradoxes. Il existe donc au moins deux mathématiques différentes et cohérentes.

3.9 L'inverse d'une fonction

Nous allons maintenant nous intéressé à la question de l'inverse d'une fonction. Nous allons approcher le problème de deux manières différentes, qui en apparence sont contradictoire, mais les deux approches sont en fait directement relié.

Definition 3.9.1. Supposons A et B sont des ensembles, $f : A \to B$ une fonction, et $y \in B$. Alors on peut définir l'ensemble inverse $f^{-1}(y)$ comme étant :

$$f^{-1}(y) = \{x \in A : f(x) = y\}$$

Remarquez que pour chaque $y \in B$, alors $f^{-1}(y)$ est un sous-ensemble de A. Il est donc important de réaliser que selon cette définition, $f^{-1} : B \to A$ n'est pas une fonction car $f^{-1}(y)$ n'est pas une valeur de A, mais bien un sous-ensemble de A.

Definition 3.9.2. Si $f : A \to B$ est une fonction, alors on dit que f est inversible s'il existe une fonction $g : B \to A$ telle que $(g \circ f)(x) = x$ pour tout $x \in A$ et $(f \circ g)(y) = y$ pour tout $y \in B$. Dans ce cas, on définit $f^{-1} = g$.

Cette dernière définition est normalement celle avec laquelle vous êtes familier. Remarquez cependant que ceci nous donne donc deux définitions différentes pour f^{-1} dans le cas où la fonction est inversible. Ceci ne crée cependant pas de difficulté si on considère équivalent un élément, et un ensemble contenant uniquement cet élément :

$$x \quad \leftrightarrow \quad \{x\}$$

Théorème 3.9.1. Une fonction f est bijective si et seulement si elle est inversible.

Exemple 3.9.1. Considérons la fonction $f : \mathbb{R} \to \mathbb{R}^+$ définie par $f(x) = x^2$, alors $f^{-1}(4) = \{-2, 2\}$. En particulier f^{-1} n'est pas une fonction car pour une valeur en entré, on obtient deux valeurs en sortie. Le problème vient du fait que la fonction f n'est pas injective. On peut donc affirmer que f n'est pas une fonction inversible.

Exemple 3.9.2. Considérons la fonction $f : \mathbb{R}^+ \to \mathbb{R}$ définie par $f(x) = x^2$, alors $f^{-1}(-4) = \varnothing$. En particulier f^{-1} n'est pas une fonction car pour une valeur en entré, on obtient aucune valeurs en sortie. Le problème vient du fait que la fonction f n'est pas surjective. On peut donc affirmer que f n'est pas une fonction inversible.

Exemple 3.9.3. Considérons la fonction $f : \mathbb{R}^+ \to \mathbb{R}^+$ définie par $f(x) = x^2$. Dans ce cas, la fonction est bijective, ce qui nous permet d'affirmer qu'elle est inversible. Il n'est pas très difficile de voir que sa fonction inverse est $f^{-1}(x) = \sqrt{x}$. Notez cependant que si on considère la première définition, on obtient $f^{-1}(4) = \{2\}$, alors que selon la seconde définition on obtient $f^{-1}(4) = 2$. Comme la fonction est bijective, la première définition nous donnera cependant toujours un ensemble contenant un seul élément. Il est donc toujours possible d'associer cet ensemble à la valeur qu'elle contient pour réconcillier ces deux définitions.

Chapitre 4

L'arithmétique

4.1 La divisibilité

Nous allons maintenant nous intéressé à étudier plus en détail les propriétés de l'ensemble des nombres naturels et l'ensemble des entiers. Dans les cours de calcul, on est habituellement intéressé à étudier des les propriétés des fonctions qui sont définies sur l'ensemble des nombres réels. Travailler avec les nombres naturels et entiers peut donc sembler un peu restrictif. Ce n'est cependant absolument pas le cas. Plusieurs propriétés peuvent être étudier dans les entiers, sans quelle puissent être définie dans les nombres réels. L'une des propriétés fondamentales des nombres naturels qui a de très nombreuses conséquences est l'axiome du bon ordre qui nous affirme que tout sous ensemble S de nombres naturels possède un minimum. Cette propriété est évidement fausse si on remplace les nombres naturels par un ensemble plus grand tel que les entiers, les rationnels, les réels ou les complexes. Bien que nous n'étudierons pas en détail cette propriété dans ce cours, sachez quelle est omniprésente dans plusieurs démonstration que nous allons rencontrer dans ce chapitre.

La première propriété que nous allons étudier en détail est la divisibilité. Dans les nombres naturels ($\mathbb{N}$), ou même dans les nombres entiers ($\mathbb{Z}$), il n'est pas toujours possible de diviser deux nombres. Si a et b sont deux nombres naturels avec $b \neq 0$, alors nous dirons intuitivement que b est divisible par a si le résultat de la division $b \div a$ est un nombre entier. Nous avons cependant besoin d'une définition plus formelle, qui n'utilise pas une opération qui n'est pas toujours définie dans les nombres naturels ou entiers.

Definition 4.1.1. Si $a, b \in \mathbb{Z}$, alors a divise b s'il existe un nombre $k \in \mathbb{Z}$ tel que $ak = b$. Nous écrirons alors $a|b$ (i.e. a divise b). De la même façon, si b n'est pas divisible par a, nous écrirons $a \nmid b$ (i.e. a ne divise pas b).

Exemple 4.1.1. Voici quelques exemples pour illustrer la définition précédente :

1. On a que $3|27$, car $3 \times 9 = 27$
2. On a que $7|49$, car $7 \times 7 = 49$
3. On a que $18 \nmid 38$, car $18 \times 2 = 36 < 38$ et $18 \times 3 = 54 > 38$

Voici maintenant un théorème énonçant certaines propriétés élémentaires de la divisibilité. Notez qu'ici les résultats du théorème sont relativement simples, et même peuvent sembler évident. Ce qui nous intéresse est surtout leur démonstration.

Théorème 4.1.1. Voici quelques propriétés de la divisibilité :

1. Si $a \in \mathbb{Z}$, alors $a|a$. C'est à dire que la relation est réflexive.
2. Si $a, b, c \in \mathbb{Z}$ sont tels que $a|b$ et $b|c$, alors $a|c$. C'est à dire la relation est transitive.
3. Si $a, b \in \mathbb{Z}$ sont tels que $a|b$ et $b|a$, alors $a = \pm b$.
4. Si $a, b, c \in \mathbb{Z}$ sont tels que $a|b$, alors $a|(bc)$.
5. Si $a, b, c, d, e \in \mathbb{Z}$ sont tels que $a|b$ et $a|c$, alors $a|(bd + ce)$.

Démonstration.

1. Cette partie est laissée en exercice.
2. Cette partie est laissée en exercice.
3. Cette partie est laissée en exercice.
4. Comme $a|b$, alors il existe un entier k tel que $ak = b$. On a donc $bc = akc = a(kc)$. Comme kc est un entier, alors $a|(bc)$.
5. Comme $a|b$ et $a|c$, alors il existe des entiers m, n tels que $am = b$ et $an = c$. On obtient donc :

$$bd + ce = amd + and = a(md + nd)$$

ce qui nous donne $a|(bd + ce)$.

□

Théorème 4.1.2. La relation de divisibilité sur les nombres naturels ($\mathbb{N}$) est une relation d'ordre partielle qui n'est pas une relation d'ordre.

Démonstration. Nous savons déjà que la relation de divisibilité sur les nombres entiers est réflexive et transitive. Elle doit donc aussi l'être sur les nombres naturels. La démonstration de l'antisymétrique est laissé en exercice. Finalement, pour montrer qu'il ne s'agit pas d'une relation d'ordre, il suffit de remarque que 2 et 3 sont des nombres naturels, mais $2 \nmid 3$ et $3 \nmid 2$. □

Remarquez finalement que la relation de divisibilité n'est pas une relation d'ordre partielle sur les nombres entiers ($\mathbb{Z}$) car elle n'est pas antisymétrique. Par exemple, remarquons que $-2|2$ et $2|(-2)$, mais $2 \neq -2$.

4.2 La division euclidienne

Nous allons maintenant introduire la division euclidienne. Il s'agit en quelque sorte d'effectuer la division avec reste que vous avez probablement déjà vu au primaire. Si a et b sont deux nombres naturels et $b \neq 0$, alors la division euclidienne de a par b est $a = br + q$ où r et q sont deux nombres naturels, et $0 \leq q < b$. On peut comprendre cette idée comme étant $a \div b = r$ reste q. N'oubliez pas que lorsque l'on parle d'entiers, il n'est pas question de travailler avec des fractions, celles ci n'existent pas en quelque sorte.

Théorème 4.2.1. **(Division euclidienne)** Si $a, b \in \mathbb{Z}$ avec $b > 0$, alors il existe des entiers q et r avec $0 \leq r < b$ tel que :

$$a = bq + r$$

Démonstration. Considérons l'ensemble $S = \{a - bq : q \in \mathbb{Z}, a - bq \geq 0\}$. Comme $S \subseteq \mathbb{N}$ et $S \neq \emptyset$. Alors, il existe un plus petit élément $r_0 \in S$ (ici nous avons utilisé la propriété du bon ordre). Donc $r_0 = a - bq_0$, que l'on peut écrire sous la forme $a = bq_0 + r_0$. Il est clair que $r_0 \geq 0$, on doit donc montrer que $r_0 < b$. Supposons au contraire que $r_0 \geq b$. Alors

$$r_1 = a - b(q_0 + 1) = a - bq_0 - b = r_0 - b \geq 0$$

Donc $r_1 \in S$ et $r_1 < r_0$ ce qui est une contradiction. Donc $0 \leq r_0 < b$. □

Exemple 4.2.1. Effectuez la division euclidienne de 28 par 3. On doit donc trouver le plus grand entier q tel que $3q < 28$. Il est facile de voir que $q = 9$, ce qui nous donne $r = 28 - 3(9) = 1$. La division euclidienne nous donne donc $28 = 3(9) + 1$.

La division euclidienne est particulièrement utile pour démontrer des théorèmes en lien avec la divisibilité. Remarquer que si a est divisible par b, alors le reste de la division euclidienne doit obligatoirement être 0.

Exemple 4.2.2. On veut démontrer que le carré d'un nombre impair est toujours un nombre impair. Pour ce faire, remarquons que si n est un nombre impair, alors $n = 2k+1$ où k est un entier (Il s'agit de la définition d'un nombre impair). On obtient donc :

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

En posant $m = 2k^2 + 2k$, on remarque que m est un entier et $n^2 = 2m + 1$. On peut donc conclure que n^2 est aussi un nombre impair.

4.3 Le plus grand commun diviseur

Nous allons maintenant tourner notre attention sur le concept du plus grand commun diviseur, que l'on dénote habituellement par PGCD (ou GCD en anglais de greatest common divisor) ou tout simplement à l'aide de parenthèse.

Definition 4.3.1. Si a et b sont des nombres entiers non nuls, alors le PGCD de a et b, dénoté (a, b) ou $\text{PGCD}(a, b)$ est le plus grand nombre naturel qui divise à la fois a et b.

Exemple 4.3.1. On veut trouver le PGCD de 58 et 132. Nous allons donc commencer par énumérer tous les diviseurs de chacun de ces deux nombres. Les diviseurs de 58 sont :

$$\{1, 2, 29, 58\}$$

Et les diviseurs de 132 sont :

$$\{1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132\}$$

On peut donc remarquer que le plus grand diviseur que les deux nombres ont en commun est 2.

Remarquez que bien que l'exemple précédent ne soit pas très difficile, énumérer tous les diviseurs peut prendre beaucoup de temps, en particulier si les nombres sont grands. Nous allons donc devoir d'ici la fin de cette section développer une méthode plus efficace pour calculer le PGCD.

Théorème 4.3.1. **(Lemme de Bézout)** Si a et b sont deux entiers non nuls, alors il existe des entiers x, y tel que

$$ax + by = (a, b)$$

Démonstration. Considérons l'ensemble $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. Par la propriété du bon ordre, il existe dans S un plus petit élément que nous appellerons s. Donc

$$s = ax_0 + by_0$$

On veut montrer que $s = (a,b)$. Supposons que s ne divise pas a. Alors par la division euclidienne on a $a = sq + r$ avec $0 < r < s$. Donc :

$$r = a - sq = a - (ax_0 + by_0)q = a - aqx_0 - bqy_0 = a(1 - qx_0) - b(qy_0)$$

Donc $r \in S$, et $r < s$ ce qui est une contradiction (s est le plus petit élément de S). Donc $s|a$. De la même manière, on montre que $s|b$. Donc s est bien un diviseur commun de a et b. On veut maintenant montrer qu'il s'agit du plus grand. Supposons que c est un diviseur quelconque de a et b, alors $c|(ax + by)$ pour tout $x, y \in \mathbb{Z}$, donc en particulier $c|s$, donc $c \leq s$. On peut donc conclure que $s = (a,b)$. □

Théorème 4.3.2. Si $a, b, c, k \in \mathbb{Z}$ et $d = (a,b)$ alors on a :

1. $\{ax + by : x, y \in \mathbb{Z}\}$ est l'ensemble des multiples de $d = (a,b)$.
2. Si $c|a$ et $c|b$, alors $c|(a,b)$.
3. $(a, b + ka) = (a,b) = (a, -b)$.
4. $(ka, kb) = |k|(a,b)$.
5. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Démonstration.

1. Posons $d = (a,b)$, $S = \{ax + by : x, y \in \mathbb{Z}\}$ et $T = \{kd : k \in \mathbb{Z}\}$. Commençons par montrer que $S \subseteq T$. Pour ce faire, prenons $s \in S$, où $s = ax_1 + by_1$. Comme $d|a$ et $d|b$ par définition du PGCD, alors $d|(ax_1 + by_1)$ et donc $d|s$. On a donc $S \subseteq T$. Maintenant, pour l'autre inclusion, prenons $t \in T$, donc $t = kd$. Comme d est le PGCD de a et b, alors il existe des entiers x_1, y_1 tels que $d = ax_1 + by_1$, ce qui nous donne :

   $$t = kd = k(ax_1 + by_1) = a(kx_1) + b(ky_1) \in S$$

   Donc $T \subseteq S$. On peut donc conclure que $S = T$, et donc l'ensemble S est bien l'ensemble des multiples de $d = (a,b)$.

2. Comme $c|a$ et $c|b$, il existe des entiers $k_1, k_2 \in \mathbb{Z}$ tel que $ck_1 = a$ et $ck_2 = b$. De plus, par le lemme de Bézout, il existe des entiers x, y tel que $ax + by = (a,b)$. On obtient donc :

   $$(a,b) = ax + by = ck_1x + ck_2y = c(k_1x + k_2y)$$

   Ce qui nous permet de conclure que $c|d$.

3. Posons $d_1 = (a, b + ka)$. Par définition, on a donc que $d_1|a$ et $d_1|(b + ka)$. Il existe donc des entiers m, n tels que $d_1m = a$ et $d_1n = b + ka$ donc :

   $$d_1n = b + ka = b + k(d_1m) = b + kd_1m \Longrightarrow b = d_1n - kd_1m = d_1(n - km)$$

   on a donc que $d_1|b$ et donc $d_1|(a,b)$. Maintenant, posons $d_2 = (a,b)$ donc par hypothèse, $d_2|a$ et $d_2|b$, ce qui nous donne que $d_2|b + ka$ et donc $d_2|(a + b + ka)$. Comme $d_1|d_2$, $d_2|d_1$ et que ces deux nombres sont positifs, alors $d_1 = d_2$, ce qui démontre la première égalité. La deuxième égalité est laissée en exercice.

4. Commençons par poser $d = (a,b)$ et supposons que $k \geq 0$. On a donc que $d|a$ et $d|b$ ce qui implique que $dk|ak$ et $dk|bk$. On a donc que $dk|(bk, ak)$. Il existe donc un entier s tel que $dks = (bk, ak)$, ce qui signifie que $dks|bk$ et $dks|ak$, et donc $ds|b$ et $ds|a$. Par définition du PGCD, on obtient donc que $s = 1$, ce qui signifie que

   $$dk = (bk, ak)$$

   La preuve lorsque $k < 0$ est semblable et est laissée en exercice.

5. En supposons que $d = (a, b)$ et $x = \left(\frac{a}{d}, \frac{b}{d}\right)$, on a donc :

$$dx = d\left(\frac{a}{d}, \frac{b}{d}\right) = |d|\left(\frac{a}{d}, \frac{b}{d}\right) = (a, b) = d$$

donc $dx = d$ ce qui implique que $x = 1$. On peut donc conclure que

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

□

L'algorithme d'Euclide est une méthode relativement simple pour calculer le PGCD de deux nombres. La méthode fait appel à la division euclidienne.

Théorème 4.3.3. (Algorithme d'Euclide) Si a et b sont des entiers non nuls tel que $a > b$. Posons $r_0 = b$ et $r_1 = a$, et on définie récursivement à l'aide de la division euclidienne :

$$r_{k-2} = q_k r_{k-1} + r_k, \quad \forall k \geq 2$$

Alors il existe un plus petit n tel que $r_n = 0$, et dans ce cas, $r_{n-1} = (a, b)$.

Démonstration. Par définition de la division euclidienne, chaque r_k doit être tel que $0 \leq r_k < r_{k-1}$. Il doit donc exister un plut petit n tel que $r_n = 0$. Maintenant, par le théorème précédant, nous avons aussi que :

$$(r_{k-1}, r_k) = (r_{k-1}, r_{k-2} - q_k r_{k-1}) = (r_{k-1}, r_{k-2}) = (r_{k-2}, r_{k-1})$$

Donc en particulier, nous avons que :

$$(a, b) = (r_{n-2}, r_{n-1}) = r_{n-1}$$

Car r_{n-2} est divisible par r_{n-1}. □

Nous allons illustrer la méthode à l'aide d'un exemple, il nous sera alors plus facile de l'expliquer.

Exemple 4.3.2. On veut à nouveau trouver le PGCD entre 58 et 132. On commence par trouver la division euclidienne entre ces deux nombres, ce qui nous donne :

$$132 = 2(58) + 16$$

On fait à nouveau la division euclidienne, mais cette fois ci en utilisant les nombres 58 et 16, ce qui nous donne :

$$58 = 3(16) + 10$$

Et on fait de même avec 16 et 10, ce qui nous donne :

$$16 = 1(10) + 6$$

Puis avec 10 et 6 :

$$10 = 1(6) + 4$$

Et avec 6 et 4 :

$$6 = 1(4) + 2$$

et finalement avec 4 et 2 :

$$4 = 2(2) + 0$$

La méthode se termine alors car nous avons obtenu un reste de 0. Le PGCD est alors le reste de la division qui précède la dernière. On remarque que la réponse est bien 2 comme nous avions déjà trouvé.

Bien que la méthode puisse sembler compliquée, elle est en fait beaucoup plus rapide (et facile) lorsque les nombres sont grands. Voici un autre exemple de calcul de PGCD :

Exemple 4.3.3. On veut trouver le PGCD de 1578 et 456. En appliquant l'algorithme d'Euclide on obtient :

$$\begin{aligned} 1578 &= 3(456) + 210 \\ 456 &= 2(210) + 36 \\ 210 &= 5(36) + 30 \\ 36 &= 1(30) + 6 \\ 30 &= 5(6) + 0 \end{aligned}$$

Le PGCD est donc le reste de l'avant dernière ligne. Le PGCD est donc 6. Vous pouvez vérifier en énumérant tous les diviseurs de chacun des deux nombres, mais vous verrez que ce sera beaucoup plus long.

Nous avons vu au début de cette section que si a et b sont des entiers non nuls et $d = (a, b)$, alors il existe des entiers x, y tels que

$$ax + by = d$$

Nous allons maintenant utiliser l'algorithme d'Euclide que nous venons de voir pour trouver une valeur de x et y qui satisfont cette équation. Il s'agit en fait de réécrire l'algorithme d'Euclide à l'envers comme l'illustre les deux exemples ci-dessous. Remarquez qu'il y a en général plus d'une solution possible pour x et y. Par contre, une seule solution nous sera suffisante pour le moment. Nous verrons plus tard comment faire pour trouver toutes les autres.

Exemple 4.3.4. On veut trouver des entiers m et n tels que $14m + 20n = (14, 20)$. L'algorithme d'Euclide nous donne :

$$\begin{aligned} 20 &= 1(14) + 6 \\ 14 &= 2(6) + 2 \\ 6 &= 3(2) + 0 \end{aligned}$$

Le PGCD est donc 2. En appliquant l'algorithme à l'envers, nous avons :

$$\begin{aligned} 2 &= 14 - 2(6) \\ &= 14 - 2(20 - 1(14)) \\ &= 14 - 2(20) + 2(14) \\ &= 3(14) - 2(20) \end{aligned}$$

Exemple 4.3.5. Trouvez des entiers m et n tels que $1144m+462n = (1144, 462)$. On commence par appliquer l'algorithme d'Euclide :

$$\begin{aligned} 1144 &= 2(462) + 220 \\ 462 &= 2(220) + 22 \\ 220 &= 10(22) + 0 \end{aligned}$$

Le PGCD est donc 22. Maintenant, pour trouver les valeurs de m et n, on a :

$$\begin{aligned} 22 &= 462 - 2(220) \\ &= 462 - 2(1144 - 2(462)) \\ &= 462 - 2(1144) + 4(462) \\ &= 5(462) - 2(1144) \end{aligned}$$

Ce qui nous donne : $m = -2$ et $n = 5$.

Théorème 4.3.4. (Lemme d'Euclide)

1. Si a, b sont des entiers non nuls pour lesquels il existe des entiers x, y tels que $ax + by = 1$, alors $(a, b) = 1$.
2. Si a, b, c sont des entiers tels que $a|bc$ et $(a, b) = 1$, alors $a|c$.

Démonstration.

1. Supposons que $ax + by = 1$ et posons $d = (a, b)$, alors $d|(ax + by)$, donc $d|1$. Maintenant, comme $d \geq 1$, alors on doit conclure que $d = 1$.
2. Comme $a|bc$, alors il existe un entier k tel que $ak = bc$. De plus, comme $(a, b) = 1$, alors il existe des entiers x, y tels que $ax + by = 1$, ce qui nous donne, en multipliant des deux côtés par c,

$$acx + bcy = c$$

On obtient donc finalement que :

$$c = acx + bcy = acx + aky = a(cx + ky)$$

on peut donc conclure que $a|c$.

□

Notez que des entiers a, b tel que $(a, b) = 1$ sont important et apparaissent souvent dans les théorèmes de la théorie des nombres comme par exemple dans le théorème d'Euclide que nous venons de démontrer. Ils sont suffisament important pour leur donner un nom. De tel entier s'appellent entiers copremiers.

4.4 Le plus petit commun multiple

Une autre notion en lien avec le PGCD est celle du plus petit commun multiple, que l'on dénote habituellement par PPCM (en anglais on parlera de LCD pour least common multiple). Si n est un nombre entier, alors un multiple de n est un nombre de la forme kn où k est aussi un nombre entier.

Definition 4.4.1. Si a et b sont des entiers non nuls, alors on définit le plus petit commun multiple de a et b dénoté $PPCM(a, b)$ ou bien $[a, b]$ comme étant le plus petit entier positif (i.e. nombre naturel) qui est à la fois un multiple de a et de b.

Exemple 4.4.1. Les nombres suivants sont des multiples de 3 :

$$3, 6, 9, 12, 15, 18, 21, 24, ...$$

Si a et b sont deux entiers positifs non nuls, alors le plus petit commun multiple (PPCM) de a et b est le plus petit nombre qui est à la fois multiple de a et de b. Une première méthode pour trouver le PPCM est d'énumérer quelques multiples de chacun des nombres, et d'identifier le plus petit qui est commun. Ceci est illustré dans l'exemple suivant :

Exemple 4.4.2. On veut trouver le PPCM de 14 et 20. On va donc énumérer les premiers multiples de chacun de ces deux nombres. Pour 14 on a :

$$14, 28, 42, 56, 70, 84, 98, 112, 126, 140, 154, 168, 182, 196, 210, ...$$

et pour 20 nous avons :

$$20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 260, 280, 300, ...$$

On remarque que le plus petit nombre que ces deux suites ont en commun est 140. Il s'agit donc du PPCM.

Remarquez que la méthode précédente n'est pas très efficace. Dans certain cas il peut être nécessaire d'énumérer une longue liste de multiples avant d'en trouver un en commun. Par contre, le théorème suivant nous aidera dans nos calculs

Théorème 4.4.1. Si a et b sont des nombres naturels, alors :

1. $[a,b] \leq ab$.
2. Si $k \in \mathbb{N}$ est tel que $a|k$ et $b|k$, alors $[a,b]|k$
3. Si $k \in \mathbb{N}$, alors $[ka,kb] = k[a,b]$
4. On a la relation suivante entre le PGCD et le PPCM : $[a,b] = \dfrac{ab}{(a,b)}$.

Démonstration.

1. Il s'agit de remarquer que $a|(ab)$ et $b|(ab)$. Le produit ab est donc un multiple commun à a et b. Le plus petit commun multiple doit donc être plus petit ou égal à ce dernier.
2. Supposons que m est le plus petit commun multiple de a et b, alors on peut calculer la division euclidienne de k par m, ce qui nous donne :

   $$k = mq + r, \qquad 0 \leq r < m$$

   ce qui peut être réécrit comme $r = k - mq$. Comme $a|k$ et $a|m$, alors $a|r$. De plus, comme $b|k$ et $b|m$, alors $b|r$. Donc r est un multiple commun de a et b qui est plus petit que le plus petit commun multiple m de a et b, ce qui est une contradiction si $r \neq 0$. Donc $k = mq$ pour un entier q, donc $m|k$.
3. Posons $m = [a,b]$ et $M = [ka,kb]$. Comme m est un multiple de a et b, alors km est un multiple de ka et kb, donc par la partie précédente $M|km$ et donc en particulier $M \leq km$. De plus, comme M est un multiple de ka et kb, alors $\dfrac{M}{k}$ est un multiple de a et b, donc $m\left|\dfrac{M}{k}\right.$, donc en particulier $m \leq \dfrac{M}{k}$, ou de façon équivalente : $mk \leq M$. On a donc :

   $$M \leq km \text{ et } km \leq M$$

   Ce qui implique que $M = km$.
4. Supposons premièrement que $(a,b) = 1$, et posons $[a,b] = m$. Donc m est un multiple de a, ce qui signifie qu'il existe un entier x tel que $m = ax$. De plus, m est aussi un multiple de b, donc $b|ax$. Comme par hypothèse $(a,b) = 1$, alors on a $b|x$, donc il existe un entier y tel que $by = x$ ce qui nous donne :

   $$m = ax = aby$$

   Maintenant par la première partie du théorème, on a que $m \leq ab$ et que $y \geq 1$, alors $y = 1$ ce qui nous donne $m = [a,b] = ab$. Ce qui démontre le théorème dans le cas ou a et b sont des entiers copremiers. Supposons maintenant que $(a,b) = d$. Dans ce cas, on a que $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, ce qui nous donne

   $$[a,b] = d\left[\frac{a}{d}, \frac{b}{d}\right] = d\frac{ab}{d^2} = \frac{ab}{d} = \frac{ab}{(a,b)}$$

   ce qui complète la démonstration si a et b sont positifs.

□

Exemple 4.4.3. Le PPCM de 14 et 20 est nécessairement plus petit (par le théorème précédent) que $14 \times 20 = 280$. Lorsque nous avons calculé la valeur exacte du PPCM, nous avons obtenu 140, ce qui est effectivement plus petit ou égal à 280.

Nous pouvons donc utiliser l'algorithme d'Euclide pour calculer le PPCM. Nous allons donc refaire l'exemple précédent, mais cette fois-ci en utilisant l'algorithme.

Exemple 4.4.4. On veut trouver le PPCM de 14 et 20. Pour ce faire, nous allons commencer par trouver le PGCD de ces deux nombres en utilisant l'algorithme d'Euclide :

$$\begin{aligned} 20 &= 1(14) + 6 \\ 14 &= 2(6) + 2 \\ 6 &= 3(2) + 0 \end{aligned}$$

Le PGCD est donc 2. En applicant la formule du théorème, on peut maintenant calculer le PPCM :

$$[14, 20] = \frac{14 \times 20}{(14, 20)} = \frac{280}{2} = 140$$

Nous obtenons donc la même réponse.

Exemple 4.4.5. On veut trouver le PPCM de 786 et 524. En appliquant l'algorithme d'Euclide, on obtient :

$$\begin{aligned} 786 &= 1(524) + 262 \\ 524 &= 2(262) + 0 \end{aligned}$$

Le PGCD est donc 262. En appliquant la formule, on obtient maintenant :

$$[786, 524] = \frac{786 \times 524}{(786, 524)} = \frac{786 \times 524}{262} = 1572$$

Exemple 4.4.6. Supposez que a est un entier positif non nul. Si $(a, 598) = 23$ et $[a, 598] = 20930$, quelle est la valeur de a ? Pour ce faire, nous avons tout simplement à appliquer le théorème 4.4, ce qui nous donne :

$$\begin{aligned} [a, 598] &= \frac{598a}{(a, 598)} \\ 20930 &= \frac{598a}{23} \\ 20930 &= 26a \end{aligned}$$

Ce qui nous donne $a = 805$.

Finalement, remarquez que comme dans le cas du PGCD, il est aussi possible de définir le PPCM de plus que deux nombres. Par exemple, si a, b et c sont des entiers, alors on définit le PPCM de ces trois nombres, dénoté $[a, b, c]$ comme étant le plus petit nombre entier m tel que $a|m$, $b|m$ et $c|m$. Comme exercice, vous pouvez essayer de relier le PPCM de trois nombres avec le PGCD de ces mêmes trois nombres.

4.5 Les nombres premiers

Nous allons maintenant aborder le concept des nombres premiers. Ces derniers servent à construire n'importe quel nombre naturel plus grand ou égal à deux. Un nombre naturel a plus grand ou égal à deux est appelé un **nombre premier** si les seuls diviseurs de a sont 1 et a. Autrement dit un nombre est premier s'il a exactement deux diviseurs (les deux diviseurs doivent être différent). Un nombre naturel est dit composé, s'il a plus que deux diviseurs, autrement dit, un nombre naturel plus grand ou égal à deux est composé s'il n'est pas premier. Faites attention, les nombres naturels 0 et 1 sont différents. Ils ne sont ni composé, ni premier. Ils forment une classe à part dans l'ensemble des nombres naturels.

Nous allons commencer par réécrire le lemme d'Euclide (i.e. théorème 4.3) pour le cas des nombres premiers :

Théorème 4.5.1. **(Lemme d'Euclide)** Supposons que p est un nombre premier, et a, b sont des entiers non nul. Si $p|(ab)$ alors $p|a$ ou $p|b$.

Démonstration. Si $p|a$, alors le théorème est automatiquement vrai (il s'agit de l'une des conclusions du théorème), alors on va supposer que p ne divise pas a. Comme les seuls diviseurs de p sont 1 et p, alors le $\text{PGCD}(p, a) = 1$. Ceci est vrai car le PGCD doit obligatoirement par définition être un diviseur des deux nombres, et p n'est pas un diviseur de a par hypothèse. On a donc que $p|(ab)$ et $\text{PGCD}(a, p) = 1$. On peut donc appliquer le lemme d'Euclide ce qui nous donne que $p|b$. Le théorème est donc vrai. □

Remarquez que l'hypothèse que p est un nombre premier est très importante dans le théorème précédent. Si p n'est pas premier, le théorème ne fonctionne pas toujours. Par exemple, nous avons que 4 divise le produit 14×18, mais 4 ne divise pas 14 ni 18. Nous allons maintenant énoncer (et démontrer) l'un des résultats les plus importants de l'antiquité.

Théorème 4.5.2. **(Théorème fondamental de l'arithmétique)** Tout nombre naturel n plus grand ou égal à 2 peut s'écrire comme un produit de nombres premiers. De plus ce produit est unique si on ordonne les membres du produit en ordre croissant.

Démonstration. Nous voulons premièrement montrer que si n est un nombre naturel non nul, alors n peut s'écrire comme produit de nombre premier. Si n est déjà un nombre premier, alors nous avons terminé. Sinon, par définition d'un nombre composé, on peut écrire n sous la forme d'un produit a_1a_2. Avec a_1, a_2 tous deux plus grand que 1, mais plus petit que n. Ensuite nous répétons la même étape avec les nombres a_1 et a_2. S'ils sont tous deux premiers, alors nous avons terminé. Sinon, nous pouvons les écrire à nouveau comme un produit. En continuant de la même façon, nous obtiendrons éventuellement un produit de nombres premiers.

Maintenant, pour montrer que le produit est unique, nous allons supposer le contraire (preuve par contradiction). Supposons que le nombre n peut s'écrire des deux façons suivantes comme produit de nombres premiers :

$$n = p_1p_2p_3...p_r = q_1q_2q_3...q_s$$

Nous avons donc que p_1 doit diviser le produit $q_1q_2q_3...q_s$, et comme p_1 est un nombre premier, alors il doit diviser l'un des q_i. Par contre, comme ce q_i est aussi premier, nous n'avons pas le choix $p_1 = q_i$. En refaisant la même étape pour tous les p_j, nous obtenons alors que tous les membres du produit doivent être identiques, sauf peut être pour l'ordre dans lequel ils sont écrits. Si on les placent en ordre croissant, les deux produits seront alors identiques. □

La question qui se pose maintenant, est comment faire pour écrire un nombre donné sous forme d'un produit de nombres premiers. L'idée se trouve en fait dans le théorème précédent. Nous allons illustrer le processus par un exemple :

Exemple 4.5.1. On veut factoriser le nombre 1176 sous forme d'un produit de nombres premiers. Premièrement remarquons que 1176 peut être divisé par 4, on peut donc écrire

$$1176 = 4 \times 294$$

Maintenant, nous savons que $4 = 2 \times 2$ et on remarque que 294 peut être divisé par 3, nous avons donc :

$$1176 = (2 \times 2) \times (3 \times 98)$$

On remarque alors que 98 est encore une fois divisible par deux, ce qui nous donne :

$$1176 = 2 \times 2 \times 3 \times (2 \times 49)$$

En continuant de la même manière, on remarque que $49 = 7 \times 7$, ce qui nous donne finalement :

$$1176 = 2 \times 2 \times 3 \times 2 \times (7 \times 7)$$

Pour compléter, nous allons tout simplement ordonner les membres du produit en ordre croissant de sorte que la factorisation soit unique. Notre réponse finale est donc :

$$1176 = 2 \times 2 \times 2 \times 3 \times 7 \times 7$$

Dans le chapitre suivant, nous allons voir quelques critères pour tester la divisibilité, ce qui va nous aider à trouver la factorisation d'un nombre sous forme d'un produit de nombres premiers. Maintenant que nous avons vu que tout nombre naturel plus grand ou égal à 2 peut s'écrire comme un produit de nombres premiers, la question suivante qui se pose est combien y a-t-il de nombres premiers ? Encore une fois, la réponse a été fournie par Euclide et son école durant l'Antiquité.

Théorème 4.5.3. **(Euclide)** Il existe un infinité de nombre premier

Démonstration. Nous allons supposer le contraire. Supposons qu'il existe seulement un nombre fini de nombres premiers, c'est à dire que $p_1, p_2, p_3, ..., p_k$ sont les seuls nombres premiers existants. Considérons maintenant le nombre

$$N = p_1 p_2 ... p_k + 1$$

Ce nombre est clairement plus grand que chacun des nombres $p_1, ..., p_k$. Si les p_i sont les seuls nombres premiers existants, alors N doit obligatoirement être divisible par certain d'entres eux, sinon il serait un nombre premier. Pourtant nous allons montrer qu'aucun des p_i ne divise N. Supposons que p_i divise N, alors on peut trouver un entier m tel que $mp_i = N$, c'est à dire que nous avons :

$$mp_i = p_1 p_2 ... p_k + 1$$

En déplaçant les termes, nous obtenons donc que

$$mp_i - p_1 p_2 ... p_k = 1$$

puis en factorisant p_i à gauche, nous pouvons donc conclure que p_i doit diviser 1. Ce qui est bien entendu une contradiction. Donc aucun des p_i ne divise N. Il doit donc exister au moins un autre nombre premier. □

Remarquez que dans le théorème précédant, rien ne nous garanti que N est un nombre premier. Tout ce que nous avons montrer c'est qu'il doit exister un autre nombre premier que les $p_1, p_2, ..., p_k$. On appelle nombre premier d'Euclide un nombre premier de la forme

$$n = p_1 p_2 p_3 ... p_k + 1$$

Les premiers nombres premiers d'Euclide sont

$$3, 7, 31, 211, 2311, 30031, 510511, ...$$

On ne sait toujours pas à l'heure actuelle s'il existe une infinité de nombres premiers d'Euclide.

4.6 La crible d'Ératosthène

On est maintenant intéressé à savoir comment trouver une liste de nombres premiers, ou bien comment vérifier si un nombre est premier ou non. Le théorème suivant va nous aider dans cette direction.

Théorème 4.6.1. Si n est un entier plus grand ou égal à 2, et n n'est pas divisible par aucun nombre premier entre 2 et $\sqrt{n}$, alors n doit être premier.

Démonstration. Supposons que n n'est pas un nombre premier, alors il existe des entiers $a, b > 1$ tel que $n = ab$. Supposons que a, b sont tous deux plus grands que $\sqrt{n}$, alors on a :

$$n = ab > \sqrt{n}\sqrt{n} = n$$

ce qui est évidement une contradiction. Donc a ou b est plus petit ou égal à $\sqrt{n}$. □

Exemple 4.6.1. Nous allons maintenant utiliser cette méthode pour trouver tous les nombres premiers entre 2 et 25. Remarquez que $\sqrt{25} = 5$, donc un nombre entre 2 et 25 est premier s'il n'est pas divisible par un nombre premier entre 2 et 5. Il est facile de voir que les nombres premiers entre 2 et 5 sont $\{2, 3, 5\}$. Donc un nombre entre 2 et 25 est premier s'il n'est pas divisible par $2, 3$ ni 5. En éliminant tous les multiples de 2, 3 et 5, nous obtenons donc la liste suivante :

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$$

Exemple 4.6.2. Est ce que le nombre 223 est premier ? Pour ce faire, nous devons vérifier que 223 n'est pas divible par un nombre premier entre 2 et $\sqrt{223}$. Comme $\sqrt{223}$ est légèrement plus petit que 15, il nous suffit de vérifier que 223 n'est pas divisible par $2, 3, 5, 7, 11, 13$. Donc nous n'avons que 6 divisions à tester. Comme aucune de ces divisions nous donne un entier, on peut donc conclure que 223 est un nombre premier.

Chapitre 5

Les nombres modulos

5.1 Introduction aux nombres modulos

Dans le chapitre précédent, nous avons mis beaucoup d'efforts à étudier le concept de la divisibilité. Ceci nous a amené à étudier des concepts tels que les nombres premiers et le plus grand commun diviseur pour n'en nommer que deux. Ce qui est important est que l'outil de base dans l'étude de la divisibilité a été la division euclidienne, et plus particulièrement le reste de la division. Il aurait donc été possible de démontrer plusieurs théorèmes du chapitre précédent en utilisant seulement des informations concernant le reste de la division. C'est la théorie des nombres modulos qui va nous permettre de mettre cette idée de manière un peu plus formelle. Pour ce faire, nous allons introduire une relation d'équivalence sur l'ensemble des nombres entiers.

Definition 5.1.1. Si a, b sont deux entiers, et n est un entier plus grand ou égal à 2, alors on écrit

$$a \equiv b \text{ (mod n) si et seulement si } n|(a-b)$$

De plus, lorsqu'il n'y a pas de danger de confusion, on remplace le symbol $\equiv$ par une simple égalité $=$.

Exemple 5.1.1. On a que $25 \equiv 19 \pmod 3$, car $25 - 19 = 6$ et $3|6$.

De manière générale, si $a \in \mathbb{Z}$, et n est un entier plus grand ou égal à 2, ce que nous souhaitons est de trouver le plus petit entier positif b tel que $a \equiv b$ (mod n). C'est ce que nous appelons le **résidu modulo**. Le résidu modulo n d'un nombre a n'est en fait rien d'autre que le reste de la division de a par n. Par abus de language, lorsque nous demanderons qu'elle est la valeur de $a \pmod n$, nous voudrons dire quel est le résidu modulo n de l'entier a. Vous pouvez imaginer les nombres modulos un peu comme un horloge. Sur un horloge après 12, nous revenons à 1. Lorsqu'il est 11h sur un horloge, alors 2h plus tard il sera 1h.

Exemple 5.1.2. Trouver la valeur de $25 \pmod 3$, ou si vous préférez de manière plus correcte, quel est le résidu modulo 3 du nombre 25 ? Comme nous avons $25 = 8(3) + 1$, alors $25 \pmod 3 = 1$.

Les nombres modulos nous permettent de diviser les entiers en classes d'équivalence. Si nous travaillons avec les nombres modulos n, où n est un nombre naturel non nul, alors nous aurons n classes d'équivalence. Nous dirons par exemple que des entiers a et b sont dans la même classe modulo n si a (mod n) = b (mod n). Nous utiliserons la notation $\mathbb{Z}_n$ pour dénoter les nombres modulos n, et nous utiliserons la notation $\overline{a}$ pour dénoter l'ensemble des entiers b pour lesquels b (mod n) = a (mod n), c'est à dire :

$$\overline{a} = \{b : a = b \pmod n\}$$

Par exemple, dans $\mathbb{Z}_3$ nous avons 3 classes d'équivalences, c'est à dire $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Ce qui nous donne :

$$\begin{aligned} \overline{0} &= \{..., -6, -3, 0, 3, 6, 9, ...\} \\ \overline{1} &= \{..., , -5, -2, 1, 4, 7, 10, ...\} \\ \overline{2} &= \{..., -4, -1, 2, 5, 8, 11, ...\} \end{aligned}$$

Théorème 5.1.1. Si n est un nombre naturel non nul. Alors on a les propriétés suivantes :

1. La relation d'égalité modulo n est une relation d'équivalence.
2. La relation d'égalité modulo n est compatible avec l'addition et la multiplication. C'est à dire que si a, b, c, d sont tel que $a = b \pmod{n}$ et $c = d \pmod{n}$, alors on a $a + c = b + d \pmod{n}$ et $ac = bd \pmod{n}$
3. $ab = ac \pmod{n} \iff b = c \left(\mod \frac{n}{(a,n)}\right)$

Démonstration.

1. Pour vérifier qu'il s'agit bien d'une relation d'équivalence on doit vérifier qu'il s'agit d'une relation réflexive, symétrique et transitive.
   (a) **(Réflexive)** Il s'agit de vérifier que $n|(a-a)$ ce qui est vrai car $n|0$.
   (b) **(Symétrique)** Si $a = b \pmod{n}$, alors cela signifie que $n|(a-b)$, il existe donc un entier k tel que $nk = a - b$, et donc $n(-k) = b - a$ ce qui implique que $n|(b-a)$ et donc $b = a \pmod{n}$.
   (c) **(Transitive)** Supposons que $a = b \pmod{n}$ et $b = c \pmod{n}$. Par définition, on a donc $n|(b-a)$ et $n|(c-b)$. Il existe donc des entiers k_1 et k_2 tel que $nk_1 = b-a$ et $nk_2 = c-b$. En additionnant ces deux équations, on obtient donc $nk_1 + nk_2 = c - a$, puis en factorisant le n, on obtient $n(k_1 + k_2) = c - a$, ce qui signifie $n|c - a$, puis par définition $a = c \pmod{n}$.
2. Nous allons traiter séparément la compatibilité avec l'addition et celle avec la multiplication.
   (a) **(Compatibilité avec l'addition)** Comme $a = b \pmod{\text{n}}$ et $c = d \pmod{\text{n}}$, alors $n|(a-b)$ et $n|(c-d)$, il existe donc des entiers k, m tels que $nk = (a-b)$ et $nm = (c-d)$, ce qui nous donne
   $$(a+c) - (b+d) = (a-b) + (c-d) = nk + nm = n(k+m)$$
   ce qui signifie que $n|[(a+c) - (b+d)]$ et donc $a + c = b + d \pmod{\text{n}}$.
   (b) **(Compatibilité avec la multiplication)** Comme $a = b \pmod{\text{n}}$ et $c = d \pmod{\text{n}}$, alors $n|(a-b)$ et $n|(c-d)$ et donc il existe des entiers k, m tels que $nk = a - b$ et $nm = c - d$ ce qui nous donne :
   $$ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b) = anm + dnk = n(am + dk)$$
   et donc $n|(ac - bd)$ ce qui nous donne $ac = bd \pmod{\text{n}}$.
3. Commençons par démontrer ($\Rightarrow$). Par hypothèse, on a que
   $$ab = ac \pmod{\text{n}} \text{ donc } n|a(b-c)$$
   Supposons que $(a, n) = d$, il existe donc des entiers x, y tels que $xd = a$ et $yd = n$ avec $(x, y) = 1$, ce qui nous donne :
   $$yd|xd(b-c) \Longrightarrow y|x(b-c)$$
   Comme $(x, y) = 1$, on obtient donc :
   $$y|(b-c)$$
   Comme $y = \frac{n}{(a,n)}$, on peut donc conclure que
   $$b = c \left(\mod \frac{n}{(a,n)}\right)$$
   Maintenant pour l'autre direction ($\Leftarrow$). Par définition, on a que
   $$\frac{n}{(a,n)} \Big| b - c$$

il existe donc un entier x tel que :

$$\frac{n}{(a,n)}x = b - c$$

En multipliant des deux côtés par a, on obtient donc :

$$\frac{n}{(a,n)}ax = a(b-c) \Longrightarrow n\left(\frac{a}{(a,n)}\right)x = a(b-c)$$

Comme $(a,n)|a$, on obtient donc

$$n|a(b-c) \Longrightarrow ab = ac \pmod{n}$$

□

Exemple 5.1.3. On veut trouver la valeur de 34×55 modulo 3. Nous pourrions, bien entendu, calculer le produit 34×55 et ensuite calculer la valeur du modulo. Par contre il est plus simple de calculer les modulos en premier. Nous savons que $34 = 11(3) + 1$ et $55 = 18(3) + 1$ ce qui nous donne que $34 \equiv 1 \pmod 3$ et $55 \equiv 1 \pmod 3$. Et donc :

$$34 \times 55 \equiv 1 \times 1 \pmod 3 \equiv 1 \pmod 3$$

De la même façon, nous avons que :

$$34 + 55 \equiv 1 + 1 \pmod 3 \equiv 2 \pmod 3$$

Exemple 5.1.4. On veut trouver le dernier chiffre du produit 876×254. On remarque que le dernier chiffre du produit, n'est en fait rien d'autre que la valeur de $876 \times 254 \pmod{10}$, ce qui nous donne :

$$876 \times 254 \pmod{10} \equiv 6 \times 4 \pmod{10} \equiv 24 \pmod{10} \equiv 4 \pmod{10}$$

Le dernier chiffre est donc 4.

Supposons maintenant que n est un entier positif non nul et que a, b, c, d sont des entiers tels que $a \equiv b \pmod{\text{n}}$ et $c \equiv d \pmod{\text{n}}$. Alors nous avons déjà vu que

$$a^c \equiv b^c \pmod{\text{n}}$$

ceci étant tout simplement une application du fait que l'égalité modulo est compatible avec la multiplication. Par contre, en général il est **faux** de dire que a^c est égal à $a^d \pmod{\text{n}}$. Une petite astuce sera donc nécessaire pour calculer des exposants.

5.2 Derniers chiffres d'un expression

Comme première application des nombres modulos, nous allons regarder comment calculer le dernier chiffre d'un expression, ou même les deux ou trois derniers chiffres. Pour ce faire, il suffit de remarquez que trouver le dernier chiffre d'un expression revient à trouver son résidu modulo 10. Ceci est facile à voir, car le dernier chiffre correspond au reste de la division par 10. De la même manière, trouver les deux derniers chiffres reviendra à trouver le résidu modulo 100, car les deux derniers chiffres correspondent au reste de la division par 100.

Exemple 5.2.1. Trouver le dernier chiffre de l'expression 342^{18}. Pour ce faire, remarquons premièrement que $342 = 2 \pmod{10}$, et donc :

$$342^{18} \pmod{10} \equiv 2^{18} \pmod{10}$$

Maintenant, pour calculer 2^{18} nous allons utiliser une petite astuce. Nous avons :

$$\begin{aligned}
2^1 &\equiv 2 \pmod{10} \\
2^2 &\equiv 2 \times 2 \pmod{10} \equiv 4 \pmod{10} \\
2^4 &\equiv 2^2 \times 2^2 \pmod{10} \equiv 16 \pmod{10} \equiv 6 \pmod{10} \\
2^8 &\equiv 2^4 \times 2^4 \pmod{10} \equiv 36 \pmod{10} \equiv 6 \pmod{10} \\
2^{16} &\equiv 2^8 \times 2^8 \pmod{10} \equiv 36 \pmod{10} \equiv 6 \pmod{10}
\end{aligned}$$

Finalement, on remarque que $18 = 16 + 2$, et donc $2^{18} = 2^{16} \times 2^2$, ce qui nous donne finalement :

$$\begin{aligned} 342^{18} \pmod{10} &\equiv 2^{18} \pmod{10} \equiv 2^{16} \times 2^2 \pmod{10} \equiv 6 \times 4 \pmod{10} \\ &\equiv 24 \pmod{10} \equiv 4 \pmod{10} \end{aligned}$$

Nous pouvons donc affirmer que le dernier chiffre est 4.

Dans l'exemple précédant, nous aurions pu calculer directement la valeur de 342^{18}, ce qui nous aurais donné

$$342^{18} = 4097037216620966201473718623746777319410499584$$

Par contre, il est plutôt difficile de trouver ce dernier à la main, et même la plupart des calculatrices ne vous donneront pas cette valeur.

Exemple 5.2.2. Trouvez le dernier chiffre de 4583^{934}. Premièrement, on a que

$$4583^{934} \equiv 3^{934} \pmod{10}$$

Ensuite, pour calculer $3^{934} \pmod{10}$, on utilise la même astuce que précédemment :

$$\begin{aligned} 3^1 &\equiv 3 \pmod{10} \\ 3^2 &\equiv 9 \pmod{10} \\ 3^4 &\equiv 3^2 \times 3^2 \equiv 9 \times 9 \equiv 81 \equiv 1 \pmod{10} \\ 3^8 &\equiv 3^4 \times 3^4 \equiv 1 \times 1 \equiv 1 \pmod{10} \\ 3^{16} &\equiv 3^8 \times 3^8 \equiv 1 \times 1 \equiv 1 \pmod{10} \\ 3^{32} &\equiv 1 \pmod{10} \\ 3^{64} &\equiv 1 \pmod{10} \\ 3^{128} &\equiv 1 \pmod{10} \\ 3^{256} &\equiv 1 \pmod{10} \\ 3^{512} &\equiv 1 \pmod{10} \\ 3^{1024} &\equiv 1 \pmod{10} \end{aligned}$$

Ensuite, on remarque que $934 = 512 + 256 + 128 + 32 + 4 + 2$, ce qui nous donne :

$$\begin{aligned} 3^{934} &= 3^{512} \times 3^{256} \times 3^{128} \times 3^{32} \times 3^4 \times 3^2 \\ &\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 9 \pmod{10} \\ &\equiv 9 \pmod{10} \end{aligned}$$

Et donc le dernier chiffre est un 9.

Exemple 5.2.3. On veut trouver les deux derniers chiffres de 99^{2453}. Pour ce faire, nous allons devoir travailler modulo 100. Si nous utilisons exactement la même astuce que précédemment, on peut facilement remarquer que le calcul sera long. En effet, nous devons calculer :

$$\begin{aligned} 99^1 &\equiv 99 \pmod{100} \\ 99^2 &\equiv ??? \pmod{100} \\ 99^4 &\equiv ??? \pmod{100} \\ 99^8 &\equiv ??? \pmod{100} \\ 99^{16} &\equiv ??? \pmod{100} \\ 99^{32} &\equiv ??? \pmod{100} \\ 99^{64} &\equiv ??? \pmod{100} \\ 99^{128} &\equiv ??? \pmod{100} \\ 99^{256} &\equiv ??? \pmod{100} \\ ... &\equiv ..... \end{aligned}$$

Bien entendu, aucun de ces calculs n'est particulièrement difficile, par contre c'est effectivement long à calculer. Pour simplifier les choses, remarquons que $99 \equiv -1 \pmod{100}$. Et donc trouver les deux derniers chiffres de 99^{2453} revient à trouver le résidu modulo 100 de $(-1)^{2453}$. Nous savons que $(-1)^a = 1$ si a est pair, et $(-1)^a = -1$ si a est impair. Comme dans notre exemple, l'exposant est impair, nous avons donc :

$$99^{2453} \pmod{100} \equiv (-1)^{2453} \pmod{100} \equiv -1 \pmod{100} \equiv 99 \pmod{100}$$

Remarquez que la dernière étape ci-dessus est nécessaire car la réponse finale doit obligatoirement être entre 0 et 99. Les deux derniers chiffres sont donc 99.

5.3 Les critères de divisibilités

Nous allons maintenant nous intéressé à une application particulièrement intéressante des nombres modulos. Il s'agit des tests de divisibilités. Vous avez probablement rencontré certain d'entre eux à l'école élémentaire sans justification. L'idée pour construire un test de divisibilité consiste à séparer un nombre en unité, dizaine, centaine, etc. Notez qu'ici au chiffre qui se trouve à la position des unités, et de même pour les dizaines, centaines, etc. On pourra donc écrire un entier n sous la forme :

$$n = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0, \qquad 0 \leq a_i \leq 9, \forall i$$

Donc dans notre expression, a_0 est le chiffre des unités, a_1 le chiffre de dizaine, et ainsi de suite. En réduisant le tout modulo k, où k représente le nombre par lequel on veut savoir si n est divisible, on peut alors obtenir un test de divisibilité. Notez qu'il est aussi possible d'obtenir d'autre test de divisiblité en faisant des groupements légèrement différent. Par exemple, plutôt que de regarder chaque chiffre un par un, on peut très bien les grouper deux par deux. Dans ce cas, on pourra écrire un expression de la forme :

$$n = 100^n a_n + 100^{n-1} a_{n-1} + ... + 100^2 a_2 + 100 a_1 + a_0, \qquad 0 \leq a_i \leq 9, \forall i$$

Dans ce cas, a_0 représente les deux derniers chiffres de n, a_1 les deux chiffres précédent, etc. On procède ensuite exactement de la même façon que précédement en réduisant modulo k.

Théorème 5.3.1. **(Critères de divisibilités)** Si n est un entier non nul, alors :

1. n est divisible par 2 si le dernier chiffre de n est divisible par 2
2. n est divisible par 3 si la somme des chiffres qui le composent est divisible par 3
3. n est divisible par 4 si le nombre formé des deux derniers chiffres de n est divisible par 4
4. n est divisible par 5 si le dernier chiffre de n est divisible par 5
5. n est divisible par 6 s'il est divisible par 2 et par 3
6. n est divisible par 8 si le nombre formé de ses trois derniers chiffres est divisible par 8.
7. n est divisible par 9 si la somme des chiffres qui le composent est divisible par 9
8. n est divisible par 10 si son dernier chiffre est un 0.
9. n est divisible par 11 si les unités moins les dizaines plus les centaines moins les milliers .... est divisible par 11.

Démonstration.

1. On peut écrire n sous la forme :

   $$n = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$$

   avec $0 \leq a_i \leq 9$. En calculant le tout modulo 2, on obtient donc :

   $$n = 0^n a_n + 0^{n-1} a_{n-1} + ... + 0^2 a_2 + 0^1 a_1 + a_0 = a_0 \pmod{2}$$

   Comme n est divisible par 2 si et seulement si $n = 0 \pmod{2}$, on a donc que n est divisible par 2 si et seulement si $a_0 = 0 \pmod{2}$, c'est à dire si et seulement si a_0 est divisible par 2.

2. On utilise la même idée que précédemment. On peut écrire n sous la forme :

$$n = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$$

avec $0 \leq a_i \leq 9$. En calculant le tout modulo 3, on obtient donc :

$$n = 1^n a_n + 1^{n-1} a_{n-1} + ... + 1^2 a_2 + 1^1 a_1 + a_0 = a_n + a_{n-1} + ... + a_2 + a_1 + a_0 \pmod 3$$

Donc un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

3. Exercice
4. Exercice
5. Exercice
6. Exercice
7. Exercice
8. Exercice
9. On commence par écrire un nombre n sous la forme :

$$n = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$$

avec $0 \leq a_i \leq 9$. On remarque que $10 = -1 \pmod{11}$, ce qui nous donne :

$$n = (-1)^n a_n + (-1)^{n-1} a_{n-1} + ... + 1^2 a_2 - 1^1 a_1 + a_0 \pmod{11}$$

Donc un nombre est divisible par 11 si les unités moins les dizaines plus les centaines moins les milliers .... est divisible par 11.

□

Exemple 5.3.1. Est-ce que le nombre 100100100 est divisible par 3 ? Le vérifier en calculant la division peut nous prendre un certain temps à la main, rien de très compliqué, juste un peu long. Par contre, en appliquant le critère de divisibilité que nous venons de démontrer, on remarque qu'il s'agit d'additionner les chiffres qui le composent. On obtient donc $1+0+0+1+0+0+1+0+0 = 3$. Comme $3|3$, le nombre est donc divisible par 3.

Exemple 5.3.2. Est-ce que le nombre 57823 est divisible par 11 ? Pour ce faire, il suffit de calculer $3-2+8-7+5 = 7$. Comme $11 \nmid 7$, on peut donc conclure que 57823 n'est pas divisible par 11.

Remarquez que dans notre théorème, nous avons énoncé uniquement les critères de divisibilité les plus connus. Il en existe bien sur plusieurs autres. Notez cependant que le nombre 7 est absent de notre liste, ce qui peut sembler un peu curieux. La raison vient du fait que le critère que nous obtenons pour la divisiblité par 7 à l'aide de notre méthode est un peu étrange, beaucoup plus difficile à mémoriser, un très peu utilisé. Plutôt que de le faire de manière générale comme nous avons procédé précédement, nous allons le regarder à partir d'un exemple numérique.

Exemple 5.3.3. Est-ce que le nombre 784 est divisible par 7 ? Pour ce faire, écrivons le nombre sous la forme $(7 \times 10^2) + (8 \times 10^1) + (4 \times 10^0)$. Et maintenant trouvons la valeur de 10^k modulo 7.

$$\begin{aligned} 10^0 &= 1 \\ 10^1 &= 3^1 \pmod 7 = 3 \pmod 7 \\ 10^2 &= 10^1 \times 10^1 \pmod 7 = 3 \times 3 \pmod 7 = 9 \pmod 7 = 2 \pmod 7 \end{aligned}$$

Nous avons donc que

$$\begin{aligned} 784 &= (7 \times 10^2) + (8 \times 10^1) + (4 \times 10^0) \\ &= (7 \times 2) + (8 \times 3) + (4 \times 1) \pmod 7 = 14 + 24 + 4 \pmod 7 \\ &= 42 \pmod 7 = 0 \pmod 7 \end{aligned}$$

On peut donc conclure que 784 est bien divisible par 7.

Remarquez qu'il aurait sans doute été plus facile d'effectuer directement la division pour vérifier que 784 est effectivement divisible par 7. Par contre, la méthode ci-dessous est très générale. Par exemple, si on vous demande ensuite si le nombre 598 est divisible par 7, vous pourriez directement écrire :

$$598 \equiv (5 \times 2) + (9 \times 3) + (8 \times 1) \pmod 7 \equiv 45 \pmod 7 \equiv 3 \pmod 7$$

Donc il n'est pas divisible par 7.

5.4 Les théorèmes de Fermat, Euler et Wilson

Dans ce chapitre, nous allons étudier 3 théorèmes particulièrement important en théorie des nombres. Le théorème d'Euler, entre autre, joue un rôle particulièrement important en cryptographie.

Definition 5.4.1.

1. Si $x = y \pmod n$ alors on dit que y est un résidu de x modulo n
2. Un ensemble $\{x_1, x_2, ..., x_n\}$ est appelé un système complet de résidu modulo n si pour chaque entier y, il existe un seul x_i tel que $x_i = y \pmod n$.
3. Un ensemble $\{x_1, x_2, ...x_k\}$ est appelé un système réduit de résidu modulo n si $(x_i, n) = 1$ pour tout i et si pour chaque entier y tel que $(y, n) = 1$, il existe un seul x_i tel que $x_i = y \pmod n$.

Definition 5.4.2. Si n est un entier plus grand ou égal à 2, alors on définit $\phi(n)$ comme étant le nombre d'éléments dans un système réduit de résidus modulo n. C'est à dire que $\phi(n)$ est le nombre d'entiers m tels que $0 \leq m < n$ et $(m, n) = 1$.

Théorème 5.4.1. **(Théorème d'Euler)** Si $a, n \in \mathbb{Z}$ sont tels que $(a, n) = 1$, alors :

$$a^{\phi(n)} = 1 (\text{mod } n)$$

Démonstration. Supposons que $\{x_1, x_2, ..., x_{\phi(n)}\}$ est un système réduit modulo n et supposons que $(a, n) = 1$. On va commencer par démontrer que $\{ax_1, ax_2, ..., ax_{\phi(n)}\}$ est aussi un système réduit modulo n. Comme ces deux ensembles ont le même nombre d'éléments, il s'agit de démontrer que $ax_i \neq ax_j \pmod n$ si $i \neq j$.

$$\begin{aligned} ax_i = ax_j \pmod n &\Rightarrow n | a(x_i - x_j) \\ &\Rightarrow n | (x_i - x_j) \text{ car } (a, n) = 1 \\ &\Rightarrow x_i = x_j \pmod n \\ &\Rightarrow i = j \text{ car } \{x_1, x_2, ..., x_n\} \text{ est un système réduit modulo n} \end{aligned}$$

Il s'agit donc bien d'un système réduit modulo n. Le produit des éléments de ces deux systèmes réduits modulo n doit donc être égal modulo n. On a donc :

$$\prod_{i=1}^{\phi(n)} ax_i = \prod_{i=1}^{\phi(n)} x_i \pmod n$$

Et maintenant, en sortant le a du produit, on obtient un facteur $a^{\phi(n)}$, ce qui nous donne :

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} x_i \pmod n$$

Finalement, comme $(n, x_i) = 1$ pour tout i, on a donc que

$$\left(n, \prod_{i=1}^{\phi(n)} x_i \right) = 1$$

En utilisant les propriétés des modulos, on peut donc simplifier le produit de chaque côté, ce qui nous laisse l'égalité que nous recherchions :

$$a^{\phi(n)} = 1 \pmod{n}$$

□

Nous somme maintenant prêt à énoncer le petit théorème de Fermat. Dans cette section, nous allons le regarder comme un simple corollaire au théorème d'Euler, mais plusieurs approche différente sont possible pour le démontrer.

Théorème 5.4.2. **(Petit théorème de Fermat)** Si p est un nombre premier et $a \in \mathbb{N}$ tel que $p \nmid a$. Alors :

$$a^{p-1} = 1 \pmod{p}$$

Démonstration. Il s'agit d'une conséquence directe du théorème d'Euler. Si p est un nombre premier, alors $\phi(p) = p - 1$. On obtient donc :

$$a^{p-1} = a^{\phi(n)} = 1 \pmod{n}$$

□

Le petit théorème de Fermat est souvent utilisé comme technique probabiliste pour déterminer si un nombre est premier ou non. L'idée est la suivante. Si on veut vérifier si un nombre naturel n est premier, on peut calculer

$$a^{n-1} \pmod{n}$$

pour différentes valeurs de a. Du moment qu'on trouve un entier a pour lequel $a^{n-1} \neq 1 \pmod{n}$, on peut affirmer que le nombre n n'est pas un nombre premier. D'un autre côté, si après avoir testé plusieurs valeurs de a, on obtient toujours $a^{n-1} = 1 \pmod{n}$, alors on est presque certain que le nombre n est premier. Il faut cependant faire très attention car le petit théorème de Fermat ne peut absolument pas nous garantir que le nombre est premier. En effet, il existe quelques entiers, appelé nombres de Carmichael, qui satisfont le petit théorème de Fermat pour tout entier a, mais qui ne sont pas premiers. Le plus petit nombre de Carmichael est 561. Plusieurs questions restent encore ouvertes concernant les nombres de Carmichael. Nous n'irons cependant pas plus loin dans cette direction. Pour compléter cette section, nous allons finalement voir un théorème qui cette fois nous permettra d'affirmer qu'un nombre est premier. Il s'agit cette fois d'un si et seulement si. Bien que les calculs nécessaires pour vérifier qu'un nombre est premier à l'aide du théorème de Wilson sont trop longs pour être d'un grand intérêt, le théorème est particulièrement utile pour son côté théorique.

Théorème 5.4.3. **(Théorème de Wilson)** Si $n \in \mathbb{N}$ tel que $n > 1$. Alors :

$$n \text{ est premier } \iff (n-1)! = -1 \pmod{n}$$

Démonstration.
(⇒) Supposons que n est un nombre premier. Si $n = 2$ ou $n = 3$, le résultat est facile à démontrer, il suffit de remplacer dans l'équation. Nous allons donc supposons que n est un nombre premier plus grand ou égal à 5. D'après le petit théorème de Fermat, pour chaque $x \in \{1, 2, ..., (n-1)\}$, il existe un $y = x^{n-2}$ tel que $xy = 1 \pmod{n}$. Supposons que z est un autre entier dans $\{1, 2, ..., (n-1)\}$ tel que $xz = 1$, alors on a :

$$xz = xy \pmod{n} \Longrightarrow z = y \pmod{n} \text{ car } (x, n) = 1$$

En d'autres mots, pour chaque $x \in \{1, 2, ..., (n-1)\}$, il existe un unique $y \in \{1, 2, ..., (n-1)\}$ tel que $xy = 1 \pmod{n}$.

Maintenant, si on suppose que $x = y$, alors on a $x^2 = 1 \pmod{n}$, ce qui signifie que $n|(x^2-1) \Rightarrow n|(x-1)(x+1)$. Comme n est, par hypothèse, un nombre premier, alors on obtient que $n|(x-1)$ ou $n|(x+1)$. De plus, on remarque que $n|(x-1)$ est possible seulement si $x = 1$. De plus, la condition que $n|(x+1)$ est possible seulement si $x = n-1$. En d'autres mots, pour chaque $x \in \{2,3,...,n-2\}$, il existe un unique $y \in \{2,3,...,n-2\}$ tel que $x \neq y$ et $xy = 1 \pmod{n}$. C'est à dire que tous les nombres dans l'ensemble $\{2,3,...,n-2\}$ peuvent être groupés en pairs pour lesquels le produit est 1 modulo n.

Ensuite, il est facile de remarquer que $1 = 1 \pmod{n}$ et $n-1 = -1 \pmod{n}$. Ceci nous permet d'affirmer que :

$$\prod_{k=1}^{n-1} k = (n-1)! = -1 \pmod{n}$$

Ce qui est exactement ce que nous voulions démontrer.

(⇐) Supposons que n n'est pas un nombre premier. Alors il existe a et b tel que $ab = n$ avec $a, b < n$. Si $a \neq b$, alors le produit $(n-1)!$ contient les facteurs a et b, et donc est un multiple de n. On peut donc conclure que si n est composé et n'est pas un carré parfait, alors $(n-1)! = 0 \pmod{n}$. Si au contraire $n = p^2$ où p est un nombre premier, alors p et $2p$ sont tous deux des facteurs de $(n-1)!$, donc en particulier, en multipliant p et $2p$ on remarque de $(n-1)!$ est un multiple de $(n-1)!$, ce qui signifie que $(n-1)! = 0 \pmod{n}$. Donc si $(n-1)! = -1 \pmod{n}$, alors n ne peut pas être composé, et donc n doit être un nombre premier. □

5.5 L'équation $ax = b$ en modulo

Nous allons maintenant nous intéresser à la résolution des équations algébriques en modulo. Lorsque vous avez commencé à étudier l'algèbre au secondaire, l'une des premières équations que vous avez rencontré avait la forme $ax = b$. Il semble donc approprié de commencer par cette équation dans le contexte des modulos. Remarquez cependant que la solution n'est pas aussi simple que celle que vous connaissez pour les nombres réels. En effet, dans la plupart des cas il n'est pas possible de tout simplement diviser par a étant donné que la division n'est pas bien définie. Le théorème d'Euler, ainsi que le petit théorème de Fermat peuvent cependant nous permettre de contourner ce problème.

Théorème 5.5.1. Si a, b, n sont des entiers, $n > 1$, et $(a, n) = 1$, alors l'équation

$$ax = b \pmod{n}$$

possède exactement une solution.

Démonstration. Premièrement, par le théorème de Euler, si $(a, n) = 1$, alors

$$a \cdot (a^{\phi(n)-2}b) = a^{\phi(n)-1}b = b \pmod{n}$$

donc $x = a^{\phi(n)-2}b$ est une solution de l'équation. Maintenant, supposons que y est aussi une solution de l'équation, alors on a :

$$ax = ay \pmod{n} \Rightarrow x = y \pmod{n} \text{ car } (a, n) = 1$$

Donc la solution est unique. □

Exemple 5.5.1. On veut trouver la solution de l'équation

$$5x = 8 \pmod{13}$$

Premièrement, on remarque que $(5, 13) = 1$, donc par le théorème précédent, il doit y avoir exactement une solution. Il y a deux méthode pour trouver cette solution.

Première méthode : Comme 13 est un nombre premier, par le petit théorème de Fermat on a que :

$$5^{12} = 1 \pmod{13}$$

Ce qui nous donne :

$$\begin{aligned} 5x &= 8 \pmod{13} \\ 5^{11} \cdot 5x &= 5^{11}8 \pmod{13} \\ 5^{12}x &= 5^{11}8 \pmod{13} \\ x &= 5^{11}8 \pmod{13} \\ x &= 12 \pmod{13} \end{aligned}$$

Deuxième méthode : On commence par utiliser l'algorithme d'Euclide pour trouver une solution de l'équation $5x + 13y = 1$. Comme $(5, 13) = 1$, nous savons déjà que cette équation possède une solution, mais nous allons tout de même utiliser l'algorithme d'Euclide pour le calculer :

$$13 = 2(5) + 3$$

$$5 = 1(3) + 2$$

$$3 = 1(2) + 1$$

$$2 = 2(1) + 0$$

Maintenant, en réécrivant l'algorithme d'Euclide à l'envers, on obtient :

$$1 = 3 - 1(2) = 3 - 1[5 - 1(3)] = 3 - 1(5) + 1(3) = 2(3) - 1(5)$$

$$= 2[13 - 2(5)] - 1(5) = 2(13) - 4(5) - 1(5) = 2(13) - 5(5)$$

Donc une solution de l'équation $5x + 13y = 1$ est donnée par $5(-5) + 13(2) = 1$. Maintenant, en multipliant le tout par 8, on obtient :

$$5(-40) + 13(16) = 8$$

Finalement, en calculant le tout modulo 13, on obtient :

$$5(-40) = 8 \pmod{13}$$

La solution est donc $x = -40 = -40 + 4(13) = 12 \pmod{13}$.

Théorème 5.5.2. Si a, b, n sont des entiers et $n > 1$, alors l'équation

$$ax = b \pmod{n}$$

possède au moins une solution si et seulement si $(a, n)|b$. Dans ce cas, elle a exactement (a, n) solutions qui sont données par :

$$x = x_0 + \frac{kn}{(a, n)} \pmod{n}, \quad k \in \mathbb{Z}$$

où x_0 est une solution particulière de l'équation

$$\frac{a}{(a, n)}x = \frac{b}{(a, n)} \left(\mod \frac{n}{(a, n)} \right)$$

Démonstration. Premièrement, notons que $ax = b \pmod{n}$ a une solution si et seulement si il existe un entier x tel que $n|(ax - b)$, ce qui est le cas si et seulement s'il existe des entiers x et y tels que $(ax - b) = (-n)y$, ce qui nous donne finalement qu'il existe une solution si et seulement s'il existe des entiers x et y tels que

$$ax + ny = b$$

Maintenant, nous avons déjà vu que l'ensemble $\{ax + ny\}$ est l'ensemble de tous les multiples de (a, n). Il existe donc une solution si et seulement si $(a, n)|b$, c'est à dire si b est un multiple de (a, n).

On va donc supposer que $(a, n)|b$, c'est à dire que nous sommes dans le cas où il y a une solution. Donc a, b et n sont tous les 3 divisibles par (a, n). En utilisant le théorème du début du chapitre sur les propriétés des modulos, on a donc :

$$\begin{aligned} ax = b \pmod{n} &\iff (a,n)\frac{ax}{(a,n)} = (a,n)\frac{b}{(a,n)} \pmod{n} \\ &\iff \frac{a}{(a,n)}x = \frac{b}{(a,n)} \left(\mod \frac{n}{(a,n)}\right) \end{aligned}$$

Donc si x_0 est une solution de cette dernière équation, alors toutes les autres solutions sont données en ajoutant ou soustrayant des multiples de $\frac{n}{(a,n)}$, c'est à dire que toutes les autres x qui satisfont l'équation sont de la forme :

$$x = x_0 + \frac{kn}{(a,n)} \pmod{n}$$

car seules les solutions modulos n nous intéressent (les autres étant équivalentes). □

Exemple 5.5.2. On veut trouver les solutions de l'équation

$$21x = 6 \pmod{96}$$

Pour ce faire, commençons par calculer le PGCD de 96 et 21 :

$$\begin{aligned} 96 &= 4(21) + 12 \\ 21 &= 1(12) + 9 \\ 12 &= 1(9) + 3 \\ 9 &= 3(3) + 0 \end{aligned}$$

On a donc : $(96, 21) = 3$. Comme $3|6$, il doit donc y avoir des solutions. Nous allons donc commencer par trouver une solution particulière x_0 à l'équation :

$$7x = 2 \ (\mod 32)$$

Comme $(7, 32) = 1$, alors on peut appliquer le théorème d'Euler qui nous donne :

$$7^{\phi(32)} = 1 \pmod{32}$$

Comme $\phi(32) = 16$, on a donc :

$$\begin{aligned} 7x_0 &= 2 \ (\mod 32) \\ 7^{15} \cdot 7x_0 &= 7^{15} \cdot 2 \ (\mod 32) \\ 7^{16}x_0 &= 7^{15} \cdot 2 \ (\mod 32) \\ x_0 &= 7^{15} \cdot 2 \ (\mod 32) \\ x_0 &= 14 \ (\mod 32) \end{aligned}$$

Par le théorème, on a donc que les solutions de l'équation originale sont :

$$x = 14 \ (\mod 96)$$

$$x = 14 + \frac{96}{3} \ (\mod 96) = 14 + 32 \ (\mod 96) = 46 \ (\mod 96)$$

$$x = 14 + \frac{96 \cdot 2}{3} \ (\mod 96) \ (\mod 96) = 14 + 64 = 78 \ (\mod 96)$$

5.6 La cryptographie RSA

Depuis le début de ce chapitre, nous avons vu plusieurs résultats nous permettant de calculer rapidement certaines valeurs. Par contre, il ne semble pas y avoir beaucoup d'applications concrètes à ce que nous avons vu jusqu'à présent. Dans cette section, les choses vont changer. Nous allons voir que les résultats vus depuis le début du chapitre sont en fait très utilisés dans la pratique. L'application que nous allons voir s'appelle la cryptographie, autrement dit le codage des messages secrets. La cryptographie n'est pas un sujet nouveau. Elle est utilisé depuis au moins l'Antiquité. Par contre, trouver une façon efficace de coder un message est relativement complexe. Avec les ordinateurs modernes, la plupart des codes utilisés dans l'Antiquité ou au moyen-âge peuvent être décryptés en quelques minutes tout au plus. La méthode que nous allons voir s'appelle la cryptographie RSA. Il s'agit de l'une des techniques de codage les plus couramment utilisées entre autres sur internet. La technique repose sur la difficulté de factoriser un grand nombre. Plus le nombre est grand, plus un ordinateur prendra de temps à le factoriser (ici on ne parle pas en minutes, mais bien en mois ou années). Donc, le temps de décrypter le message, son contenu devient souvent inutile, car trop vieux.

Remarquez ici qu'il n'est pas impossible de décrypter le message. Donc si vous envoyez, par exemple, votre numéro de carte de crédit sur internet, et que quelqu'un intercepte le numéro (qui a été bien entendu crypté), il pourra le décoder. Par contre si la méthode pour coder le numéro a été bien choisie, un ordinateur moderne pourrait prendre facilement 100 ans à le décrypter. Donc le temps que mettra la personne qui a intercepté le message à le décoder et à obtenir votre numéro de carte de crédit, il est pratiquement certain que le numéro ne sera plus utilisable de toute façon.

La technique que nous allons voir est pratiquement identique à ce qu'on utilise sur internet. Nous allons cependant tricher un peu en choisissant des nombres relativement petit pour simplifier les calculs. Vous devez cependant vous rappeler que pour que votre code soit sécuritaire, vous devez en pratique choisir des nombres les plus grands possible. Voici maintenant les étapes de la méthode :

Étape 1 : Choisir deux nombres premiers p et q les plus grands possible

Étape 2 : Calculer les valeurs n et ϕ de la façon suivante :

$$n = pq \quad \text{et} \quad \phi(n) = (p-1)(q-1)$$

La formule pour le calcul de $\phi(n)$ sera justifiée à la fin de ce chapitre. Pour le moment, notez seulement que ce $\phi(n)$ est le même que nous avons utilisé dans le théorème d'Euler.

Étape 3 : Choisir un nombre naturel non nul a qui est copremier avec ϕ. C'est à dire un entier positif a tel que $(a, \phi(n)) = 1$.

Étape 4 : Trouver un nombre b tel que $ab = 1 (\text{mod } \phi)$. Pour trouver ce b, on remarque que parce que $(a, \phi(n)) = 1$, alors il existe b et k tels que

$$ab + k\phi(n) = 1$$

que l'on peut trouver en utilisant l'algorithme d'Euclide. En calculant le tout modulo $\phi(n)$, on obtient donc

$$ab = 1 \pmod{\phi(n)}$$

Étape 5 : Envoyez la clé de codage (a, n) à votre correspondant. Il encodera son message à l'aide de la formule suivante :

$$x^a \pmod{\text{n}}$$

Ici x représente la valeur à coder. Il vous envoie alors le message codé.

Étape 6 : Vous décodez le message à l'aide de la clé (b, n), c'est à dire à l'aide de la formule suivante :

$$y^b \pmod{\text{n}}$$

où y représente le message codé que vous avez recu. Nous allons démontrer à la fin de cette section que cette formule permet bien de décrypter le message.

Remarquez que n'importe quelle personne interceptant la clé (a, n) pourrait coder un message et vous l'envoyer. Par contre, vous êtes le seul à connaître la clé (b, n) pour décoder le message. Si les nombres p et q sont petits, il est facile de factoriser n, et donc de trouver la clé pour décoder le message. Par contre, si p et q sont très grands, il est pratiquement impossible de factoriser n dans un temps raisonnable, et donc on ne peut pas calculer la clé pour décoder le message.

Exemple 5.6.1. Votre correspondant souhaite vous envoyer un message crypté. Il vous demande donc de lui envoyer une clé de cryptage. Vous devez donc choisir deux nombres premiers (en théorie le plus grand possible). Ici nous allons choisir $p = 5$ et $q = 13$. On calcule ensuite $n = 5 \times 13 = 65$ et $\phi = 4 \times 12 = 48$. On doit maintenant choisir un nombre copremier avec 48. Pour ce faire, il s'agit de choisir un nombre premier différent de 5 et 13. Choisissons $a = 11$. Puis, on doit trouver un nombre b tel que $ab = 1 \pmod{48}$. Pour ce faire il y a un astuce. Commençons par appliquer l'algorithme d'Euclide aux nombres 11 et 48, ce qui nous donne :

$$\begin{aligned} 48 &= 4(11) + 4 \\ 11 &= 2(4) + 3 \\ 4 &= 1(3) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

Nous allons maintenant appliquer l'algorithme d'Euclide à l'envers pour trouver des entiers b et m tels que $48m + 11b = 1$. Nous avons donc :

$$\begin{aligned} 1 &= 4 - 1(3) \\ &= 4 - 1(11 - 2(4)) = 4 - 1(11) + 2(4) = 3(4) - 1(11) \\ &= 3(48 - 4(11)) - 1(11) = 3(48) - 12(11) - 1(11) = 3(48) - 13(11) \end{aligned}$$

Le coefficient du nombre 11 est dans la même classe modulo 48 que le nombre b que nous cherchons. On peut donc trouver b en calculant $-13 + 48 = 35 = b$.

La clé que nous devons envoyer à notre correspondant est $(11, 65)$. La clé de décryptage est $(35, 65)$. Nous devons bien entendu garder cette dernière secrète. Nous devons être les seuls à la connaître. Même notre correspondant ne la connait pas. Prenons maintenant la place de notre correspondant qui souhaite vous envoyer le mot "Bonjour". Commençons par coder chacune des lettres en valeur numérique en utilisant la grille suivante :

a	1	n	14
b	2	o	15
c	3	p	16
d	4	q	17
e	5	r	18
f	6	s	19
g	7	t	20
h	8	u	21
i	9	v	22
j	10	w	23
k	11	x	24
l	12	y	25
m	13	z	26

Donc le mot "Bonjour" peut s'écrire numériquement par :

$$2 - 15 - 14 - 10 - 15 - 21 - 18$$

Nous devons maintenant crypter chacune de ces valeurs à l'aide de la clé $(11, 65)$

On veut premièrement calculer $2^{11} \pmod{65}$.

$$\begin{aligned} 2^1 &= 2 \pmod{65} \\ 2^2 &= 4 \pmod{65} \\ 2^4 &= 2^2 \times 2^2 = 16 \pmod{65} \\ 2^8 &= 2^4 \times 2^4 = 16 \times 16 = 256 = 61 \pmod{65} \\ 2^{11} &= 2^8 \times 2^2 \times 2^1 = 61 \times 4 \times 2 \pmod{65} = (-4) \times 4 \times 2 \pmod{65} \\ &= -16 \times 2 = -32 \pmod{65} = 33 \pmod{65} \end{aligned}$$

On fait maintenant de même avec $15^{11} \pmod{65}$.

$$\begin{aligned}
15^1 &= 15 \\
15^2 &= 225 = 30 \\
15^4 &= 15^2 \times 15^2 = 30 \times 30 = 900 = 55 \pmod{65} \\
15^8 &= 15^4 \times 15^4 = 55 \times 55 = (-10) \times (-10) \pmod{65} = 100 \pmod{65} \\
&= 35 \pmod{65} \\
15^{11} &= 15^8 \times 15^2 \times 15^1 = 35 \times 30 \times 15 \pmod{65} = (-30) \times 30 \times 15 \pmod{65} \\
&= -900 \times 15 \pmod{65} = 10 \times 15 \pmod{65} = 150 \pmod{65} = 20 \pmod{65}
\end{aligned}$$

Puis avec $14^{11} \pmod{65}$.

$$\begin{aligned}
14^1 &= 14 \\
14^2 &= 196 = 1 \pmod{65} \\
14^4 &= 14^2 \times 14^2 = 1 \times 1 \pmod{65} = 1 \pmod{65} \\
14^8 &= 14^4 \times 14^4 = 1 \times 1 \pmod{65} = 1 \pmod{65} \\
14^{11} &= 14^8 \times 14^2 \times 14^1 = 1 \times 1 \times 14 \pmod{65} = 14 \pmod{65}
\end{aligned}$$

En continuant de la même façon, nous obtenons :

$$\begin{aligned}
10^{11} &= 30 \pmod{65} \\
15^{11} &= 20 \pmod{65} \\
21^{11} &= 31 \pmod{65} \\
18^{11} &= 47 \pmod{65}
\end{aligned}$$

Donc le message que vous recevez de votre correspondant est :

$$33 - 20 - 14 - 30 - 21 - 31 - 47$$

Nous voulons maintenant décrypter le message reçu. Commençons par $33^{35} \pmod{65}$:

$$\begin{aligned}
33^1 &= 33 \\
33^2 &= 1089 = 49 \pmod{65} \\
33^4 &= 33^2 \times 33^2 = 49 \times 49 \pmod{65} = 2401 \pmod{65} = 61 \pmod{65} \\
33^8 &= 33^4 \times 33^4 = 61 \times 61 \pmod{65} = (-4) \times (-4) \pmod{65} = 16 \pmod{65} \\
33^{16} &= 33^8 \times 33^8 = 16 \times 16 \pmod{65} = 256 \pmod{65} = 61 \pmod{65} \\
33^{32} &= 33^{16} \times 33^{16} = 61 \times 61 \pmod{65} = 16 \pmod{65} \\
33^{35} &= 33^{32} \times 33^2 \times 33^1 = 16 \times 49 \times 33 \pmod{65} = 25872 \pmod{65} = 2 \pmod{65}
\end{aligned}$$

Ce qui correspond bien à la lettre "b", et en continuant de la même façon, on peut donc retrouver le message complet : "Bonjour".

Nous allons maintenant compléter cette section en démontrant que la formule pour décrypter le message est bel et bien valide, mais avant, nous allons justifier la formule que nous avons utilisée pour calculer $\phi(n)$.

Théorème 5.6.1. Supposons que p et q sont des nombres premiers, alors

$$\phi(pq) = (p-1)(q-1)$$

Démonstration. Posons $n = pq$, alors les seuls diviseurs de n sont $1, p, q, n$. Donc si a est un entier tel que $(a, n) \neq 1$, alors a doit être un multiple de p ou de q. On a donc que $\frac{n}{q} = p$ est le nombre de multiples de q et $\frac{n}{p} = q$ est le nombre de multiples de p. Aussi, comme p et q sont des nombres premiers distincts, alors $[p, q] = n$, il y a donc 1 seul multiple commun de p et q qui est inférieur ou égal à n. Il y a donc $p + q - 1$ entier a tel que $(a, n) \neq 1$, ce qui nous donne finalement :

$$\phi(n) = n - (p + q - 1) = pq - p - q + 1 = p(q - 1) - (q - 1) = (p - 1)(q - 1)$$

□

Théorème 5.6.2. Supposons que p et q sont des nombres premiers et $n = pq$. Supposons aussi que a est un entier tel que $(a, \phi(n)) = 1$, et b est un entier tel que $ab = 1 \pmod{\phi(n)}$. Supposons finalement que x est un entier et $y = x^a \pmod{n}$, alors on a :

$$x = y^b \pmod{n}$$

Démonstration. Par hypothèse, on a que $ab = 1 \pmod{\phi(n)}$, on a donc que $\phi(n) | (ab - 1)$, c'est à dire qu'il existe un entier k tel que :

$$k\phi(n) = ab - 1 \Longrightarrow ab = k\phi(n) + 1$$

Par le théorème d'Euler, on a que $x^{\phi(n)} = 1 \pmod{n}$. On obtient donc que :

$$y^b = (x^a)^b = x^{ab} = x^{k\phi(n)+1} = (x^{\phi(n)})^k x = 1^k x = x \pmod{n}$$

□

Chapitre 6

Quelques outils essentiels

6.1 La notation sigma

La notation sigma est une façon d'écrire une somme de manière condensé. L'idée est la suivante. Supposons que nous somme intéressé à calculer (ou étudier) la somme suivante :

$$1 + 2 + 3 + 4 + ... + 97 + 98 + 99 + 100$$

L'écriture d'une telle somme est particulièrement lourde. En particulier, pour pouvoir l'écrire en une seule ligne, il devient nécessaire d'utiliser des ... ce qui nous semble pas nécessairement très mathématiques. La notation sigma permet de réécrire la somme sous la forme :

$$\sum_{i=1}^{100} i$$

qui avec un peu de pratique, devient beaucoup plus simple à écrire et manipuler. De façon plus générale, on aura la définition suivante.

Definition 6.1.1. Si $f(x)$ est une fonction (possiblement définie seulement sur certain entier) et $a, b \in \mathbb{Z}$ avec $a < b$, alors on écrira :

$$\sum_{i=a}^{b} f(i) = f(a) + f(a+1) + f(a+2) + f(a+3) + ... + f(b-2) + f(b-1) + f(b)$$

Exemple 6.1.1. Évaluer la somme suivante :

$$\sum_{i=1}^{5} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$$

Exemple 6.1.2. Écrire sous forme de notation sigma la somme de tout les entiers impair entre 11 et 101. On a donc :

$$\begin{aligned} S &= 11 + 13 + 15 + 17 + 19 + 21 + ... + 99 + 101 \\ &= 11 + (11+2) + (11+4) + (11+6) + ... + (11+88) + (11+90) \\ &= (11 + 2(0)) + (11 + 2(1)) + (11 + 2(2)) + (11 + 2(3)) + ... + (11 + 2(44)) + (11 + 2(45)) \\ &= \sum_{i=0}^{45} (11 + 2i) \end{aligned}$$

Remarquer que dans l'exemple précédent, on aurait pu trouver plusieurs façon d'écrire la même somme. Par exemple, les deux sommes suivantes représente aussi la somme de tout les entiers impairs entre 11 et 101 :

$$\sum_{i=5}^{50} (2i+1) \qquad \text{et} \qquad \sum_{i=1}^{46} (9 + 2i)$$

Exercice 6.1.1. Vérifier que les deux sommes ci-dessus représente bien la somme de tout les entiers impairs entre 11 et 101.

Théorème 6.1.1. **(Propriétés des sommes)** Si a_i et b_i sont des suites, c est un nombre réel (ou complexe), et k, m, n sont des entiers tel que $k < m < n$, alors on a les propriétés suivantes :

1. $\sum_{i=1}^{n} 1 = n$
2. $\sum_{i=1}^{n} ca_i = c\sum_{i=1}^{n} a_i$
3. $\sum_{i=k}^{m} a_i + \sum_{i=m+1}^{n} a_i = \sum_{i=1}^{n} a_i$
4. $\sum_{i=1}^{n}(a_i \pm b_i) = \sum_{i=1}^{n} a_i \pm \sum_{i=1}^{n} b_i$

Exemple 6.1.3. Sachant que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, calculer la somme $\sum_{i=1}^{n+1}(6i+3)$. Pour ce faire, en utilisant les propriétés que nous venons de voir, on obtient :

$$\begin{aligned}
\sum_{i=1}^{n+1}(6i+3) &= \sum_{i=1}^{n}(6i+3) + (6(n+1)+3) \\
&= 6\sum_{i=1}^{n} i + \sum_{i=1}^{n} 3 + (6n+9) \\
&= 6\frac{n(n+1)}{2} + 3n + (6n+9) \\
&= 3n^2 + 12n + 9
\end{aligned}$$

Remarquez qu'il existe une notation semblable pour le produit. Dans ce cas, on utilise la lettre grecque pi majuscule. On a donc par exemple :

$$\prod_{i=1}^{10} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 3628800$$

Cette notation, bien qu'importante à connaitre, est beaucoup moins souvent rencontré que celle pour les sommes. Elle sera utilisé que très rarement dans ce cours.

6.2 Les sommes arithmétiques et géométriques

Cette section commence avec une histoire concernant l'un des plus grand mathématicien de l'histoire, Carl Friedrich Gauss. À l'age de 7 ans, son instituteur J.G.Büttner, donne à ses étudiants la tâche d'additionner tous les entiers de 1 à 100. Bien que le problème aurait dû prendre un temps considérable aux étudiants, le jeune Gauss donne la réponse très rapidement : 5050. Comment a-t-il fait ? [6]

L'idée est particulièrement simple, il s'agit de remarquer que la somme peut être réécrite sous la forme :

$$(1+100) + (2+99) + (3+98) + (4+97) + ... + (50+51)$$

Nous obtenons donc 50 termes, chacun d'entre eux ayant une somme de 101. Ceci nous permet donc d'affirmer que :

$$\sum_{i=1}^{100} i = 50(101) = 5050$$

Le problème peut être généraliser à la somme des n premiers entiers. Ce type de somme est appelé sommes arithmétiques. On est donc amené au théorème suivant :

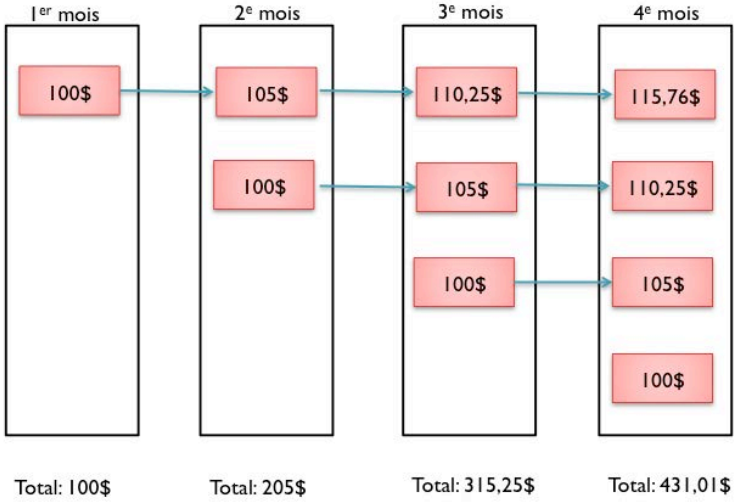
Théorème 6.2.1. Si n est un entier positif, alors on a la formule suivante pour la somme des n premiers entiers positifs :

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Exemple 6.2.1. On veut calculer la somme $\sum_{i=10}^{50}(7i+3)$. Pour ce faire, il suffit de remarquer que :

$$\begin{aligned}\sum_{i=10}^{50}(7i+3) &= \sum_{i=1}^{50}(7i+3) - \sum_{i=1}^{9}(7i+3) = 7\left(\sum_{i=1}^{50} i\right) + \left(\sum_{i=1}^{50} 3\right) - 7\left(\sum_{i=1}^{9} i\right) - \left(\sum_{i=1}^{9} 3\right) \\ &= 7\left(\frac{50(51)}{2}\right) + 3(50) - 7\left(\frac{9(10)}{2}\right) - 3(9) = 8925 + 150 - 315 - 27 = 8733\end{aligned}$$

Le second type de sommes que nous voulons regarder dans cette section sont les sommes géométriques. Pour l'illustrer, considérer le problème suivant. Imaginer que vous placer 100$ à la banque, et chaque mois vous ajouter 100$. Si la banque vous donne 5% d'intérêt par mois, combien d'argent aurez-vous après 5 ans.



Pour résoudre le problème, supposons que la somme est S. En analysant le problème, il est facile de voir que S peut être calculer par la somme suivante :

$$S = 100 + 100(1,05) + 100(1,05)^2 + 100(1,05)^3 + 100(1,05)^4 + ... + 100(1,05)^{60}$$

Maintenant, en multipliant le tout par $1,05$, on obtient donc :

$$1,05S = 100(1,05) + 100(1,05)^2 + 100(1,05)^3 + 100(1,05)^4 + ... + 100(1,05)^{60} + 100(1,05)^{61}$$

En remarque alors que la plupart des termes sont commun aux deux sommes. En effectuant la soustraction, on obtient donc :

$$1,05S - S = 100(1,05)^{61} - 100$$

Pour évaluer la somme, il suffit alors d'isoler le S, ce qui peut être fait facilement. On obtient donc finalement :

$$S = \frac{100(1,05)^{61} - 100}{0,05} \approx 37226,29\$$$

Encore une fois, la méthode peut être généralisé. On est donc amené à énoncé le théorème suivant :

Théorème 6.2.2. Si n est un entier positif, et a, q des nombres réels, on a la formule suivante :

$$\sum_{i=0}^{n} aq^i = \frac{a(q^{n+1}-1)}{q-1}$$

Exemple 6.2.2. On veut évaluer la somme $\sum_{i=5}^{20} \frac{5}{2^i}$. Pour ce faire, il suffit d'appliquer les propriétés des sommes en combinaison avec le théorème précédent. On a donc :

$$\begin{aligned}\sum_{i=5}^{20} \frac{5}{2^i} &= \sum_{i=0}^{20} \frac{5}{2^i} - \sum_{i=0}^{4} \frac{5}{2^i} = \sum_{i=0}^{20} 5\left(\frac{1}{2}\right)^i - \sum_{i=0}^{4} 5\left(\frac{1}{2}\right)^i = \frac{5\left(\frac{1}{2^{21}}\right)-1}{\frac{1}{2}-1} - \frac{5\left(\frac{1}{2^5}\right)-1}{\frac{1}{2}-1} = \left(2-10\left(\frac{1}{2^{21}}\right)\right) - \left(2-10\left(\frac{1}{2^5}\right)\right) \\ &= 10\left(\frac{1}{2^5} - \frac{1}{2^{21}}\right) = 10\left(\frac{2^{16}-1}{2^{21}}\right) = 5\left(\frac{2^{16}-1}{2^{20}}\right) = \frac{327675}{1048576}\end{aligned}$$

6.3 L'induction

Il arrive souvent en mathématiques qu'il soit possible de deviner ou prédire un résultat à partir de cas particulier (souvent en utilisant de petites valeurs de la variable). Le problème est que même si le résultat est vraie pour de petite valeur, ce n'est pas garantie qu'il soit toujours vrai. La question devient alors comment faire pour démontrer que la formule est belle et bien toujours vraie. L'induction est une méthode générale qui permet de répondre à cette question. C'est ce que nous allons étudier dans cette section.

Théorème 6.3.1. **(Principe d'induction)** Si P est une propriété satisfaisant les deux conditions suivantes :

1. La propriété P est vraie pour un entier a.
2. En faisant l'hypothèse que la propriété P est vraie pour un entier k (avec $k \geq a$), on peut démontrer qu'elle est aussi vraie pour l'entier $k+1$.

Alors on peut conclure que la propriété P est vraie pour tous les entiers plus grand ou égal à a.

À partir du théorème, on remarque donc qu'une démonstration par induction doit se faire en 3 étapes :

1. On commence par choisir l'entier de départ a. Il s'agit du premier entier pour lequel on veut montrer que la propriété est vraie. On doit alors démontrer que la propriété est vraie pour l'entier a.
2. On fait l'hypothèse que la propriété est vraie pour un entier $n \in \mathbb{Z}$
3. On démontre que la propriété est encore vraie pour $n+1$.

Si on parvient à compléter les trois étapes, on peut alors conclure que la propriété est vraie pour tout entier plus grand ou égal à a. Nous allons maintenant voir quelques exemples d'application du principe d'induction.

Exemple 6.3.1. On veut démontrer que pour tout nombre naturel n, on a :

$$1+2+3+4+\ldots+n = \frac{n(n+1)}{2}$$

Ou écrit de manière symbolique, on veut démontrer que :

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Pour ce faire, nous allons appliquer le principe d'induction.

1. On doit démontrer que la propriété est vraie lorsque $n = 1$. Pour ce faire, on remarque que :

$$\sum_{i=1}^{1} i = 1 \qquad \text{et} \qquad \frac{1(1+1)}{2} = 1$$

donc la propriété est vraie lorsque $n = 1$.

2. Supposons maintenant que la propriété est vraie lorsque $n = k$, où k est un entier plus grand ou égal à 1. C'est à dire, on suppose que

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

3. On veut maintenant vérifier que la propriété est vraie pour $n = k+1$. On a donc :

$$\sum_{i=1}^{k+1} i = \Big(\sum_{i=1}^{k} i\Big) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k^2+k+2k+2}{2} = \frac{(k+1)(k+2)}{2}$$

Donc à partir de notre hypothèse, on a bien que la propriété est vraie pour $n = k+1$.

Par le principe d'induction, on peut donc conclure que la propriété est vraie pour tout $n \in \mathbb{N}$.

Exemple 6.3.2. On veut utiliser l'induction pour démontrer que pour tout entier $n \geq 1$, on a que $n+4 < 7n^2$. Pour ce faire, nous allons suivre les 3 étapes d'une démonstration par induction :

1. On doit commencer par démontrer que la propriété est vraie si $n = 1$, en remplaçant dans l'équation on a : $1 + 4 < 7(1)^2$ ce qui est vrai car $5 < 7$. La propriété est donc vraie pour $n = 1$.
2. On fait maintenant l'hypothèse que l'inégalité est vraie pour $n = k$. C'est à dire on suppose que $k + 4 < 7k^2$.
3. On veut maintenant démontrer que la propriété est encore vraie pour $n = k+1$ on a donc :

$$\begin{aligned}
(k+1)+4 &= (k+4)+1 \\
&< 7k^2+1 \quad \text{(hypothèse d'induction)} \\
&< (7k^2+1)+(14k+6) \\
&= 7k^2+14k+7 \\
&= 7(k^2+2k+1) \\
&= 7(k+1)^2
\end{aligned}$$

Ce qui est exactement ce que nous voulions montrer.

On peut donc conclure que $n + 4 < 7n^2$ pour tout $n \geq 1$.

Exemple 6.3.3. On veut utiliser l'induction pour démontrer que $8^n - 3^n$ est divisible par 5 pour tout entier $n \geq 1$. Pour ce faire, commençons par nous rappeller qu'un entier a est divisible par 5 si on peut l'écrire sous la forme $a = 5b$ où b est aussi un entier. Nous allons maintenant appliquer l'induction.

1. Comme première étape on doit démontrer que la propriété est vraie si $n = 1$. Dans ce cas, on a $8^1 - 3^1 = 5$, ce qui est évidement divisible par 5. Donc la propriété est satisfaite pour une première valeur.
2. Nous faisons maintenant l'hypothèse que la propriété est vraie pour $n = k$. C'est à dire, on suppose que $8^k - 3^k$ est divisible par 5.
3. On veut maintenant montrer que la propriété est aussi vrai pour $n = k+1$, on a donc :

$$\begin{aligned}
8^{k+1} - 3^{k+1} &= 8 \cdot 8^k - 3 \cdot 8^k + 3 \cdot 8^k - 3 \cdot 3^k \\
&= 5 \cdot 8^k + 3(8^k - 3^k)
\end{aligned}$$

Comme $8^k - 3^k$ est divisible par 5 par l'hypothèse de la seconde étape, il existe donc un entier m tel que $8^k - 3^k = 5m$. On obtient donc :

$$\begin{aligned}
8^{k+1} - 3^{k+1} &= 5 \cdot 8^k + 3(8^k - 3^k) \\
&= 5 \cdot 8^k + 3(5m) \\
&= 5\left(8^k + 3m\right)
\end{aligned}$$

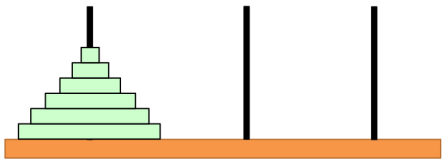
Et donc $8^{k+1} - 3^{k+1}$ est aussi divisible par 5

On peut donc conclure que $8^n - 3^n$ est divisible par 5 pour tout entier $n \geq 1$.

Exemple 6.3.4. Le problème mathématique des tours de Hanoï a été inventé par Édouard Lucas. Il est publié dans le tome 3 de ses Récréations mathématiques, parues à titre posthume en 1892. Le problème consiste à déplacer des disques de diamètres différents d'une tour de départ à une tour d'arrivée en passant par une tour intermédiaire, et ceci en un minimum de coups, tout en respectant les règles suivantes :

1. On ne peut déplacer plus d'un disque à la fois ;
2. On ne peut placer un disque que sur un autre disque plus grand que lui ou sur un emplacement vide.
3. On suppose que cette dernière règle est également respectée dans la configuration de départ.

La question est alors combien de coup est nécessaire pour résoudre le problème avec n disques de départ.



Il existe plusieurs méthodes pour résoudre ce problème. Nous allons dans le cours en présenter un total de 3. Dans chaque cas, la première étape consiste à essayer de trouver une relation de récurrence. Pour ce faire, remarquons que si nous avons un seul disque, un seul coup est nécessaire. Si nous avons deux disques, il s'agit de déplacer le petit disque sur la tour intermédiaire, on déplace ensuite le plus grand disque sur la tour finale, puis on déplace le petit disque sur la tour finale. Donc trois coups sont nécessaires. Maintenant, si nous avons n disques, nous devons commencer par déplacer les $n-1$ plus petits disques sur la tour intermédiaire, plus on déplace le plus grand disque sur la tout finale, et finalement on déplace les $n-1$ plus petit disque sur la tour finale. Donc si on dénote le nombre de coup nécessaire pour déplacer n disque par C_n, on obtient donc la relation suivante :

$$C_n = C_{n-1} + 1 + C_{n-1} = 2C_{n-1} + 1$$

Donc à partir de la valeur de C_1 que nous avons trouvé, on peut ensuite calculer la valeur de C_n pour chaque entier positif n. On obtient donc le tableau suivant :

n	1	2	3	4	5	6	7
C_n	1	3	7	15	31	63	127

Maintenant, en observant les valeurs obtenues, on est amener à faire l'hypothèse que $C_n = 2^n - 1$. Pour le démontrer, on utilise l'induction. On a donc :

1. Si $n = 1$, nous avons $2^1 - 1 = 1$, ce qui correspond à la valeur que nous avions calculer.
2. Supposons que notre formule est vrai pour $n = k$, c'est à dire supposons que $C_k = 2^k - 1$.
3. Si $n = k + 1$, on obtient alors :

$$\begin{aligned} C_{k+1} &= 2C_k + 1 \\ &= 2\left(2^k - 1\right) + 1 \\ &= 2^{k+1} - 2 + 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

Par induction, on peut donc affirmer que notre formule est correcte. La solution du problème des tour de Hanoi est donc

$$C_n = 2^n - 1$$

Exemple 6.3.5. Nous allons maintenant essayer une seconde pour résoudre le problème de la tour de Hanoi. Le point de départ est à nouveau d'essayer de trouver une relation de récurrence. Comme cette partie est identique à ce que nous venons de faire, nous allons tout simplement utiliser la relation de récurrence comme point de départ :

$$\begin{cases} C_n = 2C_{n-1} + 1, & \forall n \geq 2 \\ C_1 = 1 \end{cases}$$

Pour résoudre l'équation de récurrence, on remarque les égalités suivantes :

$$\begin{aligned} C_n = 2C_{n-1} + 1 &= 2\left(2C_{n-2} - +1\right) + 1 = 2^2 C_{n-2} + 2 + 1 \\ &= 2^2\left(2C_{n-3} + 1\right) + 2 + 1 = 2^3 C_{n-3} + 2^2 + 2 + 1 \\ &= 2^3\left(2C_{n-4} + 1\right) + 2^2 + 2 + 1 = 2^4 C_{n-4} + 2^3 + 2^2 + 2 + 1 \\ &= \ldots \\ &= 2^{n-1} + 2^{n-2} + \ldots + 2^3 + 2^2 + 2 + 1 \\ &= \sum_{i=0}^{n-1} 2^i = \frac{2^n - 1}{2 - 1} = 2^n - 1 \end{aligned}$$

Ce qui est la même solution que nous avions déjà obtenu.

Dans certain cas, le principe d'induction, tel que nous l'avons énoncé, n'est pas suffisant pour démontrer un résultat. Lorsqu'on applique de manière stricte le principe d'induction, on utilise uniquement la valeur précédente pour démontrer qu'une propriété est vraie pour une certaine valeur. Nous allons maintenant énoncer une version généralisée du principe d'induction qui nous permettra d'utiliser plusieurs valeurs précédentes pour démontrer un énoncé.

Théorème 6.3.2. (Principe d'induction généralisé) Si P est une propriété satisfaisant les deux conditions suivantes :

1. La propriété est vraie pour tous les entiers entre a et b (avec $a \leq b$).
2. En faisant l'hypothèse que la propriété est vraie pour tous les entiers entre a et k (avec $k \geq b$), on peut démontrer qu'elle est aussi vraie pour l'entier $k + 1$.

Alors on peut conclure que la propriété P est vraie pour tous les entiers plus grand ou égal à a.

Exemple 6.3.6. Nous allons maintenant nous intéressé au problème des pièces de monnaies de Frobenius. Au Royaume-Unis, les pièces de monnaie ont les dénominations 1 penny, 2 pence, 5 pence, 10 pence, 20 pence, 50 pence, 1 pound et 2 pounds. En utilisant seulement des pièces de 2 pence et 5 pence, quel est le plus grand montant d'argent qu'il est impossible de faire ?

Par essaie et erreur, on peut facilement construire le tableau suivant :

Montant	Représentation
1	impossible
2	2
3	impossible
4	2 + 2
5	5
6	2 + 2 + 2
7	5 + 2
8	2 + 2 + 2 + 2
9	5 + 2 + 2

Nous allons maintenant utiliser le principe d'induction généralisé pour montrer qu'il est possible de réaliser tous les entiers supérieurs ou égal à 4 (donc 3 est le plus grand montant qu'il est impossible à faire). Nous

savons déjà qu'il est possible de faire 4 et 5. Supposons qu'il est possible de réaliser tous les montants d'argent entre 4 et k avec $k \geq 6$. On veut maintenant montrer qu'il est possible de faire $k+1$. Pour ce faire, il suffit de remarquer que par hypothèse il est possible de faire $k-1$, et qu'en ajoutant une pièce de 2 pence, on obtient $k+1$. Il est donc possible de réaliser $k+1$. Par le principe d'induction généralisé, il est donc possible de faire tous les montants d'argent supérieur ou égal à 4 pence.

Exemple 6.3.7. Considérons la suite de nombres naturels définie par la relation

$$x_n = 7x_{n-1} - 10x_{n-2} \text{ avec } x_0 = 1 \text{ et } x_1 = 2$$

Utilisez l'induction pour démontrer que $x_n = 2^n$ pour tout $n \geq 0$.

1. Pour $n = 0$ et $n = 1$, on a bien l'égalité. Remarquez que l'on doit vérifier les deux premières valeurs car nous utilisons les deux valeurs précédentes dans notre troisième étape.
2. Supposons que $x_n = 2^n$ pour tout $n \leq k$
3. On veut maintenant montrer que l'équation est vrai pour $n = k+1$:

$$\begin{aligned} x_{k+1} &= 7x_k - 10x_{k-1} \\ &= 7(2^k) - 10(2^{k-1}) \\ &= 2^{k-1}(7 \cdot 2 - 10) \\ &= 2^{k-1}(2^2) \\ &= 2^{k+1} \end{aligned}$$

Ce qui complète la démonstration.

6.4 Le théorème du binôme

Nous allons maintenant utiliser l'induction pour démontrer le théorème du binôme. L'idée du théorème est essentiellement de nous permettre de développer rapidement des expressions de la forme $(a+b)^n$ en utilisant le triangle de Pascal.

Definition 6.4.1. Si $n \in \mathbb{N}$, alors on définit la factorielle, dénoté $n!$, comme étant :

$$n! = \begin{cases} 1 & \text{si } n = 0 \\ 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n & \text{si } n > 0 \end{cases} \tag{6.1}$$

Definition 6.4.2. Si $n, i \in \mathbb{N}$ avec $i \leq n$, alors on définit $\binom{n}{i}$ comme étant :

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

Lemme 6.4.1. *Si $n, i \in \mathbb{N}$ tel que $i \leq n$, alors on a :*

$$\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$$

Démonstration.

$$\begin{aligned} \binom{n}{i-1} + \binom{n}{i} &= \frac{n!}{(i-1)!(n-i+1)!} + \frac{n!}{i!(n-i)!} = \frac{n!i!(n-i)! + n!(i-1)!(n-i+1)!}{i!(i-1)!(n-i+1)!(n-i)!} \\ &= \frac{n!i! + n!(i-1)!(n-i+1)}{i!(i-1)!(n-i+1)!} = \frac{n!i + n!(n-i+1)}{i!(n-i+1)!} \\ &= \frac{n!(n+1)}{i!(n-i+1)!} = \frac{(n+1)!}{i!(n-i+1)!} = \binom{n+1}{i} \end{aligned}$$

□

Théorème 6.4.1. **(Théorème du binôme)** Pour tout $n \in \mathbb{N}$, on a

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

Démonstration. On fait la preuve par induction

1. Si $n = 0$, on a l'égalité $1 = 1$ qui est évidement vraie.
2. Supposons que l'égalité est vraie pour n
3. On doit montré que c'est toujours vrai pour $n+1$:

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

Ce qui complète la preuve. □

Nous pouvons maintenant utiliser ce théorème pour calculer rapidement certains produits. Pour ce faire, nous allons regarder premièrement le triangle de Pascal :

Triangle de Pascal

$n = 0$:					1					
$n = 1$:				1		1				
$n = 2$:			1		2		1			
$n = 3$:		1		3		3		1		
$n = 4$:	1		4		6		4		1	
$n = 5$:	1	5		10		10		5		1

La triangle est obtenu en plaçant premièrement un 1 sur la première ligne, et toutes les autres lignes sont obtenues en commençant et terminant par un 1, et les autres valeurs sont la somme des deux valeurs qui se trouve immédiatement au dessus. Le triangle de Pascal n'est en fait qu'une manière visuelle de représenter le lemme et est utilisé pour calculer rapidement les coefficients de la forme $\binom{n}{i}$. Par exemple, si on souhaite trouver la valeur de $\binom{4}{2}$, on regardera dans la ligne identifié $n = 4$, puis on prendra le 3^e élément. Attention, il ne s'agit pas d'un typo. Le premier élément de chaque ligne est l'élément $i = 0$. On aura donc :

$$\binom{4}{2} = 6$$

Ce qui correspond à la valeur que vous auriez obtenu en calculant les factoriels (vous devriez le vérifier!!!).

Exemple 6.4.1. On veut utiliser le triangle de Pascal pour calculer le produit $(x+2)^5$. On a donc :

$$\begin{aligned}
(x+2)^5 &= x^5 + 5x^4(2)^1 + 10x^3(2)^2 + 10x^2(2)^3 + 5x(2)^4 + 2^5 \\
&= x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32
\end{aligned}$$

Exemple 6.4.2. On veut utiliser le triangle de Pascal pour calculer le produit $(4x-1)^3$. On a donc :

$$\begin{aligned}
(4x-1)^3 &= 1(4x)^3 + 3(4x)^2(-1)^1 + 3(4x)^1(-1)^2 + 1(-1)^3 \\
&= 64x^3 - 48x^2 + 12x - 1
\end{aligned}$$

6.5 Les nids de pigeons

Le principe des nids de pigeons, aussi appelé principe des tiroirs de Dirichlet, est un principe mathématiques particulièrement simple à énoncer et à comprendre, et qui a plusieurs application particulièrement intéressante en mathématiques.

Théorème 6.5.1. **(Principe des nids de pigeons)** Si on souhaite placer $n+1$ objets ou plus dans n boites, alors au moins une boite contiendra deux objets ou plus.

Exemple 6.5.1. On veut montrer que dans une classe de 13 élèves, au moins deux élèves sont né le même mois. Pour ce faire, commençons par identifier nos boites et nos objets. On a donc :

Objets : Les élèves (13)
Boites : Les mois de l'année (12)

Comme nous avons plus d'objets que de boites, le principe des nids de pigeon nous affirme donc qu'au moins une boite contiendra plus qu'un objet, c'est à dire qu'au moins deux élèves sont né le même mois.

Exemple 6.5.2. Dans le cours MATH-1234, les résultats de l'examen final sont des entiers entre 0 et 100. Combien d'étudiants sont nécessaire pour être certain que deux étudiants obtiennent le même résultat ? Premièrement, remarquons qu'il y a 101 entiers entre 0 et 100, car les deux extrémités sont incluse. Il est possible qu'un étudiant obtienne 0%, et il est possible qu'un étudiant obtienne 100%. Intuitivement, le nombre minimal d'étudiant nécessaire devrait donc être 102. Nous allons donc le démontrer en deux étapes :

1. Premièrement, nous voulons montrer que 101 étudiants n'est pas suffisant. Pour ce faire, un exemple est suffisant (Penser au démonstration par contre-exemple). Donc si on a 101 étudiants et que leur résultats sont respectivement :

   $$\{0\%, 1\%, 2\%, 3\%, 4\%, ..., 99\%, 100\%\}$$

   alors tout les étudiants ont obtenues des résultats différent. On peut donc affirmer que dans une classe de 101 étudiants on ne peut pas être certain que deux étudiants obtiennent le même résultat.
2. Dans un deuxième temps, on veut montrer qu'avec 102 étudiants on peut être certain que deux étudiants obtiennent le même résultat. Pour ce faire, on applique le principe des nids de pigeon :

   Objets : Les étudiants (102)
   Boites : Les différents résultats possible (101)

Par le principe des nids de pigeon, comme nous avons plus d'objet que de boite, au moins une boite contiendra plus qu'un objet, c'est à dire qu'au moins deux étudiants auront le même résultat.

Exemple 6.5.3. Supposons que vous possédez exactement 8 paires de bas bleus, et 10 paires de bas rouges, et supposons qu'après avoir fait votre lavage, vous décidé de former des paires aléatoirement, sans tenir compte de la couleur de chaque bas. Démontrer qu'on peut être certain qu'au moins une des paires formé contiendra deux bas de la même couleur. Premièrement, remarquer qu'il est tout à fait possible qu'aucune pair ne contienne deux bas bleus (pouvez-vous trouver un exemple ?), on va donc chercher à démontrer qu'au moins une paire contiendra deux bas rouge. Pour ce faire, on applique le principe des nids de pigeons.

Objets : Les bas rouges (20)
Boites : Les paires de bas (18)

Par le principe des nids de pigeon, comme il y a plus d'objet que de boite, alors au moins une boite contiendra deux objets. Dans ce cas, ceci signifie qu'au moins une paire de bas contiendra deux bas rouges.

Exemple 6.5.4. Lors d'une soirée, 20 personnes sont invités. Au début de la soirée, un certain nombre de poignées de main sont échangé. Bien entendu, personne ne se sert la main à lui même. Démontrer qu'on peut être certain qu'au moins deux des invités on serré la main au même nombre de personnes. Ici le problème est

un peu plus difficile. Il est facile d'identifier que nos objets devrait être les différents invités, mais que sont nos boites ? Comme nous voulons montrer que deux invités on serré le même nombre de poignées de main, nous allons donc choisir le nombre de poignée de main comme nos objet. Une personne pourra donc avoir serré 0 poignée de mains, 1 poignée de mains, 2 poignée de mains, ... etc, jusqu'à 19 poignées de mains. il y a donc 20 possibilités pour le nombre de poignées de main. On a donc :

Objets : Les invités (20)
Boites : Le nombre de poignées de main (20)

Le problème étant que nous avons autant d'objet que de boite. Le principe des nids de pigeons ne peut donc pas s'appliquer directement. Pour remédier au problème, il s'agit de remarquer qu'il est impossible qu'un invité n'est serré aucune poignée de mains, alors qu'un autre invité est serré la main à tout le monde. On va donc pouvoir séparer le problème en deux cas disjoint.

1. Dans un premier temps, supposons que tout les invitées ont serrés au moins une poignée de main. Donc la boite correspondant aux personnes ayant serré aucune poignée de mains est disparu. On a donc :

   Objets : Les invités (20)
   Boites : Le nombre de poignées de main (19)

   Donc si tout les invitées on serré au moins une poignée de main, par le principe des nids de pigeons on peut être certain qu'au moins deux invités ont serré le même nombre de poignées de main.
2. Dans un deuxième temps, supposons qu'au moins un invité n'a serré aucune poignée de main. Donc la boite correspondant aux personnes ayant serré la main de tous les autres invités est disparu. On a donc :

   Objets : Les invités (20)
   Boites : Le nombre de poignées de main (19)

   Donc si au moins un invité n'a serré la main à personne, par le principe des nids de pigeons on peut être certain qu'au moins deux invités ont serré le même nombre de poignées de main.

En combinant ces deux résultats, on peut donc conclure qu'au moins deux invités on serré la main au même nombres de personnes.

Definition 6.5.1. On définie les deux fonctions suivantes :

1. La fonction plancher est la fonction $\lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}$ définie comme étant le plus grand entier inférieur ou égal à x.
2. La fonction plafond est la fonction $\lceil x \rceil : \mathbb{R} \to \mathbb{Z}$ définie comme étant le plus petit entier supérieur ou égal à x.

Noter que bien qu'il s'agisse du vocabulaire adopté pour ce cours, les appellations fonction plancher et fonction plafond sont des traductions littérale de l'anglais, et sont des termes peut commun en français. De plus, la notation $\lceil x \rceil$ est couramment utilisé à la place de $\lfloor x \rfloor$. Cette notation sera cependant à éviter dans ce cours pour éviter de la confusion.

Théorème 6.5.2. **(Principe des nids de pigeons généralisés)** Si on veut placer n objets dans r boites, alors au moins une boite contiendra au moins $\left\lceil \frac{n}{r} \right\rceil$ objets.

Chapitre 7

La combinatoire

7.1 Introduction et méthodes élémentaires

La combinatoire est une discipline des mathématiques qui consiste à étudier l'art de compter le nombre de possibilités d'avoir certaine configuration. Il s'agit d'une discipline directement relié à la théorie des probabilité, et en conséquence à la statistique. La combinatoire fait aussi sont apparition dans plusieurs autres domaines des mathématiques, comme par exemple en géométrie, analyse et algèbre.

La méthode la plus simple pour résoudre un problème de combinatoire consiste à **énumérer toutes les possibilités**, puis de compter directement combien nous en avons. Il s'agit bien entendu d'une méthode qui peut devenir rapidement très longue, mais elle reste néanmoins toujours (en théorie) possible à utiliser. Voici quelques exemples illustrant la méthode.

Exemple 7.1.1. Combien y a-t-il de façons différentes de tirer trois fois (consécutif) à pile ou face ? Si on dénote pile par P et face par F, on obtient les possibilités suivante :

PPP - PPF - PFP - PFF - FPP - FPF - FFP - FFF

Nous avons donc 8 possibilités.

Exemple 7.1.2. Combien y a-t-il de façons différentes de tirer trois fois (consécutif) à pile ou face sans avoir deux piles consécutifs ? Pour ce faire, il s'agit de regarder toutes les possibilités que nous avons énumérer dans l'exemple précédent, et d'éliminer celle qui contiennent deux piles consécutifs. On a donc les possibilités suivantes :

PFP - PFF - FPF - FFP - FFF

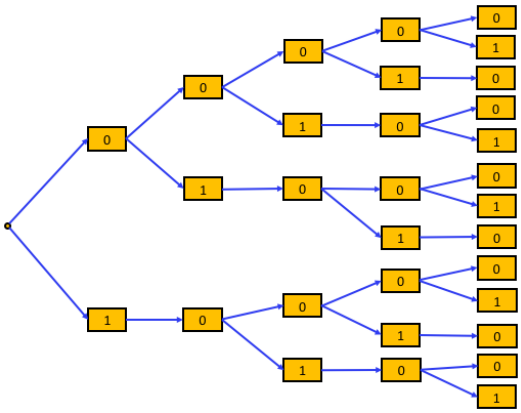
Nous avons donc 5 possibilités.

Énumérer toutes les possibilités peut devoir rapidement difficile pour deux raisons principales

1. Si le nombre de possibilités est élevé, faire une liste complète devient trop long.
2. Le manque d'ordre dans nos énumérations fait qu'il est particulièrement facile d'oublier certaines possibilités.

La première difficulté sera traiter dans les prochaines sections en développant différentes formules permettant de simplifier les calculs. Par contre, la deuxième difficulté peut dans certain cas être résolus facilement en introduisant différentes techniques d'organisation de nos différentes possibilités. L'une de ces techniques particulièrement utile consiste à présenter les possibilités sous forme d'un **diagramme en arbres**. Ceci est illustré dans l'exemple ci-dessous :

Exemple 7.1.3. Combien y a-t-il de chaine binaire de longueur 5 qui n'ont pas deux 1 consécutifs ? Pour ce faire, nous allons construire un diagramme en arbre. On a donc 13 différentes possibilités.



Exercice 7.1.1. Au hockey, dans la LNH, le gagnant d'une ronde de série éliminatoire est la première équipe à remporter 4 victoires sur un maximum de 7 parties joués. C'est ce qu'on appelle une série 4 de 7. Combien y a-t-il de configuration différente possible pour les victoires / défaites dans une telle série ?

7.2 Principe du produit, de la somme et d'inclusion-d'exclusion

Nous allons maintenant nous intéresser aux différents principes de base de la combinatoire : Le principe du produit, le principe de la somme et le principe d'inclusion-d'exclusion.

Théorème 7.2.1. **(Principe du produit)** S'il y a n_1 façons de compléter la tâche 1 et n_2 façons de compléter la tâche 2, alors il y a $n_1 n_2$ façons de compléter la tâche 1 et la tâche 2.

Exemple 7.2.1. Si une classe est composé de 25 femmes et 20 hommes, alors il y a $20 \times 25 = 500$ façons de choisir un homme et une femme parmi les étudiants de la classe.

Exemple 7.2.2. Dans une grande compagnie, on attribue à chaque employé un code d'identification. Ce code est formé de 2 lettres, suivi de 3 chiffres. Combien de code différent peut-on attribuer ? Pour ce faire, remarquons que le problème revient à choisir une lettre ET une lettre ET un chiffre ET un chiffre ET un chiffre. Il s'agit donc d'une application du principe du produit.

LETTRE - LETTRE - CHIFFRE - CHIFFRE - CHIFFRE

Comme il y a 26 lettres et 10 chiffres, on obtient donc :

$$26 \times 26 \times 10 \times 10 \times 10 = 26^2 \times 10^3 = 676\ 000 \text{ possibilités}$$

Théorème 7.2.2. **(Principe de la somme)** Si une tâche peut être complété soit de n_1 façons ou de n_2 façons, et aucune de ces méthodes sont en commun, alors il y a $n_1 + n_2$ façons de compléter la tâche.

Exemple 7.2.3. Si une classe est composé de 25 femmes et 20 hommes, alors il y a $20 + 25 = 45$ façons de choisir un étudiant dans la classe.

Exemple 7.2.4. Pour satisfaire les exigences de son programme d'étude, un étudiant doit choisir un cours d'informatique, de mathématiques ou de statistique. S'il y a 10 cours d'informatique, 20 cours de mathématiques et 15 cours de statistiques (tous accessible à l'étudiant), combien y a-t-il de façon pour l'étudiant de choisir son cours ? Ici on remarque que l'étudiant doit en fait choisir un cours d'informatique

OU un cours de mathématiques OU un cours de statistique. En faisant l'hypothèse qu'aucun cours n'appartient à plus qu'une discipline, on remarque donc qu'il s'agit d'une application du principe de la somme. On a donc :

$$10 + 20 + 15 = 45 \text{ possibilités}$$

Théorème 7.2.3. **(Principe d'inclusion-d'exclusion)** Si une tâche peut être complété soit de n_1 façons ou de n_2 façons, et qu'il y a n_3 de ces méthodes qui sont en commun, alors il y a $n_1 + n_2 - n_3$ façons de compléter la tâche.

Ce dernier théorème est plus facilement compris si on réalise qu'il s'agit en fait d'une méthode pour déterminer la cardinalité de l'union de deux ensembles. En effet, si A et B sont des ensembles, alors on a l'égalité suivante :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Exemple 7.2.5. Combien y a-t-il de mots de 5 lettres commençant par A ou se terminant par ZZ ? Notez qu'ici un mot fait référence à un agencement de lettre quelconque et pas nécessairement un mot que l'on peut trouver dans un dictionnaire français ou anglais. Par exemple $ABCZZ$ serait un mot acceptable. Ici, le OU nous fait penser qu'il s'agit du principe de la somme. Mais en portant un attention particulière au problème, on réalise que ce n'est pas le cas, car il y a plusieurs mots qui comme par A et se termine par ZZ. Il s'agit donc d'une application du principe d'inclusion-d'exclusion. Le nombre de possibilité sera donc donné par :

(Nombre de mots commençant par A) + (Nombre de mots terminant par ZZ) - (Nombre de mots commençant par A et terminant par ZZ)

Maintenant, pour calculer chacune ces composantes, on remarque qu'il s'agit d'application du principe du produit. Pour le nombre de mot commençant par A, on a donc :

$$1 \times 26 \times 26 \times 26 \times 26 = 26^4 = 456\ 976 \text{ possibilités}$$

Pour le nombre de mots se terminant par ZZ, on a :

$$26 \times 26 \times 26 \times 1 \times 1 = 26^3 = 17\ 576 \text{ possibilités}$$

Puis le nombre de mots commençant par A et se terminant par ZZ est donné par :

$$1 \times 26 \times 26 \times 1 \times 1 = 26^2 = 676 \text{ possibilités}$$

Le principe d'inclusion-d'exclusion nous affirme donc que le nombre de mot commençant par A ou se terminant par ZZ est donné par :

$$26^4 + 26^3 - 26^2 = 456976 + 17576 - 676 = 473\ 876 \text{ possibilités}$$

Exercice 7.2.1. Si n est un nombre naturel, $A = \{1, 2, 3, ..., n\}$ et $B = \{1, 2\}$

1. Combien y a-t-il de relations entre A et B ?
2. Combien y a-t-il de fonctions $f : A \to B$?
3. Combien y a-t-il de fonctions $f : B \to A$?
4. Combien y a-t-il de fonctions surjectives $f : A \to B$?
5. Combien y a-t-il de fonctions injectives $f : B \to A$?
6. Combien y a-t-il de fonctions bijectives $f : A \to B$?

7.3 Combinaison, arrangement et permutation

En combinatoire, la question de savoir combien il y a de façon de choisir r objet parmi n revient très souvent. Dans cette section, nous allons donc développer des formules simples permettant de répondre à cette question dans chacun des quatres cas qui peuvent se poser dépendant que le problème se fait avec ou sans remise, et avec ou sans ordre.

Definition 7.3.1. Un arrangement est une disposition ordonné d'un certain nombre d'élément choisi d'un ensemble donné. Dans le cas particulier ou tout les éléments de l'ensemble sont choisi et ordonné, on parle alors de permutation.

Le cas le plus simple est celui d'un arrangement avec remise. Supposons que nous voulons faire un arrangement de r objet choisi parmi n et que les répétitions sont permise (donc avec remise), le principe du produit nous affirme donc que nous aurons :

$$\underbrace{n \times n \times n \times ... \times n}_{r \text{ fois}} = n^r$$

possibilités. Dans le cas d'un arrangement de r objets parmi n, l'idée reste relativement semblable lorsque l'on pense en terme de la règle du produit. On aura donc n façons de choisir le premier objet, puis $(n-1)$ façons de choisir le second, puis $(n-2)$ façons de choisir le troisième, et ainsi de suite jusqu'à $(n-r+1)$ façon pour le dernier. On obtient donc :

$$n \times (n-1) \times (n-2) \times (n-3) \times ... \times (n-r+1) = \frac{n \times (n-1) \times (n-2) \times ... \times 2 \times 1}{(n-r) \times (n-r-1) \times (n-r-2) \times ... \times 2 \times 1} = \frac{n!}{(n-r)!}$$

Definition 7.3.2. Un combinaison est une disposition non-ordonné d'un certain nombre d'élément choisi d'un ensemble donné.

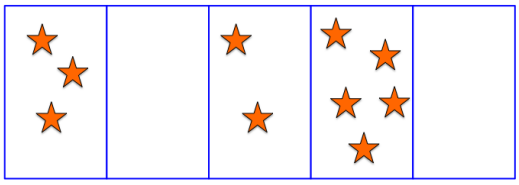
Lorsque l'ordre des objets choisis n'est pas importante, le problème se complique un peu. Dans un premier temps, supposons que nous voulons choisir r objets parmi n sans ordre et sans remise. Nous savons déjà qu'avec ordre, il y a $\frac{n!}{(n-r)!}$ façon de résoudre ce problème. De plus chacune de ces arrangement peut être réordonné de $r!$ façon différente. Donc chacune de ces arrangement donne lieu à $r!$ arrangement qui son équivalente si on ne tient pas compte de l'ordre. Il suffit donc de diviser le nombre d'arrangement par $r!$ pour obtenir le nombre de combinaison. On a donc la formule suivante :

$$\frac{n!}{r!(n-r)!}$$

Exemple 7.3.1. Dans une classe de 50 étudiants, combien y a-t-il de façons différentes de former une équipe de 2 étudiants ? Pour ce faire, on commence par remarquer que le problème se fait sans remise et sans ordre. La formule que nous venons de développer s'applique donc.

$$\frac{50!}{2!(50-2)!} = \frac{50!}{2!\ 48!} = \frac{49 \times 50}{2} = 1225 \text{ possibilités}$$

Le dernier des 4 problèmes consiste à trouver un nombre de combinaison de r objet choisi parmi n, mais cette fois avec remise. Il s'agit du plus difficile des 4 problèmes. Nous allons donc illustrer le problème à l'aide d'un cas particulier, puis revenir à la solution générale par la suite. Supposons qu'on veut choisir 10 objets parmi 5 types différent, avec remise et sans ordre. La première étape de la résolution consiste à réaliser que le problème est en fait équivalent à celui de placer 10 étoiles dans 5 cases différentes. En effet, chaque case correspond à un type d'objet, et les étoiles consiste à choisir un objet de ce type. Voici un exemple de l'une des configurations possible.



Ensuite, il s'agit de remarquer que la configuration ci-dessus peut être réécrite de manière symbolique sous la forme :

$$***||**|*****|$$

Ou chaque $*$ représente une étoile, et les barres verticales $|$ représentent la délimitation entre chacune des cases. Notez qu'il est inutile de placer une barre verticale au tout début et à la toute fin, car celle-ci serait fixe pour chacune des configuration possible. Donc seule les délimitations entre deux cases sont notés. Le problème est donc équivalent à trouver combien il y a de façon d'arranger 10 étoiles et 4 barres verticales. C'est ici le point le plus intéressant. Ce dernier problème est en fait équivalent à sélectionner 10 emplacement pour nos étoiles, sur une possibilité de 14 emplacement au total. Notre configuration qui nous a servi d'exemple peut donc être illustré comme suit :

Il s'agit donc de choisir 10 cases parmi 14, sans ordre et sans remise, ce que nous savons déjà faire. Le nombre de possibilité est donc :

$$\frac{14!}{10!\,4!}$$

Maintenant, pour le problème général de choisir r objets parmi n sans ordre et avec remise, la solution est très semblable. Il faudra donc trouvé combien il y a de façon d'arranger r étoiles et $n-1$ barres verticales. Le $n-1$ venant du fait que si nous avons n cases, alors il doit y avoir $n-1$ délimitations entre les cases. Ensuite, on réalise que le problème revient donc à placer r étoiles dans $r+n-1$ emplacement, sans ordre et sans remise. La solution générale doit donc être :

$$\frac{(r+n-1)!}{r!(n-1)!}$$

Exemple 7.3.2. Au Canada, les billets de banques viennent en dénomination de 5\$, 10\$, 20\$, 50\$ et 100\$. Combien y a-t-il de façon de choisir 4 billets de banques (pas nécessairement différent) ? Comme il est tout à fait acceptable de choisir plusieurs fois la même dénomination, le problème est avec remise. Par contre, l'ordre dans lequel les billets sont choisir n'a pas d'importance, le problème est donc sans ordre. On peut donc appliquer la formule que nous venons de développer. On a donc :

$$\frac{(4+5-1)!}{4!(5-1)!} = \frac{8!}{4!\,4!} = \frac{5\times 6\times 7\times 8}{2\times 3\times 4} = \frac{1680}{24} = 70 \text{ possibilités}$$

Les 4 façons de compter que nous avons étudié dans cette section sont résumé dans le théorème ci-dessous sous forme d'un tableau.

Théorème 7.3.1. Le nombre de façon de choisir r objet parmi n, en supposons que les n objets sont tous distincts, est donné par le tableau suivant :

	Sans remise	Avec remise
Sans ordre	$\frac{n!}{r!(n-r)!}$	$\frac{(n+r-1)!}{r!(n-1)!}$
Avec ordre	$\frac{n!}{(n-r)!}$	n^r

7.4 Permutation d'objet indistingable

Nous avons vu dans la section précédente qu'il y a $n!$ différente permutation de n objets. Le problème étant que pour que cette formule soit valide, les n objets doivent tous être distincts. Qu'arrive-t-il si certain de ces n objets sont identiques ? Ces ce que nous allons regarder dans cette section.

Supposons que nous avons n_1 objets de type 1, n_2 objets de type 2 et n_3 objets de type 3. Combien y a-t-il de façon d'ordonner ces $n_1 + n_2 + n_3$ objets ? Pour ce faire, on commence par placer les objets de type n_1. Pour ce faire, il s'agit de choisir n_1 positions parmi $n_1 + n_2 + n_3$ emplacement possible. On a donc :

$$\frac{(n_1 + n_2 + n_3)!}{n_1!(n_1 + n_2 + n_3 - n_1)!} = \frac{(n_1 + n_2 + n_3)!}{n_1!(n_2 + n_3)!}$$

Maintenant, il nous reste $n_2 + n_3$ emplacement vide pour les objets restant. Nous allons placer les objets de type 2. On doit donc choisir n_2 emplacement parmi un total de $n_2 + n_3$ emplacement restante. On a donc :

$$\frac{(n_2 + n_3)!}{n_2!(n_2 + n_3 - n_2)!} = \frac{(n_2 + n_3)!}{n_2!\ n_3!}$$

On remarque ensuite que les n_3 emplacement restante doivent être remplie par les objets de type 3. Il y a donc seulement une possibilité pour placer les objets de ce type. Finalement, remarquons que nous avons placer les objets de type 1 ET les objets de type 2 ET les objets de type 3. Il s'agit donc d'appliquer le principe du produit pour compléter le problème. On a donc :

$$\frac{(n_1 + n_2 + n_3)!}{n_1!(n_2 + n_3)!} \cdot \frac{(n_2 + n_3)!}{n_2!\ n_3!} = \frac{(n_1 + n_2 + n_3)!}{n_1!\ n_2!\ n_3!}$$

Cette formule peut être généralisé, ce que nous allons énoncé sous forme d'un théorème.

Théorème 7.4.1. Le nombre de permutation de n_1 objets de type 1, n_2 objets de type 2, n_3 objets de type 3,...,n_k objets de type k est donné par la formule :

$$\frac{(n_1 + n_2 + n_3 + ... + n_k)!}{n_1!\ n_2!\ n_3!\ ...\ n_k!}$$

Exemple 7.4.1. En mathématiques, un mot est une combinaison de lettre ordonné qui peut avoir un sens ou non en français. Combien y a-t-il de mots différents que l'on peut former à l'aide des lettres du mot MISSISSIPPI ? Pour ce faire, on commence par compter le nombre de lettre de chaque type :

Lettre	Fréquence
M	1
I	4
S	4
P	2

En applicant la formule du théorème, on obtient donc :

$$\frac{(1 + 4 + 4 + 2)!}{1!\ 4!\ 4!\ 2!} = \frac{11!}{1!\ 4!\ 4!\ 2!} = 34650 \text{ possibilités}$$

7.5 Les relations de récurrence

En 1202, Leonardo Pisano dit Fibonacci, un mathématicien italien, énonce dans son livre liber abaci le problème connu aujourd'hui sous le nom du problème des lapins. Au premier mois, il y a une paire de lapereaux, trop jeune pour procréer. Si chaque couple de lapereaux prend un mois avant de devenir adulte, et si chaque couple adulte donne naissance chaque mois à un couple de lapereaux après un mois de gestation,

combien de lapin aurons nous après x mois ? Ce problème donna naissance à ce qu'on appelle aujourd'hui la suite de Fibonacci, et il est facile d'en trouver les premières valeurs de la suite. On a donc :

$$1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

Si on dénote par F_n le nombre de lapin présent au n^e mois, alors on remarque facilement la relation suivante :

$$F_n = F_{n-1} + F_{n-2}, \quad \forall n \geq 3$$

De plus, bien que la relation de s'applique pas pour $n = 1$ et $n = 2$, leur valeur sont facile à identifier dans le problème. On a donc $F_1 = F_2 = 1$. Une suite définie de cette manière porte le nom de suite définie par récurrence.

Théorème 7.5.1. Si r_1 et r_2 sont les racines du polynôme $r^2 = c_1 r + c_2$, alors la solution générale de l'équation définie par récurrence

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

peut avoir l'une des deux formes suivantes :

1. Si $r_1 \neq r_2$, alors la solution générale a la forme $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ où α_1 et α_2 sont des constantes.
2. Si $r_1 = r_2$, alors la solution générale a la forme $a_n = \alpha_1 r_1^n + \alpha_2 n r_1^n$ où α_1 et α_2 sont des constantes.

Nous allons maintenant nous attaquer à la solution du problème des lapins

Exemple 7.5.1. Quelle est la solution de la suite définie par récurrence suivante :

$$\begin{cases} F_n = F_{n-1} + F_{n-2} \\ F_1 = 1 \\ F_2 = 1 \end{cases}$$

Pour appliquer le théorème, on doit commencer par trouver les racines du polynôme suivant :

$$x^2 = x + 1 \quad \Rightarrow \quad x^2 - x - 1 = 0$$

Ce qui nous donne :

$$r_1 = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad r_2 = \frac{1-\sqrt{5}}{2}$$

Ce qui nous donne une solution générale de la forme :

$$F_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Il reste maintenant à trouver les deux constantes. Pour ce faire, on utilise la valeur de F_1 et F_2, ce qui nous donne le système d'équations linéaires suivant :

$$\begin{cases} \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right) = 1 \\ \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 = 1 \end{cases}$$

Ce qui a comme solution les valeurs $\alpha_1 = \frac{1}{\sqrt{5}}$ et $\alpha_2 = \frac{-1}{\sqrt{5}}$. La solution de l'équation définie par récurrence est donc :

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Exemple 7.5.2. On veut résoudre l'équation définie par récurrence suivante :

$$\begin{cases} a_n = -4a_{n-1} + 77a_{n-2}, \quad \forall n \geq 3 \\ a_1 = 41 \\ a_2 = 683 \end{cases}$$

Pour ce faire, on doit commencer par résoudre l'Équation $r^2 = -4r + 77$ c'est à dire trouver les racines du polynôme $r^2 + 4r - 77 = 0$.

$$r = \frac{-4 \pm \sqrt{4^2 - 4(1)(-77)}}{2(1)} = \frac{-4 \pm \sqrt{324}}{2} = \frac{-4 \pm 18}{2} = -2 \pm 9 = 7 \text{ et } -11$$

Donc la solution de l'équation aura donc la forme :

$$a_n = 7^n\alpha_1 + (-11)^n\alpha_2, \quad \forall n \geq 1$$

Pour trouver α_1 et α_2, on utilise les valeurs $a_1 = 41$ et $a_2 = 683$, ce qui nous amène au système d'équations linéaires suivant :

$$\begin{cases} 7\alpha_1 - 11\alpha_2 = 41 \\ 49\alpha_1 + 121\alpha_2 = 683 \end{cases} \Rightarrow \begin{cases} 49\alpha_1 - 77\alpha_2 = 287 \\ 49\alpha_1 + 121\alpha_2 = 683 \end{cases} \Rightarrow 198\alpha_2 = 396 \Rightarrow 2$$

Puis en remplaçant dans la première équation on trouve $\alpha_1 = 9$, ce qui nous donne la solution suivante :

$$a_n = 9(7)^n + 2(-11)^n, \quad \forall n \geq 1$$

Exemple 7.5.3. On veut résoudre l'équation définie par récurrence suivante :

$$\begin{cases} a_n = 8a_{n-1} - 16a_{n-2}, \quad \forall n \geq 3 \\ a_1 = 20 \\ a_2 = 128 \end{cases}$$

Pour ce faire, on commence par trouver les solutions de l'équation $r^2 = 8r - 16$, c'est à dire trouver les racines du polynôme $r^2 - 8r + 16 = 0$.

$$r = \frac{8 \pm \sqrt{(-8)^2 - 4(1)(16)}}{2(1)} = \frac{8 \pm 0}{2} = 4$$

Donc la seule racine est r. On peut donc affirmer que la solution aura la forme

$$a_n = \alpha_1(4)^n + \alpha_2 n(4)^n$$

Il faut maintenant trouver la valeur des constantes, pour ce faire, on doit résoudre le système d'équations linéaires suivant :

$$\begin{cases} 4\alpha_1 + 4\alpha_2 = 20 \\ 16\alpha_1 + 32\alpha_2 = 128 \end{cases} \Rightarrow \begin{cases} 16\alpha_1 + 16\alpha_2 = 80 \\ 16\alpha_1 + 32\alpha_2 = 128 \end{cases} \Rightarrow 16\alpha_2 = 48 \Rightarrow \alpha_2 = 3$$

Puis en utilisant la première équation on obtient $\alpha_1 = 2$. La solution est donc :

$$a_n = 2(4)^n + 3n(4)^n, \quad \forall n \geq 1$$

7.6 Les fonctions génératrices

Le théorème que nous avons vu dans la section précédente est particulièrement utile, et permet de résoudre facilement plusieurs équations définie par récurrence. Le problème étant cependant que si nous avons une équation définie par récurrence qui n'a pas la forme prescrite, la méthode échoue. Par exemple, la relation obtenu en essayant de résoudre le problème des tours de Hanoi ne peut pas être résolu avec le théorème. Il

existe une méthode beaucoup plus générale (mais aussi plus difficile) pour résoudre des récurrences. Il s'agit de la méthode des fonctions génératrices.

L'idée est relativement simple. Si a_n est une suite, alors on lui associe la série $\sum_{i=0}^{\infty} a_n x^n$. Comme il s'agit d'une bijection, si on parvient à trouver les coefficient dans la série, on aura trouvé notre suite. Pour pouvoir utiliser cette idée, deux théorèmes nous serons particulièrement utile :

Théorème 7.6.1. **(Séries géométriques)** Si $a, q \in \mathbb{R}$ tel que $|q| < 1$, alors on a l'égalité suivante :

$$\sum_{k=0}^{\infty} q^n = \frac{1}{1-q}.$$

Démonstration. Une démonstration complète nécessite des bases de calcul différentiel et intégral. Pour les besoins de notre cours, nous allons donc seulement en donner une idée. Nous avons déjà démontré en utilisant l'induction que si $a, q \in \mathbb{R}$ et $q \neq 1$, alors on a :

$$\sum_{k=0}^{n} aq^k = \frac{a\left(q^{n+1}-1\right)}{q-1} = \frac{a\left(1-q^{n+1}\right)}{1-q}$$

Maintenant, remarquons que si $-1 < q < 1$, alors q^n devient de plus en plus proche de 0 lorsque n augmente. En particulier, si n est proche de l'infinie, alors q^n deviendra tellement proche de 0, qu'il nous sera impossible de le distinguer de 0. La notion de limite permet de formaliser cette idée, mais pour nous notre idée intuitive sera suffisante. En remplaçant n par l'infinie dans notre équation, on obtient donc que $q^n = 0$, ce qui nous donne finalement :

$$\sum_{k=0}^{\infty} aq^k = \frac{a(1-0)}{1-q} = \frac{a}{1-q}$$

□

Théorème 7.6.2. **(Fractions partielles)** Pour tout $a, b, c, d, e, f \in \mathbb{R}$ tel que $cf - ed \neq 0$, il existe des constantes $A, B \in \mathbb{R}$ satisfaisant l'égalité ci-dessous :

$$\frac{ax+b}{(cx+d)(ex+f)} = \frac{A}{cx+d} + \frac{B}{ex+f}$$

Démonstration. L'idée est dé réécrire notre équation sous forme de système d'équations linéaires, et de montrer ensuite que ce système doit avoir au moins une solution.

$$\frac{ax+b}{(cx+d)(ex+f)} = \frac{A}{cx+d} + \frac{B}{ex+f} = \frac{A(ex+f)+B(cx+d)}{(cx+d)(ex+f)} = \frac{(Ae+Bc)x+(Af+Bd)}{(cx+d)(ex+f)}$$

Ce qui nous donne le système d'équations linéaires suivant (Les inconnues étant A et B).

$$\begin{cases} eA + cB = a \\ fA + dB = b \end{cases} \Rightarrow \begin{cases} efA + cfB = af \\ efA + edB = eb \end{cases}$$

En faisant la soustraction, on obtient donc $(cf - ed)B = af - eb$. Cette dernière aura donc exactement une solution tant que $cf - ed \neq 0$. Une fois que la valeur de B est connu, on peut ensuite calculer A à partie de la première équation du système :

$$eA + cB = a \quad \Rightarrow \quad A = \frac{a - cB}{e}, \quad \text{si } e \neq 0$$

Dans le cas ou $e = 0$, il nous faut utiliser la seconde équation, ce qui nous donne :

$$fA + dB = b \quad \Rightarrow \quad A = \frac{b - dB}{f}, \quad \text{si } f \neq 0$$

On note finalement que e et f ne peuvent pas être simultanément 0, car autrement on aurait $cf - ed = 0$, ce qui nous avons exclut. On peut donc toujours trouver des constantes A et B qui satisfont l'équation. □

Comme première application de la méthode des fonctions génératrices, nous allons appliquer la théorie pour résoudre le problème des tours de Hanoi.

Exemple 7.6.1. On veut utiliser la technique des fonctions génératrices pour résoudre le problème des tours de Hanoi, c'est à dire résoudre l'équation définie par récurrence suivante :

$$\begin{cases} C_n = 2C_{n-1} + 1 \\ C_1 = 1 \end{cases}$$

Considérons la somme infinie ci-dessous (appelé série) qui a comme coefficient les éléments de notre suite.

$$\sum_{i=1}^{\infty} C_i x^i$$

Le x ici représente une variable, de sorte qu'on peut imaginer les différents C_i comme étant les coefficients d'un polynôme de degré infinie. Notons que si nous parvenons à trouver les coefficient qui se trouve dans notre série, nous aurons en même temps les différents éléments de notre suite. En utilisant la relation de récurrence, on a donc :

$$\begin{aligned} \sum_{i=1}^{\infty} C_i x^i &= \sum_{i=2}^{\infty} C_i x^i + C_1 x = \sum_{i=2}^{\infty} \left(2C_{i-1} + 1\right) x^i + C_1 x = 2\sum_{i=2}^{\infty} C_{i-1} x^i + \sum_{i=2}^{\infty} x^i + x \\ &= 2\sum_{i=1}^{\infty} C_i x^{i+1} + \sum_{i=2}^{\infty} x^i + x = 2x\sum_{i=1}^{\infty} C_i x^i + \sum_{i=0}^{\infty} x^i - 1 - x + x = 2x\sum_{i=1}^{\infty} C_i x^i + \frac{1}{1-x} - 1 \end{aligned}$$

Maintenant, en isolant la somme, on obtient :

$$(1 - 2x)\sum_{i=1}^{\infty} C_i x^i = \frac{1}{1-x} - 1 \qquad \Rightarrow \qquad \sum_{i=1}^{\infty} C_i x^i = \frac{1}{(1-x)(1-2x)} - \frac{1}{1-2x}$$

Maintenant, rendu à cette étape, on utilise la décomposition en fractions partielles qui nous affirme qu'il existe des constantes A et B de sorte qu'on est l'égalité suivante :

$$\frac{1}{(1-x)(1-2x)} = \frac{A}{1-x} + \frac{B}{1-2x} = \frac{A(1-2x) + B(1-x)}{(1-x)(1-2x)} = \frac{(-2A - B)x + (A + B)}{(1-x)(1-2x)}$$

Comme les dénominateurs sont égaux, les numérateurs doivent aussi être égaux, ce qui nous amène à résoudre le système d'équations linéaires suivant :

$$\begin{cases} -2A - B = 0 \\ A + B = 1 \end{cases}$$

qui a comme solution $A = -1$ et $B = 2$. En revenant à notre somme, on a donc :

$$\begin{aligned} \sum_{i=1}^{\infty} C_i x^i &= \frac{1}{(1-x)(1-2x)} - \frac{1}{1-2x} = \frac{-1}{1-x} + \frac{2}{1-2x} - \frac{1}{1-2x} = \frac{-1}{1-x} + \frac{1}{1-2x} = -\sum_{i=0}^{\infty} x^i + \sum_{i=0}^{\infty} (2x)^i \\ &= -\sum_{i=0}^{\infty} x^i + \sum_{i=0}^{\infty} 2^i x^i = \sum_{i=0}^{\infty} \left(2^i - 1\right) x^i = \sum_{i=1}^{\infty} \left(2^i - 1\right) x^i \end{aligned}$$

Finalement, pour que les deux sommes (séries) soient égales, les coefficients doivent être égaux, ce qui nous donne :

$$C_i = 2^i - 1$$

Ce qui est encore une fois la même solution que nous avions déjà trouvé.

Exemple 7.6.2. On veut résoudre l'équation de récurrence suivante :

$$\begin{cases} a_n = 5a_{n-1} + 14a_{n-2}, \quad \forall n \geq 2 \\ a_0 = 7 \\ a_1 = 22 \end{cases}$$

Méthode 1 Nous allons commencer par utiliser le théorème de la section précédente. Pour ce faire, on doit trouver les racines du polynôme suivant :

$$\lambda^2 = 5\lambda + 14 \quad \Rightarrow \quad \lambda^2 - 5\lambda - 14 = 0 \quad \Rightarrow \quad (\lambda - 7)(\lambda + 2) = 0$$

Les racines sont donc $\lambda_1 = 7$ et $\lambda_2 = -2$. La solution de l'équation de récurrence aura donc la forme suivante :

$$a_n = C_1(7)^n + C_2(-2)^n$$

Pour trouver les constantes, on utilise les conditions initiale :

$$\begin{cases} a_0 = 7 = C_1 + C_2 \\ a_1 = 22 = 7C_1 - 2C_2 \end{cases}$$

De la première équation, on obtient $C_1 = 7 - C_2$, puis en remplaçant dans la seconde on obtient :

$$22 = 7(7 - C_2) - 2C_2 = 49 - 7C_2 - 2C_2 = 49 - 9C_2 \quad \Rightarrow \quad 9C_2 = 27 \quad \Rightarrow \quad C_2 = 3$$

Ce qui nous donne finalement $C_1 = 7 - 3 = 4$. La solution de l'équation de récurrence est donc :

$$a_n = 4(7)^n + 3(-2)^n, \quad \forall n \geq 0$$

Méthode 2 : Nous allons maintenant appliquer la méthode des fonctions génératrices.

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n &= 7 + 22x + \sum_{n=2}^{\infty} a_n x^n = 7 + 22x + \sum_{n=2}^{\infty} (5a_{n-1} + 14a_{n-2})x^n = 7 + 22x + 5\sum_{n=2}^{\infty} a_{n-1}x^n + 14\sum_{n=2}^{\infty} a_{n-2}x^n \\ &= 7 + 22x + 5x\sum_{n=2}^{\infty} a_{n-1}x^{n-1} + 14x^2\sum_{n=2}^{\infty} a_{n-2}x^{n-2} = 7 + 22x + 5x\sum_{n=1}^{\infty} a_n x^n + 14x^2\sum_{n=0}^{\infty} a_n x^n \\ &= 7 + 22x + 5x\left(\sum_{n=0}^{\infty} a_n x^n - a_0\right) + 14x^2\sum_{n=0}^{\infty} a_n x^n = 7 + 22x + 5x\left(\sum_{n=0}^{\infty} a_n x^n - 7\right) + 14x^2\sum_{n=0}^{\infty} a_n x^n \\ &= 7 + 22x + 5x\sum_{n=0}^{\infty} a_n x^n - 35x + 14x^2\sum_{n=0}^{\infty} a_n x^n \end{aligned}$$

Ce qui nous donne :

$$\left(1 - 5x - 14x^2\right)\sum_{n=0}^{\infty} a_n x^n = 7 + 22x - 35x = 7 - 13x \quad \Rightarrow \quad \sum_{n=0}^{\infty} a_n x^n = \frac{7 - 13x}{1 - 5x - 14x^2} = \frac{7 - 13x}{(1 - 7x)(1 + 2x)}$$

On applique maintenant la décomposition en fraction partielle. On cherche des constantes A et B telle que :

$$\frac{7 - 13x}{(1 - 7x)(1 + 2x)} = \frac{A}{1 - 7x} + \frac{B}{1 + 2x} = \frac{A(1 + 2x) + B(1 - 7x)}{(1 - 7x)(1 + 2x)} = \frac{(2A - 7B)x + (A + B)}{(1 - 7x)(1 + 2x)}$$

Ce qui nous donne le système d'équations linéaires suivant :

$$\begin{cases} 2A - 7B = -13 \\ A + B = 7 \end{cases} \quad \Rightarrow \quad A = 4 \text{ et } B = 3$$

En revenant à notre série, on a donc :

$$\sum_{n=0}^{\infty} a_n x^n = \frac{4}{1 - 7x} + \frac{3}{1 + 2x} = 4\sum_{n=0}^{\infty} (7x)^n + 3\sum_{n=0}^{\infty} (-2x)^n = \sum_{n=0}^{\infty} \left(4(7)^n + 3(-2)^n\right) x^n$$

Ce qui nous donne finalement :

$$a_n = 4(7)^n + 3(-2)^n, \quad \forall n \geq 0$$

Chapitre 8

La théorie des graphes

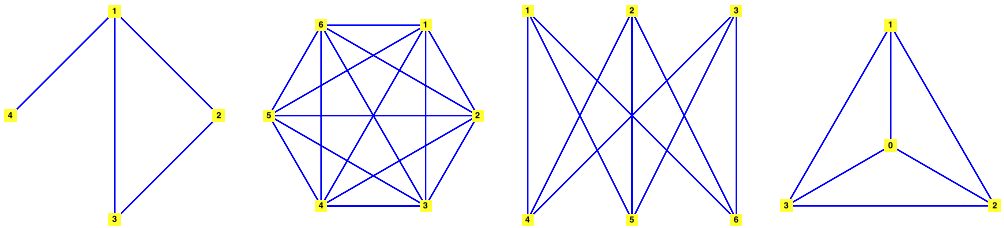
8.1 Les graphes et les arbres

Nous avons déjà vu qu'une relation peut être représenté sous forme d'un graphe. Lorsque la relation n'est pas symétrique, le graphe doit être orienté, i.e. l'ordre des liens est importante. Plutôt que de regarder un graphe comme étant une simple relation, nous voulons dans ce chapitre prendre un approche un peu différente et étudier directement les graphes, et en particulier regarder les graphes comme étant une représentation de certain problème concret. La théorie des graphes est un sujet important des mathématiques, et fait encore aujourd'hui l'objet de beaucoup de recherche. C'est cependant son application à l'informatique qui l'a rendu particulièrement célèbre. Il s'agit en effet d'un exemple de structure de donnés particulièrement importante en programmation. Nous allons commencer par énoncé quelques définitions simples qui nous servirons de points de départ à notre étude de la théorie des graphes.

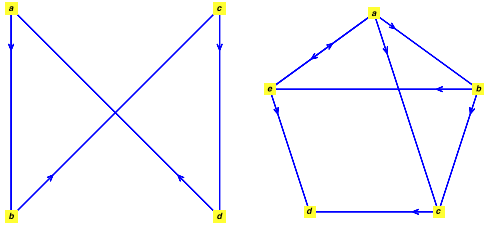
Definition 8.1.1. Voici quelques définitions fondamentales en théorie des graphes :

1. Un graphe $G = (V, E)$ est une collection V de sommet, et E d'arrête, ou chaque arrête relie un ou deux des sommets.
2. Un graphe orienté $G = (V, E)$, aussi appelé digraphe, est une collection V de sommet, et E d'arrête, ou chaque arrête est un lien orienté d'un sommet à lui même, ou entre deux sommets.
3. Une graphe simple $G = (V, E)$ est un graphe ne contenant aucune boucle, ou une boucle est définit comme une arrête allant d'un sommet à lui même.

Exemple 8.1.1. Voici quelques exemples de graphes :



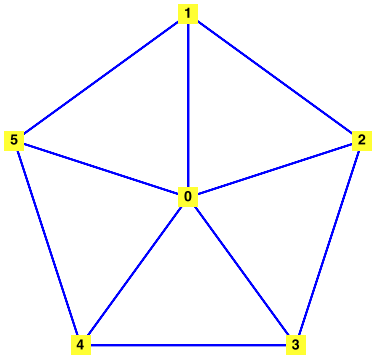
Exemple 8.1.2. Voici quelques exemples de graphes orientés :



Definition 8.1.2. Si $G = (V, E)$ est un graphe, alors on définit :

1. Le voisinage d'un sommet $x \in V$ est l'ensemble des sommets qui sont des extrémités des arrêtes commençant à x.
2. Le degré d'un sommet $x \in V$ est le nombre d'arrête connecté au sommet x. On le dénote par $\deg(x)$.

Exemple 8.1.3. Identifier le voisinage et le degré de chacun des sommets du graphes ci-dessous.



$\text{Voisinage}(0) = \{1, 2, 3, 4, 5\}$ $\quad \deg(0) = 5$
$\text{Voisinage}(1) = \{0, 2, 5\}$ $\quad \deg(1) = 3$
$\text{Voisinage}(2) = \{0, 1, 3\}$ $\quad \deg(2) = 3$
$\text{Voisinage}(3) = \{0, 2, 4\}$ $\quad \deg(3) = 3$
$\text{Voisinage}(4) = \{0, 3, 5\}$ $\quad \deg(4) = 3$
$\text{Voisinage}(5) = \{0, 1, 4\}$ $\quad \deg(5) = 3$

Il existe un lien simple, mais particulièrement important entre le degré des sommets et le nombre d'arrête. Ce lien porte le nom du théorème des poignées de mains.

Théorème 8.1.1. (Le théorème des poignées de mains) Si $G = (V, E)$ est un graphe (non orienté) avec m arrête, alors

$$2m = \sum_{v \in V} \deg(v)$$

Démonstration. Il s'agit de remarquer que chaque arrête contribue au degré de deux sommets (pas nécessairement distinct). Donc en additionnant le degré de chacun des sommets, on aura compter deux fois chacune des arrêtes, ce qui nous donne la formule. □

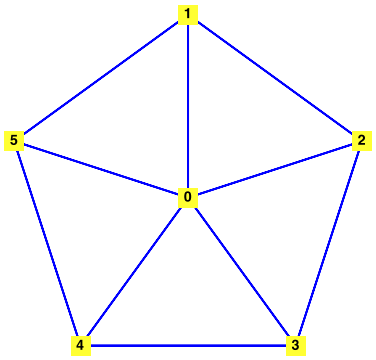
Corollaire 8.1.1. Un graphe (non-orienté) a un nombre pair de sommet de degré impair.

Démonstration. L'ensemble V des sommets peut être diviser en deux sous-ensembles disjoints : V_p l'ensemble des sommets ayant un degré pair, et V_i l'ensemble des sommets ayant un degré impair. Par le théorème des poignées de mains, si m dénote le nombre d'arrête, on a donc la formule suivante :

$$2m = \sum_{v \in V_p} \deg(v) + \sum_{v \in V_i} \deg(v)$$

Par définition, $2m$ est un nombre pair. De plus, $\sum_{v \in V_p} \deg(v)$ est une somme de nombre pair, et donc doit être pair. Pour avoir l'égalité, il est donc nécessaire que $\sum_{v \in V_i} \deg(v)$ soit aussi un nombre pair. Par contre, si $v \in V_i$, alors $\deg(v)$ est impair. Pour avoir une somme de nombre impair qui soit pair, on doit donc avoir un nombre pair de terme (ceci est une généralisation du fait que la somme de deux nombres impairs est un nombre pair.) Comme nous avons un nombre pair de termes, il y a donc un nombre pair d'élément dans V_i, c'est à dire qu'il y a un nombre pair de sommet de degré impair. □

Exemple 8.1.4. On veut vérifier le théorème des poignées de mains et son corollaire pour le graphe ci-dessous. Remarquez qu'il s'agit du graphe de l'exemple précédent.



$\deg(0) = 5$
$\deg(1) = 3$
$\deg(2) = 3$
$\deg(3) = 3$
$\deg(4) = 3$
$\deg(5) = 3$

En additionnant le degré de chacun des sommets, on obtient donc

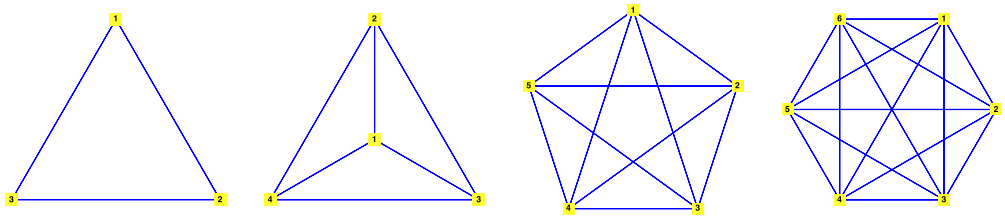
$$\sum_{v \in V} \deg(v) = 5 + 3 + 3 + 3 + 3 + 3 = 20 = 2(10)$$

le théorème des poignées de mains nous affirme donc qu'on devrait avoir 10 arrêtes, ce qui est facile à vérifier. De plus, selon le corollaire il doit y avoir un nombre pair de sommet de degré impair. Il est facile d'observer que le degré de chaque sommet est impair, comme nous avons 6 sommets, le graphe respecte bien le corollaire.

Definition 8.1.3. Certain graphe joue un rôle particulièrement important dans la théorie et porte des noms particulier. En voici quelques exemples :

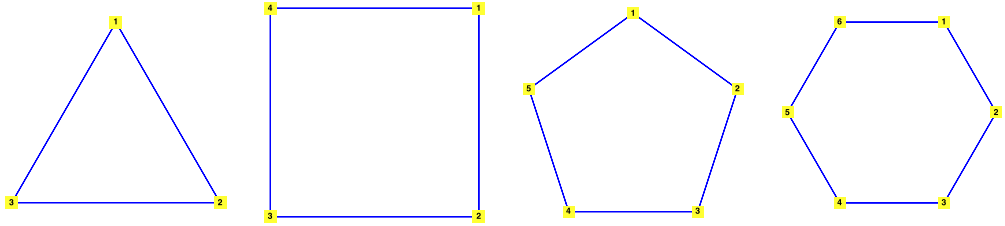
1. Le graphe complet à n sommets, dénotés K_n, est un graphe pour lequel chacun des sommets est relié à tous les autres par un arrête.

Graphe K_3 Graphe K_4 Graphe K_5 Graphe K_6



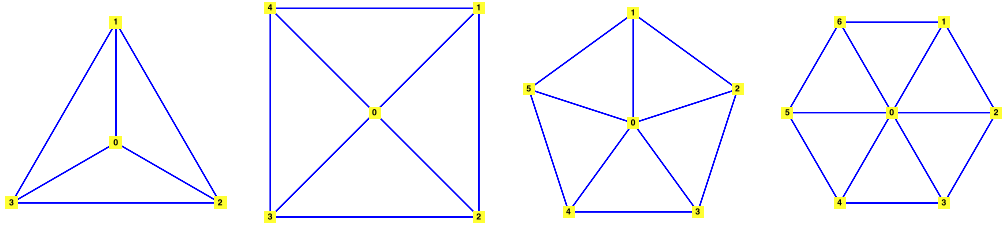
2. Les graphes cycliques à n sommets, dénotés C_n, est un graphe pour lequel le premier sommet est relié par un arrête au second, puis le second au troisième, le troisième au quatrième, et ainsi de suite jusqu'au dernier qui est relié au premier.

Graphe C_3 Graphe C_4 Graphe C_5 Graphe C_6



3. Les graphes roues à n sommets, dénotés W_n, est un graphe formé d'une roue à $n-1$ sommets, auquel on ajoute un sommet qui est relié par un arrête à tout les autres.

Graphe W_4 Graphe W_5 Graphe W_6 Graphe W_7

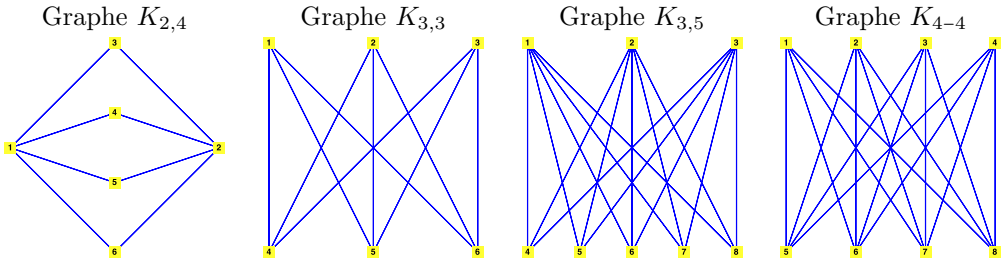


8.2 Les graphes biparties et le couplage

Dans plusieurs applications, les graphes servent à représenter des liens entres deux ensembles disjoints, ceci nous amène à parler de graphes biparties.

Definition 8.2.1. Une graphe simple $G = (V, E)$ est dit bipartie si on peut partitionner V en deux sous-ensemble V_1 et V_2 disjoint de sorte que chaque arrête relie au sommet de V_1 avec un sommet de V_2.

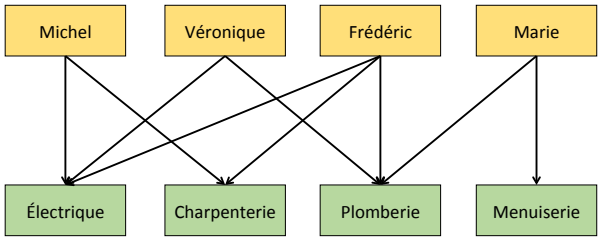
Exemple 8.2.1. Le graphe bipartie complet m, n, dénoté $K_{m,n}$ est un graphe formé d'un ensemble V_1 contenant m sommet et d'un ensemble V_2 contenant n sommet et pour lequel chaque sommet de V_1 est relié à chaque sommet de V_2 par un arrête.



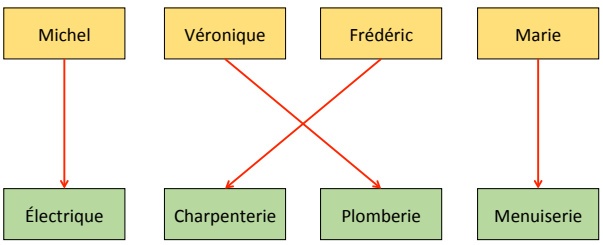
Les graphes biparties interviennent souvent dans les applications de la théorie des graphes, en particulier dans les problèmes de couplage. Si V_1 et V_2 sont des ensembles (disjoints), un couplage est une association des éléments de V_1 avec ceux de V_2 de sorte que chaque élément de V_1 soit connecté par un arrête à un élément de V_2, et aucun arrête n'ait de sommet en commun.

Pour illustrer le concept de problème de couplage, considérons le problème suivant. Imaginons qu'une compagnie a 4 employés, chacun avec des compétences spécifiques. Une journée, 4 tâches doivent être distribuées parmi les employés : Un travail électrique, de charpenterie, de plomberie et de menuiserie. Le graphe ci-dessous représente quel employé possède les compétences pour chacune des 4 tâches.

Figure 1

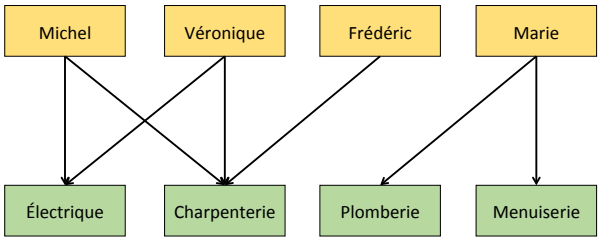


Est-il possible d'attribuer exactement une tâche à chacun des employés en respectant les compétences de chacun d'entre eux ? Par essaie et erreur, dans notre cas, il est relativement facile de trouver une telle association. Ceci est illustré ci-dessous :



Regardons maintenant l'exemple suivant, identique au précédent, mais les compétences de chacun ont été modifié.

Figure 2



Cette fois, aucun couplage n'est possible. En effet, Marie est la seule personne qualifié pour le travail de plomberie, et pour celui de menuiserie, mais elle ne peut pas faire les deux.

La question est maintenant de savoir s'il est possible de trouver un critère permettant de vérifier si un graphe bipartie admet ou non un couplage. C'est le théorème des mariages de Hall qui nous permet de répondre à cette question.

Théorème 8.2.1. **(Le théorème des mariages de Hall)** Si $G = (V, E)$ est un graphe bipartie avec sous-ensembles disjoints V_1 et V_2. Il existe un couplage entre V_1 et V_2 si et seulement si

$$|N(S)| \geq |S|, \quad \forall S \subseteq V_1$$

Où $N(S)$ dénote le nombre de sommet de V_2 qui sont connectés à un élément de S.

Démonstration. Nous allons démontrer uniquement le si du théorème. L'autre implication est plus simple et vous est laissé en exercice. La démonstration se fait en utilisant le principe d'induction généralisé.

1. Supposons que $|V_1| = 1$, c'est à dire supposons que V_1 contient un seul sommet. Dans ce cas, si $|N(V_1)| \geq 1$, alors il existe au moins un lien entre l'élément de V_1, et un élément de V_2. En choisissant l'un de ces liens, on obtient un couplage.
2. Supposons que si $|V_1| \leq k$ et les hypothèse du théorème sont satisfaite, alors il existe un couplage.
3. Nous voulons maintenant démontrer que le théorème est toujours valide si $|V_1| = k + 1$. Pour ce faire, on doit traiter deux cas.
   (a) Cas 1 : Supposons que $|N(S)| > |S|$ pour tout $S \subset V_1$. Notez qu'ici on s'intéresse seulement aux sous ensembles propre de V_1. Dans ce cas, on choisit un arrête quelconque du graphe G. Supposons que cette arrête relie un sommet $a \in V_1$ avec un sommet $b \in V_2$. On veut montrer que le graphe obtenu en retirant les sommets a et b du graphe, ainsi que tous les arrêtes qui leur sont connectés. Ceci est relativement simple. Si $S \subseteq V_1 \backslash \{a\}$, alors $N(S)$ contient soit autant de sommet qu'originalement, ou un sommet de moins (le sommet b). Dans tous les cas, on a $|N(S)| \geq |S|$. Comme les conditions du théorème sont satisfaite, en appliquant notre hypothèse d'induction on obtient un couplage.
   (b) Cas 2 : Supposons qu'il existe un $S \subset V_1$ tel que $|N(S)| = |S|$. Dans ce cas, comme $|S| \leq k$, notre hypothèse d'induction est satisfaite pour l'ensemble S. Il existe donc un couplage entre S et V_2. Dénotons par T l'ensemble des éléments de V_2 qui font partie de ce couplage. Considérons maintenant le graphe bipartie G_2 obtenu en retirant les sommets de S et T, ainsi que les arrêtes relié à au moins un sommet de S ou T. Les sommets de G_2 nous donne donc les sous-ensembles disjoints $V_3 = V_1 \backslash S$ et $V_4 = V_2 \backslash T$. Nous voulons montrer que le graphe G_2 satisfait notre hypothèse d'induction. Supposons au contraire qu'il existe un ensemble $K \subseteq V_3$ pour lequel $|N(K)| < |K|$ dans le graphe G_2. Dans ce cas, si on considère l'ensemble de sommet $S \cup K$ dans le graphe original G, on doit avoir
   $$|N(S \cup K)| < |S| + |K| = |S \cup K|$$
   Car par hypothèse nous avons $|N(S)| = |S|$ et $N(K)$ contient moins que $|K|$ élément qui ne sont pas déjà compter dans $N(S)$. Cette derniére inégalité est en contradiction avec les hypothèses du

théorème, ce qui nous permet d'affirmer que le graphe G_2 satisfait notre hypothèse d'induction. Il existe donc un couplage entre les éléments de V_3 et ceux de V_4. En combinant ceci avec le couplage que nous avions déjà obtenu entre les éléments de S et T, on a donc obtenu un couplage entre les éléments de V_1 et V_2 dans notre graphe d'origine.

□

Le théorème de Hall porte le nom de théorème des mariages du à sa formulation originale en terme de filles et de garçons désirant se marié. Le problème original s'énonce comme suit. Sur une ile, se trouve un certain nombre de fille, chacune connaissant un certain nombre de garçons, sous quelle condition les filles peuvent marier des garçons de sorte que chacune des filles marie un garçon qu'elle connait.

Pour illustrer l'utilisation du théorème, nous allons commencer par l'appliquer à l'exemple de la figure 1.

Élément de S	$\lvert N(S)\rvert$	$\lvert S\rvert$
Michel	2	1
Véronique	2	1
Frédéric	3	1
Marie	2	1
Michel,Véronique	3	2
Michel,Frédéric	3	2
Michel,Marie	4	2
Véronique,Frédéric	3	2
Véronique,Marie	3	2
Frédéric,Marie	4	2
Michel, Véronique, Frédéric	3	3
Michel, Véronique, Marie	4	3
Michel, Frédéric, Marie	4	3
Véronique, Frédéric, Marie	4	3
Michel, Véronique, Frédéric, Marie	4	4

Comme l'inégalité est satisfaite dans tous les cas, le théorème affirme donc qu'un couplage est possible. C'est ce que nous avions d'ailleurs pu observer par essaie et erreur. Considérons maintenant le problème de la figure 2. Remarquons l'inégalité suivante :

$$|N(\{\text{Michel, Véronique, Frédéric}\})| = 2 < 3$$

Comme cette dernière contredit le théorème de Hall, on peut donc conclure qu'aucun couplage n'est possible.

Les deux exemples que nous avons traité jusqu'à présent peuvent être facilement résolu sans utiliser le théorème de Hall, et ce de manière plus intéressante que ce que le théorème nous permet de faire. Nous allons maintenant utiliser un problème plus intéressant et pour lequel le théorème joue un rôle important.

Exemple 8.2.2. Si on divise un jeu de carte standard (52 cartes) en 13 piles de 4 cartes, alors il est toujours possible de choisir une carte de chaque pile de sorte qu'on est une carte de chaque valeur (As, 2, 3, ..., 10, valet, dame, roi). On peut considérer le graphe $G = (V, E)$ contenant les sommets $V = V_1 \cup V_2$ où V_1 représente les 13 différentes piles et V_2 représente les 13 valeurs possible. Une arrête est dessiné entre un sommet de V_1 et un sommet de V_2 si une pile contient une carte d'une certaine valeur. Le problème ici est qu'il n'est pas possible de prévoir à l'avance la valeur des cartes de chaque pile, donc les arrêtes sont en quelque sorte aléatoire. Par contre, comme il y a 4 cartes de chaque type, chaque sommet de V_1 sera relié à V_2 par 1, 2, 3 ou 4 arrêtes. Donc si on choisit $\{v_1, v_2, ..., v_k\} \in V_1$, alors on aura un total de $4k$ cartes, comme il y 4 cartes de chaque valeurs, on aura donc un minimum de k carte de valeur différentes parmi les $4k$ cartes. On a donc :

$$|N(\{v_1, v_2, ..., v_k\})| \geq k = |\{v_1, v_2, ..., v_k\}|$$

Par le théorème des mariages de Hall, on peut donc affirmer qu'un couplage existe, ce qui signifie dans notre cas qu'il est possible de choisir une carte dans chaque pile de sorte qu'un on est une carte de chaque valeur.

8.3 Les graphes eulériens / hamiltoniens et la connexité

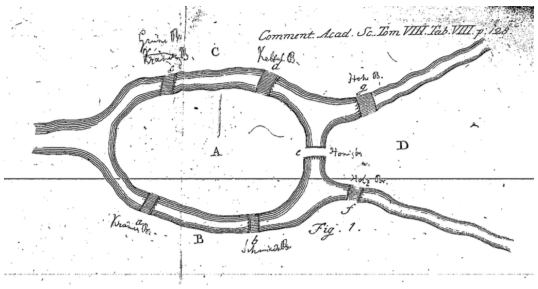
Avant d'entreprendre la théorie de cette section, il nous est nécessaire de faire quelques définitions importantes, la plupart étant relativement intuitive.

Definition 8.3.1. Si $G = (V, E)$ est un graphe, alors on définit les termes suivant :

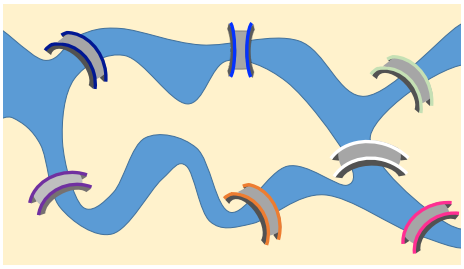
1. Un trajet d'un sommet $u \in V$ à un sommet $v \in V$ est une collection ordonné $v_1, v_2, v_3, ..., v_k$ de sommet de V telle que $u = v_1$, $v = v_k$ et pour laquelle pour chaque v_i, v_{i+1} dans la collection, il existe une arrête reliant ces deux sommets. Dans ce cas, on dit que le trajet est de longueur k. Si aucun des sommets ne se répète dans la collection, alors on dit que le trajet est simple.
2. Un circuit dans un graphe est un trajet ayant le même point de départ que d'arriver.
3. Le graphe G est dit connexe si pour tout $u, v \in V$ il existe un trajet de u à v.

L'un des problèmes les plus célèbre de la théorie des graphes, est le problème des sept ponts de Königsberg énoncé pour la première fois par Leonhard Euler en 1736. La ville de Königsberg en Prusse (aujourd'hui Kaliningrad en Russie) est traversé par le fleuve Prégel, sur lequel se trouve deux iles. À l'époque d'Euler, 7 ponts permettait de traverser le fleuve comme illustré sur le schéma ci-dessous. Le problème que se posa Euler était de savoir s'il serait possible de trouver un chemin à travers la ville lui permettant de traverser chacun des 7 ponts exactement une fois [3]. La solution d'Euler par la négative a servi de point de départ pour l'étude de la théorie des graphes.

Schéma de la publication originale d'Euler



Représentation moderne du problème des ponts



La démonstration d'Euler est relativement simple. Il s'agit de supposer l'existence d'un trajet. Comme le graphe est connexe, le trajet devra parcourir chacun des 4 endroits qui se trouve sur la carte (la rive nord, la rive sud et chacune des deux iles). L'un de ces endroits est le point de départ, et l'un des ces endroits est le point d'arrivé. Notez que le point de départ peut être identique ou différent du point d'arrivé. Les endroits qui ne sont ni le point de départ, ni le point d'arrivé sont qualifié de point intermédiaire. Notons qu'il doit obligatoirement y avoir 2 ou 3 points intermédiaire (2 si le point de départ est distinct du point d'arrivé, et 3 autrement). Considérons maintenant plus en détail l'un de ces points intermédiaire. Le graphe étant connexe, cet endroit doit être relié au reste de la carte par un certain nombre de pont que le trajet doit traverser. Comme un point intermédiaire n'est pas le point d'arrivé par définition, chaque fois que notre trajet traverse un pont pour aller au point intermédiaire, il doit obligatoirement traverser un second point pour en sortir. Notre point intermédiaire doit donc avoir un nombre pair de pont. Maintenant, en observant la carte, on remarque que les différents endroit ont respectivement 3, 5, 3 et 3 ponts. Il n'y a donc aucun endroit qui peut servir de point intermédiaire, mais pourtant nous savons qu'un point intermédiaire doit exister. Il s'agit donc d'une contradiction. On peut donc conclure qu'un trajet traversant tous les ponts exactement une fois ne peut pas exister, ce qui complète la démonstration.

L'existence ou non d'un tel trajet peut en fait être étudié pour n'importe quel graphe connexe. Aujourd'hui un graphe admettant un tel trajet porte le nom de graphe eulérien comme l'énonce la définition suivante :

Definition 8.3.2. Un trajet eulerien dans un graphe $G = (V, E)$ est un trajet permettant de traverser tous les arrêtes du graphe exactement une fois. Un trajet euclérien ayant le même point de départ que d'arriver est appellé un circuit eulérien. Un graphe possédant un trajet eulérien est qualifié de graphe eulérien.

Il est maintenant temps de caractériser les graphes admettant un trajet eulérien, et les graphes admettant un circuit eulérien. C'est ce que nous allons faire immédiatement.

Théorème 8.3.1. Un graphe connexe est eulérien (i.e. possède un trajet eulérien) si et seulement si le graphe possède exactement 0 ou 2 sommets de degré impair. De plus, le graphe possède un circuit eulérien si et seulement si tous les sommets sont de degré pair.

Démonstration.

1. Nous allons commencer par démontrer qu'un graphe connexe possède un circuit eulérien si et seulement si tous les sommets sont de degré pair.
   (⇒) Supposons que le graphe G possède un circuit eulérien. Considérons premièrement le point de départ, qui est aussi le point d'arriver. Chaque fois qu'on quitte ce sommet, on passe par un arrête, chaque fois qu'on y revient, on traverse une seconde arrête. Notez aussi que comme il s'agit de notre point d'arriver, chaque fois qu'on quitte ce sommet, on doit obligatoirement y revenir. Comme ceci ce fait toujours par pair, le sommet de départ est de degré pair.
   (⇐) Supposons que tous les sommets de G sont de degré pair. Prenons un sommet $u \in V$, et dessinons un trajet commençant à u le plus long possible. Ce trajet reviendra obligatoirement au sommet u car il est impossible de rester coincé à un autre sommet, car chaque sommet est de degré pair, chaque fois qu'on arrivera à un sommet autre que le point de départ, il y aura toujours un arrête restant pour quitter ce sommet. Le problème étant que notre circuit ne passe pas nécessairement par tout les arrêtes. Considérons maintenant le graphe G_1 obtenu en retirant de graphe G tous les arrêtes ayant été utilisé dans notre circuit, ainsi que les sommets qui ne sont plus connecté à des arrêtes. Choisissons maintenant un sommet u_1 de G_1 faisant parti du circuit original, et construisons dans G_1 un circuit le plus long possible. Notez que u_1 existe, car le graphe est connexe. De plus, le degré de chaque sommet de G_1 doit être pair, de sorte que notre trajet se terminera obligatoirement au sommet u_1. Maintenant que nous avons obtenu un second circuit, on peut l'insérer dans l'original, de sorte que nous avons un nouveau circuit plus long que l'original. On continue de répéter la même étape, tant que nous n'obtenons pas un circuit passant par tout les sommets. Notre graphe possède donc un circuit eulérien.
2. Nous allons maintenant démontrer que graphe connexe possède un trajet eulérien qui n'est pas un circuit si et seulement si le graphe possède exactement 2 sommets de degré impair.
   (⇒) L'argument ici est similaire à celui que nous avons fait pour les circuits. La seule distinction étant que pour le sommet de départ, on commence par traverser un arrête, puis chaque fois que nous revisitons ce sommet nous devons continuer notre chemin, donc le sommet de départ est de degré impair. Le même argument s'applique pour le sommet d'arriver. (⇐) Supposons que tous les sommets de G sont de degré pair, sauf pour des sommets u et v qui sont de degré impair. Ajoutons un arrête entre u et v, de sorte que chaque sommet soit de degré pair. On peut donc trouver un circuit eulérien. En retirant l'arrête que nous avons ajouter, notre circuit devient alors un trajet eulérien qui n'est pas un circuit.

□

On peut aussi se poser une autre question semblable à celle posé par Euler. Plutôt que de chercher à parcourir chacune des arrêtes d'un graphe exactement une fois, pourrait-on chercher à parcourir tout les sommets d'un graphe exactement une fois ? On parle alors de trajet ou circuit Hamiltonien.

Definition 8.3.3. Un trajet hamiltonien dans un graphe $G = (V, E)$ est un trajet permettant de traverser tous les sommets du graphe exactement une fois. Un trajet hamiltonien ayant le même point de départ que d'arriver est appellé un circuit hamiltonien. Un graphe possédant un trajet hamiltonien est qualifié de graphe hamiltonien.

La caractérisation des graphes hamiltoniens est beaucoup plus difficile que l'étude des graphes eulériens. Nous pouvons cependant énoncés deux théorèmes permettant d'affirmer l'existence d'un circuit hamiltonien : Le théorème d'Ore et le théorème de Dirac.

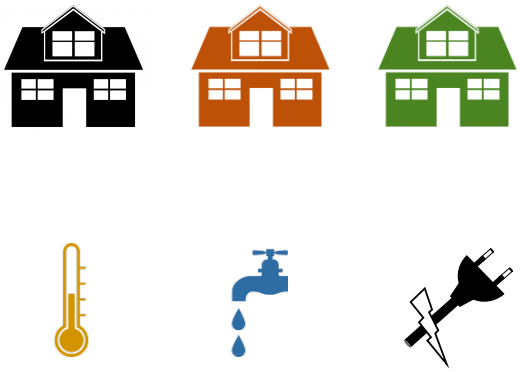
Théorème 8.3.2. **(Théorème d'Ore)** Si G est un graphe simple avec n sommets, $n \geq 3$, est tel que $\deg(u) + \deg(v) \geq n$ pour toute pair de sommet non-adjacent u et v, alors G possède un circuit hamiltonien.

Théorème 8.3.3. **(Théorème de Dirac)** Si G est un graphe simple avec n sommet, $n \geq 3$, est tel que le degré de chaque sommet est au moins $\frac{n}{2}$, alors G possède un circuit hamiltonien.

8.4 Les graphes planaires

En 1917, Henry Dudeney énonce dans son livre une énigme mathématique qui selon lui est très ancienne : Le problème des trois utilitaires. Dans un plan (donc en deux dimensions) se trouve trois maisons. Chacune d'elle doit être relié à trois utilitaire : L'eau, le gaz et l'électricité. Est-il possible d'effectué ces liens sans qu'aucun lien ne se croise ? [2]

FIGURE 8.1 – Le problème des 3 utilitaires



Definition 8.4.1. Un graphe $G = (V, E)$ est dit planaire, s'il est possible de le dessiner sur une feuille de papier (un plan) sans qu'aucune arrête ne se croise.

Le problème des trois utilitaires revient donc à savoir si le graphe $K_{3,3}$ est planaire. Depuis le début du chapitre, nous avons étudié nos graphes basés sur leur sommet et leur arrête. Dans le cas des graphes planaire, on peut ajouter un troisième élément : Les faces. Une face est tout simplement une région délimité par des arrêtes. Elle n'a pas besoin d'être borné, ce qui veut que la région extérieur d'un graphe se qualifie de face. On peut alors définir la notion de degré d'une face, que l'on définie comme le nombre d'arrêtes qui délimite la face. On peut alors obtenir facilement un résultat similaire au théorème des poignées de main. Si on considère F comme étant l'ensemble des faces d'un graphe planaire, et si on dénote e le nombre d'arrête, alors on obtient la formule suivante :

$$\sum_{f \in F} \deg(f) = 2e$$

Cette formule ce justifie facilement en réalisant que chaque arrête touche à deux faces (possiblement deux fois la même face), donc en additionnant le degré de chaque face, on aura compter chacune des arrêtes deux fois. Nous allons maintenant énoncé un théorème particulièrement important pour les graphes planaires, et qui permet de faire un lien entre le nombre de sommet, d'arrête et de face d'un tel graphe. Il s'agit de la formule d'Euler.

Théorème 8.4.1. **(La formule d'Euler)** Si G est un graphe planaire simple et connexe avec e arrêtes et v sommet. Si r dénote le nombre de région dans une représentation planaire du graphe G, alors on a la formule suivante :

$$r = e - v + 2$$

Démonstration. La démonstration se fait par induction sur le nombre d'arrêtes. Si G possède une seule arrête, comme le graphe est simple, il doit donc avoir deux sommets, mais une seule face. On a donc : $1 - 2 + 2 = 1$. La formule est vrai pour $e = 1$. Supposons que la formule est vraie pour tout graphe ayant au plus k arrêtes, et on veut montrer que la formule est encore vrai pour un graphe ayant $k + 1$ arrêtes. Considérons G_1 un sous graphe de G obtenu en retirant une arrête. Deux cas peuvent alors se présenter :

1. Si G_1 est un graphe connexe possédant r région et v sommet, alors la formule d'Euler s'applique par hypothèse d'induction. On doit donc avoir la relation $r = k - v + 2$. De plus, le graphe G dans ce cas doit avoir $r + 1$ région et v sommet. On peut donc vérifier que l'équation suivante est bien satisfaite :

$$r + 1 = (k + 1) - v + 2$$

2. Si G_1 n'est pas connexe, alors l'un des sommets n'est pas connecter au reste du graphe. Dans ce cas, en retirant ce sommet, un obtient un graphe G_2 qui est aussi un sous-graphe de G. Comme G_1 et G_2 on le même nombre d'arrête, alors G_2 a par hypothèse k arrêtes. De plus, supposons que G_2 possède r régions et v sommet, alors le graphe G doit avoir aussi r régions, mais $v + 1$ sommet. On peut donc vérifier que l'équation suivante est bien satisfaite :

$$r = (k + 1) - (v + 1) + 2$$

□

La formule d'Euler possède plusieurs conséquences importantes. Le corollaire suivant en résume quelques unes.

Corollaire 8.4.1. La formule d'Euler possède les conséquences suivantes :

1. Si G est un graphe simple, connexe et planaire ayant e arrêtes et $v \geq 3$ sommets, alors $e \leq 3v - 6$.
2. Si G est un graphe simple, connexe et planaire, alors il existe au moins un sommet v tel que $\deg(v) \leq 5$.
3. Si G est un graphe simple, connexe et planaire ayant e arrêtes et $v \geq 3$ sommets, et s'il n'existe aucun circuit de longueur 3, alors $e \leq 2v - 4$.

Démonstration.

1. Premièrement, comme le graphe est simple, le degré de chacune des faces doits être au moins 3. Si on dénote par F l'ensemble des faces et par r le nombre de face, on a donc la relation suivante :

$$2e = \sum_{f \in F} \deg(f) \geq \sum_{f \in F} 3 = 3r$$

En réarrangeant les termes, on a donc $r \leq \frac{2}{3}e$. En remplaçant cet inégalité dans la formule d'Euler, on obtient donc :

$$\frac{2}{3}e \geq e - v + 2 \quad \Rightarrow \quad 0 \geq \frac{1}{3}e - v + 2 \quad \Rightarrow \quad \frac{1}{3}e \leq v - 2 \quad \Rightarrow \quad e \leq 3v - 6$$

2. Premièrement, supposons que e représente le nombre d'arrête, v le nombre de sommet, et V l'ensemble des sommets. Rappelons nous que le théorème des poignées de mains nous affirme que

$$2e = \sum_{x \in V} \deg(x)$$

Nous allons travailler par contradiction. Supposons que le degré de chacun des sommets est au moins 6, c'est à dire $\deg(x) \geq 6$ pour tout $x \in V$, et en remplaçant dans le théorème des poignées de mains, on obtient donc :

$$2e = \sum_{x \in V} \deg(x) \geq 6v \quad \Rightarrow \quad e \geq 3v \quad \Rightarrow \quad v \leq \frac{1}{3}e$$

Puis on remplace dans l'inégalité que nous avons obtenu dans la partie précédente, ce qui nous donne :

$$e \leq 3v - 6 \leq 3\left(\frac{1}{3}e\right) - 6 = e - 6 \quad \Rightarrow \quad 0 \leq -6$$

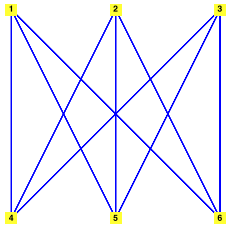
ce qui est une contradiction. L'hypothèse que le degré de chaque sommet est au moins 6 est donc fausse. Il doit donc exister au moins un sommet de degré au plus 5.

3. La démonstration est similaire à la première partie et vous est laissé en exercice.

□

Le formule d'Euler que nous venons de démontrer peut maintenant nous permettre de résoudre le problème des trois utilitaires par la négative. C'est ce que nous allons faire immédiatement.

Exemple 8.4.1. Dans un plan (donc en deux dimensions) se trouve trois maisons. Chacune d'elle doit être relié à trois utilitaire : L'eau, le gaz et l'électricité. Est-il possible d'effectué ces liens sans qu'aucun lien ne se croise ? Premièrement, remarquons que la question est en fait de savoir si le graphe $K_{3,3}$ est planaire.



Maintenant, il est facile de voir qu'il ne peut pas exister dans le graphe de circuit de longueur 3 car ceci signifierait que deux maisons sont reliés ensembles, ou que deux utilitaires sont reliés ensembles. De plus, le graphe possède $e = 9$ arrêtes et $v = 6$ sommets. Finalement, si on suppose que le graphe est planaire, la troisième partie du corollaire nous affirme que $e \leq 2v - 4$. En remplaçant les valeurs, on a donc l'inégalité $9 \leq 2(6) - 4 = 8$, ce qui est bien sur une contradiction. Notre hypothèse est donc fausse, le graphe n'est pas planaire.

Exemple 8.4.2. On veut montrer que le graphe K_5 n'est pas planaire. Pour ce faire, remarquons que K_5 possède $e = 10$ arrête et $v = 5$ sommets. Si le graphe est planaire, la première partie du corollaire doit s'appliquer, ce qui nous donne $e \leq 3v - 6$, c'est à dire $10 \leq 3(5) - 6 = 9$ qui est bien entendu une contradiction. Le graphe K_5 ne peut donc pas être planaire.

Bien que la formule d'Euler soit particulièrement intéressante et puisse nous permettre de démontrer que certain graphe ne sont pas planaire, il ne s'agit pas d'une caractérisation des graphes planaires. Une caractérisation est donné par le théorème de Kuratowaski [7] qui est énoncé ci-dessous.

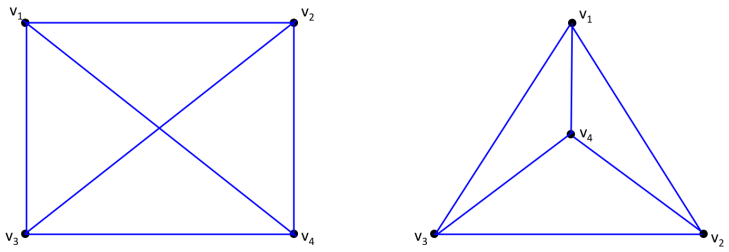
Théorème 8.4.2. Un graphe G n'est pas planaire si et seulement si G contient un sous-graphe qui est homéomorphique à $K_{3,3}$ ou K_5.

La démonstration du théorème est trop compliqué pour le niveau du cours. Si vous êtes curieux, vous êtes invité à consulter l'article original de Kuratowski qui date de 1930 [7]. La question de vérifier si un graphe est planaire ou non ce traduit donc aux deux approches suivantes :

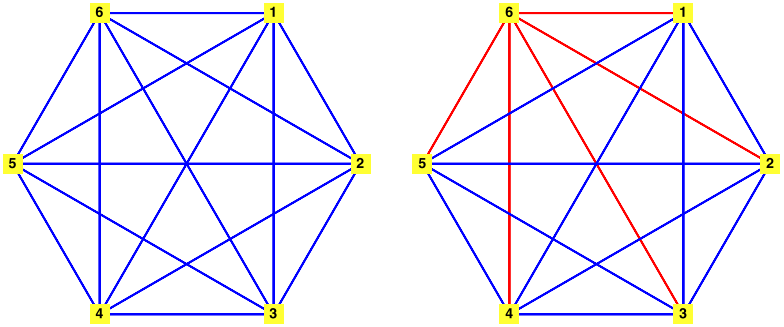
1. Pour montrer qu'un graphe est planaire, il suffit de le redessiner sous forme planaire.

2. Pour montrer qu'un graphe n'est pas planaire, il suffit d'identifier $K_{3,3}$ ou K_5 comme sous graphe.

Exemple 8.4.3. Est-ce que le graphe de gauche ci-dessous est planaire ? Pour ce faire, il s'agit de remarquer que le graphe gauche peut être redessiné sous la forme de droite qui lui est équivalente. On peut donc affirmer que le graphe est bel et bien planaire.



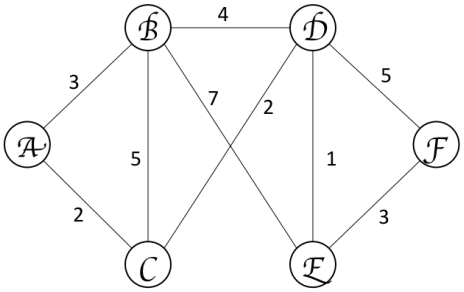
Exemple 8.4.4. Est-ce que le graphe de gauche ci-dessous est planaire ? Pour ce faire, il s'agit de remarquer qu'en enlevant de sommet 6 et toutes les arrêtes illustré en rouge dans le graphe de droite, il nous reste un sous-graphe qui est équivalent à K_5. Le graphe n'est donc pas planaire.



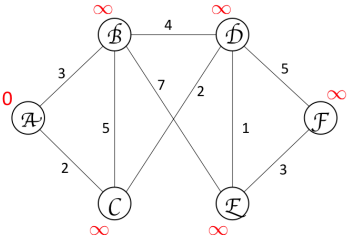
8.5 Le problème du plus court trajet

La théorie des graphes joue un rôle important dans plusieurs domaine d'application. Dans un premier temps on peut l'utiliser simplement comme un outil pour représenter des donnés, comme par exemple pour représenter les différents vols d'une compagnie aérienne. Mais ce sont dans les réponses aux différentes questions concernant les donnés que toutes la puissance de la théorie des graphes peut être observé. L'une des questions particulièrement importante concerne le problème de trouver le plus court trajet entre deux sommets. La solution à ce problème est donné par l'algorithme de Dijkstra qui a été décrit pour la première fois en 1956.

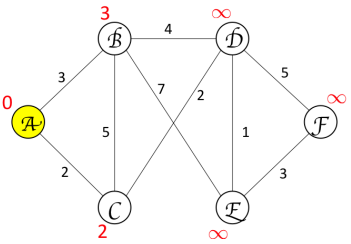
Exemple 8.5.1. On veut trouver le plus court trajet entre le point A et le point F dans le graph ci-dessous.



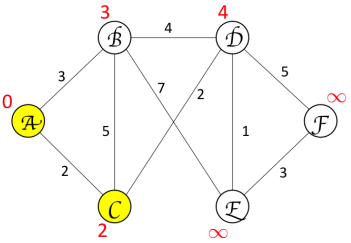
Pour ce faire, on applique l'algorithme de Dijkstra, que nous allons décrire ci-dessous étape par étape.



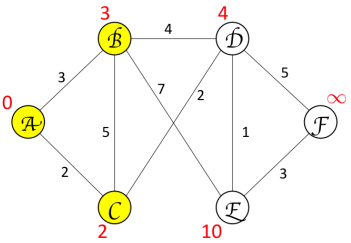
On commence par donner une valeur à chacun des sommet du graph (en rouge). Le point de départ a une valeur de 0, et tous les autres sommets la valeur ∞.



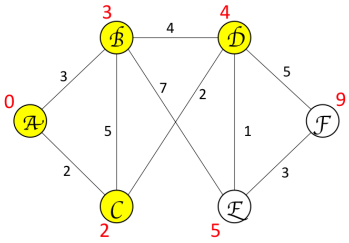
On prend la sommet ayant la plus petite valeur (ici A), et pour chacun des sommets adjacent, on additionne la valeur de A avec la distance vers les autres sommets. Si cette valeur est plus petite que celle de ces sommets, on la remplace. Donc dans notre cas, on remplace la valeur de B par 3, et la valeur de C par 2. On colore ensuite le sommet A en jaune.



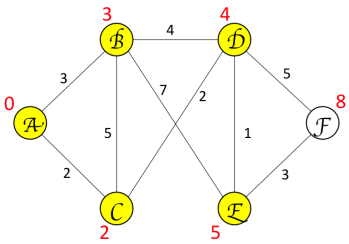
Parmi les sommets qui ne sont pas en jaune, on choisi celui ayant la plus petite valeur (ici le sommet C), puis on ajuste la distance vers chacun des sommets adjacent si cette distance est plus petite que celle que nous avions déjà. On colore ensuite le sommet C en jaune.



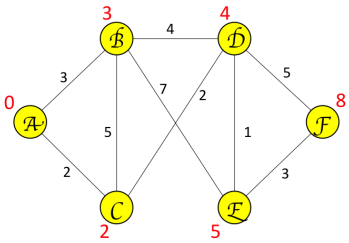
On répète ensuite la même étape. On choisit le sommet ayant la plus petite valeur parmi ceux qui ne sont pas encore colorié, puis on ajuste la distance pour les sommets adjacents.



Idem à l'étape précédente.

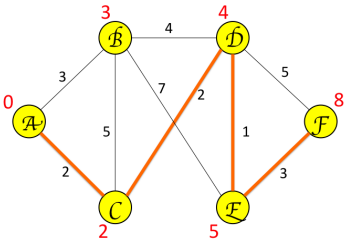


Idem à l'étape précédente.



Idem à l'étape précédente. Notez qu'à cette étape il nous restait seulement un sommet, ce qui nous indique que l'algorithme est terminé.

La valeur du sommet F indique la plus courte distance entre A et F. Dans notre cas il s'agit d'une distance de 8. Le plus court trajet entre A et F est donc le trajet passant par les sommets $A-C-D-E-F$ comme illustré sur la figure.



8.6 Les problèmes de coloriage

Combien de couleur sont nécessaire au minimum pour dessiner une carte géographique de sorte qu'il n'y ait jamais deux pays adjacent de la même couleur ? Ce problème peut en fait être traduit dans le langage de la théorie des graphes. Il suffit de remplacer les pays par les sommets d'un graphe, et les arrête représente des pays ayant une frontière commune. Ce problème a été rendu célèbre, car il s'agit du premier théorème important ayant été démontré par un ordinateur. Encore aujourd'hui, les seules démonstration connu de ce théorème sont fait à l'aide d'un ordinateur, ce qui rend la démonstration controversé. Bien que le théorème ne soit pas remis en doute, certain mathématicien ne sont toujours pas prêt à accepter la validité d'une démonstration fait par un ordinateur.

Definition 8.6.1. Un coloriage d'un graphe simple est l'assignation d'une couleur à chacun des sommets, de sorte qu'il n'y est jamais deux sommets adjacent de même couleur.

La question devient alors combien de couleur au minimum est-il nécessaire d'avoir pour pouvoir dessiner n'importe quel graphe. C'est le théorème des 4 couleurs qui répondit à cette question.

Théorème 8.6.1. **(Théorème des 4 couleurs)** Tout graphe planaire G peut être colorier à l'aide d'un maximum de 4 couleurs différentes.

Ce théorème a été démontrer pour la première fois par Kenneth Appel et Wolfgang Haken en 1976.

Bibliographie

[1] Jean-Marie De Koninck and Armel Mercier. *Introduction à la théorie des nombres*. Modulo, 1994.

[2] Henry Dudeney. *Amusements in mathematics*. Thomas Nelson, 1917.

[3] Leonhard Euler. Solutio problematis ad geometriam situs pertinentis. *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, 8 :128–140, 1736.

[4] Ralph P. Grimaldi. *Discrete and combinatorial mathematics an applied introduction*. Addison Wesley, 3rd edition edition, 1994.

[5] John M. Harris, Jeffry L. Hirst, and Michael J. Mossinghoff. *Combinatorics and graph theory*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2008.

[6] Stephen Hawking. *Et dieu créa les nombres*. Dunod, 2006.

[7] Kazimierz Kuratowski. Sur le problème des courbes gauches en topologie. *Fund. Math.*, 15 :271–283, 1930.

[8] Claude Levesque. *Sur le sentier des mathématiques*. Loze-Dion éditeur inc., 2007.

[9] George E. Martin. *Counting : the art of enumerative combinatorics*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2001.

[10] Kenneth H. Rosen. *Mathématiques discrètes*. Chenelière/McGraw-Hill, édition révisée edition, 2002.

[11] Kenneth H. Rosen. *Discrete mathematics and its applications*. McGraw-Hill, seventh edition edition, 2012.

[12] Sheldon M. Ross. *Initiation aux probabilités*. Presses polytechniques et universitaires romandes, 1999.

[13] Daniel J. Velleman. *How to prove it*. Cambridge University Press, Cambridge, second edition, 2006. A structured approach.

Index

$\aleph_0$, 38
$\mathfrak{c}$, 38
Égalité d'ensembles, 20
Équivalence, 6

Aleph 0, 38
Algorithme d'Euclide, 42
Algorithme de Dijkstra, 102
Arrête, 91
Arrangement, 82
Axiome, 14

Cardinalité, 20
Cardinalité du continuum, 38
Circuit, 97
Codomaine, 32
Coefficient binomial, 74
Combinaison, 82
Complément, 21
Composition de fonctions, 34
Conjecture, 14
Conjonction, 6
Connecteurs logiques, 5
Contradiction, 7
Corollaire, 14
Couplage, 94
Crible d'Ératosthène, 49
Critères de divisibilité, 55
Cryptographie RSA, 62

Démonstration par contradiction, 15
Degré d'un sommet, 92
Différence (Théorie des ensembles), 21
Différence symétrique, 21
Disjonction, 6
Divisibilité, 39
Division euclidienne, 40
Domaine, 32

Ensemble, 19
Ensemble puissance, 22
Ensemble vide, 19

Factorielle, 74
Fibonacci, 85
Fonction, 32
Fonction plafond, 77
Fonction plancher, 77
Fonctions bijectives, 38
Fonctions génératrices, 87
Fonctions injectives, 35
Fonctions inversible, 38
Fonctions surjectives, 37
Formule d'Euler, 99
Fractions partielles, 87

Graphe, 91
Graphes bipartie complets, 94
Graphes biparties, 94
Graphes complet, 93
Graphes connexes, 97
Graphes cycliques, 93
Graphes eulérien, 97
Graphes hamiltonien, 98
Graphes planaires, 99
Graphes roues, 93

Image, 34
Implication, 6
Inclusion, 20
Intersection, 21
Inverse d'une fonction, 38

Lemme, 14
Lemme d'Euclide, 44, 47
Lemme de Bézout, 41
Loi de De Morgan, 9, 24

Nombres complexes, 19, 20
Nombres copremiers, 44
Nombres entiers, 19
Nombres modulos, 51
Nombres naturels, 19
Nombres premiers, 47
Nombres premiers d'Euclide, 49
Nombres réels, 19
Nombres rationnels, 19, 20

Paradoxe de Russell, 25
Permutation, 82
Petit théorème de Fermat, 58
Plus grand commun diviseur, 41

Plus petit commun multiple, 45
Prédicat, 10
Preuve d'existence, 16
Preuve directe, 14
Preuve par contraposé, 15
Principe d'inclusion-d'exclusion, 81
Principe d'induction, 70
Principe d'induction généralisé, 73
Principe de la somme, 80
Principe des nids de pigeons, 76
Principe des nids de pigeons généralisés, 77
Principe du produit, 80
Problème des lapins, 85
Problème des ponts de Königsberg, 97
Problème des trois utilitaires, 99
Problème du Mississippi, 84
Produit cartésien, 22
Proposition, 14
Proposition équivalente, 7
Proposition logique, 5

Relation, 27
Relation antisymétrique, 28
Relation d'équivalence, 31
Relation d'ordre, 31
Relation d'ordre partielle, 31
Relation réflexive, 28
Relation symétrique, 28
Relation transitive, 28

Séries géométriques, 87
Sommes arithmétiques, 69
Sommes géométriques, 70
Sommet, 91
Sous-ensemble, 20

Table de vérité, 5
Tautologie, 7
Théorème, 14
Théorème d'Euclide, 48
Théorème d'Euler, 57
Théorème d'Ore, 98
Théorème de Dirac, 99
Théorème de Wilson, 58
Théorème des mariages de Hall, 95
Théorème des poignées de mains, 92
Théorème du binôme, 75
Théorème fondamental de l'arithmétique, 47
Tour de Hanoï, 72, 73
Trajet, 97
Trajet eulerien, 97
Trajet hamiltonien, 98
Triangle de Pascal, 75

Union, 21

Voisinage, 92