Mathématiques de base, logique élémentaire et rédaction de preuves

MATH F-104

BA1 en sciences mathématiques

Dimitri Leemans

Notes rédigées par Simone Gutt

2020-2021

Table des matières

Chapitre 1

Ensembles et Applications.

1.1 Opérations sur les ensembles.

Intuitivement, un ensemble S est une collection d'objets appelés éléments. On dénote le fait qu'un élément a soit dans S par $a \in S$ et on dit que a **appartient à** S. C'est cette notion d'appartenance qui est fondamentale. (Nous ne définissons pas ici la notion d'ensemble !)

On peut décrire un ensemble en extension ; ceci veut dire qu'on donne explicitement tous les éléments de l'ensemble. L'ensemble qui contient les éléments a, b, c et uniquement ceux-là est noté

$$S = \{a, b, c\} \qquad (= \{b, a, c\}).$$

Par exemple, l'ensemble S_1 des nombres entiers positifs qui divisent 24 est

$$S_1 = \{1, 2, 3, 4, 6, 8, 12, 24\}.$$

On peut peut également décrire un ensemble en compréhension, c'est-à- dire par une propriété. L'ensemble S des éléments a qui vérifie une propriété P se note

$$S = \{a \,|\, a \text{ vérifie la propriété } P\}.$$

Par exemple, l'ensemble S_1 des nombres entiers positifs qui divisent 24 peut se noter

$$S_1 = \{a \,|\, a \text{ est un entier positif qui divise } 24\}.$$

Un ensemble particulier est **l'ensemble vide**, noté ϕ, qui ne contient aucun élément.

Si A et B sont deux sous-ensembles de S, on dit que A **est inclus à** B ou que B contient A (et on note $A \subset B$ ou $A \subseteq B$ ou $B \supset A$ ou $B \supseteq A$) si tout élément a de A est aussi dans B.

La propriété $A = B$ signifie $A \subseteq B$ et $B \subseteq A$. Si $A \subset B$ et $A \neq B$ on dit que A est un sous-ensemble propre de B.

Si A et B sont deux sous-ensembles de S, la collection des éléments c tels que $c \in A$ et $c \in B$ est appelée **l'intersection** $A \cap B$ de A et B. Plus généralement, si $\{A_\alpha, \alpha \in I\}$ est une collection de sous-ensembles de S, l'intersection $\cap_{\alpha \in I} A_\alpha$ est l'ensemble des éléments c qui appartiennent à tous les A_α.

Si A et B sont deux ensembles de S, la collection des éléments c tels que c appartient au moins à l'un des deux ensembles est appelée l'**union** $A \cup B$ de A et B. Plus généralement, si $\{A_\alpha, \alpha \in I\}$ est une collection de sous-ensembles de S, l'union $\cup_{\alpha \in I} A_\alpha$ est l'ensemble des éléments c tels que c appartienne à au moins l'un des A_α.

La **collection des sous-ensembles** (ou parties) d'un ensemble donné S est noté $\mathcal{P}(S)$. On considère l'ensemble S tout entier et l' ensemble vide ϕ comme deux éléments de $\mathcal{P}(S)$.

Remarque. L'introduction de l'ensemble vide ϕ permet d'écrire $A \cap B = \phi$ pour indiquer que les ensembles A et B n'ont aucun élément commun.

Si A est un sous-ensemble de l'ensemble S, le complémentaire de A dans S, noté A^c ou $\overline{A}$ est constitué de tous les éléments de S qui ne sont pas dans A. On a donc $S = A \cup A^c$ et $A \cap A^c = \phi$.

Exercice.

1. Si $S = \{a, b, c\}$ décrire tous les éléments de $\mathcal{P}(S)$.
   Réponse : les éléments de $\mathcal{P}(S)$ sont :

$$\phi \quad \{a\} \quad \{b\} \quad \{c\} \quad \{a, b\} \quad \{a, c\} \quad \{b, c\} \quad S$$

2. Si S est un ensemble fini de n éléments, montrez que $\mathcal{P}(S)$ contient 2^n éléments.

Une **partition** d'un ensemble S est la donnée d'une famille $\mathcal{P}'$ de sous-ensembles non vides de S tel que tout élément de S appartienne à un et un seul de ces sous-ensembles.

1.2 Ensemble produit.

Si S et T sont deux ensembles, on définit l'**ensemble produit** $S \times T$ comme étant la collection des couples (s, t) où $s \in S$ et $t \in T$. Dans le produit $S \times T$ deux éléments (s, t) et(s', t') sont considérés comme égaux si et seulement si $s = s'$ et $t = t'$.

Exemple. Si S est un ensemble de m éléments $S = \{s_1, \ldots, s_m\}$ et T est un ensemble de n éléments $T = \{t_1, \ldots, t_n\}$, alors $S \times T$ consiste en les $m \cdot n$ éléments

$$S \times T = \{(s_i, t_j\}; 1 \leq i \leq m \text{ et } 1 \leq j \leq n\}.$$

Plus généralement, si $S_1, \ldots, S_r$ sont des ensembles, le produit

$$\prod_{i=1}^{r} S_i = S_1 \times S_2 \times \ldots S_r$$

est la collection des r-uples $(s_1, s_2, \ldots, s_r)$ où la i-ème composante s_i est un élément de S_i.

De même, si S_i est un ensemble pour tout entier positif i, le produit $\prod_{i=1}^{\infty} S_i$ est l'ensemble des suites $(s_1, s_2, \ldots, s_r, \ldots)$ où la i-ème composante s_i est un élément de S_i.

Exercice : Si $\mathbb{Z}_2$ est un ensemble fini de 2 éléments $\mathbb{Z}_2 = \{0, 1\}$, décrire tous les éléments de $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

1.3 Applications.

Une **application** f d'un ensemble S dans un ensemble T est une correspondance qui associe à chaque élément $s \in S$ un (et un seul) élément $t \in T$ appelé **image** de s par f. On note $f(s)$ ou s^f ou $(s)^f$ l'image par f de s dans T.

A une application f de S dans T (on note $f : S \to T$), on associe un sous-ensemble de $S \times T$, appelé **graphe de** f et noté $Gr(f)$, consistant en les éléments (s, s^f).

Remarquons que le graphe de f est un sous-ensemble de $S \times T$ qui a les 2 propriétés suivantes :

1. Si $s \in S$, il existe un élément de la forme (s, t) dans le graphe
2. Si (s, t_1) et (s, t_2) sont dans le graphe, alors $t_1 = t_2$.

Exemple. Soit $\mathbb{R}$ l'ensemble des nombres réels. L'ensemble $\mathbb{R} \times \mathbb{R}$ s'identifie aux points du plan. Soit $f : \mathbb{R} \to \mathbb{R}$ une application (c'est-à-dire une fonction de $\mathbb{R}$ dans $\mathbb{R}$). Le graphe de f est l'ensemble des points de $\mathbb{R}^2$ de la forme $(x, f(x))$; il s'agit de la notion usuelle du graphe d'une fonction.
Si $f(x) = 2x + 3$ pour chaque $x \in \mathbb{R}$, le graphe de f s'identifie aux points de la droite $\{(x, 2x + 3) \,|\, x \in \mathbb{R}\} \subset \mathbb{R}^2$.

Une application $f : S \to T$ est dite **surjective** si, tout élément $t \in T$ est l'image par f d'au moins un élément de S.

Une application $f : S \to T$ est dite **injective** si des points distincts de S ont toujours des images par f distinctes dans T, ou de manière équivalente, si $f(s_1) = f(s_2) \Rightarrow s_1 = s_2$.

Si une application $f : S \to T$ est à la fois injective et surjective, elle est dite **bijective** ; dans ce cas, on peut construire **l'application inverse**, notée f^{-1}, de T dans S qui associe à un élément $t \in T$ l'unique élément s de S tel que $f(s) = t$.

Deux applications f et g de S dans T sont dites **égales** si et seulement si $f(s) = g(s)$ pour tout $s \in S$. Ainsi $f = g$ si et seulement si ces deux applications ont le même graphe.

Si R, S et T sont trois ensembles, et si on a deux applications $f : R \to S$ et $g : S \to T$, on définit **l'application composée** $g \circ f$ $(f \cdot g)$ de R dans S par

$$(g \circ f)(r) = g(f(r)) \quad \text{pour tout } r \in R.$$

[de manière équivalente, $r^{f \cdot g} = (r^f)^g$].
Clairement, la loi de composition est associative : si $f : R \to S$ $g : S \to T$ et $h : T \to U$ sont des applications $(h \circ g) \circ f = h \circ (g \circ f)$.

Les bijections d'un ensemble S dans lui-même sont appelées les **transformations** de S. Parmi celles-ci se trouve l'application identité, notée I (ou I_S pour préciser l'ensemble S), qui envoie tout élément de s sur lui-même.

Si $\alpha : S \to T$ est une bijection, on a clairement

$$\alpha^{-1} \circ \alpha = I_S,\ \alpha \circ \alpha^{-1} = I_T,\ \alpha \circ I_S = \alpha,\ I_T \circ \alpha = \alpha.$$

Le concept d'ensemble produit permet de définir la notion de fonction de plusieurs variables. Une fonction de deux variables de S à valeurs dans T est une application de $S \times S$ dans T. En particulier une application de $S \times S$ dans S est appelée une **loi de composition** dans S.

Exemple.

1) La correspondance qui associe à un nombre réel a positif tout nombre x réel dont le carré vaut a n'est pas une application univaluée puisqu'elle fait correspondre $+2$ et -2 à 4.
2) $\mathbb{R} \to \mathbb{R}$ $x \mapsto e^x$ est une application injective, non surjective.
3) $\mathbb{R} \to \mathbb{R}$ $x \mapsto 2x$ est une application bijective.
4) $\mathbb{Z} \to \mathbb{Z}$ $a \mapsto 2a$ est une application injective, non surjective.
5) $\mathbb{R} \to \mathbb{R}$ $x \mapsto \log x$ n'est pas une application de $\mathbb{R}$ dans $\mathbb{R}$ puisque le logarithme d'un nombre négatif ou nul n'est pas défini.
6) La rotation d'un angle α du plan $\mathbb{R}^2$ autour d'un point P du plan est une application bijective de $\mathbb{R}^2$ dans $\mathbb{R}^2$. Que vaut son inverse ?

1.4 Relations.

Une **relation** (binaire) entre l' ensemble S et l'ensemble T est un sous-ensemble $\mathcal{R}$ de $S \times T$; de manière intuitive un élément $x \in S$ est en "relation R" avec un élément y de T, ssi le couple (x, y) appartient à $\mathcal{R}$; dans ce cas, on note xRy.

Par exemple, nous avons vu que le graphe d'une application f de S dans T est une relation $Gr(f) \subset S \times T$ telle que pour tout $s \in S$ il existe un et un seul $t \in T$ tel que le couple (s,t) appartienne à $Gr(f)$. Réciproquement une relation $\mathcal{R} \subset S \times T$ est le graphe d'une application f de S dans T si et seulement si pour tout $s \in S$ il existe un et un seul $t \in T$ tel que le couple (s,t) appartienne à $\mathcal{R}$; l'application est dfinie par $f(s) = t$ ssi $(s,t) \in \mathcal{R}$.

Une **fonction** f de $\mathbb{R}$ dans $\mathbb{R}$ est une relation $\mathcal{F} \subset \mathbb{R} \times \mathbb{R}$ telle que pour tout $s \in \mathbb{R}$ il existe au plus un $t \in \mathbb{R}$ tel que le couple (s,t) appartienne à $\mathcal{F}$. Dans ce cas, on appelle **domaine de la fonction** f, et on note $Dom(f)$, l'ensemble des $s \in \mathbb{R}$ tel qu'il existe un couple $(s,t) \in \mathcal{F}$. La fonction définit ainsi une application, encore notée f, de son domaine à valeurs dans $\mathbb{R}$.

Une **relation d'équivalence** $\sim$ sur un ensemble S est une relation, notée ici $\sim$, sur S, qui satisfait aux trois conditions suivantes :

1. réflexivité : $a \sim a$ pour tout $a \in S$
2. symétrie : $a \sim b \Rightarrow b \sim a$
3. transitivité : $a \sim b$ et $b \sim c \Rightarrow a \sim c$

Exemples.

1. (Congruence) Soit $\mathbb{Z}$ l'ensemble des nombres entiers, sur lequel on définit la relation
$$a \sim b \text{ si } a - b \text{ est un multiple de 3.}$$
On vérifie [exercice] que $\sim$ est une relation d'équivalence. Si $a \in \mathbb{Z}$, l'ensemble $\overline{a}$ (ou $[a]_\sim$) des éléments b tels que $b \sim a$ est l'ensemble des nombres entiers congrus à a modulo 3. Remarquons que la collection $\{\overline{0}, \overline{1}, \overline{2}\}$ est une partition de $\mathbb{Z}$ (c'est-à-dire une décomposition de $\mathbb{Z}$ comme union de sous-ensembles disjoints).
2. Soit $\mathbb{R}^2$ l'ensemble des points du plan et définissons $x \sim y$ si x et y appartiennent à la même droite horizontale. C'est une relation d'équivalence [exercice]. Si $x \in \mathbb{R}^2$, l'ensemble $\overline{x}$ des points y tels que $y \sim x$ est la droite horizontale passant par x. Remarquons que la collection de ces droites horizontales est une partition de $\mathbb{R}^2$.
3. Une application $f\colon A \to B$ définit une relation d'équivalence, notée $\sim$ sur A comme suit :
$$x \sim y \iff f(x) = f(y).$$

1.4.1 Classes d'équivalence.

Soit S un ensemble et $\sim$ une relation d'équivalence sur S. Si $a \in S$, on note $\overline{a}$ le sous-ensemble de S constitué des éléments b tels que $b \sim a$. Remarquons que $a \in \overline{a}$ (car $a \sim a$ par réflexivité) et que si b_1 et $b_2 \in \overline{a}$ alors $b_1 \sim b_2$ (car $b_1 \sim a$; $b_2 \sim a$ et on a la transitivité). Donc $\overline{a}$ est une collection d'éléments équivalents. De plus, $\overline{a}$ est une

collection maximale de ce type ; on veut dire par là que si $c \in S$ est équivalent à un des éléments b de $\overline{a}$ alors $c \in \overline{a}$ (en effet $b \sim a$ et $c \sim b \Rightarrow c \sim a \Rightarrow c \in \overline{a}$). On appelle $\overline{a}$ la **classe d'équivalence** déterminée par (ou contenant) l'élément a.

Proposition 1.1. *La collection des classes d'équivalence distinctes donne une partition de S.*

Démonstration : Montrons d'abord que si $b \in \overline{a}$ alors $\overline{a} = \overline{b}$. Si $b \in \overline{a}$, alors $\overline{b} \subseteq \overline{a}$ par transitivité de la relation $\sim$, car

$$\left.\begin{array}{l} c \in \overline{b} \Rightarrow c \sim b \\ b \in \overline{a} \Rightarrow b \sim a \end{array}\right\} \Rightarrow c \sim a \Rightarrow c \in \overline{a}.$$

Par symétrie $a \in \overline{b}$ donc $\overline{a} \subset \overline{b}$, dès lors $\overline{a} = \overline{b}$.

On voit dès lors que deux classes d'équivalence sont soit identiques, soit ont une intersection vide ; en effet, si $c \in \overline{a} \cap \overline{b}$, alors $c \in \overline{a}$ donc $\overline{a} = \overline{c}$; de même $\overline{b} = \overline{c}$ donc $\overline{a} = \overline{b}$. ∎

1.4.2 Ensemble quotient.

Soit S un ensemble et $\sim$ une relation d'équivalence sur S ; la collection des classes d'équivalence (distinctes) définies par la relation $\sim$ est appelée l'**ensemble quotient** de S par la relation $\sim$ et est noté $S/\sim$. Il faut remarquer que $S/\sim$ n'est pas un sous-ensemble de S mais un sous-ensemble de la collection $\mathcal{P}(S)$ des parties de S.

Exemples :

1. Dans le premier exemple du §4 où $S = \mathbb{Z}$ et $a \sim b$ si $a - b$ est un multiple de 3, on a 3 classes d'équivalentes distinctes :
   — $\overline{0}$ = l'ensemble des multiples de $3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$
   — $\overline{1}$ = l'ensemble des nombres entiers congrus à 1 modulo 3

   $$= \{\ldots, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$$

   — $\overline{2}$ = l'ensemble des nombres entiers congrus à 2 modulo 3

   $$= \{\ldots, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$$

   L'ensemble quotient $S/\sim$ est donc constitué de 3 éléments $S/\sim = \{\overline{0}, \overline{1}, \overline{2}\}$ et chacun de ces éléments est une partie de $\mathbb{Z}$.
2. Dans le second exemple du §4 où $S = \mathbb{R}^2$ et où $x \sim y$ si x et y appartiennent à la même droite horizontale, une classe latérale est une droite horizontale et $S/\sim$ est l'ensemble des droites horizontales du plan. (Chaque élément de $S/\sim$ représente une droite du plan).

Chapitre 2

Logique et preuves.

Les mathématiques sont une science exacte théorique et déductive. Elles sont basées sur des fondements abstraits et le reste de la théorie découle par déductions logiques. La logique est le langage qui permettra d'exprimer les affirmations mathématiques, de comprendre comment celles-ci s'articulent, et d'en déduire de nouvelles. Les fondements de toute théorie logique sont des affirmations, appelées axiomes ou postulats, que l'on suppose vraies, et toutes les autres affirmations de la théorie vont se déduire logiquement de ces axiomes et postulats. Les axiomes sont généralement des affirmations suffisamment simples pour qu'il y ait un consensus à leur sujet.

Montrer qu'une nouvelle affirmation mathématique est vraie consiste à en donner une preuve ; cela consiste à montrer qu'une certaine affirmation est vraie moyennant certaines hypothèses. Autrement dit, on suppose que des hypothèses $H_1, H_2, \ldots, H_n$ sont vraies (ce peuvent être des axiomes ou des propriétés déjà démontrées) et on montre par déduction qu'une thèse T est vraie.

2.1 Propositions, Tables de vérité et Connecteurs logiques

Définition 2.1. *Une* **proposition** *est une affirmation ayant une valeur logique qui peut être soit vraie, soit fausse.*

On notera une proposition par une lettre majuscule comme $P, Q, \ldots$ La valeur logique "vrai" sera représentée par 1, et la valeur logique "faux" sera représentée par 0.

Exemple 2.1. *Les affirmations ci-dessous sont des propositions :*
$P_1 =$ *"les étudiants de BA1 math sont tous présents"*,
$P_2 =$ *"il fait beau"*,
$P_3 =$ "$1 + 1 = 2$".

Définition 2.2. *Un* **connecteur logique** *permet de combiner une ou deux propositions pour former une nouvelle proposition, dont la valeur logique est déterminée par les propositions de départ.*

Nous considérerons les cinq connecteurs logiques suivants :

1. **la négation**, notée $\neg$ on *non*, associe à une proposition P la proposition $\neg P$, lue "*non*P" ; la proposition $\neg P$ est vraie si P est fausse et $\neg P$ est fausse si P est vraie.
2. **la conjonction**, notée $\wedge$, associe à deux propositions P, Q la proposition $P \wedge Q$, dite "P et Q", qui n'est vraie que si P et Q sont vraies
3. **la disjonction**, notée $\vee$, associe à deux propositions P, Q la proposition $P \vee Q$, dite"P ou Q", qui est vraie dès que l'une au moins des deux propositions P et Q est vraie.
4. **l'implication**, notée $\Rightarrow$, associe à deux propositions P, Q la proposition $P \Rightarrow Q$, dite "P implique Q", qui est vraie sauf dans le cas où P est vraie et Q est fausse.
5. **l'équivalence**, notée $\Leftrightarrow$, associe à deux propositions P, Q la proposition $P \Leftrightarrow Q$, dite "P si et seulement si Q", ou en abrégé "P ssi Q" qui est vraie quand P et Q ont la même valeur de vérité (donc quand P et Q sont toutes les deux vraies ou quand P et Q sont toutes les deux fausses).

On peut définir de manière équivalente ces connecteurs logiques par leur **table de vérité**, i.e. le tableau donnant la valeur logique de la proposition qu'ils définissent à partir des valeurs de vérités des propositions de départ :

P	$\neg P$
0	1
1	0

Q \ P	0	1
0	0	0
1	0	1

$P \wedge Q$

Q \ P	0	1
0	0	1
1	1	1

$P \vee Q$

Q \ P	0	1
0	1	0
1	1	1

$P \Rightarrow Q$

Q \ P	0	1
0	1	0
1	0	1

$P \Leftrightarrow Q$

Notons que la disjonction logique $\vee$ correspond au ou non exclusif alors que dans le langage courant le ou est parfois utilisé dans un sens exclusif. En logique, $P \vee Q$ sera vraie dès que l'une des propositions P ou Q est vraie, même quand les deux propositions sont vraies .

De manière générale, lorsqu'une proposition P est formée au moyen de connecteurs logiques à partir de propositions $Q_1, \ldots, Q_n$, on la notera $P(Q_1, \ldots, Q_n)$ pour mettre en évidence cette dépendence.

Définition 2.3. *Une proposition $P(Q_1, \ldots, Q_n)$ est* **une tautologie** *si P est vraie quelles que soient les valeurs logiques de $Q_1, \ldots, Q_n$.*

Exemple 2.2. *La proposition $P(Q) = Q \vee \neg Q$ est une tautologie. Pour vérifier ceci, on calcule la table de vérité de $P(Q)$:*

Q	*0*	*1*
$\neg Q$	*1*	*0*
$P(Q)$	*1*	*1*

La dernière ligne ne comprenant que des "1", on voit que P est bien une tautologie.

Exemple 2.3. *La proposition $P(Q_1, Q_2) = Q_1 \Rightarrow (Q_1 \vee Q_2)$ est une tautologie. Pour vérifier ceci, on calcule la table de vérité de $P(Q_1, Q_2)$:*

Q_1	*0*		*1*	
Q_2	*0*	*1*	*0*	*1*
$Q_1 \vee Q_2$	*0*	*1*	*1*	*1*
$P(Q_1, Q_2)$	*1*	*1*	*1*	*1*

La dernière ligne ne comprenant que des "1", on voit que P est bien une tautologie.

Définition 2.4. *On dit que deux propositions $P_1(Q_1, \ldots, Q_n)$ et $P_2(Q_1, \ldots, Q_n)$, dépendant des mêmes propositions $Q_1, \ldots, Q_n$, sont* **équivalentes** *si elles ont la même valeur logique, quelles que soient les valeurs logiques de $Q_1, \ldots, Q_n$. On notera alors $P_1 \simeq P_2$.*

Exemple 2.4. *Les propositions* $\begin{cases} P_1(Q_1, Q_2) = (Q_1 \Rightarrow Q_2) \\ P_2(Q_1, Q_2) = \neg(Q_1 \wedge \neg Q_2) \end{cases}$ *sont équivalentes. En effet, leurs tables de vérité sont :*

Q_1	*0*		*1*	
Q_2	*0*	*1*	*0*	*1*
$P_1(Q_1, Q_2)$	*1*	*1*	*0*	*1*

Q_1	*0*		*1*	
Q_2	*0*	*1*	*0*	*1*
$\neg Q_2$	*1*	*0*	*1*	*0*
$Q_1 \wedge \neg Q_2$	*0*	*0*	*1*	*0*
$P_2(Q_1, Q_2)$	*1*	*1*	*0*	*1*

Les dernières lignes étants identiques, on voit que P_1 est bien équivalente à P_2.

L'exemple plus haut correspond à la situation suivante : dire "s'il fait beau dimanche prochain, j'irai à la mer" est équivalent à affirmer "si je ne vais pas à la mer dimanche prochain, c'est qu'il ne fait pas beau". Ou encore "si le prix des pommes est inférieur ou égal à 1 Euro le kilo, j'en achète 3 kg" est équivalent à "si je n'achète pas 3kg de pommes, c'est que le prix au kg est supérieur à 1 Euro".

Exemple 2.5. *Les propositions* $\begin{cases} P_1(Q_1, Q_2) = (Q_1 \Leftrightarrow Q_2) \\ P_2(Q_1, Q_2) = (Q_1 \Rightarrow Q_2) \wedge (Q_2 \Rightarrow Q_1) \end{cases}$ *sont équivalentes. En effet, leurs tables de vérité sont :*

Q_1	*0*		*1*	
Q_2	*0*	*1*	*0*	*1*
$P_1(Q_1, Q_2)$	*1*	*0*	*0*	*1*

Q_1	*0*		*1*	
Q_2	*0*	*1*	*0*	*1*
$Q_1 \Rightarrow Q_2$	*1*	*1*	*0*	*1*
$Q_2 \Rightarrow Q_1$	*1*	*0*	*1*	*1*
$P_2(Q_1, Q_2)$	*1*	*0*	*0*	*1*

Les dernières lignes étants identiques, on voit que P_1 est bien équivalente à P_2.

Vu la table de vérité du connecteur logique $\Leftrightarrow$, on a le lien suivant entre tautologie et équivalence :

Deux propositions P_1 et P_2 sont équivalentes
ssi
la proposition $P_1 \Leftrightarrow P_2$ est une tautologie.

Pour aller plus loin : remarques sur le calcul propositionnel

Les propositions comportant de nombreux connecteurs logiques peuvent être très compliquées. Il est donc utile de savoir les manipuler afin de simplifier (standardiser) leur expression. Les exemples 2.4 et 2.5 montrent qu'il est possible d'éliminer les implications et équivalences, et de ne garder que les connecteurs logiques $\neg$, $\wedge$ et $\vee$.
Pour standardiser plus l'expression d'une proposition $P(Q_1, \ldots, Q_n)$ on peut faire porter les négations directement sur les propositions élémentaires $Q_1, \ldots, Q_n$, en utilisant les lois de de Morgan :

$$\begin{aligned} \neg(P_1 \wedge P_2) &\simeq \neg P_1 \vee \neg P_2, \\ \neg(P_1 \vee P_2) &\simeq \neg P_1 \wedge \neg P_2. \end{aligned}$$

Pour établir ces équivalences, il suffit de comparer les tables de vérité des propositions de gauche et de droite, et de vérifier que les dernières lignes sont bien identiques. Par exemple, pour établir la première équivalence, on a

P_1	0		1	
P_2	0	1	0	1
$P_1 \wedge P_2$	0	1	1	1
$\neg(P_1 \wedge P_2)$	1	0	0	0

P_1	0		1	
P_2	0	1	0	1
$\neg P_1$	1	0	1	0
$\neg P_2$	1	1	0	0
$\neg P_1 \wedge \neg P_2$	1	0	0	0

Pour choisir l'ordre dans lequel on écrit les connecteurs logiques $\wedge$ et $\vee$, on utilise les lois de distributivité entre celles-ci :

$$\begin{aligned} P_1 \vee (P_2 \wedge P_3) &\simeq (P_1 \vee P_2) \wedge (P_1 \vee P_3), \\ P_1 \wedge (P_2 \vee P_3) &\simeq (P_1 \wedge P_2) \vee (P_1 \wedge P_3). \end{aligned}$$

De nouveau, ces équivalences se vérifient au moyen de tables de vérité. La dénomination "lois de distributivité" se justifie par l'analogie avec la loi de distributivité de la multiplication sur l'addition :

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad \text{pour tout } a, b, c \in \mathbb{R}.$$

Il y a néanmoins une différence essentielle entre $\wedge$, $\vee$ et $+, \cdot$: en effet, $\wedge$ se distribue sur $\vee$ ET $\vee$ se distribue sur $\wedge$, alors que seul $\cdot$ se distribue sur $+$. Cette complète symétrie entre $\wedge$ et $\vee$ montre qu'il ne peut y avoir de règle de priorité entre ces deux opérations, de sorte que l'utilisation de parenthèses est indispensable.
En utilisant ces lois de distributivité, on peut faire en sorte que tous les $\vee$ soient effectués avant les $\wedge$, ou le contraire. Dans le premier cas, on a mis la proposition $P(Q_1, \ldots, Q_n)$ sous forme normale conjonctive :

$$\wedge_{i=1}^{p} \vee_{j=1}^{q_i} \tilde{Q}_{ij} = (Q_{11} \vee \ldots \vee Q_{1q_1}) \wedge \ldots \wedge (Q_{p1} \vee \ldots \vee Q_{pq_p}),$$

avec $\tilde{Q}_{ij}$ correspondant soit à l'une des propositions élémentaires Q_{ij}, soit à sa négation $\neg Q_{ij}$. Dans le deuxième cas, on a mis la proposition $P(Q_1, \ldots, Q_n)$ sous forme normale disjonctive :

$$\vee_{i=1}^{p} \wedge_{j=1}^{q_i} \tilde{Q}_{ij} = (Q_{11} \wedge \ldots \wedge Q_{1q_1}) \vee \ldots \vee (Q_{p1} \wedge \ldots \wedge Q_{pq_p}).$$

2.2 Quantificateurs

Les propositions sont souvent des affirmations qui dépendent de divers types d'objets (par exemple des nombres, des ensembles, des fonctions, ...). Une proposition P qui implique un tel objet x sera notée $P(x)$; par exemple, on a,

$$P(n) = \text{“ le nombre entier } n \text{ est un nombre pair”}.$$

Une proposition peut dépendre de plusieurs objets, par exemple

$$Q(z, y) = \text{“ le magasin } y \text{ a en stock la marchandise } z\text{”}$$

Pour préciser si tous les objets x ont la propriété ou seulement certains d'entre eux, on utilise d'autres symboles, appelés quantificateurs.

Le **quantificateur universel**, noté $\forall$, se lit “pour tout” et permet, à partir d'une proposition $P(x)$ faisant intervenir un objet x, de construire une nouvelle proposition, de la forme :

$$\forall x, P(x),$$

Cette nouvelle proposition est vraie si quel que soit l'objet x, la proposition $P(x)$ est vraie.

Exemple 2.6. *Pour la proposition $P(n)$ définie par “l'entier n est pair”, la proposition $\forall n, P(n)$ est fausse car tous les entiers n ne sont pas pairs.*
Pour la proposition $Q(x)$ définie par “$(x+1)^2 = x^2 + 2x + 1$”, la proposition $\forall x, Q(x)$ est vraie, car l'identité ci-dessus est vraie quelle que soit la valeur de x.

Pour démontrer une proposition de la forme $\forall x, P(x)$, c'est-à-dire pour vérifier que cette proposition est vraie, on ne peut pas se restreindre à une ou plusieurs valeurs de x. Il faut au contraire laisser x tel quel dans l'argument, sans lui donner de valeur.

Exemple 2.7. *Pour tenter de démontrer la proposition $\forall n, n$ impair $\Rightarrow n$ premier, on pourrait être tenter de dire : cela marche pour $n = 3$, $n = 5$, $n = 7$, donc c'est certainement vrai en général. Evidemment, cette proposition est fausse, comme le cas $n = 9 = 3 \cdot 3$ le montre. Un tel raisonnement erroné est appelé “preuve par l'exemple” et est proscrit par la logique.*

Exemple 2.8. *Pour démontrer la proposition $\forall n, n$ impair $\Rightarrow n^2$ impair, on peut procéder comme suit. On prend un entier n impair quelconque et on utilise le fait qu'un entier n est impair si et seulement si il peut s'écrire $n = 2k + 1$ où k est un entier. Mais $n = 2k + 1 \Rightarrow n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$; comme $2k^2 + 2k$ est un entier pour k entier, on en déduit que n^2 est impair.*

Le **quantificateur existentiel**, noté $\exists$, se lit “il existe” et permet, à partir d'une proposition $P(x)$ faisant intervenir un objet x, de construire une nouvelle proposition, de la forme :

$$\exists x, P(x),$$

qui est vraie s'il existe (au moins) un objet x pour lequel la proposition $P(x)$ est vraie.

Exemple 2.9. *Pour la proposition $P(n) =$ "n est un carré parfait", la proposition $\exists n, P(n)$ est vraie, car la proposition $P(n)$ est vraie lorsque $n = 25$.*

Pour démontrer la proposition $\exists x, P(x)$, il suffit d'exhiber un objet x particulier qui satisfait la proposition $P(x)$. Une démonstration basée sur ce principe consistera donc le plus souvent en la construction d'un tel objet.

Bien entendu, la proposition $P(x)$ figurant après $\forall x$ ou $\exists x$ peut elle-même contenir des quantificateurs, de sorte qu'une proposition peut contenir un nombre arbitraire de quantificateurs.

Exemple 2.10. *Etant donnée une fonction f et un point x du domaine de f, la proposition*

$$\forall \epsilon > 0, \exists \delta > 0, |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$$

signifie que la fonction f est continue au point x.

Pour manipuler des propositions contenant des quantificateurs, il est nécessaire de savoir calculer la négation d'une telle proposition. Commençons par déterminer la négation d'une proposition de la forme $\forall x, P(x)$. Une telle proposition sera fausse si $P(x)$ n'est pas vérifiée pour tous les objets x, c'est-à-dire si l'on peut trouver (au moins) un objet x tel que $P(x)$ est fausse. En d'autres termes,

$$\neg(\forall x, P(x)) \simeq \exists x, \neg P(x).$$

De manière similaire, on peut calculer la négation d'une proposition de la forme $\exists x, P(x)$. Une telle proposition sera fausse si $P(x)$ n'est vérifiée pour aucun objet x, c'est-à-dire si pour tous les objets x, la proposition $P(x)$ est fausse. On a donc

$$\neg(\exists x, P(x)) \simeq \forall x, \neg P(x).$$

Cette deuxième négation peut aussi être déduite de la première. En effet, en posant $P(x) = \neg Q(x)$ dans la première négation, on obtient

$$\neg(\forall x, \neg Q(x)) \simeq \exists x, \neg(\neg Q(x)) \simeq \exists x, Q(x).$$

En prenant la négation membre à membre, on en déduit

$$\neg\neg(\forall x, \neg Q(x)) \simeq \forall x, \neg Q(x) \simeq \neg(\exists x, Q(x)),$$

ce qui est la deuxième négation, avec $Q(x)$ à la place de $P(x)$.

2.3 Techniques de démonstrations

En mathématiques, on a souvent besoin de vérifier qu'une proposition est une tautologie. Lorsque cette proposition prend la forme d'une implication de la forme $H \Rightarrow T$, cela signifie qu'il faut vérifier que la thèse T est vraie, lorsque l'on suppose que l'hypothèse H l'est aussi. En pratique, l'hypothèse H sera de la forme $H = H_1 \wedge \ldots \wedge H_n$, c'est-à-dire sera composée de plusieurs hypothèses. Le raisonnement permettant de vérifier que T est vraie si $H_1, \ldots, H_n$ le sont est appelé une démonstration. Nous allons présenter différentes techniques permettant de faire des démonstrations.

2.3.1 Preuve directe

La technique plus simple et la plus courante consiste à construire une chaîne d'implications qui transforment progressivement les hypothèses $H_1, \dots H_n$ en la thèse T : on part de la proposition $P_0 = H_1 \wedge \dots \wedge H_n$, supposée vraie, puis on établit une série d'implications $P_i \Rightarrow P_{i+1}$ jusqu'à ce que $P_k = T$. On obtient alors

$$H_1 \wedge \dots \wedge H_n = P_0 \Rightarrow P_1 \Rightarrow \dots \Rightarrow P_k = T.$$

Exemple 2.11. *Si on veut montrer que le carré d'une nombre pair est un nombre pair. On utilise la définition d'un nombre pair : un nombre entier n est pair s'il existe un nombre entier k tel que $n = 2k$. Si $n = 2k$ on a $n^2 = 2k \times 2k = 2(2k^2)$. Comme $k' := 2k^2$ est un nombre entier si k est un nombre entier, on a que $n^2 = 2k'$ avec k' entier, donc n^2 est pair.*

2.3.2 Preuve par contraposition

La preuve par contraposition est une technique basée sur l'équivalence

$$(H \Rightarrow T) \simeq (\neg T \Rightarrow \neg H),$$

que l'on vérifie aisément au moyen de tables de vérité ou par calcul propositionnel. Ainsi, au lieu de démontrer $H \Rightarrow T$, on peut de manière équivalente montrer que $\neg T \Rightarrow \neg H$.

Exemple 2.12. *Si un nombre pair est le carré d'un nombre entier, c'est le carré d'un nombre pair. On veut donc montrer*

$$x^2 \text{ pair } \rightarrow x \text{ pair }.$$

Il est équivalent de montrer que si x n'est pas pair (donc x est impair) alors x^2 n'est pas pair, ce que nous avons déjà montré.

2.3.3 Preuve par l'absurde

Une preuve par l'absurde est basée sur la proposition logique

$$(H \wedge \neg T) \Rightarrow (P \wedge \neg P)$$

pour une certaine proposition P. En d'autres termes, en plus des hypothèses H, on suppose que la thèse est fausse, et l'on cherche à en déduire une proposition $P \wedge \neg P$ qui n'est jamais vraie. On dit alors que l'on a obtenu une contradiction, ce qui montre que notre hypothèse supplémentaire $\neg T$ était absurde. En d'autres termes, T est en fait vraie sous les hypothèses H.

Pour justifier le fait que ce procédé montre bien la proposition $H \Rightarrow T$, on calcule

$$\begin{aligned}
(H \wedge \neg T) \Rightarrow (P \wedge \neg P) &\simeq \neg\left((H \wedge \neg T) \wedge \neg(P \wedge \neg P)\right) \\
&\simeq \neg\left((H \wedge \neg T) \wedge (\neg P \vee P)\right) \\
&\simeq \neg(H \wedge \neg T) \\
&\simeq (H \Rightarrow T).
\end{aligned}$$

La troisième équivalence est une conséquence du fait que $\neg P \vee P$ est une tautologie.

Exemple 2.13. *Pour montrer la proposition :* $\sqrt{2}$ *est un nombre irrationnel, on veut montrer que*

$$x^2 = 2 \Rightarrow x \text{ est irrationnel.}$$

On procède par l'absurde en supposant que $x^2 = 2$ *et que* x *n'est pas irrationnel, donc peut s'écrire sous forme de fraction* $x = \frac{a}{b}$ *avec* a *et* b *des entiers positifs premiers entre eux (sinon on pourrait simplifier la fraction !). On a alors* $x^2 = \frac{a^2}{b^2} = 2$ *donc* $a^2 = 2b^2$ *est pair, et dès lors* a *est pair. On écrit* $a = 2c$*. L'égalité* $a^2 = 2b^2$ *devient* $4c^2 = 2b^2$ *donc* $b^2 = 2c^2$ *est pair, ce qui montre que* b *est pair. On arrive à la contradiction voulue :* 2 *est un facteur commun à* a *et* b *or on a supposé que* a *et* b *étaient premiers entre eux.*

La preuve par contraposition est très similaire à la preuve par l'absurde, car si on suppose $\neg T \wedge H$, alors on obtiendrait $\neg H \wedge H$, qui est une proposition toujours fausse, donc une contradiction.

2.3.4 Preuve par récurrence

La preuve par récurrence est une technique permettant de démontrer des propositions de la forme

$$\forall n \in \mathbb{N}_0, P(n).$$

L'ensemble des naturels positifs $\mathbb{N}_0 = \{1, 2, 3, \ldots\}$ est l'ensemble des entiers positifs. Cet ensemble est caractérisé par le fait que :

— $1 \in \mathbb{N}_0$,

— tout élément $n \in \mathbb{N}_0$ a un successeur $n + 1 \in \mathbb{N}_0$.

En effet, tout naturel $n \in \mathbb{N}_0$ est obtenu en passant un suffisamment grand nombre de fois au successeur à partir de l'élément $1 \in \mathbb{N}_0$. Cette description de $\mathbb{N}_0$ mène à une technique pour démontrer la proposition ci-dessus. Une preuve par récurrence, appelée aussi preuve par induction, se déroule en deux étapes :

— on montre que $P(1)$ est vraie,

— on montre que si $P(n)$ est vraie, alors $P(n+1)$ l'est aussi, quelque soit $n \in \mathbb{N}_0$.

En d'autres termes, on se base sur l'équivalence

$$\forall n \in \mathbb{N}_0, P(n) \simeq \left(P(1) \wedge \forall n \in \mathbb{N}_0, P(n) \Rightarrow P(n+1)\right).$$

Une erreur fréquemment commise avec cette technique est d'oublier de démontrer $P(1)$!

Exemple 2.14. *On veut montrer que pour tout nombre naturel* $n > 0$ *on a*

$$\sum_{k=1}^{n} k^2 \,(= 1^2 + 2^2 + 3^2 + \ldots = n^2) = \frac{n(n+1)(2n+1)}{6}.$$

La proposition $P(n)$ *est définie par la relation ci-dessus* $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$*. Pour* $n = 1$ *le membre de gauche est égal à* 1 *et le membre de droite à* $\frac{1\times2\times3}{6} = 1$ *donc la*

proposition $P(1)$ est vraie.
On suppose maintenant que $P(n)$ est vraie. Le membre de gauche de $P(n+1)$ sécrit

$$\begin{aligned}\sum_{k=1}^{n+1} k^2 &= \sum_{k=1}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)}{6}\left(n(2n+1) + 6(n+1)\right) = \frac{(n+1)(2n^2+7n+6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}\end{aligned}$$

et est donc bien égal au membre de droite de $P(n+1)$.

Chapitre 3

Les nombres entiers.

3.1 Les nombres naturels non nuls.

Le système des nombres naturels non nuls $\{1, 2, 3, \ldots\}$ est un point de départ pour la construction de systèmes plus élaborés. Cet ensemble $\mathbb{N}_0$ est caractérisé par les **axiomes de Peano** [1]**-Dedekind** [2]

(i) $\mathbb{N}_0$ n'est pas vide

(ii) Il existe une application injective S de $\mathbb{N}_0$ dans $\mathbb{N}_0$

(iii) L'image de $\mathbb{N}_0$ par S est un sous-espace propre de $\mathbb{N}_0$

(iv) Tout sous-ensemble de $\mathbb{N}_0$ qui contient un élément qui n'appartient pas à l'image de $\mathbb{N}_0$ par S, et qui contient l'image par S de chacun de ses éléments coïncide avec $\mathbb{N}_0$.

Remarques :

1. Par les propriétés iii et iv, il n'existe qu'un élément de $\mathbb{N}_0$ qui n'appartient pas à l'image de $\mathbb{N}_0$ par S, on le note 1 et on note $S(1) = 2$, $S(2) = 3$, etc...
2. L'addition des nombres naturels est définie comme l'unique loi de composition binaire sur $\mathbb{N}_0$, notée $+$, telle que

$$\begin{cases} 1 + y = S(y) & \forall y \in \mathbb{N}_0 \\ S(x) + y = S(x + y) & \forall x, y \in \mathbb{N}_0 \end{cases}$$

On déduit de cette définition et des axiomes de Peano, les propriétés :

$$\left.\begin{array}{lll} \text{a1 :} & \text{associativité} & x + (y + z) = (x + y) + z \\ \text{a2 :} & \text{commutativité} & x + y = y + x \\ \text{a3 :} & \text{être simplifiable} & x + z = y + z \Rightarrow x = y \end{array}\right\} \forall x, y, z \in \mathbb{N}_0$$

Remarquons que l'axiome 4 est la base des preuves par récurrence : si une propriété $E(n)$ est vraie pour $n = 1$ et est vraie pour $S(n)$ dès qu'elle est vraie

1. Peano Giuseppe (1858-1932) professeur à Turin.

2. Dedekind Richard (1831-1916) professeur à Göttingen, Zürich et Brunswick (Allemagne), un des créateurs de la théorie algébrique des nombres et de la théorie des ensembles ;

pour n, alors l'ensemble des nombres naturels s pour lesquels $E(s)$ est vraie est $\mathbb{N}_0$ tout entier.
Par exemple pour montrer a1 on fait une récurrence sur x. En effet

$$1 + (y + z) = S(y + z) = S(y) + z = (1 + y) + z$$

et si a1 est vraie pour x on a :

$$\begin{aligned} S(x) + (y + z) &= S(x + (y + z)) = S((x + y) + z) = \\ &= S(x + y) + z = (1 + (x + y)) + z \\ &= ((1 + x) + y) + z = (S(x) + y) + z \end{aligned}$$

[Les propriétés a2 et a3 sont laissées comme exercice].

3. La multiplication des nombres naturels est définie comme l'unique loi de composition sur $\mathbb{N}_0$, notée $\cdot$, telle que

$$\begin{cases} 1 \cdot y = y \quad \forall y \in \mathbb{N}_0 \\ S(x) \cdot y = xy + y \end{cases}$$

On en déduit les propriétés [exercice] :

$$\left.\begin{array}{lll} m_1 : & \text{associativité} & x \cdot (y \cdot z) = (x \cdot y) \cdot z \\ m_2 : & \text{commutativité} & x \cdot y = y \cdot x \\ m_3 : & \text{être simplifiable} & x \cdot z = y \cdot z \Rightarrow x = y \end{array}\right\} \forall x, y, z \in \mathbb{N}_0$$

De plus, on a la propriété de distributivité

$$x \cdot (y + z) = x \cdot y + x \cdot z \qquad \forall x, y, z \in \mathbb{N}_0$$

4. Le troisième concept fondamental dans $\mathbb{N}_0$ est celui d'ordre ; on dit que a est plus grand que b (et on note $a > b$ ou $b < a$) si l'équation $a = b + x$ a une solution appartenant à $\mathbb{N}_0$.
Cette relation a les propriétés :

O1 : asymétrie si $x > y$ alors on ne peut avoir $y \geq x$

O2 : transitivité $x > y$ et $y > z \Rightarrow x > z$

O3 : trichotomie : pour tout couple (x, y) d'éléments de $\mathbb{N}_0$, une et une seule des 3 relations suivantes est vraie

$$x > y \qquad x = y \qquad \text{ou} \qquad x < y$$

O4 : être bien ordonné : tout sous ensemble P non vide de $\mathbb{N}_0$ contient un plus petit élément, c'est-à-dire un nombre $l \in P$ tel que $l \leq s \ \forall s \in P$.

Les relations principales entre l'ordre et les lois d'addition et de multiplication sont les suivantes :

$$\begin{array}{ll} OA & a > b \Leftrightarrow a + c > b + c \\ & \qquad\qquad\qquad\qquad a, b, c \in \mathbb{N}_0 \\ OM & a > b \Leftrightarrow ac > bc \end{array}$$

Remarque. Le fait de compter et de représenter le résultat par un symbole est présent dans les plus anciens documents humains. C'est chez les Babyloniens que l'on a vu apparaître les débuts de l'algèbre et de l'arithmétique : on a trouvé des tablettes comportant des tables pour des calculs comportant des additions et des multiplications et pour résoudre des équations de degré deux et trois.
Le nombre nul et les symboles $0, 1, \ldots, 9$ ainsi que les nombres entiers négatifs apparurent en Inde et furent repris par les Arabes. Le premier manuscrit hindou où apparut pour la première fois le zéro est le manuscrit de Bakhali du quatrième siècle après J.-C.

Remarque. L'ensemble des nombres naturels, noté $\mathbb{N}$, est l'ensemble des entiers positifs ou nul ; cet ensemble peut également se définir par les axiomes de Peano. On a bien sûr que $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$.

3.2 Les nombres entiers construits à partir de $\mathbb{N}_0$.

Dans l'ensemble $\mathbb{N}_0$ l'équation $x + b = a$ pour a et b donné dans $\mathbb{N}_0$ n'a pas toujours une solution $x \in \mathbb{N}_0$: par exemple, l'équation $x + 3 = 2$ n'a pas de solution dans $\mathbb{N}_0$. On va construire un ensemble plus grand que $\mathbb{N}_0$, c'est-à-dire un ensemble avec une loi d'addition dans lequel $\mathbb{N}_0$ s'injecte, tel que l'équation mentionnée ait toujours une solution. L'idée est de regarder l'ensemble des équations possibles, donc l'ensemble des couples (a, b) d'éléments de $\mathbb{N}_0$ et de définir une relation déquivalence sur ces équations, traduisant le fait que deux équations seront dites équivalentes si elles ont la même solution.

Considérons l'ensemble $\mathbb{N}_0 \times \mathbb{N}_0$ muni de la relation d'équivalence

$$(a, b) \sim (c, d) \text{ ssi } a + d = b + c.$$

La classe d'équivalence $\overline{(a, b)}$ de (a, b) joue le rôle de l'entier habituellement noté $a - b$. L'ensemble des classes d'équivalence est noté $\mathbb{Z}$ et appelé l'ensemble des nombres entiers.
Si on représente le couple (a, b) par un point du plan d'abcisse a et d'ordonnée b, alors la classe $\overline{(a, b)}$ est l'ensemble des points sur la droite de pente 1 passant par (a, b) ayant pour coordonnées des nombres naturels.

Comment définit-on l'**addition** des nombres entiers ? Remarquons que si $(a,b) \sim (a',b')$ et si $(c,d) \sim (c',d')$ alors $(a+c, d+d) \sim (a'+c', b'+d')$; en effet

$$\left.\begin{array}{l}(a,b) \sim (a',b') \Rightarrow a+b' = a'+b \\ (c,d) \sim (c',d') \Rightarrow c+d' = c'+d\end{array}\right\} \Rightarrow \begin{array}{c} a+c+b'+d' = a'+c'+b+d \\ \Downarrow \\ (a+c, b+d) \sim (a'+c', b'+d')\end{array}$$

on en déduit que l'entier $\overline{(a+c, b+d)}$ est une fonction de $\overline{(a,b)}$ et $\overline{(c,d)}$, qu'on appelle la somme des deux entiers $\overline{(a,b)}$ et $\overline{(c,d)}$:

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

On vérifie que les propriétés a1, a2, a3 (associativité, commutativité et simplifiabilité) sont toujours vraies.
De plus, si on pose $0 = \overline{(a,a)}$ (en remarquant que $\overline{(a,a)} \sim \overline{(b,b)}$ $\forall a, b \in \mathbb{N}_0$), on a

a4 : existence d'un neutre pour l'addition : $0 + x = x$ $\forall x \in \mathbb{Z}$.
Si $x = \overline{(a,b)}$, on note $\overline{(b,a)}$ par $-x$ et on a :

a5 : existence d'un inverse à chaque entier pour l'addition : $x + (-x) = 0$.

Les propriétés (a1 $\rightarrow$ a5) se résument en disant que $(\mathbb{Z}, +)$ est un groupe commutatif.

De manière semblable, pour définir la **multiplication** de nombres entiers, on pose

$$\overline{(a,b)}\overline{(c,d)} = \overline{(ac+bd, ad+bc)}$$

Cette loi est bien définie car [exercice]

$$\left.\begin{array}{l}(a,b) \sim (a',b') \\ (c,d) \sim (c',d')\end{array}\right\} \Rightarrow (ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c').$$

Les propriétés m1, m2 et d sont toujours vérifiées, ainsi que la propriété m3 si z est différent de zéro. Remarquons qu'on a également

m4 : existence d'un neutre pour la multiplication $\overline{(2,1)} \cdot x = x$ $\forall x \in \mathbb{Z}$.

Les propriétés (a1 ... a5, d, m1 ... m5) se résument en disant que $(\mathbb{Z}, +)$ est un anneau intègre ou domaine d'intégrité.

Une relation d'**ordre** est définie sur les entiers par $\overline{(a,b)} > \overline{(c,d)}$ si $a + d > b + c$. Cette relation est bien définie [exercice] et vérifie O1, O2, O3 et OA. La propriété OM devient

OM' : si $z > 0$ alors $x > y \Rightarrow xz > yz$.

Remarquons que si l'on note $a = \overline{(a+1, 1)}$, les nombres naturels sont des nombres entiers et l'on a

$$\overline{(a,b)} = \overline{(a+1,1)} + \overline{(1,b+1)} = \overline{(a+1,1)} - \overline{(b+1,1)} = a - b.$$

On retrouve les lois usuelles :

$$(a-b)+(c-d)=\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}=a+c-b-d$$

$$(a-b)\cdot(c-d)=\overline{(a,b)}\cdot\overline{(c,d)}=\overline{(ac+bd,ad+bc)}=ac+bd-ad-bc$$

$$(a-b)>(c-d) \text{ si } a+d>c+b.$$

On a :

$$\begin{cases} a-a=\overline{(a,a)}=0 \\ -(a-b)=(b,a)=b-a \end{cases}$$

1. Caractérisation de $\mathbb{Z}$.
   L'ensemble $\mathbb{Z}$ est caractérisé par le fait d'être un anneau intègre (a1 $\to$ a5, d, m1 $\to$ m4) muni d'une relation d'ordre telle que l'ensemble des éléments positifs ($\{z, z>0\}$) soit bien ordonné (O4).
2. Divisibilité dans $\mathbb{Z}$.
   L'équation $ax=b$ à coefficients entiers n'a pas toujours une solution entière x. L'investigation de cette situation est le premier problème en théorie des nombres.

3.3 Divisibilité et Factorisation dans $\mathbb{Z}$

Définition 3.1. *Un entier b est* **divisible** *par un entier a s'il existe un entier d tel que $b=ad$. On écrit alors $a \mid b$ (a divise b), on dit que b est un multiple de a, ou que a est un facteur ou diviseur de b.*

Propriétés.

1. Les seuls diviseurs entiers de 1 sont $+1$ et -1 ;
2. Tous les entiers divisent 0 mais 0 ne divise que 0 ;
3. La relation $\mid$ est

$$\begin{cases} \text{réflexive (càd } a \mid a \ \forall a \in \mathbb{Z}) \\ \text{transitive (càd } a \mid b \text{ et } b \mid c \Rightarrow a \mid c) \\ \text{si} a \mid b \text{ et } b \mid a \text{ alors } a = \pm b \end{cases}$$

   donc $\mid$ est une relation d'ordre (partiel) sur $\mathbb{N}_0$.

Théorème 3.1 (Division Euclidienne)**.** *Si a et $b \in \mathbb{Z}$ et $b \neq 0$, il existe des entiers uniques q et r tels que*

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

Démonstration. Supposons $b>0$ (le raisonnement est analogue - et laissé comme exercice - si $b<0$). Si l'on représente les multiples entiers de b sur un axe réel, le point représentant a doit tomber dans un de ces intervalles soit $[bq, b(q+1))$. Alors $a=bq+r$

avec $0 \leq r < b$. Les entiers q et r sont uniques ; en effet si $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$ et si on suppose (ce qui n'est bien entendu pas restrictif) que $q' \geq q$ on a :

$$r - r' = b(q' - q) \text{ mais } |r - r'| < b$$

donc $q' - q = 0$. Dès lors $q = q'$ et $r = r'$. ∎

Remarquons que tout nombre entier n est divisible par $1, -1, n$ et $-n$.

Définition 3.2. *Un* **nombre premier** *est un nombre naturel p qui n'est pas égal à 1 et qui n'est divisible que par $1, -1, p$ et $-p$.*

Exemples :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

Un théorème fondamental d'arithmétique dit que tout nombre entier positif peut se factoriser de manière "essentiellement" unique en un produit de nombres premiers. Nous allons prouver ce théorème en utilisant la notion de plus grand commun diviseur.

Définition 3.3. *Un entier d non négatif est un* **plus grand commun diviseur** *(p.g.c.d) de deux entiers a et b ssi*

$$\begin{array}{llll} d \mid a, & & d \mid b, & \\ c \mid a & et & c \mid b & \Rightarrow c \mid d. \end{array}$$

Pour montrer l'existence du p.g.c.d. de deux nombres entiers, on décrit d'abord les sous-groupes de $\mathbb{Z}$.

Théorème 3.2. *Tout sous-ensemble S non vide de $\mathbb{Z}$ fermé pour la soustraction (c'est-à-dire tel que $x - y \in S$ $\forall x, y \in S$) - on dit encore tout sous-groupe de $\mathbb{Z}, +$ - soit est restreint à $\{0\}$, soit contient un plus petit nombre entier positif m et consiste en tous les multiples entiers de m.*

Démonstration. supposons que S contienne un élément non nul $a \in \mathbb{Z}$; dès lors, $a - a \in S$ et $-a = 0 - a \in S$. Dès lors, il existe un élément positif, $|a| \in S$, et donc un plus petit nombre entier positif $m \in S$. Clairement, les multiples entiers de m appartiennent à S (car $m \in S$ et si $km \in S$, on a $(k+1)m = km - (-m) \in S$; d'autre part $-km = 0 - (km) \in S$ donc par récurrence sur k, tous les multiples de m appartiennent à S).
L'ensemble S ne contient pas d'autres éléments que des multiples de m car si $a \in S$, on écrit, en vertu du théorème 1, $a = mq + r$ où $m, r \in \mathbb{Z}$ et $0 \leq r < m$. Dès lors, $a - mq = r$ est un nombre entier non négatif et inférieur à m appartenant à S ; comme m est le plus petit entier positif appartenant à S, $r = 0$ et $a = mq$. ∎

Théorème 3.3. *Si a et b sont deux entiers, ils possèdent un unique p.g.c.d. et celui-ci peut s'écrire comme une combinaison linéaire de a et b à coefficients entiers.*

Démonstration. Remarquons que si a et b sont nuls alors 0 est l'unique pgcd de a et b. Supposons donc que l'un au moins soit non nul et considérons le sous-ensemble S de $\mathbb{Z}$ défini par $S = a\mathbb{Z} + b\mathbb{Z} = \{am + bn \mid n, m \in \mathbb{Z}\}$; c'est clairement (le montrer comme exercice) un sous-groupe de $\mathbb{Z}, +$. Par le théorème 3.2, $S = d\mathbb{Z}$ où d est le plus petit entier positif dans l'ensemble S. Comme $d \in S$, il s'écrit $d = sa + tb$; il est clair que $c \mid a$ et $c \mid b \Rightarrow c \mid sa + tb = d$; de plus, comme $a = a \cdot 1 + b \cdot 0$ et de même $b = a \cdot 0 + b \cdot 1$, a et b appartiennent à $S = d\mathbb{Z}$, et donc $d \mid a$ et $d \mid b$. Dès lors, d est un p.g.c.d. de a et b. Remarquons que si d et d' sont 2 p.g.c.d. de a et b, on a nécessairement $d' = \pm d$ (car $d \mid d'$ et $d' \mid d$) ; comme ils sont tous deux supposés non négatifs, $d = d'$. ∎

Notation : on notera $\text{pgcd}(a, b)$ l'unique p.g.c.d. de deux nombres entiers ; remarquons que $\text{pgcd}(a, 0) = a \ \forall a \in \mathbb{Z}$.

Algorithme d'Euclide. Pour trouver explicitement le p.g.c.d. de deux entiers a et b non nuls, on procède comme suit : on peut supposer que a et b sont positifs puisque

$$\text{pgcd}\ (a, b) = \text{pgcd}\ (-a, b) = \text{pgcd}\ (a, -b) = \text{pgcd}\ (-a, -b)$$

Par le théorème 1 on a

$$a = bq_1 + r_1 \qquad \text{où} \qquad 0 \leq r_1 < b$$

et clairement, par le théorème 3, p.g.c.d.(a, b)=p.g.c.d.(b, r_1) puisque

$$a\mathbb{Z} + b\mathbb{Z} = (bq_1 + r_1)\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r_1\mathbb{Z}.$$

Si $r_1 \neq 0$, on répète cette opératon

$$b = r_1q_2 + r_2 \qquad \text{où} \qquad 0 \leq r_2 < r_1$$

et p.g.c.d.(a, b)=p.g.c.d.(b, r_1)=p.g.c.d.(r_1, r_2).
On arrive ainsi à

$$\begin{array}{rcl} a = bq_1 + r_1 & 0 < & r_1 < b \\ b = r_1q_2 + r_2 & 0 < & r_2 < r_1 \\ & & \qquad\qquad (*) \\ r_1 = r_2q_3 + r_3 & 0 < & r_3 < r_2 \\ & \vdots & \\ r_{n-1} = r_nq_{n+1} + 0 & & \end{array}$$

Comme les restes $r_1, r_2, \ldots$ sont des entiers non négatifs décroissants, il doit exister un entier n $(n \geq 0)$ tel que le reste r_{n+1} soit nul.

L'argument utilisé plus haut montre que

$$\begin{array}{rcl} \text{pgcd}(a, b) & = & \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2) = \ldots = \text{pgcd}(r_{n-1}, r_n) \\ & = & \text{pgcd}(r_n, 0) \end{array}$$

et donc, le p.g.c.d. de deux entiers a et b non nuls est le dernier reste non nul (r_{n-1}) dans l'algorithme ($*$) de divisions successives.

Exercices :

1. Utiliser cet algorithme pour calculer pgcd $(213, 24)$.
2. Montrer que cet algorithme peut être utilisé pour représenter pgcd (a, b) comme combinaison linéaire entière explicite de a et b.
3. Un entier m est un plus petit commun multiple (p.p.c.m) de deux entiers a et b non nuls si $a \mid m$, $b \mid m$ et $(a \mid k$ et $b \mid k) \Rightarrow m \mid k$ Montrer que deux entiers non nuls possèdent un et un seul p.p.c.m positif (aide : considérer le sous-ensemble $a\mathbb{Z} \cap b\mathbb{Z}$).

Décomposition en facteurs premiers.

Définition 3.4. *Deux nombres entiers non nuls a et b sont dits* **relativement premiers** *(on dit aussi* **premiers entre eux** *si pgcd $(a, b) = 1$.*

Remarque. [Identité de Bézout [1]] Deux nombres entiers a et b sont premiers entre eux si et seulement s'il existe deux nombres entiers u et v tels que $1 = au + bv$.

Proposition 3.1 (Lemme de Gauss)**.** [2] *Si a et b sont relativement premiers et si $b \mid ac$, alors $b \mid c$.*

Démonstration : comme $1 = as + bt$, $c = acs + bct$, donc $b \mid (ac)(s) + (b)(ct) = c$. ■

Corollaire 3.1. *Si p est premier et $p \mid ab$ où a et $b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$.*

Démonstration : si p ne divise pas a, p et a sont relativement premiers donc, par la proposition 3.1, p divise b. ■

Théorème 3.4 (Factorisation)**.** *Tout entier non nul peut s'exprimer comme $+1$ ou -1 multiplié par un produit de nombres premiers. Cette expression est unique, à l'ordre dans lequel on écrit ces nombres près.*

Démonstration. soit a un nombre réel non nul, clairement $a = \pm a'$ où $a' = |a|$ est positif. On va montrer que a' peut s'écrire comme un produit de nombres premiers, par un raisonnement par récurrence.
Si $a' = 1$ ou a' est premier, la proposition est vraie ; supposons qu'elle soit vraie pour

1. Etienne Bézout (1730-1783) mathématicien français
2. Carl Friedrich Gauss (1777-1857) astronome, mathématicien et physicien allemand

tout entier positif inférieur à a'. Si a' n'est pas premier, il s'écrit $a' = bc$ où $0 < b < a'$ et $0 < c < a'$; donc, par hypothèse de récurrence on a :

$$\left.\begin{array}{l} b = p_1 \dots p_k \\ c = p'_1, \dots p'_l \end{array}\right\} \text{ où les } p_i, p'_j \text{ sont des nombres premiers}$$

Dès lors $a = \pm 1 \cdot p_1 \dots p_k p'_1 \dots p'_l$ ce qui montre l'existence d'une factorisation.
Pour prouver l'unicité de la décomposition, supposons $a = \pm 1 p_1 \dots p_m = \pm 1 q_1 \dots q_m$ où les p_i, q_j sont premiers. Le signe de a est déterminé par $(\pm)$; les $+1$ (ou -1) doivent donc coïncider dans les deux expressions. Comme $p_1 \mid a$, $p_1 \mid q_1 \dots q_m$ et par le corollaire de la proposition 1, $p_1 = q_i$ pour un certain i. En permutant les facteurs q_j (c'est-à-dire en les renumérotant), on peut supposer $p_1 = q_1$ donc $p_2 \dots p_m = q_2 \dots q_n$. En itérant le raisonnement, chaque facteur p_j est égal à un facteur q_j (en renumérotant) ce qui montre le théorème. ∎

Remarque. Les propriétés de factorisation exposées ci-dessus dans le cadre de l'anneau intègre des nombres entiers seront généralisées à d'autres cas ; en particulier, des raisonnements très parallèles permettront la décomposition en facteurs des polynômes réels, complexes ...

Théorème 3.5 (Euclide). [1] *L'ensemble des nombres entiers premiers est infini.*

Démonstration. (par l'absurde). Supposons que $p_1, p_2, \dots, p_n$ soient les seuls entiers premiers. Définissons $m = \Pi_{k=1}^{n} p_k + 1$. Alors m est un nombre entier qui n'est divisible par aucun des p_i ce qui contredit le théorème précédent. ∎

3.4 Arithmétique modulaire

Définition 3.1. *Soient a, b, m trois entiers avec $m \neq 0$. On dit que a est congru à b modulo m, et on note $a \equiv b \bmod m$, si il existe un entier k tel que $a = b + km$.*

Par le théorème de division d'Euclide 3.1 on peut écrire $a = mq + r$ avec q et r des entiers tels que $0 \leq r < m$, donc tout entier est congru à $0, 1, \dots, m-2$ ou $m-1$ modulo m. Pour cette raison, les entiers $0, 1, \dots, m-1$ sont identifiés à leurs classes de congruence modulo m, et on note $\mathbb{Z}_m = \{0, \dots, m-1\}$ l'ensemble de ces classes de congruence. On peut munir cet ensemble $\mathbb{Z}_m$ de deux opérations : l'addition modulo m, notée $+_m$, et la multiplication modulo m, notée $._m$. Remarquons que $\mathbb{Z}_m$ muni de l'addition modulo m est un groupe commutatif, car cette opération est associative, admet pour neutre 0, admet un inverse $-k \bmod m$ pour tout $k \in \mathbb{Z}_m$ et est commutative.

Proposition 3.2. *Soient a, b, m trois entiers avec $a, m \neq 0$ et $pgcd(a, m) = 1$. Alors l'équation $ax \equiv b \bmod m$ admet une unique solution $x \in \{0, \dots, m-1\}$.*

1. Euclide, mathématicien grec du 3ème siècle avant J.-C.

Démonstration. Montrons d'abord l'existence d'une solution. Comme $\text{pgcd}(a, m) = 1$, par le théorème 3.3, il existe des entiers s, t tels que $sa + tm = 1$. En multipliant par b, on a $a(sb) + tbm = b$ et $x = sb$ est une solution de l'équation $ax \equiv b \bmod m$. Il est clair que tout entier y congru à x modulo m est encore une solution, donc on a bien une solution dans $\{0, \ldots, m-1\}$.

Montrons maintenant que cette solution est unique. Si x_1 et x_2 sont des solutions, alors $a(x_1 - x_2) \equiv 0 \bmod m$. En multipliant l'équation $sa + tm = 1$ membre à membre par $x_1 - x_2$, on a $x_1 - x_2 = sa(x_1 - x_2) + t(x_1 - x_2)m$ est un multiple de m. Donc $x_1 \equiv x_2 \bmod m$ et la solution modulo m est unique, ou, de manière équivalente, il n'y a qu'une solution dans l'ensemble $\{0, \ldots, m-1\}$.. ∎

Remarquons que l'hypothèse $\text{pgcd}(a, m) = 1$ est nécessaire. En effet, l'équation $2x \equiv 1 \bmod 4$ n'admet aucune solution dans $\{0, 1, 2, 3\}$, et l'équation $2x \equiv 2 \bmod 4$ en admet deux : $x = 1$ et $x = 3$.

Lorsque $m = p$ est premier et $b = 1$, la proposition 3.2 signifie que tout entier $a = 1, \ldots, p-1$ admet un inverse modulo p. En particulier, l'ensemble $\mathbb{Z}_p$ muni de l'addition et de la multiplication modulo p est un corps commutatif (on dit aussi un champ). En effet, $\mathbb{Z}_p$ muni de l'addition modulo p est un groupe commutatif, et $\mathbb{Z}_p \setminus \{0\}$ est un groupe commutatif, car la multiplication modulo p est associative, admet pour neutre 1, admet pour tout $a \in \mathbb{Z}_p \setminus \{0\}$ un inverse qui est l'unique solution de $ax = 1 \bmod p$, et est commutative. Nous avons donc obtenu un exemple de corps fini, puisque $\mathbb{Z}_p$ comporte exactement p éléments. Rappelons que $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs comportant un nombre infini d'éléments.

Pour trouver l'inverse de $a \neq 0$ dans $\mathbb{Z}_p$, il suffit de considérer les puissances successives $a^2, a^3, a^4, \ldots$ de a. Comme $\mathbb{Z}_p$ est fini, on obtiendra que $a^m \equiv a^n \bmod p$ pour des entiers m et n suffisamment grands (en fait, il suffit que l'un des deux soit au moins p). Alors $a^{m-n} \equiv 1 \bmod p$ et donc a^{m-n-1} est l'inverse de a. Nous allons voir maintenant qu'il est possible de préciser l'exposant qu'il faut utiliser pour trouver l'inverse de a.

Théorème 3.6 (Petit Théorème de Fermat)**.** *Soient $a \neq 0$ un entier et p un nombre premier. Alors*

$$a^{p-1} \equiv 1 \ \textit{mod}\ p.$$

Il existe plusieurs preuves de ce théorème dont la première connue est due à Leibniz. Cette preuve utilise la formule du binôme

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n,$$

dans laquelle les nombres $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, appelés coefficients binomiaux, représentent le nombre de manières de choisir un ensemble de k objets parmi une collection de n objets. Le développement ci-dessus est alors une conséquence du fait que, lorsque l'on effectue le produit

$$\underbrace{(a+b)\ldots(a+b)}_{n \text{ fois}},$$

on obtient un terme $a^{n-k}b^k$ autant de fois que l'on peut choisir k parenthèses parmi les n facteurs pour y prendre le terme b, alors que l'on prend le terme a dans les autres.

Démonstration. [du théorème 3.6] Prenons $n = p$ dans la formule du binôme. Remarquons que le coefficient binomial $\binom{p}{k}$ est un multiple de p lorsque $1 \leq k \leq p-1$. En effet, les factorielles $k!$ et $(p-k)!$ du dénominateur ne contiennent alors que des facteurs strictement inférieurs au nombre premier p, donc ne sont pas multiples de p. Par contre, le numérateur $p!$ est un multiple de p, donc $\binom{p}{k}$ l'est aussi.

On en déduit que $(a+b)^p \equiv a^p + b^p \bmod p$. Montrons alors par induction sur a que $a^p \equiv a \bmod p$. Lorsque $a = 2$, c'est une conséquence de $2^p = (1+1)^p \equiv 1^p + 1^p = 2 \bmod p$. En supposant que la propriété est vraie pour a, on la démontre pour $a+1$ en calculant $(a+1)^p \equiv a^p + 1^p \equiv a + 1 \bmod p$.

En multipliant membre à membre la congruence $a^p \equiv a \bmod p$ par l'inverse de a dans $\mathbb{Z}_p$, on obtient la relation $a^{p-1} \equiv 1 \bmod p$. ∎

Remarquons que, dans la proposition 3.2, il n'est pas nécessaire que m soit premier pour qu'un entier a satisfaisant $\operatorname{pgcd}(a, m) = 1$ ait un inverse modulo m. En fait un élément a dans $\{1, \ldots, m-1\}$ possède un inverse modulo m si et seulement si $\operatorname{pgcd}(a, m) = 1$ [exercice].

Définition 3.2. *La fonction d'Euler ϕ associe à tout entier $m \geq 1$ le nombre $\phi(m)$ d'entiers dans $\{1, \ldots, m\}$ qui sont premiers avec m.*

Par exemple, si $m = p$ est un nombre premier, alors $\phi(p) = p-1$. Le petit théorème de Fermat se généraliser de la manière suivante.

Théorème 3.7 (Théorème d'Euler)**.** *Soient $a, m \neq 0$ des entiers premiers entre eux. Alors*

$$a^{\phi(m)} \equiv 1 \ \textit{mod}\ m.$$

Démonstration. Soient $b_1, \ldots, b_{\phi(m)}$ les entiers dans $\{1, \ldots, m\}$ qui sont premiers avec m. Ce sont exactement tous les éléments de $\mathbb{Z}_m$ qui admettent un inverse pour la multiplication. Comme a est premier avec m, alors a admet aussi un inverse modulo m, de même que $ab_1, \ldots ab_{\phi(m)}$. Ainsi, ces nombres sont les mêmes que $b_1, \ldots, b_{\phi(m)}$ modulo m, mais dans un ordre différent. Par conséquent, en multipliant tous les nombres de ces collections, on obtient

$$b_1 \ldots b_{\phi(m)} \equiv (ab_1) \ldots (ab_{\phi(m)}) \bmod m,$$

et après avoir réordonné les facteurs

$$b_1 \ldots b_{\phi(m)} \equiv a^{\phi(m)} b_1 \ldots b_{\phi(m)} \bmod m.$$

En multipliant membre à membre cette congruence par les inverses de $b_1, \ldots, b_{\phi(m)}$ dans $\mathbb{Z}_m$, on obtient la relation $a^{\phi(m)} \equiv 1 \bmod m$. ∎

Au vu de ce résultat, il est important de savoir calculer la fonction d'Euler ; nous savons déjà que si p est premier, alors $\phi(p) = p - 1$.

Proposition 3.3. *Si p est un nombre premier et n un entier ≥ 1 on a*

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

Démonstration. Les entiers qui ne sont pas premiers avec p^n sont les multiples de p. Comme un entier sur p l'est, il y a $\frac{p^n}{p} = p^{n-1}$ nombres qui sont des multiples de p dans l'ensemble $\{1, 2, \ldots, p^n\}$ et donc $p^n - p^{n-1} = p^{n-1}(p-1)$ entiers premiers avec p parmi les p^n entiers $1, 2, \ldots, p^n$. ∎

Pour calculer la valeur de la fonction d'Euler en un entier quelconque, nous aurons du résultat suivant qui permet d'étendre l'étude des congruences linéaires à des systèmes de congruences.

Théorème 3.8 (Théorème du reste chinois)**.** *Soient $m_1, \ldots, m_k \neq 0$ des entiers deux à deux premiers entre eux. Soient $a_1, \ldots, a_k$ des entiers. Alors le système de congruences*

$$\begin{cases} x & \equiv & a_1 & \textit{mod } m_1 \\ & \cdots & & \\ x & \equiv & a_k & \textit{mod } m_k \end{cases}$$

admet une unique solution x modulo $m = m_1 \ldots m_k$.

Proof Procédons par induction sur l'entier $k \geq 1$. Lorsque $k = 1$, le théorème est une conséquence de la proposition 3.2. Vérifions aussi la propriété pour $k = 2$, car cela nous sera utile pour montrer l'étape derécurrence. Comme m_1 et m_2 sont premiers entre eux, il existe par le théorème 3.3 des entiers s et t tels que $sm_1 + tm_2 = 1$. Posons $x = a_2 sm_1 + a_1 tm_2$. Alors $x \equiv a_1 tm_2 \equiv a_1(1 - sm_2) \equiv a_1 \mod m_1$ et de même $x \equiv a_2 sm_1 \equiv a_2 \mod m_2$, de sorte que x est une solution. Si x_1 et x_2 sont deux solutions, alors $x_1 - x_2 \equiv 0 \mod m_1$ et $x_1 - x_2 \equiv 0 \mod m_2$, de sorte que $x_1 - x_2$ est un multiple de m_1 et de m_2 donc de $\frac{m_1 m_2}{\text{pgcd}(m_1, m_2)} = m_1 m_2 = m$, de sorte que $x_1 \equiv x_2 \mod m$. Ce signifie bien que la solution est unique modulo m.

Supposant que le théorème est vrai pour k congruences, démontrons le pour $k+1$ congruences. Par l'hypothèse d'induction, les k premières congruences ont une unique solution a_0 modulo $m_0 = m_1 \ldots m_k$, de sorte que les solutions du système de $k+1$ congruences sont les solutions du système de deux congruences

$$\begin{cases} x & \equiv & a_0 & \mod m_0 \\ x & \equiv & a_{k+1} & \mod m_{k+1}. \end{cases}$$

Les entiers m_0 et m_{k+1} sont premiers entre eux. En effet, si un nombre premier les divise tous les deux, alors p divise $m_1 \ldots m_k$, donc divise l'un d'entre eux, disons m_i. Mais alors m_i et m_{k+1} ne sont pas premiers entre eux, ce qui contredit l'hypothèse du théorème. Or, nous venons de montrer qu'un tel système a une unique solution modulo $m_0 m_{k+1} = m$. Cette solution est l'unique solution du système de $k+1$ congruences initial. □

On utilise le théorème du reste chinois pour calculer la fonction d'Euler en utilisant la propriété suivante.

Proposition 3.4. *Soient $a, b \geq 1$ deux entiers premiers entre eux. Alors*

$$\phi(ab) = \phi(a)\phi(b).$$

PROOF Soient $c_1, \ldots, c_{\phi(a)}$ les $\phi(a)$ entiers de $\{1, \ldots, a\}$ qui sont premiers avec a. De même, soient $d_1, \ldots, d_{\phi(b)}$ les $\phi(b)$ entiers de $\{1, \ldots, b\}$ qui sont premiers avec b. Pour un i tel que $1 \leq i \leq \phi(a)$ et un$j$ tel que $1 \leq j \leq \phi(b)$, on considère le système de congruences

$$\begin{cases} x & \equiv & c_i & \mod a, \\ x & \equiv & d_j & \mod b, \end{cases}.$$

Par le théorème du reste chinois, ce système de congruences admet une unique solution $x = x_{ij}$ puisque a et b sont premiers entre eux. Cet entier x_{ij} est un entier premier avec ab. En effet, il est premier avec a en vertu de la première congruence car un nombre qui divise x_{ij} et a doit diviser c_i et a or ces deux derniers nombres sont premiers entre eux. De même, x_{ij} est premier avec b en vertu de la deuxième congruence et du fait que d_j et b sont premiers entre eux. De plus, les solutions x_{ij} sont forcément distinctes, pour des valeur différentes de i et de j. On obtient ainsi $\phi(a)\phi(b)$ entiers dans $\{1, \ldots, ab\}$ qui sont premiers avec ab.

Inversement, si x est un entier de $\{1, \ldots, ab\}$ premier avec ab, alors x est premier avec a, de sorte que x est congru à l'un des c_i modulo a. De même, x est congru à l'un des d_j modulo b. Par conséquent, les $\phi(a)\phi(b)$ entiers construits ci-dessus sont tous les $\phi(ab)$ entiers de $\{1, \ldots, ab\}$ premiers avec ab. En particulier, on a bien $\phi(ab) = \phi(a)\phi(b)$. □

Corollaire 3.2 (Fonction d'Euler pour un entier $N > 1$ arbitraire)**.** *L'entier N admet une unique factorisation $N = p_1^{n_1} \ldots p_k^{n_k}$ avec les p_i des nombres premiers distincts et les n_i des nombres entiers ≥ 1.*

$$\begin{aligned} \phi(N) &= \phi(p_1^{n_1}) \ldots \phi(p_k^{n_k}) \\ &= p_1^{n_1-1}(p_1 - 1) \ldots p_k^{n_k-1}(p_k - 1). \end{aligned}$$

Ce résultat s'obtient en appliquant la proposition 3.4 inductivement au produit $p_1^{n_1} \ldots p_k^{n_k}$ et en utilisant la proposition 3.3.

3.4.1 Application : détection d'erreurs et cryptographie RSA

L'arithmétique modulaire possède de nombreuses applications dans le domaine de la détection d'erreurs, ainsi qu'en cryptographie.

Détection d'erreurs

Lorsque l'on transmet des données, une petite partie des données peut être altérée durant la transmission, de sorte que les données reçues peuvent contenir des erreurs. Une manière de détecter la présence d'erreurs, est d'introduire de la redondance dans les données.

Numéros de comptes bancaires belges.
Les numéros de comptes bancaires belges sont structurés en 3 groupes de chiffres : xxx-yyyyyyy-zz. Les trois premiers chiffres représentent l'institution bancaire auprès de laquelle le compte a été ouvert. Les sept chiffres suivants représentent le numéro de compte au sein de cette institution bancaire. Ces dix chiffres suffisent à déterminer de manière univoque un compte bancaire. Les deux derniers chiffres sont redondants, et ont pour but d'éviter les transactions bancaires vers des comptes erronés. Ils se calculent à partir des dix premiers chiffres de la manière suivante :

> le nombre zz est la classe de congruence du nombre à 10 chiffres xxxyyyyyyy modulo 97.

Pourquoi a t-on choisi de travailler modulo 97 ?
Comme le nombre zz a deux chiffres (choix a priori du volume de la redondance), si on travaille modulo N, il faut que $N \leq 100$. Pour maximiser le nombre possible de valeurs de zz, il faut que N soit aussi grand que possible. Mais si on commet une erreur sur un seul chiffre en transcrivant un numéro de compte, alors soit le nombre zz est modifié, soit le nombre à dix chiffres augmente ou diminue de $10^a b$, avec $0 \leq a \leq 9$ et $1 \leq b \leq 9$. Dans ce dernier cas, il faut faire en sorte que $10^a b$ ne soit pas un multiple de N, pour que cette erreur soit détectable. De même, si on échange deux chiffres consécutifs dans les dix premiers chiffres, alors le nombre à dix chiffres augmente ou diminue de $9 \cdot 10^a b$, avec $0 \leq a \leq 9$ et $1 \leq b \leq 9$. Ce nombre ne peut être un multiple de N. Pour éviter d'obtenir des écarts qui soient des multiples de N pour différents types d'erreurs, il vaut mieux choisir N premier. Le plus grand nombre premier inférieur ou égal à 100 est 97. Il est donc naturel de faire ce choix.

Numéros de comptes bancaires européens (IBAN).
Les numéros de comptes bancaires européens, ou IBAN (pour International Bank Account Number), sont construits à partir des numéros de comptes nationaux, en ajoutant l'information du pays d'origine et une redondance pour détecter d'éventuelles erreurs. L'IBAN du compte bancaire belge xxx-yyyyyyy-zz s'écrit sous la forme

$$\text{BE}\alpha\alpha \text{ xxxy yyyy yyzz},$$

où les lettres BE indiquent l'origine belge du compte et le nombre à deux chiffres $\alpha\alpha$ est une redondance calculée à partir du reste du numéro de compte, de la manière suivante :

$$\alpha\alpha = 98 - \text{xxxyyyyyyyyzzBE00 mod } 97.$$

Dans cette formule, le nombre xxxyyyyyyyyzzBE00 est obtenu en remplaçant chaque lettre par deux chiffres suivant la règle A = 10, B = 11, ..., Z = 35. Ainsi, une erreur simple dans le numéro de compte belge ou l'origine du pays pourra être détectée facilement.

Codes ISBN.
Chaque livre possède un numéro d'identification propre, appelé ISBN (pour International Standard Book Number). De même, chaque périodique a un numéro ISSN (pour

International Standard Serial Number). Ce numéro est très utile pour l'inventaire de libraires et pour les classements dans les bibliothèques.. Il est important que ce nombre contienne une certaine redondance, pour éviter de confondre des livres au contenu a priori très différents !

Un numéro ISBN-10 est de la forme

A-B-C-d.

Les parties A, B et C ont des longueurs variables alors que d est constitué d'un seul caractère, mais tout code ISBN-10 est de longueur 10. La partie A correspond à la zone géographique ou linguistique d'origine du livre. La partie B permet d'identifier l'éditeur du livre dans la zone A. Le numéro C permet d'identifier le livre publié auprès de l'éditeur B. Enfin, le chiffre d est une redondance permettant de détecter des erreurs. Un code ISBN-10 sera correct si, lorsque on note a_i le $i$ème chiffre du code ISBN-10 en partant de la droite, pour $1 \leq i \leq 10$, alors

$$\sum_{i=1}^{10} i\ a_i \equiv 0 \bmod 11.$$

Par conséquent, puisque $d = a_1$, on obtient ce chiffre de contrôle à partir des 9 premiers chiffres par la formule $d = -\sum_{i=2}^{10} i\ a_i \bmod 11$. Pour qu'une erreur sur chaque chiffre soit détectable, il faut que d soit calculé modulo un entier qui n'est pas divisible par les nombres de 2 à 10. Le plus petit entier faisant l'affaire est 11, mais un entier modulo 11 peut valoir 10, qui comporte deux chiffres. Pour résoudre ce problème, on remplace 10 par le caractère X (dix en chiffres romain), afin que d soit toujours constitué d'un seul caractère.

Cryptographie

Lorsque l'on transmet une information confidentielle sur un canal qui peut être écouté par une tierce personne, il faut crypter cette information afin qu'elle ne soit lisible que par son destinataire.

Les techniques de cryptographie modernes sont basées sur l'arithmétique, et comprennent un nombre infini de codages possibles, dépendant de divers paramètres entiers. Ils permettent à une personne A (Alice) d'envoyer un message à une personne donnée B (Bob) sans que toute autre personne E (Eve) puisse le comprendre. Pour qu'on puisse lui envoyer des messages confidentiels, B publie au monde entier une clé publique, qui consiste en des paramètres numériques à utiliser dans un algorithme donné et connu de tous afin de coder son message pour B. Une fois codé, le message ne peut pas être décodé directement au moyen de la clé publique seule. La technique de décodage consiste à appliquer un autre algorithme donné et connu de tous, mais avec d'autres paramètres numériques, formant une clé privée, et cette clé n'est connue que de B, de sorte que seul lui peut lire les messages qui lui sont destinés. Pour que E parvienne à décoder le message, il lui faudrait trouver le moyen de calculer la clé privée à partir de la clé publique. En pratique, ce calcul revient à résoudre un problème d'arithmétique compliqué, dont le temps de calcul est très long.

La méthode de cryptage par clé publique/privée utilisée le plus largement dans le monde est la méthode RSA (pour ses inventeurs Rivest, Shamir et Adleman).
La première étape est la création des deux clés par Bob :

1. choisir deux nombres premiers distincts p et q (grands !),
2. calculer leur produit $n = pq$,
3. calculer $\phi(n) = (p-1)(q-1)$,
4. choisir un entier e premier avec $\phi(n)$,
5. calculer l'entier positif $d < \phi(n)$ tel que $e \cdot d \equiv 1 \bmod \phi(n)$,
6. faire connaître la clef pulique (n, e), Bob garde pour lui la clé privée est (n, d) .

La deuxième étape est le cryptage par Alice d'un message destiné à Bob :

1. représenter le message par une succession d'entier positifs $M_i < \min(p, q)$,
2. remplacer chaque entier M_i par l'entier $C_i = M_i^e \bmod n$.

La troisième est le décryptage du message par Bob :

1. remplacer chaque entier C_i par l'entier $C_i^d \bmod n$, qui n'est autre que M_i,
2. reconstituer le message à partir des entiers M_i ainsi calculés.

Le fait que $M_i \equiv C_i^d \bmod n$ est une conséquence du fait que $e \cdot d \equiv 1 \bmod \phi(n)$, ce qui implique $e \cdot d = 1 + k\phi(n)$ pour un certain entier k. Alors,

$$C_i^d = M_i^{e \cdot d} = M_i^{1+k\phi(n)} \equiv M_i \bmod n,$$

en vertu du Théorème d'Euler 3.7 ; en effet M_i est premier avec n puisque les seuls nombres non premiers avec n sont des multiples de p ou de q et $M_i < \min(p, q)$.

Pour que E parvienne à calculer la clé privée (n, d) à partir de la clé publique (n, e), il lui faut inverser d modulo $\phi(n)$. Mais pour cela, il lui faut d'abord calculer $\phi(n) = (p-1)(q-1)$, ce qui nécessite la connaissance des nombres premiers p et q, gardés secrets. En d'autres termes, le problème d'arithmétique que E doit résoudre est la factorisation d'un entier n donné en deux facteurs premiers p et q. Lorsque ces nombres sont très grands, cette factorisation est généralement très longue à effectuer.

3.5 Les nombres rationnels.

Un autre aspect de l'équation $ax = b$ où a et $b \in \mathbb{Z}$, $a \neq 0$ conduit à étendre la notion de nombres pour avoir toujours une solution ; cela nous conduit à étudier de cette manière le cas des nombres rationnels.

Considérons dans $\mathbb{Z} \times \mathbb{Z}$ le sous-ensemble S des couples (a, b) d'entiers où b est non nul, et considérons sur S la relation d'équivalence $\sim$ définie par

$$(a, b) \sim (a', b') \text{ ssi } ab' = ba'$$

Définition 3.5. *L'ensemble $\mathbb{Q}$ des nombres rationnels est l'ensemble quotient $S/\sim$, sur lequel la somme et le produit sont définis par :*

$$\begin{aligned} \overline{(a,b)} + \overline{(c,d)} &= \overline{(ad+bc, bd)} \\ \overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(ac, bd)} \end{aligned}$$

si $\overline{(a,b)}$ désigne la classe d'équivalence du couple (a,b) dans S.

Remarques :
1. La somme et le produit sont bien définis ;en effet :

$$\left.\begin{array}{l}(a,b) \sim (a',b') \\ (c,d) \sim (c',d')\end{array}\right\} \Rightarrow \begin{array}{l} ab' = ba' \\ cd' = c'd \end{array}$$

$$\Rightarrow \left\{\begin{array}{l} (ad+bc)\cdot b'd' = ab'\cdot dd' + cd'\cdot bb' = a'b\cdot dd' + c'd\cdot bb' = (a'd' + b'c')\cdot bd \\ ac\cdot b'd' = ab'\cdot cd' = a'bc'd = a'c'\cdot bd \end{array}\right.$$

$$\Rightarrow \begin{array}{l}(ad+bc, bd) \sim (a'd'+b'c', b'd') \\ (ac, bd) \sim (a'c', b'd')\end{array}, \qquad \text{donc}$$

l'addition et la multiplication sont bien définies sur $S/\sim = \mathbb{Q}$.
2. On note généralement $\overline{(a,b)} = a/b$; la notion d'égalité de classes d'équivalence se traduit en l'égalité des fractions : $a/b = a'/b'$ ssi $ab' = a'b$ et la somme et le produit donnent les lois usuelles sur les fractions

$$\left\{\begin{array}{l} a/b + c/d = (ad+bc)/bd \\ a/b \cdot c/d = ac/bc \end{array}\right.$$

Propriétés :

1. L'ensemble $\mathbb{Q}$ muni de l'addition et de la multiplication est un anneau intègre, dans lequel tout élément non nul a un inverse pour la multiplication (en effet : a/b est non nul si $a \neq 0$; dès lors, b/a existe et $a/b \cdot b/a = 1/1$ qui est le neutre pour la multiplication) ; on dit que $\mathbb{Q}$ est un champ.
2. L'ensemble $\mathbb{Q}$ contient un sous-ensemble qui "est" $\mathbb{Z}$. En effet, chaque entier a détermine un nombre rationnel $a/1$ et on a

$$\left\{\begin{array}{l} a/1 + b/1 = (a+b)/1 \\ a/1 \cdot b/1 = ab/1 \end{array}\right.$$

3. Tout champ "contenant" $\mathbb{Z}$, contient un sous-ensemble qui "est" $\mathbb{Q}$.
4. Les nombres rationnels sont ordonnés, si l'on définit $a/b > 0$ quand $a \cdot b$ est un entier positif (on dit qu'un champ est ordonné s'il est ordonné en tant qu'anneau intègre, c'est-à-dire si on a une relation $>$ vérifiant O1, O2, O3, OA et OM'.

Les nombres rationnels sont caractérisés par la propriété 3 ; ils forment l'unique "extension minimale" de $\mathbb{Z}$ en un champ. Cette construction de l'extension minimale d'un anneau intègre en un champ sera reprise plus loin.

3.6 Les nombres réels.

Les grecs utilisaient une approche géométrique pour la notion de nombre réels ; pour eux, un nombre réel a était simplement le rapport entre deux segments de droite. Ils savaient déjà que ces rapports ne sont pas tous donnés par des nombres rationnels. Par exemple, si l'on considère un triangle isocèle rectangle dont les deux côtés égaux sont de longueur c, le rapport a de la longueur h de l'hypothénuse sur la longueur c,

$$a = \frac{h}{c} \quad \text{noté } a = \sqrt{2} \text{ car } a^2 = 2,$$

n'est pas un nombre rationnel.
En effet, si $a = p/q$ où p et $q \in \mathbb{Z}$ n'ont pas de facteur commun (c'est-à-dire $\text{pgcd}(p, q) = 1$ et que la fraction est non simplifiable)), alors $p^2 = 2q^2$ donc p^2 et dès lors p est divisible par 2, mais alors $p = 2p'$ où $p' \in \mathbb{Z}$ et $2p'^2 = q^2$ ce qui montre que q est également divisible par 2, d'où la contradiction.

En fait, la plupart des nombres réels sont non seulement irrationnels (c'est-à-dire n'appartiennent pas à $\mathbb{Q}$) mais de plus sont transcendants (c'est-à-dire ne satisfont pas à une équation algébrique ; ceci n'est pas le cas de $x = \sqrt{2}$ puisque $x^2 - 2 = 0$).

Définition 3.6. *Un champ ordonné F est dit* **complet** *ssi tout sous-ensemble non vide S de F constitué d'éléments positifs de F, possède une borne inférieure dans F.*

Postulat. Les nombres réels $\mathbb{R}$ forment un champ ordonné complet.

Remarque. A isomorphisme près, il n'existe qu'un tel champ et on peut construire les nombres réels soit par coupures de Dedekind, soit comme limites de suites de nombres rationnels. Une coupure de Dedekind est une partie propre A non vide de $\mathbb{Q}$, stable par minorant et ne possédant pas de plus grand élément. Un réel x est alors représenté par l'ensemble A de tous les rationnels strictement inférieurs à x.

Remarquons que certaines équations réelles n'ont pas de solutions réelles, par exemple $x^2 + 1 = 0$; ceci conduit à considérer les nombres complexes.

3.7 Les nombres complexes.

Définition 3.7. *Un* **nombre complexe** *est un couple (x, y) - souvent noté $x + iy$ - de nombres réels ; x est appelée partie réelle et y partie imaginaire de $x + iy$. Les nombres complexes peuvent être additionnés et multipliés avec les règles :*

$$\begin{aligned} (x + iy) + (x' + iy') &= (x + x') + i(y + y') \\ (x + iy) \cdot (x' + iy') &= xx' - yy' + i(xy' + yx') \end{aligned}$$

Propriétés :

1. L'ensemble $\mathbb{C}$ des nombres complexes muni de l'addition et de la multiplication définies ci-dessus est un champ qui contient $\mathbb{R}$ (on identifie un réel x au nombre complexe $(x, 0)$ donc $x + i \cdot 0$) et qui contient un élément noté i tel que $i^2 = -1$ (l'élément i est l'élément $0 + i \cdot 1$ ou encore le couple $(0, 1)$).
2. Remarquons que tout anneau intègre D contenant $\mathbb{R}$ et contenant un élément i (avec $i^2 = -1$), contient un sous-ensemble "engendré" par $\mathbb{R}$ et i qui "est" $\mathbb{C}$; nous généraliserons plus loin cette notion d'"extension".

Représentation dans le plan de Gauss.

A chaque nombre complexe $z = x + iy$ on peut associer un point $p = (x, y)$ du plan et réciproquement. En utilisant des coordonnées polaires dans ce plan (r, θ), on a

$$|z| = r = (x^2 + y^2)^{\frac{1}{2}} \qquad \arg z \overset{\text{déf}}{=} \theta = \arg \operatorname{tg} y/x \quad (\text{si } z \neq 0)$$

clairement $|z| \geq 0$ et $|z| = 0$ ssi $z = 0$. $|z|$ est appelé le **module** du nombre complexe z et $\arg z$ est appelé son **argument**. Réciproquement, on a (x, y) en fonction de (r, θ) par les formules :

$$x = r \cos\theta \quad y = r \sin\theta, \text{ donc } z = |z|(\cos\theta + i \sin\theta)$$

L'importance de ce passage aux coordonnées polaires repose sur les **formules de Moivre** (à démontrer comme exercice) : si z et z' sont deux nombres complexes et si zz' est leur produit on a :

$$|zz'| = |z| \cdot |z'| \quad \arg(zz') = \arg z + \arg z'$$

En particulier, les nèmes racines complexes de l'unité (c'est-à-dire les nombres z tels que $z^n = 1$) sont des nombres z tels que $|z| = 1$ (puisque $|z^n| = |z|^n = 1$) et tels que $n \arg z = 2k\pi$ où $k \in \mathbb{Z}$ (puisque $\arg z^n = n \arg z = \arg 1$) ; ce sont donc les sommets d'un polygone régulier à n côtés inscrit dans le cercle de rayon 1.

Attention

$$|z + z'| \leq |z| + |z'|$$

Exercice : construire les racines sixièmes de 1 dans $\mathbb{C}$.

Conjugué complexe.

La correspondance qui envoie $z = x + iy$ sur $x - iy$, noté $\overline{z}$ et appelé le complexe conjugué de z, est une bijection de $\mathbb{C}$ dans $\mathbb{C}$. De plus, c'est un "automorphisme" de champ car

$$\overline{(z + z')} = \overline{z} + \overline{z'} \text{ et } \overline{(z \cdot z')} = \overline{z} \cdot \overline{z'}.$$

Remarquons que $\overline{(\overline{z})} = z \ \forall z \in \mathbb{C}$.
De plus, $\overline{z} + \overline{z}$ est réel ($x = 1/2(z + \overline{z})$), $z - \overline{z}$ est imaginaire pur ($iy = \frac{1}{2}(z - \overline{z})$), et le produit $z\overline{z}$ est un nombre réel positif ; en fait $z\overline{z} = |z|^2$ [exercice].

3.7.1 Théorème "fondamental" d'algèbre.

On a vu que les nombres complexes étaient obtenus en ajoutant à $\mathbb{R}$ une racine imaginaire i de l'équation $z^2 + 1 = 0$. Faut-il ajouter d'autres racines imaginaires d'autres polynômes pour agrandir encore notre champ ? La réponse est que ce procédé s'arrête : dès qu'on a ajouté i, et donc construit $\mathbb{C}$, toute équation polynomiale à coefficients complexes a des racines dans $\mathbb{C}$. De manière précise, on a

Théorème 3.9 (Euler - Gauss)**.** *Tout polynôme $p(z) = a_0 + a_1 z + \ldots + a_n z^n$, $a_n \neq 0$, de degré n positif, à coefficients complexes (càd $a_0, \ldots, a_n \in \mathbb{C}$) admet une racine complexe (càd qu'il existe un nombre complexe z tel que $p(z) = 0$.*

De nombreuses preuves de ce théorème existent ; nous donnons ci-dessous une idée d'une telle démonstration, qui n'est pas purement algébrique.
Idée de la démonstration : le polynôme $p(z)$ a les mêmes racines que

$$\begin{aligned} q(z) &= z^n + (a_{n-1}/a_n)z^{n-1} + \ldots + (a_0/a_n) \\ &= z^n + c_{n-1}z^{n-1} + \ldots + c_0 \end{aligned}$$

On peut donc se restreindre au cas où le coefficient du terme non nul de plus haut degré vaut 1.

Si z décrit un cercle γ_r de rayon r autour de 0 dans le plan complexe, alors $q(z)$ décrit une courbe continue γ'_r dans un plan complexe. On veut montrer que l'origine 0 de ce plan "image" (représentant les valeurs de $q(z)$) est l'image par q d'un point z. Considérons le nombre $n(r)$ de fois que la courbe γ'_r s'enroule autour de 0 dans le sens inverse des aiguilles d'une montre ; c'est clairement un nombre entier sauf si γ'_r passe par 0 mais dans ce cas le théorème est démontré.

Si $r = 0$, γ'_r est réduit au point $w = q(0)$ et donc $n(0) = 0$. Si r est suffisamment grand, $n(r)$ vaut le degré n du polynôme q. En effet

$$q(z) = z^n(1 + \sum_{k=1}^{n} c_{n-k}z^{-k})$$

et par la formule de Moivre :

$$\arg(q(z)) = n \arg z + \arg(1 + \sum_{k=1}^{n} c_{n-k}z^{-k}).$$

Dès lors, quand z parcourt le cercle γ_r dans le sens inverse des aiguilles d'une montre, $\arg q(z)$ varie de $n2\pi$ plus le changement d'argument dans $(1 + \sum c_{n-k}z^{-k})$. Si $|z| = r$ est suffisemment grand, $u = 1 + \sum c_{n-k}z^{-k}$ reste dans le cercle $|u - 1| < 1/2$ (cercle de rayon $1/2$ centré en 1) et donc s'enroule autour de 0 zéro fois. Donc si r est suffisemment grand $n(r) = n$.
Il est géométriquement clair qu'une courbe qui s'enroule $n \neq 0$ fois autour de zéro ne peut être déformée continument en un point sans passer à un moment de la déformation par 0. Or γ'_r quand r varie est déformée continuement donc γ'_r doit passer par 0 pour un certain r' et quand ça arrive, $q(z) = 0$. ∎