Ensembles, Nombres, Géométrie plane

UQàM MAT1150

Christophe Reutenauer
Laboratoire de combinatoire et d'informatique mathématique,
Université du Québec à Montréal

13 décembre 2023

Table des matières

1 Introduction

Les sections 2, 3, 4, 5, 6, 7 et 9 sont tirées des notes de cours “Algèbre 1”, de Jacques Labelle et de l'auteur [3].

Remerciements : Anissa Amroun, pour plusieurs discussions et suggestions.

Première partie
Ensembles

2 Ensembles

La notion d'*ensemble* est fondamentale en mathématiques. Les termes “groupement”, “famille” ou “collection” donnent une intuition de cette notion.

Comme exemples d'ensembles, citons l'ensemble des nombres premiers, l'ensemble des points d'une droite, l'ensemble des droites dans un plan, l'ensemble des étudiants de l'UQàM.

Les objets qui composent un ensemble sont appelés *éléments* de cet ensemble. On représente souvent les ensembles par des majuscules et leurs éléments par des minuscules. Si a est un élément de l'ensemble A, on écrit $a \in A$ et on lit $\ll$ a *appartient à* A $\gg$ ou $\ll$ a est un élément de A $\gg$. Si a n'est pas élément de A, on écrit $a \notin A$ et on lit $\ll$ a n'appartient pas à A $\gg$ ou $\ll$ a n'est pas un élément de A $\gg$.

L'écriture $A = \{a_1, a_2, ..., a_m\}$ signifie que A est composé des éléments $a_1, a_2, ..., a_m$; il peut y avoir des répétitions d'éléments : par exemple, $\{a, b, a\}$ représente le même ensemble que $\{a, b\}$ ou $\{b, a\}$.

On appelle *définition par extension* d'un ensemble une telle définition : on fait la liste de ses éléments, répétiitons permises, entre une accolade ouvrante et une accolade fermante.

Un ensemble peut être constitué d'un nombre fini ou infini d'éléments. Si A possède un nombre fini d'éléments, $|A|$ dénote son nombre d'éléments, qu'on appelle aussi *cardinalité* de A.

L'ensemble qui ne contient aucun élément est appelé l'*ensemble vide* et on le représente par le symbole $\emptyset$. Sa cardinalité est 0.

Un ensemble qui ne contient qu'un seul élément s'appelle un *singleton*.

On utilisera les notations suivantes : $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels ; $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ est l'ensemble des

entiers relatifs ; $\mathbb{Q}$ est l'ensemble des nombres rationnels (les fractions) ; $\mathbb{N}^* = \{1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels non nuls ; $\mathbb{R}$ est l'ensemble des nombres réels.

On utilise souvent, pour définir un ensemble, une notation comme $B = \{x \in A \mid P(x)\}$ (on écrit aussi $B = \{x \in A, P(x)\}$) ; cette notation signifie que B est l'ensemble des éléments de A qui possèdent la propriété P. Ainsi, on aura pour tout élément x de A : $x \in B$ si et seulement si $P(x)$. Autrement dit, si l'on veut montrer qu'un élément x de A est en fait dans B, il suffit de montrer que $x \in A$ a la propriété P. Et vice-versa, si x a la propriété P, il est dans B.

Des exemples : $\{n \in \mathbb{N} \mid \frac{n}{2} \in N\}$ désigne l'ensemble des nombres naturels pairs ; $\{n \in \mathbb{N} \mid \exists m \in \mathbb{N}, n = m^2\}$ désigne l'ensemble des carrés dans $\mathbb{N}$.

Soient A et B deux ensembles. Si A et B sont constitués des mêmes éléments, on dit qu'ils sont *égaux* et on écrit $A = B$. Si tous les éléments de A appartiennent à B, on dit que A est *contenu* ou *inclus* dans B, ou encore que A est un *sous-ensemble* ou une *partie* de B, et on écrit $A \subset B$ ou $B \supset A$ (on dit aussi que B contient A). Remarquez que $\emptyset$ et A sont des sous-ensembles particuliers de A ; un sous-ensemble autre que ceux-ci est un sous-ensemble *propre* de A.

On note $\mathcal{P}(X)$ l'ensemble des parties de X ; donc les éléments de $\mathcal{P}(X)$ sont les parties de X. Par exemple, si $X = \{1, 2, 3\}$, $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, X\}$. C'est un ensemble de cardinalité 8.

Dans la pratique, quand on veut montrer qu'un ensemble A est inclus dans un ensemble B, on doit montrer qu'un élément quelconque de A est forcément dans B. Autrement dit que : $\forall x \in A \Rightarrow x \in B$. De plus, pour montrer que $A = B$, on doit montrer que $A \subset B$ et $B \subset A$.

On appelle *réunion* ou *union* de deux ensembles A et B le nouvel ensemble formé de tous les éléments qui appartiennent à A ou à B ou aux deux ; on le note $A \cup B$ et on lit "A union B". Donc

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

On appelle *intersection* de deux ensembles A et B le nouvel ensemble formé des éléments communs à A et B ; on la note $A \cap B$ et on lit "A inter B " :

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

Si $A \cap B = \emptyset$, on dit que A et B sont *disjoints*, sinon on dit que A et B se rencontrent, ou se coupent.

La réunion de plusieurs ensembles $A_1, \ldots, A_n$ est notée $A_1 \cup \cdots \cup A_n$, ou $\bigcup_{i=1}^{i=n} A_i$, ou encore $\bigcup_{1 \leq i \leq n} A_i$. Une telle intersection est dite *disjointe* si les ensembles A_i sont deux à deux disjoints : $\forall i, j = 1, \ldots, n,\ i \neq j \Rightarrow A_i \cap A_j = \emptyset$.

Des notations analogues sont utilisées pour l'intersection de plusieurs ensembles.

Le *couple ordonné* ayant a comme première composante et b comme seconde composante se note (a, b). Si A et B sont des ensembles, le *produit cartésien* de A et B est

$$A \times B = \{(a, b) \mid a \in A \text{ et } b \in B\}.$$

Exercice 1. *Soit $A = \{1, 2, 3\}$ et $B = \{4, 5\}$. Écrire les ensembles suivants : a) $A \times B$; b) $\mathcal{P}(A)$; c) $\mathcal{P}(\mathcal{P}(B))$.*

Exercice 2. *a) Vrai ou faux. Soit $A = \{1, 2, 4, \{2, 3\}\}$: $\{1, 2\} \in A$? ; $\{1, 2\} \subset A$?.*

b) Soit $B = \{1, 2, 4, \{2, 3\}, \{1, 2\}\}$: $\{1, 2\} \in B$? ; $\{1, 2\} \subset B$?.

Exercice 3. *Soit $X = \{\emptyset, \{\emptyset\}\}$. Vrai ou faux. a) $\emptyset \in X$; b) $\emptyset \subset X$; c) $\{\emptyset\} \in X$; d) $\{\emptyset\} \subset X$; e) $\{\{\emptyset\}\} \in X$; f)$\{\{\emptyset\}\} \subset X$.*

Exercice 4. *Décrire l'ensemble $\{x \in \mathbb{N} \mid \exists a, b \in \mathbb{N}, a, b \geq 2, x = ab\}$. On peut commencer par énoncer lesquels des nombres de 1 à 10 sont dans cet ensemble.*

Exercice 5. *Soit A un ensemble de cardinalité n ; montrer que $\mathcal{P}(A)$ est de cardinalité 2^n.*

Exercice 6. *Lois de De Morgan : ce dont les identités ${}^c({}^cA) = A$, ${}^c(A \cup B) = {}^cA \cap {}^cB)$, ${}^c(A \cap B) = {}^cA \cup {}^cB)$, où $A, B \in \mathcal{P}(E)$, E est un ensemble, et ${}^cA = E \setminus A$ (le* complément *de A dans E).*

Exercice 7. *Soient A, B des sous-ensembles de E. Montrer que $A \cup B$ (resp. $A \cap B$) est le plus petit (resp. le plus grand) sous-ensemble de E qui contient A et B (resp. qui est contenu dans A et dans B). Ici, plus petit et plus grand fait référence à l'inclusion.*

Exercice 8. *Soient A, B des ensembles. On $A \setminus B$ l'ensemble $\{x \in A \mid x \notin B\}$, et on l'appelle la* différence *de A et B.*

a) Montrer que $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$ (cet ensemble, s'appelle la différence symétrique *de A et B).*

b) Montrer que $A \cap B = A \setminus (A \setminus B)$.

3 Relations et fonctions

Définition 3.1. *Soient A, B des ensembles. Une* relation de A vers B *est un sous-ensemble R de $A \times B$.*

Une relation $R \subset A \times B$ est dite *fonctionnelle* si pour tout $a \in A$, il existe un et un seul $b \in B$ tel que $(a, b) \in R$.

Si R est une relation fonctionnelle, incluse dans $A \times B$, elle définit une *fonction* f de A vers B ; on écrit ceci $f : A \to B$; on dit que A est l'*ensemble de départ* de f et B son *ensemble d'arrivée*. L'ensemble de départ de f est aussi appelé *domaine de définition* de f.

On dit aussi *application* au lieu de fonction.

Soit $f : A \to B$. Pour un élément a donné, l'unique b tel que $(a, b) \in R$ s'appelle l'*image* de a par la fonction f et il est noté $f(a)$. Intuitivement une fonction de A vers B est donc une règle qui permet d'associer à tout élément $a \in A$ un et un seul élément $b \in B$; cet élément b est noté $f(a)$: $f(a) = b$. On dit aussi que a *est envoyé sur* b *par* f, ou que f *associe* b à a. On écrit $a \overset{f}{\mapsto} b$, ou bien $a \mapsto b$ si la fonction f est sous-entendue. Appelons aussi *antécédent de* $b \in B$ *par* f tout élément $a \in A$ tel que $b = f(a)$.

Pour montrer que deux fonction f, g sont *égales*, il faut montrer qu'elles ont même ensemble de départ, même ensemble d'arrivée, et que pour tout x dans l'ensemble de départ, on a $f(x) = g(x)$.

Si $X \subset A$, alors $f(X) = \{f(x) \mid x \in X\}$ est appelé l'*image (directe)* de X par f. Donc $f(X)$ est l'ensemble des images de tous les éléments de X. On a aussi

$$\forall b \in B : b \in f(X) \Leftrightarrow \exists a \in X, b = f(a).$$

L'ensemble $f(A) \subset B$ s'appelle l'*image* de f ; on le note $\mathcal{I}(f)$.

Si $Y \subset B$, alors $f^{-1}(Y) = \{x \in X | f(x) \in Y\}$ est appelé l'*image réciproque* (ou *inverse*) de Y par f.

ATTENTION ! La notation $f^{-1}(Y)$ ne signifie pas que la fonction réciproque f^{-1} de f existe. C'est simplement une notation. Elle est peut-être trompeuse, mais elle est tout-à-fait standard en mathématiques.

On a : $f^{-1}(Y)$ est l'ensemble des antécédents de tous les éléments de Y. On a aussi :

$$\forall a \in A : a \in f^{-1}(Y) \Leftrightarrow f(a) \in Y.$$

Si $Y = \{y\}$ est un singleton, on écrit aussi simplement $f^{-1}(y)$ au lieu de $f^{-1}(\{y\})$.

Proposition 3.2. *Soit $f : A \to B$. Si $X_1 \subset A$ et $X_2 \subset A$, alors*
a) $X_1 \subset X_2 \Rightarrow f(X_1) \subset f(X_2)$ *;*
b) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$ *;*
c) $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$.
Si $Y_1 \subset B$ et $Y_2 \subset B$, alors
d) $Y_1 \subset Y_2 \Rightarrow f^{-1}(Y_1) \subset f^{-1}(Y_2)$ *;*
e) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$ *;*
f) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.
De plus, si $X \subset A$ et $Y \subset B$, alors $f(f^{-1}(Y)) \subset Y$ et $X \subset f^{-1}(f(X))$.

La démonstration pourrait être laissée en exercice, car elle n'utilise pas d'idée difficile. Au contraire, il suffit à chaque étape du raisonnement d'utiliser soit une définition, soit une des hypothèses, soit une propriété déjà démontrée, et le cheminement s'impose quasiment de lui-même [1]. Le lecteur est convié à lire et à comprendre chaque argument de la preuve.

Démonstration. a) Supposons que $X_1 \subset X_2$. Soit $b \in f(X_1)$; par définition de ce dernier, il existe $a \in X_1$ tel que $b = f(a)$. Alors par l'hypothèse $a \in X_2$. Donc $b = f(a) \in f(X_2)$ par définition de ce dernier. On en déduit que $f(X_1) \subset f(X_2)$.

b) Supposons que $b \in f(X_1 \cup X_2)$; alors il existe $a \in X_1 \cup X_2$ tel que $b = f(a)$. Alors, $a \in X_1$ ou $x \in X_2$. Si $a \in X_1$, alors $f(a) \in f(X_1)$, donc $b = f(a) \in f(X_1) \cup f(X_2)$. Si $a \in X_2$, on a symétriquement $b \in f(X_1) \cup f(X_2)$. On en déduit $f(X_1 \cup X_2) \subset f(X_1) \cup f(X_2)$.

Pour l'inclusion réciproque, on utilise a) : comme $X_1 \subset X_1 \cup X_2$, on a $f(X_1) \subset f(X_1 \cup X_2)$. Symétriquement, $f(X_2) \subset f(X_1 \cup X_2)$. On en déduit que $f(X_1) \cup f(X_2) \subset f(X_1 \cup X_2)$.

Finalement $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.

c) Si $b \in f(x_1) \cap f(X_2)$, alors $b \in f(x_1)$ et il existe donc $a \in X_1$ tel que $b = f(a)$; donc $b \in f(X_1)$. Symétriquement, $b \in f(X_1)$. Donc $b \in f(X_1) \cap f(X_2)$. On en déduit $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$.

d) Supposons que $Y_1 \subset Y_2$. Soit $a \in f^{-1}(Y_1)$. Par définition de l'image réciproque, on a $f(a) \in Y_1$. Donc $f(a) \in Y_2$. Donc $a \in f^{-1}(Y_2)$ par définition de l'image réciproque.

e) Soit $a \in f^{-1}(Y_1 \cup Y_2)$. Alors $f(a) \in Y_1 \cup Y_2$. Donc $f(a) \in Y_1$ ou $f(a) \in F(Y_2)$. Dans le premier cas $a \in f^{-1}(Y_1)$ et dans le second cas, $a \in f^{-1}(Y_2)$. Dans les deux cas, $a \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$. On en déduit $f^{-1}(Y_1 \cup Y_2) \subset f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

1. C'est le cas des raisonnements sans astuce. Ce n'est pas le cas de toutes les démonstrations, loin de là.

Pour l'inclusion réciproque, on utilise d) : comme Y_1 et Y_2 sont tous deux sous-ensembles de $Y_1 \cup Y_2$, on obtient par d) que $f^{-1}(Y_1)$ et $f^{-1}(Y_2)$ sont tous deux sous-ensembles de $f^{-1}(Y_1 \cup Y_2)$. On en déduit que $f^{-1}(Y_1) \cup f^{-1}(Y_2) \subset f^{-1}(Y_1 \cup Y_2)$.

f) L'inclusion $f^{-1}(Y_1 \cap Y_2) \subset f^{-1}(Y_1) \cap f^{-1}(Y_2)$ découle de d).

Réciproquement, soit $a \in f^{-1}(Y_1) \cap f^{-1}(Y_2)$. Alors $a \in f^{-1}(Y_1)$ et $a \in f^{-1}(Y_2)$. Donc $f(a) \in Y_1$ et $f(a) \in Y_2$. Donc $f(a) \in Y_1 \cap Y_2$. Donc $a \in f^{-1}(Y_1 \cap Y_2)$. On déduit que $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$. □

Attention, dans c) on n'a pas l'égalité en général ; voir l'exercice 16.

L'ensemble des fonctions de A à B est noté B^A (cette notation s'explique par le fait que si A et B sont finis et $|A| = n$, $|B| = m$, alors $|B^A| = m^n = |B|^{|A|}$).

Si $f : A \to B$ et $g : B \to C$ sont des fonctions, alors $g \circ f$, appelée *composée* (ou *composition*) de f et g, est la fonction de A vers C définie par

$$g \circ f(a) = g(f(a)), \forall a \in A.$$

La composition des fonctions est une opération associative (exercice !). De plus, la *fonction identité* est un élément neutre : si $f : E \to F$, on a $id_F \circ f = f = f \circ id_E$, où id_E est la fonction $E \to E$ qui envoie tout $e \in E$ sur lui-même.

Exemple 3.3. *La composée de* $f(x) = x^2 + 1$, $\mathbb{R} \to \mathbb{R}_+$, *par la fonction* $g(x) = \sqrt{x}$, $\mathbb{R}_+ \to \mathbb{R}$, *est la fonction* $g \circ f(x) = \sqrt{x^2 + 1}$.

Soit $f : A \to B$ une fonction. On dit que :

1. f est *injective* si pour tous $a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$. Ce qui équivaut à : pour tous $a_1, a_2 \in A$, $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$, ou encore à : pour tout $b \in B$, $f^{-1}(b)$ a au plus un élément. On dit alors aussi que f est une *injection*.
2. f est *surjective* si $f(A) = B$. Ce qui équivaut à : pour tout $b \in B$, il existe $a \in A$ tel que $f(a) = b$, ou encore : pour tout $b \in B$, $f^{-1}(b)$ a au moins un élément. On dit alors aussi que f est une *surjection*.
3. f est *bijective* si f est injective et surjective. Ce qui équivaut à : pour tout $b \in B$, il existe un et un seul $a \in A$ tel que $f(a) = b$, ou encore à : pour tout $b \in B$, $|f^{-1}(b)| = 1$. Dans ce cas, on dit aussi que c'est une *bijection*.

On a aussi : f est injective (resp. surjective, resp. bijective) si et seulement si tout $b \in B$ a au plus (resp. a au moins, resp. a exactement) un antécédent par f.

Exemple 3.4. *La fonction de* $\mathbb{R}$ *dans* $\mathbb{R}$ *qui à* x *associe* x^2 *n'est pas injective ; en effet, on a* $1 \neq -1$ *mais* $f(1) = f(-1)$.

Exemple 3.5. *La fonction de* $\mathbb{R}$ *dans* $\mathbb{R}$ *qui à* x *associe* x^3 *est injective ; en effet, tout réel a une unique racine cubique. Donc,* $\forall v \in R$*, il existe au plus un* $x \in R$ *tel que* $f(x) = v$.

Exemple 3.6. *La fonction de* $\mathbb{N}$ *dans* $\mathbb{N}$ *qui à* n *associe* $2n$ *est injective ; en effet, pour tout entier naturel* n *il existe au plus un entier naturel* p *tel que* $2p = n$.

Exemple 3.7. *La fonction de* $\mathbb{R}$ *dans* $\mathbb{R}$ *qui à* x *associe* x^2 *n'est pas surjective ; en effet, il n'existe pas de* $x \in \mathbb{R}$ *tel que* $-1 = x^2$.

Exemple 3.8. *La fonction de* $\mathbb{R}$ *dans* $\mathbb{R}$ *qui à* x *associe* x^3 *est surjective ; en effet, tout réel a une unique racine cubique. Donc,* $\forall v \in R$*, il existe au moins un* $x \in R$ *tel que* $f(x) = v$.

Exemple 3.9. *La fonction de* $\mathbb{N}$ *dans* $\mathbb{N}$ *qui à* $2n$ *et* $2n + 1$ *associe* n *est surjective ; en effet, tout entier naturel* n *est l'image par cette fonction de* $2n$ *(et aussi de* $2n + 1$*).*

Si f est bijective alors la *fonction réciproque* $f^{-1} : B \to A$ est définie par $f^{-1}(b) = a$ si et seulement si $f(a) = b$. Donc $f^{-1} \circ f = id_A$ et $f \circ f^{-1} = id_B$. On a

$$\forall x \in E, \forall y \in F : y = f(x) \Leftrightarrow x = f^{-1}(y). \tag{1}$$

Exemple 3.10. *La fonction exponentielle est une bijection de* $\mathbb{R}$ *vers* $\mathbb{R}_+^*$ *; la bijection réciproque est la fonction logarithme.*

S'il existe une bijection (c'est-à-dire une fonction bijective) de A vers B, on dit que A et B sont *équipotents* (ou ont même nombre d'éléments ou même cardinalité).

Exercice 9. *Soit* R *la relation* $\{(1, 2), (1, 3), (3, 1)\}$*. Est-ce une relation fonctionnelle ? Même question avec* $\{(1, 2), (2, 3), (3, 1)\}$.

Exercice 10. *On appelle* graphe *d'une fonction* $f : A \to B$ *la relation fonctionnelle* R *qui la définit. Montrer que* $R = \{(a, b) \mid b = f(a)\} = \{(a, f(a)) \mid a \in A\}$.

Exercice 11. *Répondre par vrai ou faux (et justifier). Si* $f : A \to B$ *et* $X, Y \subset A$*, alors* $f(X \setminus Y) = f(X) \setminus f(Y)$.

Exercice 12. *Soient les fonctions $f : A \to B$ et $g : B \to C$. Montrer que pour tout $X \subset A$ et pour tout $Y \subset C$, $(g \circ f)(X) = g(f(X))$ et $(g \circ f)^{-1}(Y) = f^{-1}(g^{-1}(Y))$.*

Exercice 13. *Soient les fonctions $f : A \to B$ et $g : B \to C$. Répondre par vrai ou faux et justifier.*

a) Si f et g sont injectives, alors $g \circ f$ est injective.

b) Si $g \circ f$ est injective, alors f est injective.

c) Si $g \circ f$ est surjective, alors g est surjective.

Exercice 14. *Soit $f : A \to B$ une fonction. Prouvez que :*

a) f est surjective $\Leftrightarrow \exists h : B \to A$ telle que $f \circ h = id_B$;

b) f est injective $\Leftrightarrow \exists g : B \to A$ telle que $g \circ f = id_A$. Ici on suppose $A \neq \emptyset$.

Exercice 15. *Soit $f : X \to Y$ une fonction. Prouver que $\forall A \subset X$ et $\forall B \subset Y$ on a : $A \subset f^{-1}(f(A))$ et $f(f^{-1}(B)) \subset B$.*

Exercice 16. *Montrer, avec les notations de la proposition 3.2, que, pour tous sous-ensembles X_1, X_2 de A, on a égalité dans le c) de ce lemme, si et seulement si f est injective.*

4 Relations d'ordre

Deux types de relations sont importantes en mathématiques : les relations d'ordre, et les relations d'équivalence. Les premières sont plus faciles à comprendre, car elles mettent un ordre parmi les éléments d'un ensemble ; les secondes reviennent à regrouper les éléments d'un ensemble par "familles".

Pour une relation $R \subset E \times E$, on écrira plutôt xRy que $(x, y) \in R$; ceci met en avant l'aspect relationnel d'une relation ("x et y sont en relation"). Nous adopterons cette notation dans la suite.

Définition 4.1. *Soit E un ensemble et R une relation sur E. On dit que R est une relation d'ordre si R a les trois propriétés suivantes :*

(i) $\forall x \in E$, on a xRx ;

(ii) $\forall x, y \in E$, xRy et yRx implique $x = y$;

(iii) $\forall x, y, z \in E$, xRy et yRz implique xRz.

Une relation qui a la propriété (i) est dite *réflexive*. De même, elle est dite *anti-symétrique* dans le cas (ii), et *transitive* dans le cas (iii).

Un ensemble qui a une relation d'ordre est appelé *ensemble ordonné*. On note souvent $(E, \leq)$ un tel ensemble : E est l'ensemble et $\leq$ est la relation d'ordre.

Deux exemples fondamentaux sont les suivants.

Exemple 4.2. *On prend $E = \mathbb{N}$ (ou bien $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$), et on définit $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$. La vérification de (i), (ii) et (iii) est laissée au lecteur. Cet ordre est appelé* ordre naturel *sur E.*

Exemple 4.3. *On prend un ensemble X quelconque, et $E = \mathcal{P}(X)$, c'est-à-dire l'ensemble des sous-ensembles de X. On définit la relation d'*inclusion*, notée $\subset$, par : pour $A, B \in E$ (i.e. A, B sont des sous-ensembles de X), $A \subset B$ signifie que A est un sous-ensemble de B. Ici aussi, on peut vérifier (i), (ii) et (iii) : (i) signifie que tout ensemble est sous-ensemble de lui-même ; (ii) que si deux ensembles sont chacun sous-ensemble de l'autre, alors ils sont égaux ; et (iii) que si un premier ensemble est sous-ensemble d'un second, et le second d'un troisième, alors le premier est sous-ensemble du troisième. En notation mathématique :*

(i) $\forall A \in E, A \subset A$.

(ii) $\forall A, B \in E, A \subset B$ *et* $B \subset A \Rightarrow A = B$.

(iii) $\forall A, B, C \in E, A \subset B$ *et* $B \subset C \Rightarrow A \subset C$.

Par analogie avec l'exemple 4.2, on note souvent un ordre par $\leq$ au lieu de R.

Définition 4.4. *1. Deux éléments x, y d'un ensemble ordonné E (l'ordre est noté $\leq$) sont dits* comparables *si $x \leq y$ ou $y \leq x$.*

2. Une relation d'ordre $\leq$ sur un ensemble E est totale *si $\forall x, y \in E$, x et y sont comparables.*

L'exemple 4.2 est un ordre total, alors que l'exemple 4.3 ne l'est pas si X a au moins 2 éléments : en effet, si $X = \{x, y, ...\}$, alors $E = \{\emptyset, \{x\}, \{y\}, \ldots\}$ et les sous-ensembles $\{x\}$ et $\{y\}$ de X ne sont pas comparables pour l'inclusion : on n'a ni $\{x\} \subset \{y\}$, ni $\{y\} \subset \{x\}$.

Si l'ordre n'est pas total, on dit souvent *ordre partiel*.

Définition 4.5. *Soit E un ensemble muni d'un ordre $\leq$ et A un sous-ensemble de E. On dit que A a un* maximum*, ou* un plus grand élément*, s'il y a dans A un élément a tel que : $\forall x \in A, x \leq a$; alors a est appelé le maximum de A, et aussi plus grand élément de A.*

On définit de manière analogue un *minimum*, ou *plus petit élément*.

Soit E un ensemble muni d'une ordre $\leq$ et A un sous-ensemble de E. On dit que $a \in A$ est un élément *maximal* de A si $\forall b \in A, a \leq b \Rightarrow a = b$. En d'autres mots, $a < b$ (c'est-à-dire $a \leq b$ et $a \neq b$) avec $b \in A$ est impossible. On définit de manière analogue un élément *minimal*. On montre que tout maximum est maximal mais la réciproque est fausse.

Exemple 4.6. *Pour $E = \mathbb{N}$ avec l'ordre naturel $\leq$, prenons $A = \mathbb{N}$: alors A a un minimum, à savoir 0, mais n'a pas de maximum. De même, pour $A = \{n \in \mathbb{N} \mid n < 101\}$, nous voyons que A a le minimum 0 et le maximum 100.*

Prenons maintenant $E = \mathcal{P}(X)$ comme dans l'exemple 4.3. Alors E a le minimum $\emptyset$ et le maximum X. Mais pour $X = \{x, y, z\}$, et A le sous-ensemble de E défini par $A = \{\{x\}, \{y\}, \{z\}, \{y, z\}, \{z, x\}, \{x, y\}\}$ (on peut aussi écrire $A = \mathcal{P}(X) \setminus \{\emptyset, X\}$), on voit que A n'a ni minimum, ni maximum. Cependant les singletons $\{x\}, \{y\}$ et $\{z\}$ sont des éléments minimaux, et $\{x, z\}, \{x, y\}, \{y, z\}$ sont des éléments maximaux, de A.

Exercice 17. *Soit E un ensemble muni d'un ordre $\leq$. Soit A une partie de E. Un* majorant *de A dans E est un élément x de E tel que : $\forall a \in A, a \leq x$.*

a) Montrer que si A a un maximum, celui-ci est un majorant.

On considère l'ensemble A' des majorants de A dans E ; si cet ensemble A' a un minimum, on l'appelle le supremum de A dans E *de A, noté $sup(A)$.*

b) Montrer que si A a un maximum, celui-ci est aussi le supremum de A.

c) Dans $E = \mathbb{R}$ avec l'ordre naturel, on considère $A = \{x \in \mathbb{R} \mid x < 0\}$. Quel est l'ensemble des majorants de A ? Quel est le supremum de A ? Est-ce que A a un maximum ?

Exercice 18. *On considère l'ensemble $\mathbb{N}^*$, avec la relation (dite de* divisibilité*) $|$ définie par : $a|b$ s'il existe $n \in \mathbb{N}^*$ tel que $b = na$. Montrer que c'est une relation d'ordre qui n'est pas totale. Trouver les éléments minimaux et maximaux de $A = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$.*

Exercice 19. *On remplace partout $\mathbb{N}^*$ par $\mathbb{Z}^*$ dans l'exercice précédent. Est-ce encore une relation d'ordre ? Comparer à l'exercice 1.1.*

Exercice 20. *10. On considère l'ensemble E ordonné par $\leq$. Sur $E \times E$, on définit la relation : $(x, y)R(x', y')$ si $(x \leq x'$ et $y \leq y')$.*

a) Montrer que c'est une relation d'ordre.

b) On suppose que E a au moins deux éléments. Montrer que R n'est pas un ordre total.

Exercice 21. *On considère un ensemble E muni d'un ordre total $\leq$. Sur $E \times E$, on définit la relation R par : $(x,y)R(x',y')$ si ($x < x'$ ou ($x = x'$ et $y \leq y'$)). Montrer que R est une relation d'ordre (c'est l'ordre dit* lexicographique*). Montrer que c'est un ordre total. Montrer que $(x,y)R(x',y')$ est équivalent à ($x \leq x'$ et $y \leq y'$) ou ($x < x'$ et $y > y'$).*

Exercice 22. *Montrer que si un ensemble ordonné a un maximum, celui-ci est unique.*

Exercice 23. *Soit $X = \{a,b,c,d\}$ et $E = \mathcal{P}(X) \setminus \emptyset$.*

a) Dessiner avec des flèches représentant les couples ordonnés la relation d'inclusion $\subset$ sur E.

b) Trouver le maximum (respectivement le minimum) de E, s'il existe.

c) Trouver dans E les éléments maximaux et minimaux.

d) Trouver dans E un sous-ensemble totalement ordonné ayant quatre éléments.

Exercice 24. *Soit $\mathcal{C}$ l'ensemble des droites du plan. La relation suivante sur $\mathcal{D}$ est-elle réflexive ? symétrique ? transitive ? anti-symétrique ?*

a) $D_1 R D_2$ si $D_1 \cap D + 2 \neq \emptyset$;

b) $D_1 R' D_2$ si $D_1 = D_2$ ou $D_1 \cap D_2 = \emptyset$;

c) $D_1 R'' D_2$ si D_1 est perpendiculaire à D_2.

Exercice 25. *Vérifier les résultats de l'exercice 38 dans le cas où $E = \mathcal{P}(\mathcal{X})$ et ARB si $|A| \leq |B|$ pour $A, B \subset X$.*

Exercice 26. *Soit $E = \mathcal{P}(\mathcal{X})$ où X est un ensemble. La relation suivante sur E est-elle réflexive ? symétrique ? transitive ? anti-symétrique ?*

a) ARB si $A \cap B = \emptyset$ pour $A, B \subset X$;

b) ARB si $A \cap B \neq \emptyset$ pour $A, B \subset X$;

c) $AR"B$ si $|A| = |B|$.

Exercice 27. *Soit $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ avec la relation d'ordre : aRb si et seulement si a divise b. a) Trouver les éléments minimaux et maximaux de E. b) Trouver le minimum et le maximum de E, s'ils existent. c) Trouver le supremum (exercice 17) de $\{2,3\}$ (resp $\{3,4\}$) s'il existe.*

Exercice 28. *De manière analogue à l'exercice 17, on définit, pour un ensemble E muni d'un ordre $\leq$ et une partie A de E, un* minorant *de A dans E tout élément x dans E tel que : $\forall a \in A, x \leq a$. De plus, l'*infimum *de A, noté* $\inf(A)$*, est, s'il existe, le maximum de tous les minorants de A. Pour $E = \mathbb{R}$ et $A \subset \mathbb{R}$, on pose $-A = \{-a \mid a \in A\}$. Montrer que :*

i) $\max(A) = -\min(-A)$ *;*
ii) $\min(A) = -\max(-A)$ *;*
iii) $\sup(A) = -\inf(-A)$ *;*
iv) $\inf(A) = -\sup(-A)$.

On a adopté les notations : $\max(A)$ = *maximum de* A *et* $\min(A)$ = *minimum de* A. *De plus, dans chacune des égalités, il faut montrer que le membre de gauche est défini si et seulement si le membre de droite l'est. Pour* $A, B \subset \mathbb{R}$, *on pose :* $A + B = \{a + b \mid a \in A, b \in B\}$. *Montrer que :*

v) $\max(A + B) = \max(A) + \max(B)$ *;*
vi) $\sup(A + B) = \sup(A) + \sup(B)$.

Exercice 29. *Soit* $f : E \to F$ *une fonction, où* F *est muni d'une relation d'ordre total* $\leq$. *On définit une relation* $\leq_E$ *sur* E *par :* $x \leq_E y$ *si* $f(x) \leq f(y)$. *Montrer que* $\leq_E$ *est une relation d'ordre si et seulement si* f *est injective, et qu'alors* $\leq_E$ *est totale.*

Exercice 30. *29. Soient* R_1 *et* R_2 *deux relations d'ordre sur* E.

a) Montrer que la relation R *sur* E *définie par :* xRy *si et seulement si* (xR_1y *et* xR_2y) *est une relation d'ordre sur* E.

b) À quelles conditions cet ordre est-il total ?*

Exercice 31. *(Vrai ou faux) a) Si* $A \subset \mathbb{Z}$ *possède un minimum, alors tout sous-ensemble non-vide de* A *possède aussi un minimum.*

b) Si $B \subset \mathbb{Q}$ *possède un minimum, alors tout sous-ensemble non-vide de* B *possède un minimum.*

Exercice 32. *(Vrai ou faux). Soit* $\mathbb{Q}$ *avec l'ordre usuel. Si* $A \subset \mathbb{Q}$, $A \neq \emptyset$, *et* A *admet un majorant dans* Q, *alors* A *admet un supremum (exercice 28) dans* Q.

5 Relations d'équivalence

On utilise la définition 4.1, pour les notions de "relation réflexive" et de "relation transitive".

Définition 5.1. *Une relation* R *sur un ensemble* E *est une relation d'équivalence si elle est réflexive, transitive et de plus symétrique, c'est-à-dire :* $\forall x, y \in E, xRy \Rightarrow yRx$.

Exemple 5.2. *Soit* E *un ensemble quelconque et considérons la relation* R *sur* E *définie par :* xRy *si* $x = y$ *(autrement dit,* R *est l'égalité sur* E*). Alors* R *est une relation d'équivalence.*

Exemple 5.3. *On prend E = l'ensemble des triangles dans le plan, et on définit, pour deux triangles T_1, T_2 la relation T_1RT_2, qui signifie "T_1 et T_2 sont des triangles semblables" (i.e. leurs angles sont égaux deux à deux). Alors R est réflexive ($\forall T \in E, TRT$), symétrique ($\forall T_1, T_2 \in E, T_1RT_2 \Rightarrow T_2RT_1$) et transitive ($\forall T_1, T_2, T_3 \in E$, T_1RT_2 et $T_2RT_3 \Rightarrow T_1RT_3$). C'est une relation d'équivalence.*

Exemple 5.4. *Prenons un ensemble E quelconque et $f : E \to F$, une fonction de E vers un ensemble F. Définissons la relation sur E : xRy si $f(x) = f(y)$. On vérifie que R est une relation d'équivalence sur E.*

Définition 5.5. *Soit E un ensemble et R une relation d'équivalence sur E. Une* classe d'équivalence *de R est un sous-ensemble A de E, tel qu'il existe a dans E satisfaisant $A = \{x \in E \mid xRa\}$.*

Exemple 5.6. *(suite de l'exemple 5.2) Les classes d'équivalence sont les singletons de E, c'est-à-dire les sous-ensembles à un élément de E.*

Exemple 5.7. *(suite de l'exemple 5.3) Une classe d'équivalence doit être l'ensemble des triangles T dans le plan tel que T semblable à T_0, où T_0 est un certain triangle ; il s'ensuit qu'une classe d'équivalence pour R consiste en tous les triangles semblables à un triangle donné.*

Exemple 5.8. *(suite de l'exemple 5.4) Une classe d'équivalence est ici de la forme $\{x \in E \mid xRx_0\} = \{x \in E \mid f(x) = f(x_0)\} = f^{-1}(f(x_0))$, où x_0 est un certain élément de E.*

Avec les notations de la définition 5.5, on notera $[a]_R$ l'ensemble $\{x \in E \mid xRa\}$, appelé la *classe d'équivalence de a*. Si le contexte est clair, on note simplement $[a]$.

Le théorème suivant montre qu'avoir une relation d'équivalence sur un ensemble revient à regrouper ses éléments en sous-ensembles.

Theorem 5.9. *Soit E un ensemble et R une relation d'équivalence sur E. Alors E est la réunion disjointe des classes d'équivalence de R.*

Dans l'exemple 5.3, le théorème exprime que tout triangle est dans une classe de similitude, et une seule ; pour l'exemple 5.4, il exprime que tout élément de E a exactement une image sous la fonction f.

Lemma 5.10. *Soit R une relation d'équivalence. Les conditions suivantes sont équivalentes, pour $ab \in E$:*

(i) aRb ;
(ii) $b \in [a]$;
(iii) $[a] = [b]$;

Nous appelons *représentant* d'une classe d'équivalence tout élément $a \in E$ tel que cette classe soit égale à $[a]$.

Démonstration. Si (i) est vrai, alors $b \in [a]$ par la définition 5.5, sachant qu'on a bRa. Si on a $b \in [a]$, alors on a bRa par la même définition et donc aRb, d'où (i). Donc (i) est équivalent à (ii).

Supposons que (i) soit vrai. Soit $x \in [a]$. Alors xRa. Comme aRb, on obtient xRb par transitivité. Donc $x \in [b]$. On en déduit que $[a] \subset [b]$. L'inclusion réciproque se déduit symétriquement, car bRa par symétrie de R. □

Preuve du théorème 5.9. Il faut montrer que tout élément de E appartient à une classe d'équivalence, et que deux classes distinctes ont une intersection vide.

1. Si $x \in E$, alors $x \in [x]_R$, puisque $[x]_R = \{y \in E \mid yRx\}$ contient x car R est réflexive.

2. Soient C_1, C_2 deux classes d'équivalence. Nous pouvons trouver des éléments x_1, x_2 de E tels que, pour $i = 1, 2$, on ait $C_i = [x_i]_R$. Supposons que C_1 et C_2 n'aient pas une intersection vide, i.e. il existe $y \in C_1 \cap C_2$. On a alors, par définition de C_1 et C_2, yRx_1 et yRx_2. D'après le lemme 5.10, on a donc $[y] = [x_1], [y] = [x_2]$, d'où $C_1 = C_2$, ce qui montre que deux classes sont toujours soit d'intersection vide, soit égales, et termine la preuve. □

Définition 5.11. *Une* partition *d'un ensemble E est un ensemble de parties non vides et disjointes de E dont la réunion est E*

Par exemple, $\{A_1, \ldots, A_n\}$ est une partition de E si les A_i sont des parties de E, et si les trois conditions suivantes sont satisfaites :

$$E = \bigcup_{i=1,\ldots,n} A_i,$$

$$\forall i = 1, \ldots, n, A_i \neq \emptyset,$$

et

$$\forall i, j = 1, \ldots, n, i \neq j \Rightarrow A_i \cap A_j = \emptyset.$$

Exemple 5.12. *L'ensemble $\{\{1, 3, \}, \{2, 6, 7\}, \{4, 5\}, \{8\}, \{9\}\}$ est une partition de $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.*

Corollaire 5.13. *Soit E un ensemble avec une relation d'équivalence R. L'ensemble des classes d'équivalence de R est une partition de E*

Définition 5.14. *Soit E un ensemble et R une relation d'équivalence sur E. On appelle* (ensemble) quotient de E par R *l'ensemble des classes d'équivalence de R.*

On note E/R cet ensemble. On note p_R ou p la fonction $E \to E/R$ définie par

$$\forall x \in E, p_R(x) = [x]_R.$$

On en déduit que si $C \in E/R$, avec $x \in C$, alors $p_R(x) = C$ (en effet, $C = [x]$).

La fonction p_R est surjective, comme il découle de la définition des éléments du quotient. On l'appelle la *projection canonique* .

Theorem 5.15. *(propriété universelle du quotient) Soit E un ensemble et R une relation d'équivalence sur E. Soit $f : E \to F$ une fonction. On suppose que $\forall x, y \in E, xRy \Rightarrow f(x) = f(y)$. Il existe une unique fonction $\bar{f} : E/R \to F$ telle que*

$$f = \bar{f} \circ p_R.$$

(i) Si f est surjective, $\bar{f}$ est surjective.

(ii) Si l'on a $\forall x, y \in E, xRy \Leftrightarrow f(x) = f(y)$, alors $\bar{f}$ est injective.

Démonstration. Soit $C \in E/R$. Il existe donc $x \in E$ tel que $C = [x]$; définissons $\bar{f}(C) = f(x)$. Si nous avions pris un autre x' dans E tel que $C = [x']$, nous aurions trouvé le même $\bar{f}(C)$, car xRx' (lemme 5.10), et par hypothèse $f(x) = f(x')$. Donc la fonction $\bar{f} : E/R \to F$ est *bien définie*.

On remarque que pour tout x dans E, on a $x \in [x]$, donc la construction précédente donne

$$\bar{f}([x]) = f(x).$$

On a alors $\forall x \in E$, $f(x) = \bar{f}([x]) = \bar{f}(p_R(x)) = \bar{f} \circ p_R(x)$; donc $f = \bar{f} \circ p_R$.

Ceci prouve l'existence de la fonction $\bar{f}$.

Montrons que $\bar{f}$ est unique. C'est-à-dire : si $g : E/F \to F$ satisfait $f = g \circ p_R$, alors on doit avoir $g = \bar{f}$. Mais pour tout $C \in E/F$, et $x \in C$, on a $\bar{f}(C) = f(x)$; et $x \in C$ implique $C = [x]$, donc $p_R(x) = C$, donc $g(C) = g(p_R(x)) = f(x) = \bar{f}(C)$. D'où $\bar{f} = g$.

(i) Supposons f surjective ; soit $v \in F$. Il existe alors $x \in E$ tel que $f(x) = v$. Alors $\bar{f}([x]) = f(x) = v$, donc $\bar{f}$ est surjective.

(ii) Suposons que $\forall x, y \in E, xRy \Leftrightarrow f(x) = f(y)$. Montrons que $\bar{f}$ est injective. Soient donc C, D dans E/F tels que $\bar{f}(C) = \bar{f}(D)$. Il existe $x, y \in E$ tels que $C = p_R(x), y = p_R(y)$ car p_r est surjective. Alors $f(x) = \bar{f} \circ p_R(x) = \bar{f}(C) = \bar{f}(D) = \bar{f} \circ p_r(y) = f(y)$, donc xRy, et $C = [x] = [y] = D$. □

Exercice 33. *On définit une relation R sur $\mathbb{Z}$ par : xRy si $x-y$ est divisible par 2. Montrer que c'est une relation d'équivalence et déterminer ses classes d'équivalence.*

Exercice 34. *Vérifier l'exemple 5.4 (et sa suite). Montrer que l'ensemble des classes est $\{f^{-1}(a) \mid a \in f(E)\}$.*

Exercice 35. *On considère l'ensemble E des cercles dans le plan et la relation R sur E : C_1RC_2 si C_1 et C_2 ont même rayon. Montrer que R est une relation d'équivalence. Trouver les classes d'équivalence. Indication : on peut utiliser l'exercice 34.*

Exercice 36. *On considère $E = \mathcal{P}(X)$, où X est un ensemble fini, et l'on y définit la relation : ARB si A et B ont même nombre d'éléments. Montrer que c'est une relation d'équivalence (on peut utiliser l'exercice 34).*

Exercice 37. *Montrer que si P est une partition de E, alors la relation R définie par : $xRy \Leftrightarrow (\exists A \in P, x \in A$ et $y \in A)$, est une relation d'équivalence sur E. Montrer que P est l'ensemble des classes de R.*

Exercice 38. *Une relation de* préordre *sur un ensemble E est une relation R réflexive et transitive. On définit une autre relation, notée S, sur E, par : xSy si (xRy et yRx). Montrer que S est une relation d'équivalence. Montrer aussi que R détermine une relation d'ordre sur l'ensemble des classes d'équivalence de S.*

Exercice 39. *On définit une relation R sur $\mathbb{R}$ par : xRy si $x^2 = y^2$. Montrer que c'est une relation d'équivalence et déterminer ses classes d'équivalences. On peut utiliser l'exercice 34.*

Exercice 40. *On considère l'ensemble E de l'exercice 35 et la relation R' sur E : $C_1R'C_2$ si C_1 et C_2 sont des cercles de même centre. Montrer que c'est une relation d'équivalence. Décrire les classes d'équivalence.*

Exercice 41. *Sur l'ensemble $E = \{1, 2, 3, ..., 25\}$, définissons la relation R par : iRj si i et j ont la même somme de leurs chiffres lorsqu'écrits en base 10 (système décimal). Vérifier que R est bien une relation d'équivalence et écrire les classes d'équivalence.*

Exercice 42. *Soit T l'ensemble des triangles dans un plan. Les relations suivantes sur T sont-elles réflexives ? symétriques ? transitives ? antisymétriques ?*

a) tR_1t' si t et t' sont semblables (angles égaux) ;

b) tR_2t *si* t *et* t' *ont même aire ;*
c) tR_3t' *si* t *et* t' *ont exactement deux sommets communs ;*
d) tR_4t' *si* t *et* t' *ont le même nombre d'angles droits.*

Exercice 43. *Soit* $E = \{1, 2, 3, ..., 30\}$ *et* R *la relation d'équivalence sur* E *définie par* aRb *si* a *et* b *admettent le même nombre de diviseurs premiers. Écrire les classes d'équivalence de* R*.*

Exercice 44. *Soit* $R \subset E \times E$ *une relation.Prouver que* R *est transitive* $\Leftrightarrow R \circ R \subset R$*, où* $R \circ R = \{(x, z) \mid x \in E, z \in E$ *et* $\exists y \in E$ *avec* $(x, y) \in R$ *et* $(y, z) \in R\}$*.*

Exercice 45. *Écrire toutes les relations d'équivalence et toutes les partitions sur* $E = \{a, b, c\}$*.*

Exercice 46. ** Soient* R_1 *et* R_2 *deux relations d'équivalence sur* E*. Montrer que la relation* R *sur* E *définie par :* xRy *si et seulement si (*xR_1y *et* xR_2y*), est une relation d'équivalence. Décrire les classes d'équivalence de* R *en fonction de celles de* R_1 *et* R_2*.*

Exercice 47. ** 1. Montrer que pour tout partition sur un ensemble* E*, il existe une relation d'équivalence* R *sur* E *telle que cette partition soit égale à* E/R*. On démontre ainsi la réciproque du corollaire 5.13.*

2. Montrer qu'il existe une bijection naturelle entre les relations d'équivalence sur un ensemble E *et l'ensembles des partitions sur* E*. Indications : utiliser le corollaire 5.13 et l'exercice 37.*

Deuxième partie
Nombres

6 Les entiers naturels et le raisonnement par récurrence

On veut démontrer une propriété qu'ont tous les entiers naturels n, par exemple : "la somme de tous les entiers de 0 à n est égale à $n(n+1)/2$". Comme on considère une propriété quelconque, on va la noter $P(n)$, à lire : n a la propriété P. On veut donc montrer que $P(0)$ est vraie, ainsi que $P(1)$, $P(2)$, et ainsi de suite. On utilise pour cela, le raisonnement par *récurrence*, ou par *induction*. Commençons par l'exemple ci-dessous.

Exemple 6.1. *$P(n)$ est la propriété « la somme des entiers de 0 à n est égale à $n(n+1)/2$». La propriété $P(0)$ est vraie, puisque $0 = 0 \cdot (0+1)/2$. Nous faisons maintenant ce qu'on appelle l'*hypothèse de récurrence*, c'est-à-dire nous supposons que $P(n)$ est vraie et essayons d'en déduire $P(n+1)$. L'hypothèse de récurrence implique que la somme des entiers de 0 à n vaut $n(n+1)/2$; nous en déduisons que la somme des entiers de 0 à $n+1$ vaut $n(n+1)/2 + n + 1 = (n+1)(n/2+1) = (n+1)(n+2)/2$, ce qui démontre que $P(n+1)$ est vraie. Ainsi nous avons montré que : (i) $P(0)$ est vraie, et (ii) si $P(n)$ est vraie, alors $P(n+1)$ est vraie. Le principe de récurrence nous assure alors que $P(n)$ est vraie quel que soit l'entier naturel n.*

Principe de récurrence : On veut démontrer une propriété $P(n)$ que possèdent tous les entiers naturels n. On fait comme suit :

(i) On démontre que P(0) est vraie.

(ii) On fait l'hypothèse que $P(n)$ est vraie (*hypothèse de récurrence*), et on démontre que $P(n+1)$ est vraie. Autrement dit, on démontre que « $P(n)$ vraie » implique « $P(n+1)$ vraie ». Ceci étant fait, on est sûr que la propriété est vraie pour tous les entiers : intuitivement en effet, $P(0)$ est vraie par (i), donc $P(1)$ est vraie par (ii), donc $P(2)$ est vraie par (ii) et ainsi de suite.

Attention : pour (ii), il faut prendre un entier n quelconque, non spécifié, et pas 17, ou 1789, ou autre.

Theorem 6.2. *Tout sous-ensemble non vide de $\mathbb{N}$ a un minimum.*

Démonstration. 1. Nous commençons par démontrer qu'une certaine propriété $P(n)$ est vraie pour tout n dans $\mathbb{N}$. Puis nous verrons que le théorème s'en déduit. On prend pour $P(n)$ l'énoncé « tout sous-ensemble de $\mathbb{N}$ qui contient un entier $\leq n$ a un minimum ». Démontrons que $P(n)$ est vrai, en utilisant le principe de récurrence.

(i) $P(0)$ signifie que si un sous-ensemble de $\mathbb{N}$ contient 0, alors il a un minimum. C'est clair, puisqu'alors 0 est son minimum. Donc $P(0)$ est vraie.

(ii) L'hypothèse de récurrence est : si un sous-ensemble A de $\mathbb{N}$ contient un élément $\leq n$, alors A a un minimum (c'est la propriété $P(n)$). Nous en déduisons $P(n+1)$: en effet, soit E un sous-ensemble de $\mathbb{N}$ qui contient un élément $\leq n+1$. Si E contient un élément $\leq n$, l'hypothèse de récurrence implique que E a un minimum. Si par contre E ne contient aucun élément $\leq n$, comme il contient un élément $\leq n+1$, il doit contenir $n+1$. Mais alors $n+1$ est son minimum. Ainsi $P(n+1)$ est vraie.

2. Pour finir la preuve du théorème, soit maintenant E un sous-ensemble non vide quelconque de $\mathbb{N}$. Comme E est non vide, il existe $n \in \mathbb{N}$ tel que $n \in E$. Le fait que $P(n)$ est vraie implique alors que E a un minimum. □

Principe de récurrence (variante) : On laisse tel quel (i) et on remplace (ii) par :

(ii') on fait l'hypothèse que $P(0), P(1), \ldots, P(n)$ sont toutes vraies (*hypothèse de récurrence*), et on démontre qu'alors $P(n+1)$ est vraie.

Une autre variante consiste, au lieu de commencer par 0, à commencer par un nombre plus grand, comme dans la preuve de l'énoncé ci- dessous.

Rappelons d'abord le vocabulaire de la divisibilité : on dit qu'un entier a *divise* un entier b s'il existe un entier n tel que $b = an$; on dit alors aussi que a est un *diviseur* de b, ou que b est un *multiple* de a.

Un entier naturel est dit *premier* s'il est ≥ 2 et s'il n'est divisible que par 1 et par lui-même.

Theorem 6.3. *Tout entier naturel ≥ 2 est divisible par un entier naturel premier.*

Démonstration. Pour $n = 2$, le théorème est évident car 2 est premier et 2 est divisible par 2.

Soit n un entier ≥ 2 et supposons que pour tout entier compris entre 2 et n, k est divisible par un nombre premier. Considérons $n+1$: s'il est premier alors il est divisible par un nombre premier ; s'il n'est pas premier, alors on a $n+1 = k \cdot m$, où k est un entier naturel non nul, différent de 1 et de $n+1$. Alors k est compris entre 2 et n. Donc, par l'hypothèse de récurrence, k est divisible par un nombre premier p. Comme p divise k et que k divise $n+1$, p divise $n+1$, ce qui finit la preuve. □

Exercice 48. *Démontrer par récurrence les assertions suivantes, où n est un entier naturel quelconque. Indications : dans tous ces exercices, la difficulté est comment passer de l'expression avec n à l'expression avec $n+1$.*

a) $n^2 - n$ *est divisible par 2.*

b) $n^3 - n$ *est divisible par 3.*

c) $4^n - 1$ *est divisible par 3.*

d) $2^{2n+1} + 1$ *est divisible par 3.*

e) $9^n - 8n - 1$ *est divisible par 64.*

f) $7^n - 3^n$ *est divisible par 4.*

g) $2^n > n$.

h) si $n \geq 1$, *alors* $2^{n-1} \leq n!$.

i) $0^2 + 1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$.

j) $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

k) $0 \cdot 0! + 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$.

l) $1^3 + 2^3 + 3^3 + \cdot + n^3 = (1 + 2 + \cdot + n)^2$.

m) Tous les nombres dans cet exercice sont des entiers naturels. Montrer que si $k \geq 1$, et si $a_1, \ldots, a_k, n$ sont des nombres tels que $n \leq a_1 + \cdots + a_k$, alors il existe $b_1, c_1, \ldots, b_k, c_k$ tels que $n = b_1 + \cdots + b_k$, et que pour tout $i = 1, \ldots, k$, $a_i = b_i + c_i$.

7 Les entiers relatifs

7.1 Division euclidienne

Commençons par un exemple. Nous voulons diviser 95 par 7 ; ça ne tombe pas juste, comme on dit, mais 91 est divisible par 7, avec quotient 13, et $95 - 7 \cdot 91 = 4$. On peut écrire $95 = 7 \cdot 13 + 4$. On dit que le quotient de la division euclidienne de 95 par 7 est 13, et le reste 4.

Theorem 7.1. *Soient a, b des entiers naturels avec $b \geq 1$. Il existe des entiers q, r tels que*

$$a = bq + r, \tag{2}$$

avec $0 \leq r < b$. Les nombres q, r sont déterminés uniquement par ces conditions. On dit que q est le quotient *de la division euclidienne de a par b, et que r est le reste de cette division.*

Démonstration. C'est un énoncé du type "existence" (q, r existent) et "unicité". Les deux choses se font séparément ; commençons par l'existence.
Existence. Nous démontrons l'existence de q et r par récurrence sur a (b étant fixé).

Étape initiale : Si $a = 0$, nous pouvons prendre $q = r = 0$ et on a bien $0 \leq r < b$, puisque $b \geq 1$. Supposons maintenant prouvée l'existence de q et r pour a (hypothèse de récurrence), et prouvons l'existence d'un q' , r' tels que $a + 1 = bq' + r'$ avec $0 \leq r' < b$. Nous avons $a = bq + r$ avec $0 \leq r < b$. Par conséquent, $a + 1 = bq + r + 1$.

Dans le cas où $r + 1 < b$, nous avons $a + 1 = bq' + r'$ avec $0 \leq r' < b$ et $q' = q, r' = r+1$. Si l'on n'a pas $r+1 < b$, on doit avoir $r+1 \geq b$; mais comme $r < b$, la seule possibilité est $r+1 = b$, d'où $a+1 = bq+r+1 = bq+b = b(q+1)$. On a bien $a + 1 = bq' + r$ avec $r = 0 < b$ et $q' = q + 1$. Ceci achève la preuve de l'existence.
Unicité. Supposons que $a = bq_1 + r_1 = bq_2 + r_2$, avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$. Alors $-b < -r_2 \leq 0$, d'où par addition des inégalités : $-b < r_1 - r_2 < b$. Comme $b > 0$, on a : $|r_1 - r_2| < b$. Maintenant, nous avons aussi $b(q_1 - q_2) = r_2 - r_1$, d'où en valeurs absolues $|r_2 - r_1| = |b| \cdot |q_1 - q_2|$. Ce qui donne, puisque b est positif, $b > |r_2 - r_1| = b \cdot |q_1 - q_2|$, et donc que

$|q_1 - q_2| < 1$. Puisque $|q_1 - q_2| \in \mathbb{N}$, on a forcément $q_1 - q_2 = 0$. D'où $q_1 = q_2$ et par suite $r_1 = r_2$. □

Digression : les groupes commutatifs et leurs sous-groupes

Un *groupe commutatif* est un ensemble G avec une *opération*, c'est-à-dire une fonction $G \times G \to G$, qu'on note $(a, b) \mapsto a + b$; cette opération a les quatre propriétés suivantes :

- elle est *commutative* : $\forall a, b \in G, a + b = b + a$;
- elle est *associative* : $\forall a, b, c \in G, a + (b + c) = (a + b) + a$;
- elle a un *élément neutre* : $\exists 0 \in G, \forall a \in G, a + 0 = a$;
- tout élément a un *opposé* : $\forall a \in G, \exists b \in G, a + b = 0$. L'opposé de a est noté $-a$. Voir exercice 49 pour clarifier cette notation.

Un *sous-groupe* d'un groupe G est un sous-ensemble H de G qui contient 0, et tel que $\forall a, b \in H, a + b \in H$, et que $\forall a \in H$, $-a \in H$

L'ensemble $\mathbb{Z}$, avec son addition, est un groupe commutatif. L'ensemble des entiers pairs est un sous-groupe de $\mathbb{Z}$.

Theorem 7.2. *Pour tout sous-groupe H de $\mathbb{Z}$, il existe un entier naturel b tel que $H = \{bn \mid n \in \mathbb{Z}\}$.*

La notation pour le dernier ensemble est $b\mathbb{Z}$; c'est l'ensemble des entiers relatifs qui sont multiples de b.

Démonstration. Si $H = \{0\}$, nous prenons $b = 0$ et c'est gagné. Si $H \neq \{0\}$, H contient sûrement un entier > 0 : en effet, H contient un entier $n \neq 0$, et il contient aussi son opposé $-n$, étant un sous-groupe ; donc$n$ et $-n$ sont dans H, et l'un d'eux est > 0.

Considérons $H_+^* = \{n \in H \mid n > 0\}$. Cet ensemble est non vide, comme on vient de le voir, donc le théorème 6.2 nous assure qu'il a un minimum, que nous notons b. Nous montrons que $H = b\mathbb{Z}$. Pour ce faire, il faut montrer que $H \subset b\mathbb{Z}$ et $b\mathbb{Z} \subset H$. Pour montrer que $b\mathbb{Z} \subset H$, prenons $a \in b\mathbb{Z}$ quelconque et montrons que $a \in H$. Comme $a \in b\mathbb{Z}$, on a $a = bn$, $n \in \mathbb{Z}$. Supposons d'abord $n \geq 0$; alors $a = b + b + \cdots + b$ (n fois), donc $a \in H$, puisque H est un sous-groupe contenant b ; si $n < 0$, on a $a = -(b(-n))$ et $b(-n)$ est dans H d'après l'argument juste avant ; comme H est un sous-groupe, il contient aussi l'opposé de $b(-n)$, i.e. a, donc $a \in H$.

Montrons maintenant que $H \subset b\mathbb{Z}$. Soit donc $a \in H$ et supposons d'abord que $a > 0$. D'après le théorème 7.1, nous avons $a = bq + r, 0 \leq r < b$. Donc $r = a - bq$ est dans H, car a et bq le sont (nous avons vu ci-dessus que $bZ \subset H$), et que H est un sous-groupe. Si r était non nul, on aurait $r \in H^*, r < b$, ce qui est impossible, car b est le minimum de H^*. Donc on

doit avoir $r = 0, eta = bq \in b\mathbb{Z}$. Supposons maintenant que $a < 0$. Alors $-a > 0$ et $-a \in H$ puisque H est un sous-groupe. Donc, par ce que nous venons de voir, $-a \in b\mathbb{Z}$ et enfin $a \in bZ$. Ceci implique $H \subset b\mathbb{Z}$. □

Venons-en à la notion plus familière de plus grand diviseur commun ; par exemple, le plus grand diviseur commun de 12, 18 et 21 est 3.

Définition 7.3. *Soient $a_1, \ldots, a_k$ des entiers naturels non nuls ($k \geq 1$). Leur* plus grand diviseur commun *est le plus grand entier naturel qui les divise tous. La notation est $pgdc(a_1, \ldots, a_k)$.*

Dans la démonstration du théorème qui va suivre, la notion de sous-groupe de $\mathbb{Z}$, qui semble à priori étrangère à celle de diviseur, joue un rôle clarificateur.

Theorem 7.4. *Soit $a, b \in \mathbb{N}$ et n leur plus grand diviseur commun. Alors $n\mathbb{Z} = \{ap + bq \mid p, q \in \mathbb{Z}\}$.*

Démonstration. Comme toujours, il va falloir montrer deux inclusions. Commençons par la plus facile. Si $x = ap + bq, p, q \in \mathbb{Z}, x$ est un multiple de n, car a et b le sont ; donc $x \in n\mathbb{Z}$.

Nous montrons maintenant l'inclusion inverse $n\mathbb{Z} \subset H$, où $H = \{ap+bq \mid p, q \in Z\}$. Pour ceci, nous montrerons d'abord que H est un sous-groupe de $\mathbb{Z}$, puis en déduirons $n\mathbb{Z} \subset H\}$ en utilisant le théorème 7.2. Vérifions que H est un sous-groupe de $\mathbb{Z}$: en effet, $0 = a \cdot 0 + b \cdot 0 \in H$, et si $ap+bq, ap'+bq' \in H$, on a $(ap+bq)+(ap'+bq') = a(p+p')+b(q+q') \in H$; enfin, $-(ap + bq) = (-a)p + (-b)q \in H$. Donc H est un sous-groupe de $\mathbb{Z}$, d'après la définition d'un sous-groupe. Maintenant, le théorème 7.2 nous assure que $H = m\mathbb{Z}$, où $m \in \mathbb{N}^*$. Comme $a = a \cdot 1 + b \cdot 0 \in H$, et de même $b \in H$, on a que m divise a et b. De plus, m est dans H, et $H \subset n\mathbb{Z}$ comme nous l'avons vu au début de la preuve. Donc $m \in nZ$ et nous pouvons écrire $m = nr, r \in \mathbb{N}^*$. Mais m divise a et b, et n est le plus grand diviseur commun de a et b ; la seule possibilité est donc que $r = 1$ (sinon $m > n$) et $m = n$, d'où finalement $H = n\mathbb{Z}$. □

Le théorème nous montre que le pgdc est aussi le plus grand pour l'ordre de la division (voir l'exercice 27). Ceci est exprimé dans le corollaire qui suit.

Corollaire 7.5. *Soient $a, b, m \in \mathbb{N}^*$. Alors m divise a et b si et seulement si m divise le pgdc de a et b.*

Démonstration. Soit n le pgdc de a et b. D'après le théorème 7.4, nous avons $n = ap + bq$. Si donc m divise a et b, il divise aussi n. La réciproque est facile. □

Définition 7.6. *Deux entiers naturel non nuls sont dits* premiers entre eux *si leur pgdc est 1.*

Par exemple 4 et 15 sont premiers entre eux.

Theorem 7.7. *(théorème dit de Bézout) Deux entiers naturels non nuls a et b sont premiers entre eux si et seulement s'il existe p, q dans $\mathbb{Z}$ tels que $ap + bq = 1$.*

Par exemple : $4 \cdot 4 + 15 \cdot (-1) = 1$.

Démonstration. Si a et b sont premiers entre eux, le théorème 4.4 implique que $1 = ap + bq$. Réciproquement, si $1 = ap + bq$, tout $d \in N^*$ qui divise a et b, doit diviser 1 ; donc $pgcd(a, b) = 1$. □

L'*algorithme d'Euclide* décrit plus loin permet de calculer le pgdc de deux entiers naturels a, b non nuls. Il permet aussi de trouver i, j dans $\mathbb{Z}$ tels que $ai + bj = pgdc(a, b)$, dont l'existence nous est assuré par le théorème 7.4.

On procède comme suit : on fait la division euclidienne : $a = bq + r, 0 \leq r < b$. Si $r = 0$, on a $pgcd(a, b) = b$. Si $r \neq 0$, on a $pgdc(a, b) = pgdc(a - bq, b) = pgdc(b, r)$ (vérifier), et l'on est ramené à calculer $pgcd(b, r)$; on continue alors comme ci-dessus, avec (b, r) au lieu de (a, b). On s'arrête quand on obtient un reste nul. Le pgdc est alors l'avant-dernier reste. Comme $b + r < a + b$, on est sûr que l'algorithme va s'arrêter.

La division euclidienne et l'algorithme d'Euclide ont une interprétation matricielle. Définissons

$$P(q) = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}.$$

L'équation (2) s'écrit de manière équivalente

$$\begin{pmatrix} a \\ b \end{pmatrix} = P(q) \begin{pmatrix} b \\ r \end{pmatrix}$$

Exprimons par $q_1, \ldots, q_k$ les quotients successifs dans l'algorithme d'Euclide appliqué au couple (a, b)(il y a donc k divisions euclidiennes successives) et par $r_1, \ldots, r_k$ les reste successifs, avec $r_k = 0$ puisque c'est le dernier reste, $r_{k-1} = pgdc(a, b)$, et en posant encore $r_0 = b$. On a alors

$$\begin{pmatrix} a \\ b \end{pmatrix} = P(q_1) \cdots P(q_k) \begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix}.$$

Lorsqu'on effectue le produit des matrices, cette dernière égalité permet d'écrire a, b comme multiple de leur pgdc. Maintenant, la matrice $P(q)$ est inversible, d'inverse

$$P(q)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}.$$

Comme l'inverse d'un produit de matrice est égal au produit de leurs inverses, mais dans l'autre sens, on obtient

$$\begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix} = P(q_k)^{-1} \cdots P(q_1)^{-1} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Notons

$$\begin{pmatrix} i & j \\ \ell & m \end{pmatrix}$$

le produit de matrices dans l'équation précédente. On a alors

$$\begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix} = \begin{pmatrix} i & j \\ \ell & m \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On en déduit que

$$pgdc(a, b) = r_{k-1} = ia + jb.$$

En particulier, si a, b sont premiers entre eux, on trouve l'équation

$$ia + jb = 1. \tag{3}$$

Exemple 7.8. *On a : $a = 1255, b = 343$: $1255 = 343 \cdot 3 + 226$; $343 = 226 \cdot 1 + 117$; $226 = 117 \cdot 1 + 109$; $117 = 109 \cdot 1 + 8$; $109 = 8 \cdot 13 + 5$; $8 = 5 \cdot 1 + 3$; $5 = 3 \cdot 1 + 2$; $3 = 2 \cdot 1 + 1$; $2 = 1 \cdot 2 + 0$. Le dernier reste est nul, on s'arrête là, et le pgcd de 1255 et 343 est 1, l'avant-dernier reste.*

Exercice 49. *Montrer que dans un groupe commutatif G, on $-(-a) = a, -(a + b) = (-a) + (-b)$. On définit la* soustraction *dans G par : $a - b = a + (-b)$. Montrer que $-(a - b) = b - a$. Montrer que la soustraction n'est pas associative en général (prendre $G = \mathbb{Z}$).*

Exercice 50. *Montrer que si $a \in Z, b \in N^*$, il existe $q, r \in \mathbb{Z}$ tels que $a = bq + r, 0 \leq r < b$. Démontrer aussi l'unicité de q et r.*

Exercice 51. *Montrer que si $a, b \in \mathbb{N}^*$, on a : $b\mathbb{Z} \subset a\mathbb{Z}$ si et seulement si a divise b.*

Exercice 52. *Montrer que si $n, m \in \mathbb{N}^*$ et $n\mathbb{Z} = m\mathbb{Z}$, alors $n = m$.*

Exercice 53. ** Pour $a_1, \ldots, a_k$ dans $\mathbb{Z}$, on définit leur pgdc par : $pgdc(a_1, \ldots, a_k) = 0$ si les a_i sont tous nuls ; et si l'un d'eux au moins est non nul, $pgdc(a_1, \ldots, a_k)$ est le plus grand entier naturel non nul qui les divise tous.*

a) Démontrer que $pgdc(a_1, \ldots, a_k)\mathbb{Z} = \{a_1p_1 + \cdots + a_kp_k \forall i, p_i \in Z\}$ (imiter la preuve du théorème 7.4).

b) Démontrer qu'il existe $p_1, \ldots, p_k$ dans $\mathbb{Z}$ tels que $a_1p_1 + \cdots + a_kp_k = b$ si et seulement si $pgdc(a_1, \ldots, a_k)$ divise b.

c) Démontrer que m divise $a_1, \ldots, a_k$ si et seulement s'il divise leur pgdc.

d) Montrer que les a_i sont premiers entre eux (i.e. leur pgdc est 1) si et seulement s'il existe $p_1, \ldots, p_k$ dans $\mathbb{Z}$ tels que $1 = a_1p_1 + \cdots + a_kp_k$.

e) Montrer que $pgdc(a_1, \ldots, a_k) = pgdc(pgdc(a_1, \ldots, a_{k-1}), a_k)$.

f) En déduire un algorithme pour calculer $pgdc(a_1, \ldots, a_k)$.

g) Montrer que l'opération sur $\mathbb{Z}$: $(a, b) \mapsto pgdc(a, b)$ est commutative, associative, mais n'a pas d'élément neutre.

h) Montrer que pour $n \in \mathbb{Z}$, $pgdc(na, nb) = n \cdot pagdc(a, b)$.

Exercice 54. *Utiliser l'algorithme d'Euclide pour calculer le pgdc d de a et b, l'écrire comme $d = ap + bq$, et écrire $a = da, b = db$.*

a) a=233,b=144.

b) a=4181,b=2584.

c) a=2091,b=1479.

Exercice 55. *Montrer que si $a, b \in \mathbb{N}^*$, et $d = pgdc(a, b)$, alors $a = da', b = db', a', b' \in \mathbb{N}^*$ et $pgdc(a', b') = 1$.*

Exercice 56. ** Le* plus petit multiple commun *de deux entiers naturels non nuls a et b est le plus petit entier naturel non nul qui est un multiple à la fois de a et de b. La notation est $ppmc(a, b)$.*

a) Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = ppmc(a, b)\mathbb{Z}$.

b) Montrer que si a et b divisent m, alors $ppmc(a, b)$ divise m.

c) Montrer que $ppmc(a, b)$ divise ab.

Exercice 57. ** Soient $a, b, c \in \mathbb{Z}$. Montrer que l'équation $ax + by = c$ a une solution $(x, y) \in \mathbb{Z}^2$ si et seulement si le pgcd d de a et b divise c. Montrer qu'une solution est obtenue en trouvant x et y dans $\mathbb{Z}$ tels que $ax + by = d$, et montrer que l'équation (3) permet de résoudre cette équation. Indication : montrer que $\{ax + by \mid x, y \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.*

Exercice 58. ** Montrer que $pgdc(a,b) = pgdc(a-bq,b)$. Puis utiliser l'algorithme d'Euclide pour démontrer que si a et b sont premiers entre eux, il existe des entiers p,q tels que $ap+bq=1$ (la partie difficile du théorème de Bézout). Il s'agit donc ici de donner une autre preuve que celle dans les notes de cours.*

Exercice 59. *Montrer que si $pgdc(a,b) = 1$ et si c divise $a+b$, alors $pgdc(a,c) = 1 = pgdc(b,c)$.*

Exercice 60. *Montrer que k et $k+1$ sont toujours premiers entre eux.*

Exercice 61. *Montrer que k et $k+2$ ne sont pas toujours premiers entre eux. Donner la condition nécessaire et suffisante pour qu'ils le soient.*

Exercice 62. *Même question avec k et $k+6$.*

Exercice 63. *Montrer que k et $2k+1$ sont toujours premiers entre eux.*

Exercice 64. *Montrer que $3k+2$ et $5k+3$ sont toujours premiers entre eux.*

Exercice 65. ** Généraliser l'exercice précédent en remplaçant 2, 3 et 5 par d'autres entiers.*

Exercice 66. *Trouver le pgdc de 105 et 230 et son écriture sous la forme $230x + 105y$.*

Exercice 67. *Montrer que 512 et 243 sont premiers entre eux et trouver x, y tels que $512x + 243y = 1$.*

Exercice 68. *Trouvez avec l'algorithme d'Euclide le pgdc de : a) 267 et 112 ; b) 1500 et 11312. Dans les deux cas trouver x et y tels que $pgdc(a,b) = ax + by$.*

Exercice 69. *Soient a et b deux entiers premiers entre eux. Définissons la suite $x_n, n = 0, 1, 2, \ldots$, par $x_0 = a, x_1 = b$ et $\forall n \geq 2, x_n = x_{n-1} + x_{n-2}$. Prouvez que $\forall n, x_n$ et x_{n+1} sont premiers entre eux.*

Exercice 70. *(Vrai ou faux). Pour $a, b, c, d \in \mathbb{N}^*$, on a toujours : $pdgc(ac, bd) = pgdc(a,b)pgdc(c,d)$.*

Exercice 71. *a) Trouvez tous les sous-groupes de $\mathbb{Z}$ qui contiennent 12 et 21.*

b) Trouvez tous les sous-groupes de Z qui ne contiennent pas 24.

7.2 Une infinité de nombres premiers

Nous avons défini les nombres premiers dans la section 6. Les plus petits d'entre eux sont $2, 3, 5, 7, 11, 13, 17, \ldots$. Ceci suggère l'énoncé suivant.

Theorem 7.9. *(Euclide) Il y a une infinité de nombres premiers.*

Démonstration. On va faire ici un *raisonnement par l'absurde* : ceci consiste à supposer que la conclusion (qu'on veut démontrer) est fausse, et de là, par des arguments bien choisis, à montrer qu'on arrive à une contradiction ; on est en droit, alors, d'en déduire que la conclusion doit être vraie.

Supposons donc qu'il n'y a qu'un nombre fini de nombres premiers ; mettons qu'il y en ait k, et notons ces nombres premiers $p_1, p_2, p_3, \ldots, p_k$. On peut faire le produit $N = p_1 p_2 \cdots p_k$, et considérer $N + 1$. Ce nombre est ≥ 2, donc il admet un diviseur premier (d'après le théorème 6.3). Celui-ci se trouve parmi $p_1, \ldots, p_k$, puisque ce sont les seuls nombres premiers ; notons le p_i. Donc, p_i divise $N + 1$. Mais p_i divise aussi N. Donc p_i divise $1 = (N + 1) - N$, ce qui est absurde. De ceci, nous déduisons qu'il y a une infinité de nombres premiers. □

Une remarque très simple, mais qui sert beaucoup en théorie des nombres, est que tous les nombres premiers, sauf 2, sont impairs.

Exercice 72. *Trouver tous les couples (p_1, p_2) tels que p_1 et p_2 soient des nombres premiers et $p_1 - p_2 = 15$.*

Exercice 73. *Montrer qu'un nombre premier impair est toujours soit de la forme $4k + 1$, soit de la forme $4k + 3$, $k \in \mathbb{Z}$.*

Exercice 74. *La démonstration de la conjecture de Goldbach (1742) reste encore à trouver. Cette conjecture affirme que tout nombre pair ≥ 4 est somme de deux nombres premiers. Vérifiez-la pour $n = 80, 100, 240$.*

Exercice 75. ** Prouver qu'il y a une infinité de nombres premiers multiples de 4 moins 1, i.e. congrus à 3 modulo 4. Idée : Considérer $N = 4p_1 p_2 \ldots p_n - 1$, en imitant la preuve du théorème 7.9.*

7.3 Théorème fondamental de l'arithmétique

Nous allons maintenant examiner la factorisation des nombres en nombres premiers. Par exemple, $1400 = 2{\cdot}7{\cdot}2{\cdot}5{\cdot}2{\cdot}5 = 2{\cdot}2{\cdot}5{\cdot}7{\cdot}2{\cdot}5 = 2^3{\cdot}5^2{\cdot}7$; comme cet exemple le suggère, on ne distingue pas entre ces diverses factorisations.

Définition 7.10. *Soit $n \in \mathbb{N}^*$. Une* factorisation en nombre premiers *de n est une écriture de n sous la forme d'un produit $n = p_1 p_2 \cdots p_\ell$, où les p_i sont des nombres premiers.*

Par convention, une telle factorisation inclut la *factorisation vide*, c'est-à-dire le cas où $\ell = 0$, et correspond à $n = 1$. Elle inclut aussi le cas où $\ell = 1$, c'est-à-dire $n = p_1$. Deux factorisations sont considérées comme égales si elles ne diffèrent que par l'ordre des facteurs. Ceci étant convenu, on peut énoncer le théorème appelé *théorème fondamental de l'arithmétique*.

Theorem 7.11. *Tout entier naturel non nul admet une unique factorisation en nombres premiers.*

Nous aurons besoin d'abord de deux résultats préliminaires. Le premier est connu sous le nom de *lemme de Gauss*.

Lemma 7.12. *Soient a, b, c des entiers naturels non nuls. Si a est premier avec b et divise bc, il divise c.*

Démonstration. D'après le théorème de Bézout (théorème 7.7), il existe des entiers p, q tels que $1 = ap + bq$. Par hypothèse, il existe un entier d tel que $ad = bc$. On a alors $c = apc + bqc = apc + adq = a(pc + dq)$. Donc a divise c. □

Lemma 7.13. *(i) Si p, q sont des nombres premiers et si l'un divise l'autre, alors $p = q$.*

(ii) Si p, q sont des nombres premiers distincts, alors ils sont premiers entre eux.

Démonstration. (i) On peut supposer que $p \mid q$. Comme q premier, et que $p \neq 1$, on a $p = q$.

(ii) Prouvons l'assertion contraposée. Si p, q ne sont pas premiers entre eux, ils ont un diviseur commun $d \geq 1$. Alors, d divise p, et comme p est premier, on a $d = p$; de même, $d = q$. Donc $p = q$. □

Lemma 7.14. *Soit $p, q_1, \ldots, q_\ell$ des nombres premiers ($\ell \geq 1$). Si p divise le produit $q_1 \cdots q_\ell$, il est égal à l'un des q_i.*

Démonstration. Nous prouvons ceci par récurrence sur ℓ. Si $\ell = 1$, p divise q_1, donc $p = q_1$, car p et q_1 sont des nombres premiers. Supposons l'assertion démontrée pour ℓ, et passons à $\ell + 1$: p divise $q_1 \cdots q_{\ell+1}$; si $p = q_{\ell+1}$, c'est fini ; sinon $p \neq q_{\ell+1}$ et ces deux nombres sont premiers entre eux, par le lemme 7.13 (ii) ; alors le lemme 7.12 montre que p divise $q_1 \ldots q_\ell$; l'hypothèse de récurrence implique que p est égal à l'un des q_i. □

Démonstration du théorème 7.11. Une fois de plus, ce théorème est un énoncé d'existence et d'unicité. Nous divisons donc la preuve en deux parties.

Existence de la factorisation : nous montrons par récurrence sur n, en partant de $n = 1$, que tout entier naturel non nul n admet une factorisation en nombres premiers. Si $n = 1$, il admet la factorisation vide. Supposons maintenant l'existence prouvée pour tous les entiers de 1 à n, et passons à $n+1$. Si $n+1$ est premier, il s'écrit comme une factorisation de longueur 1. Si $n+1$ n'est pas premier, nous avons $n+1 = ab$, avec a et b plus petits que $n+1$. Nous appliquons l'hypothèse de récurrence à a et à b : ils admettent une factorisation en nombres premiers. En mettant bout à bout ces deux factorisations, nous en obtenons une pour $n+1 = ab$. Ceci achève la preuve de l'existence.

Unicité de la factorisation : nous procédons aussi par récurrence sur $n \in \mathbb{N}^*$. Si $n = 1$, il n'y a que la factorisation vide qui donne 1. Supposons l'unicité prouvée pour les nombres de 1 à n, et prouvons-la pour $n+1$. Écrivons que $n+1$ a deux factorisations : $n+1 = p_1 \cdots p_k = q_1 \cdots q_\ell (*)$, où les p_i, q_j sont des nombres premiers et $k, \ell \geq 1$ (on ne peut avoir k ou $\ell = 0$, sinon $n+1 = 1$, donc $n = 0$, contrairement à l'hypothèse ≥ 1). Le lemme 7.14 montre que p_1 est égal à l'un des q_j ; nous pouvons alors, quitte à réordonner les q_j, supposer que $p_1 = q_1$. Nous avons alors $p_2 \cdots p_k = q_2 \cdots q_\ell (**)$, et l'hypothèse de récurrence, appliquée à ce dernier produit (qui est $< n+1$), implique que les deux factorisations $(**)$ sont égales. Il en est donc de même pour les deux factorisations $(*)$ de $n+1$. Ceci termine la preuve. □

Il est souvent commode, dans une factorisation en nombres premiers, de rassembler les nombres premiers égaux, quitte à mettre des exposants ; on peut alors mettre toute factorisation sous la forme $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, où les p_i sont des nombres premiers *distincts* et les n_i des entiers naturels (on admet aussi des exposants nuls).

Ceci étant convenu, l'unicité dans le théorème 7.11 s'exprime ainsi : si $p_1, \ldots, p_k$ sont des nombres premiers distincts, $n_1, \ldots, n_k, m_1, \ldots, m_k$ sont dans $\mathbb{N}$, et si $p_1^{n_1} \cdots p_k^{n_k} = p_1^{m_1} \cdots p_k^{m_k}$, alors $n_i = m_i$ pour chaque i dans $\{1, \ldots, k\}$.

Theorem 7.15. *Soient n, m des entiers naturels non nuls, admettant les factorisations en nombres premiers $n = p_1^{n_1} \cdots p_k^{n_k}, m = p_1^{m_1} \cdots p_k^{m_k}$, où les p_i sont des nombres premiers distincts et les exposants dans $\mathbb{N}$. Alors n divise m si et seulement si : $\forall i \in \{1, \ldots, k\}$, $n_i \leq m_i$.*

Démonstration. On a

$$m = p_1^{m_1} \cdots p_k^{m_k} = p_1^{m_1 - n_1} \cdots p_k^{m_k - n_k} p_1^{n_1} \cdots p_k^{n_k} = p_1^{m_1 - n_1} \cdots p_k^{m_k - n_k} n.$$

Donc, si les inégalités sont satisfaite, n divise m.

Réciproquement, si n divise m, on a $m = nr$, $r \in \mathbb{N}$. En multipliant les factorisations de n et r, nous obtenons celle de m, d'après l'unicité dans le théorème 7.11 ; donc tout nombre premier qui apparaît avec un exposant non nul dans celle de r apparaît aussi dans celle de m. Par suite, nous pouvons écrire $r = p_1^{r_1} \cdots p_k^{r_k}$ avec des exposants r_i dans $\mathbb{N}$. Alors

$$p_1^{m_1} \cdots p_k^{m_k} = m = nr = p_1^{n_1} \cdots p_k^{n_k} p_1^{r_1} \cdots p_k^{r_k} = p_1^{n_1+r_1} \cdots p_k^{n_k+r_k}.$$

L'unicité dans le théorème 7.11, comme énoncée ci-dessus, implique alors que $m_i = n_i + r_i$ pour tous les i. □

Corollaire 7.16. *(i) Soit $a = \frac{n}{m}$, $a, m, n \in \mathbb{N}$, $m \neq 0$. Si un nombre premier p divise n mais pas m, alors p divise a.*

(ii) Si p est premier, les coefficients binomiaux $\binom{p}{i}$ sont divisibles par p quand $i = 1, \ldots, p-1$.

Démonstration. (i) On décompose n, m en produits de nombre premiers $n = p_1^{n_1} \cdots p_k^{n_k}, m = p_1^{m_1} \cdots p_k^{m_k}$, avec $p = p_1$, p_i premiers distincts. Alors $n_1 \geq 1$ et $m_1 = 0$ par hypothèse. Donc $a = p_1^{n_1 - m_1} \cdots p_k^{n_k - m_k}$ est divisible par p_1.

(ii) On a $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}$. Le numérateur est divisible par p, mais pas le dénominateur, car il est un produit de nombres plus petits que p, donc de nombres premiers plus petits que p. Comme la fraction est un entier, (i) implique cet entier n'est pas divisible par p. □

Exercice 76. *On suppose que $n = p_1^{n_1} \cdots p_k^{n_k}$, où les p_i sont des nombres premiers distincts et les n_i dans $\mathbb{N}$. Montrer qu'un nombre premier p divise n si et seulement s'il est égal à l'un des p_i avec $n_i \geq 1$.*

Exercice 77. *Soient a et b des entiers dont la factorisation en nombres premiers est $a = p_1^{n_1} \cdots p_k^{n_k}$, $b = p_1^{m_1} \cdots p_k^{m_k}$ (p_i distincts, n_i, m_i dans $\mathbb{N}$). Montrer que $pgdc(a, b) = p_1^{r_1} \cdots p_k^{r_k}$, où $r_i = \min(n_i, m_i)$.*

Exercice 78. *Sous les mêmes hypothèses, montrer que $ppmc(a, b) = p_1^{s_1} \cdots p_k^{s_k}$, où $s_i = \max(n_i, m_i)$.*

Exercice 79. *Montrer que $pgdc(a, b)ppmc(a, b) = ab$.*

Exercice 80. *On suppose que $pgdc(a, b) = p$, p premier. Montrer que $pgdc(a^2, b^2) = p^2$.*

Exercice 81. *Montrer que tout nombre naturel non nul s'écrit de manière unique comme le produit d'un nombre impair par une puissance de 2.*

Exercice 82. *Montrer que si* $a = da', b = db', d = pgdc(a,b)$, *alors* $ppmc(a,b) = da'b'$. *En déduire une méthode utilisant l'algorithme d'Euclide pour calculer* $ppmc(a,b)$.

Exercice 83. *Soit* $D(n)$ *l'ensembles des diviseurs entiers naturels de* $n \in \mathbb{N}^*$. *On considère sur* $D(n)$ *la relation d'ordre de divisibilité (cf. exercice 27). Montrer que* $D(n)$ *a un minimum et un maximum. Montrer que l'ordre est total si et seulement si* n *est la puissance d'un nombre premier.*

Exercice 84. *Soit* $a = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$. *Prouver que le nombre de diviseurs de* a *est donné par l'expression* $(n_1+1)(n_2+1)\cdots(n_k+1)$.

Exercice 85. *Trouver la plus petite valeur entière de* $n \geq 0$ *telle que* $n^2 + n + 41$ *ne soit pas un nombre premier. Même question pour* $n^2 + 79n + 1601$.

Exercice 86. *Déterminer tout les entiers qui admettent exactement trois (respectivement quatre) diviseurs. Indication : utiliser l'exercice 84.*

Exercice 87. *Soit* p *un nombre premier. Caractériser tous les entiers qui admettent exactement* p *diviseurs. Utiliser l'exercice 84.*

Exercice 88. *(Vrai ou faux). Pour* $a, b \in N$ *et* $n \geq 1$, *on a :* $pgdc(a,b)^n = pgdc(a^n, b^n)$.

Exercice 89. *27. Montrer que si* n *est un entier naturel* ≥ 5, *non premier, alors* n *divise* $(n-1)!$.

Exercice 90. * *On suppose que* $pgdc(a,b) = 8$. *Montrer que* $pgdc(a^3, b^4) = 2^9$ *ou* 2^{12}.

Exercice 91. * *Combien y a-t-il de zéros consécutifs à la droite du nombre* $10000!$, *lorsqu'on l'écrit en base 10.*

Exercice 92. * *Soit* $P(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_k n^k$ *un polynôme en* n, *à coefficients* a_i *dans* $\mathbb{N}$, *de degré* $k \leq 1$ *(donc* $a_k \neq 0$*). Prouver que (*$\exists N$ *tel que* $\forall n \geq N, P(n)$ *est premier) est faux. En d'autres mots il est impossible que* $P(n)$ *soit toujours premier à partir d'un certain rang, ou encore* $P(n)$ *est un nombre* composé *(i.e. non premier) pour une infinité de valeurs de* n. *Indication : soit* $n_0 = P(2)$. *On a* $n_0 > 2$. *Vérifier que* n_0 *divise* $P(2+n_0), P(2+2n_0), P(2+3n_0), \ldots$.

Exercice 93. ** Trouver tous les entiers entre 1 et 100000000 qui admettent exactement 13 diviseurs.*

Exercice 94. *Trouvez* $pgdc(267, 112)$ *et* $pgdc(1500, 11312)$ *en écrivant ces nombres comme produits de nombres premiers.*

Exercice 95. ** Soit* p *un nombre premier tel que* $2^p - 1$ *soit aussi premier. Trouver tous les diviseurs de* $n = 2^{p-1}(2^p - 1)$ *et vérifier que la somme des diviseurs de* n *est* $2n$*. (Un nombre satisfaisant cette dernière propriété est appelé un nombre* parfait*. Euler a démontré que tout nombre parfait pair est de cette forme mais personne ne sait s'il existe un nombre parfait impair).*

Exercice 96. ** a) Montrer que si* d *divise* n*, alors* n/d *divise aussi* n*.*

b) Prouver que n *admet un nombre impair de diviseurs si et seulement si* n *est un carré parfait.*

c) Prouver que n *est parfait (i.e. la somme de ses diviseurs est* $2n$*) si et seulement si la somme des inverses des diviseurs de* n *est 2.*

7.4 Calcul modulo un entier

Définition 7.17. *Soit* n *un entier naturel non nul. Deux entiers relatifs* a *et* b *sont* congrus modulo n *si* n *divise* $a - b$*. Notation :* $a \equiv b \mod n$.

Ceci signifie donc que $a - b = kn$, pour un entier relatif k, ou encore $a = b + kn$. Par exemple, $8 \equiv 29 \mod 7$, car 7 divise $8 - 29 = -21 = (-3) \cdot 7$, ou encore $8 = 29 + (-3) \cdot 7$.

Theorem 7.18. *Soit* $n \in \mathbb{N}^*$*. La relation sur* $\mathbb{Z}$*, qui relie* a *et* b *si* $a \equiv b \mod n$*, est une relation d'équivalence.*

On appelle cette relation d'équivalence la *congruence modulo* n.

Démonstration. On a : n divise $0 = a - a$, donc $a \equiv a \mod n$, et la relation est réflexive. Si $a \equiv b \mod n$, alors $a - b = kn$,donc $b - a = (-k)n$ et $b \equiv a \mod n$. Si $a \equiv b \mod n$ et $b \equiv c \mod n$,alors $a - b = kn$ et $b - c = \ell n$, où $k, \ell \in \mathbb{Z}$; d'où $a - c = (k + \ell)n$ et $a \equiv c \mod n$. La congruence modulo n est donc une relation réflexive, symétrique et transitive : c'est une relation d'équivalence. □

Nous allons maintenant déterminer les classes d'équivalence de la congruence modulo n. Commençons par un exemple.

Exemple 7.19. *Prenons $n = 3$ et déterminons la classe $[0]$ de 0. Par définition, $[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \mod 3\} = \{a \in \mathbb{Z} \mid 3 \text{ divise } a\} = 3\mathbb{Z}$. Ainsi la classe de 0 consiste en tous les multiples de 3. De manière analogue, la classe de 1 est l'ensemble $3\mathbb{Z}+1$ des nombres égaux à $1+$ un multiple de 3, et la classe de 2 est $3\mathbb{Z}+2$. Il n'y a pas d'autre classe, car tout entier est soit dans $3\mathbb{Z}$, soit dans $3Z+1$, soit dans $3\mathbb{Z}+2$. Il y a donc 3 classes de congruence modulo 3.*

Theorem 7.20. *Soit $n \in \mathbb{N}^*$. Pour tout a dans $\mathbb{Z}$, il existe un unique r dans $\{0, 1, \ldots, n-1\}$ tel que $a \equiv r \mod n$.*

La preuve va montrer que si $a \in N$, alors r est le reste de la division euclidienne de a par n.

Démonstration. Montrons d'abord l'existence de r. Si $a \geq 0$, par division euclidienne nous avons $a = nq + r$, où $q, r \in \mathbb{Z}, 0 \leq r \leq n-1$. Par suite $a \equiv r \mod n$. Si par contre $a < 0$, il existe $q, r \in \mathbb{Z}$ tels que $0 \leq r \leq n-1$ et $-a = nq + r$. Alors $a = n(-q') - r'$; si $r' = 0$, nousavons $a \equiv 0 \mod n$ et on prend $r = 0$. Si $r' > 0$, on a $0 < r' < n$ et donc $0 < n - r' < n$, et $a = n(-q'-1)+(n-r')$, d'où enfin $a \equiv n-r' \mod n$ et on prend $r = n-r'$.

2. Montrons maintenant l'unicité de r. Si $a \equiv r \mod n$ et $a \equiv r_1 \mod n$ avec r, r_1 dans $\{0, 1, \ldots, n-1$, alors $r \equiv r_1 \mod n$ (car la congruence modulo n est une relation d'équivalence), et donc n divise $r - r_1$; mais $|r - r_1|$ est plus petit que n, et doit donc être nul et $r = r_1$. □

Corollaire 7.21. *La congruence modulo n a n classes d'équivalence. Chacune d'elles est de la forme $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$, pour un unique r tel que $0 \leq r \leq n-1$.*

Démonstration. Chaque classe est de la forme $[a]$, pour $a \in \mathbb{Z}$. Mais le théorème 7.20 nous assure que $a \equiv r \mod n$, $0 \leq r \leq n-1$. Alors $[a] = [r]$ (lemme 5.10). Maintenant, $[r] = \{r+nk \mid k \in \mathbb{Z}\} = r+n\mathbb{Z}$. Donc toute classe est de la forme indiquée. Ces classes sont distinctes, d'après le théorème (appliqué à $a = r$), donc il y a exactement n classes. D'où aussi l'unicité dans l'énoncé. □

On peut calculer avec les congruences, comme l'indique le théorème qui suit. Par exemple, $3 \equiv -4 \mod 7$ et $12 \equiv -2 \mod 7$; on a alors $3 \cdot 12 \equiv (-4) \cdot (-2) \mod 7$, puisque $36 - 8 = 28 = 4 \cdot 7$.

Theorem 7.22. *Soient $n \in \mathbb{N}^*$ et $a, b, a', b' \in \mathbb{Z}$. Si $a \equiv b \mod n$ et $a' \equiv b' \mod n$, alors $a + a' \equiv b + b' \mod n$ et $aa' \equiv bb' \mod n$. De plus, pour tout entier $k \geq 1$, $a^k \equiv b^k$.*

Démonstration. Par hypothèse, $a = b + kn$ et $a' = b' + k'n$, $k, k' \in \mathbb{Z}$. Donc on a $a + a' = b + b' + (k + k')n$ et $a + a' = b + b' \mod n$. De plus, $aa' = (b+kn)(b'+k'n) = bb' + (kb' + bk' + kk'n)n$ et donc $aa' \equiv bb' \mod n$. La dernière assertion s'obtient par une récurrence standard, en appliquant le résultat sur le produit des congruences. □

Une application de ce résultat est que si l'on additionne et multiplie modulo n, on peut remplacer chaque nombre par un nombre congru modulo n ; on a intérêt à choisir ce dernier le plus petit possible. Ainsi, modulo 7, on peut remplacer 7 par 0, 8 par 1, 159 par 5 etc. Si l'on n'a pas peur des signes, on peut même remplacer 6 par -1, 5 par -2.

Exemple : Dans un million (respectivement un milliard) de jours, quel jour de la semaine serons-nous ? Réponse : travaillons modulo 7 : $10 \equiv 3, 10^3 \equiv 3^3 = 27 \equiv -1, 10^6 = ((10)^3)^2 \equiv (-1)^2 = 1$; $10^9 = 10^6 \cdot 10^3 \equiv 1 \cdot (-1) \equiv -1 \mod 7$. Un million : "demain " ; un milliard : "hier".

Une autre application est de munir l'ensemble des n classes modulo n d'une addition. Nous notons l'ensemble quotient de $\mathbb{Z}$ par la congruence modulo n comme suit :

$$\mathbb{Z}/(\equiv \mod n) = \mathbb{Z}/n\mathbb{Z}.$$

L'addition de deux classes est définie par

$$[a] + [b] = [a + b].$$

Pour que cette définition de l'addition de deux classes soit correcte, il faut vérifier que le côté droit $[a + b]$ ne dépend pas des représentants a et b, mais seulement de leurs classes. C'est-à-dire : $[a] = [a']$ et $[b] = [b']$, alors $[a+a'] = [b+b']$. Mais ceci découle précisément du lemme 5.10 et du théorème 7.22.

Nous laissons au lecteur le soin de vérifier que $\mathbb{Z}/n\mathbb{Z}$, avec cette addition est un groupe commutatif, comme on l'a défini dans la section 7.1.

De manière analogue, on définit le produit de deux classes modulo n par la formule

$$[a][b] = [ab].$$

Cette définition est correcte, ce qu'on vérifie comme pour l'addition.

Définition 7.23. *Soit $n \in \mathbb{N}^*$ et $[a]$ un élément de $\mathbb{Z}/n\mathbb{Z}$. On dit qu'un élément $[a]$ est* inversible *s'il existe un élément $[b]$ tel que*

$$[a][b] = [1].$$

Dans ce cas $[b]$ s'appelle l'inverse de $[b]$.

Cette égalité est équivalente à $ab \equiv 1 \mod n$, ce qui équivaut à : $\exists k \in \mathbb{Z}$ tel que

$$ab + kn = 1. \tag{4}$$

On en déduit le

Theorem 7.24. *Dans $\mathbb{Z}/n\mathbb{Z}$ un élément est inversible si et seulement si a est premier avec n. Dans ce cas, son inverse est $[b]$, où b s'obtient par l'équation de Bézout (4).*

Theorem 7.25. *(théorème des restes chinois) Soient n, m, k, ℓ des entiers avec $n, m \geq 1$ et $pgdc(n, m) = 1$. Il existe dans $\{0, 1, \ldots, nm-1\}$ un unique entier x tel que $x \equiv k \mod n$ et $x \equiv \ell \mod m$.*

Démonstration. Soient p, q tels que $pn + qm = 1$. Donc $qm \equiv 1 \mod n$ et $pn \equiv 1 \mod m$. Posons $x = pn\ell + qmk$. Alors $x \equiv qmk \equiv k \mod n$; de même, $x \equiv \ell \mod m$. L'existence de x est donc prouvée.

L'unicité se prouve ainsi : si x, x' sont deux solutions, alors $x - x'$ est divisible à la fois par m et n, donc par mn, puisque m et n sont premiers entre eux. Comme $0 \leq x - x' < nm$, il faut que $x - x' = 0$. □

Theorem 7.26. *(petit théorème de Fermat) Soit p un nombre premier. Pour tout entier a, $a^p \equiv a \mod p$.*

Démonstration. C'est vrai pour $a = 0$, Supposons le résultat vrai pour a. On a $(a+1)^p = \sum_{0 \leq i \leq p} \binom{p}{i} a^i$. D'après le corollaire 7.16, on a, modulo p : $(a+1)^p \equiv \binom{p}{p} a^p + \binom{p}{0} = a^p + 1$. Par hypothèse de récurrence, on a donc $(a+1)^p \equiv a + 1 \mod p$. □

Nous allons résoudre maintenant des équations linéaires dans $\mathbb{Z}/n\mathbb{Z}$. Prenons comme exemple la congruence : (a) $2x \equiv 3 \mod 7$. Elle peut s'écrire : (b) $[2][x] = [3]$ dans $\mathbb{Z}/7\mathbb{Z}$. Trouver un x dans $\mathbb{Z}$ qui satisfait (a) revient à trouver $[x]$ dans $\mathbb{Z}/7\mathbb{Z}$ qui satisfait (b). Par exemple, $x = 5$ est solution de (a), et $[x] = [5]$ est solution de (b). Et même, toutes les solutions de (a) sont des éléments de $5 + 7\mathbb{Z}$. Il y a donc une infinité de solutions à (a), alors qu'il n'y en a qu'un nombre fini à (b).

Définition 7.27. *La congruence $ax \equiv b \mod n$ a k solutions si l'équation $[a][x] = [b]$ dans $\mathbb{Z}/n\mathbb{Z}$ a exactement k solutions distinctes.*

Dire que $ax \equiv b \mod n$ a k solutions revient donc à dire qu'il y a k entiers solutions de cette congruence, qui sont deux à deux non congrus modulo n, et que k est maximum. Par exemple, la congruence $2x \equiv 4 \mod 6$ a les deux solutions $x = 2$ et $x = 5$, qui sont non congrus modulo 6.

Theorem 7.28. *L'équation $ax \equiv b \mod n$ a une solution dans $\mathbb{Z}$ si et seulement si le pgdc d de a et n divise b. Dans ce cas, il y a d solutions.*

Démonstration. 1. S'il y a une solution, il existe y dans $\mathbb{Z}$ tel que $ax = b+ny$. Donc $b = ax - ny$ appartient, d'après le théorème 7.4, à $d\mathbb{Z}$. Donc d divise b. Réciproquement, si d divise b, alors $b \in d\mathbb{Z}$, donc $ax+ny = b, y \in \mathbb{Z}$, d'après le même théorème. Donc $ax \equiv b \mod n$.

2. Supposons que d divise b, et montrons qu'il y a d solutions. Posons $a = da'$ et $n = dn'$. Si x est solution, alors $x, x+n', x+2n', \ldots, x+(d-1)n'$ sont d solutions deux à deux non congrus modulo n. En effet $a(x+in') = ax+ain' = ax+da'in' = ax+a'in \equiv b \mod n$ (puisque $ax \equiv b$) ; de plus, n ne se divise pas $(x+jn')-(x+in')$ si $0 \leq i < j \leq d-1$, car $0 < (j-i)n' < n$.

Nous montrons qu'il n'y en a pas d'autre : c'est-à-dire que si $ax' \equiv b \mod n$, alors x' est congru modulo n à l'une des d solutions ci-dessus. Nous avons $ax \equiv b$ et $ax' \equiv b$, donc $a(x'-x) \equiv 0 \mod n$. Donc $a(x'-x) = nr$, ce qui implique $a'(x'-x) = n'r$ n' divise $a'(x'-x)$. Comme n' et a' sont premiers entre eux (puisque $pgdc(a,n) = d$), n' divise $x'-x$: $x'-x = kn'$. Écrivons $k = i+d\ell$, $0 \leq i \leq d-1$ (division euclidienne). Alors $x' = x+kn' = x+in'+n'd\ell = x+in'+n\ell$, ce qui montre que x' est congru, modulo n, à l'une des d solutions énumérées ci-dessus, et achève la preuve. □

La preuve du théorème 7.28 montre qu'on peut effectivement trouver toutes les solutions de l'équation $ax \equiv b \mod n$. Oncalcule $d = pgdc(a,n)$ par l'algorithme d'Euclide. On teste si d divise b ; si oui, on cherche p, q dans $\mathbb{Z}$ tels que $d = ap+nq$ (voir la section 7.1). Donc $bdb' = apb'+nqb'$, et $x = pb'$ est une solution. Les d solutions cherchées sont alors $x, x+n', \ldots, x+(d-1)n'$, où ndn'.

Exercice 97. *Montrer que pour a dans $\mathbb{Z}$, la classe de a modulo a est $a+n\mathbb{Z}$. Montrer que $a+n\mathbb{Z}$ rencontre $b+n\mathbb{Z}$ si et seulement si $a \equiv b \mod n$.*

Exercice 98. *Résoudre les équations suivantes (i.e. dire s'il y a une solution, et en trouver une si oui). a)* $12x \equiv 7 \mod 21$ *; b)* $12x \equiv 7 \mod 73$ *; c)* $12x \equiv 7 \mod 35$ *; d)* $12x \equiv 33 \mod 57$. *e)* $12x \equiv 7 \mod 84$ *; f)* $12x \equiv 7 \mod 46$ *; g)* $18x \equiv 1 \mod 25$. *Indication : utiliser l'exercice 57.*

Exercice 99. *Quel est l'ensemble de toutes les solutions x de la congruence $ax \equiv 0 \mod n$? Indication : considérer d'abord le cas où a et n sont premiers entre eux. Puis, dans le cas général, diviser par le pgdc de a et n.*

Exercice 100. *On suppose que $x_0 \in \mathbb{Z}$ est une solution de $ax \equiv b \mod n$. Quel est l'ensemble de toutes les solutions de cette équation ?*

Exercice 101. ** Résoudre les systèmes de congruences suivants (voir théorème 7.25) :*

a) $2x \equiv 3 \mod 5$ *et* $3x \equiv 1 \mod 4$.

b) $x \equiv 4 \mod 6$ *et* $3x \equiv 3 \mod 10$ *;*

c) $5x \equiv 1 \mod 7$ *et* $3x \equiv 1 \mod 5$.

d) $x \equiv 1 \mod 2$ *et* $x \equiv 2 \mod 3$ *et* $x \equiv 3 \mod 4$.

Exercice 102. *Vérifier pour* $p = 2, 3, 5, 7$ *et* 11 *que* $\Pi_{i=1}^{i=p} i \equiv -1 \mod p$ *(le symbole* Π *est au produit ce que le symbole* Σ *est à l'addition).*

Exercice 103. *Vérifier pour* $p = 11$ *que pour tout* a*, on a* $a^{11} \equiv a \mod 11$ *(pour ce calcul, appliquer le principe exposé après la preuve du th. 7.6).*

Exercice 104. *Trouver tous les* $a \in \{0, 1, \ldots, 10\}$ *qui sont un carré modulo 11, i.e. ceux pour lesquels il existe un* x *tel que* $\{a = x^2 \mod 11\}$.

Exercice 105. *Dresser les tables d'addition et de multiplication de* $\mathbb{Z}/11\mathbb{Z}$.

Exercice 106. *Trouver l'inverse de* 342 *dans* $\mathbb{Z}/997\mathbb{Z}$.

Exercice 107. *Quel jour de la semaine serons-nous dans* $6^{123456789}$ *jours, si nous sommes lundi aujourd'hui ?*

Exercice 108. *Quel jour de la semaine serons-nous dans* $10^{1000000000}$ *jours si nous sommes aujourd'hui lundi ?*

Exercice 109. *Quel est le chiffre des unités de* 12354^{12354} *?*

Exercice 110. *Si je regroupe par paquets de 11 mes moutons, il en reste 5 mais si je les regroupe par paquets de 13 il en reste 2. Combien ai-je de moutons, sachant que j'en ai moins de 100 ?*

Exercice 111. *Trouver tous les* $x \in \mathbb{Z}$ *tels que* $28x \equiv 12 \mod 77$. *Même question pour* $28x \equiv 12 \mod 80$.

Exercice 112. *Qui suis-je ? Si on me divise par 2 le reste est 1, si on me divise par 3 mon reste est 2, si on me divise par 4 mon reste est 3, si on me divise par 5 mon reste est 4 et je suis plus petit que 60.*

Exercice 113. *Quel mois de l'année serons-nous dans* 10^{100} *mois après Noël de l'an 2000 ?*

Exercice 114. ** On dit que trois nombres premiers* p_1, p_2, p_3 *forment un triplet de nombres premiers si* $p_3 = p_2 + 2$ *et* $p_2 = p_1 + 2$*. Trouver tous les triplets de nombres premiers. Indication : calculer modulo 3.*

Noter que p_1 *et* p_2 *sont appelés des* nombres premiers jumeaux *si* $p_2 = p_1 + 2$ *; l'existence d'une infinité de nombres premiers jumeaux est une conjecture non-démontrée célèbre.*

Exercice supplémentaire Montrer que dans une année de 365 jours, il peut y avoir 1, 2 ou 3 vendredi 13. Indications : un mois comporte un vendredi 13 si et seulement si le 1er du mois est un lundi ; calculer quels sont les premiers jours des 12 mois de l'année, étant donné le jour du 1er janvier ; calculer modulo 7. Etendre le résultat aux années bissextiles.

7.5 Construction mathématique des nombres entiers relatifs

On définit l'ensemble $E = \mathbb{N} \times \mathbb{N}$ (intuition : un couple représente sa soustraction). On définit sur E une relation d'équivalence R par $(a,b)R(c,d)$ si et seulement si $a+d=b+c$ (égalité des somme croisées). C'est bien une relation d'équivalence. Elle est en effet réflexive, car $(a,b)R(a,b)$ puisque $a+b=b+a$. Elle est symétrique car $(a,b)R(c,d)$ implique $c+b=d+a$, donc $(c,d)R(a,b)$. Et pour la transitivité : si $(a,b)R(c,d)$ et $(c,d)R((e,f)$, alors $a+d=b+c, c+f=d+e$, donc $a+d+f=b+c+f=b+d+e$, donc en soustrayant d, on obtient $a+f=b+e$, d'où $(a,b)R(e,f)$.

On définit

$$\mathbb{Z} = E/R.$$

On définit d'abord l'addition et la multiplication dans E par $(a,b)+(a'+b') = (a+a', b+b')$ et $(a,b)\cdot(a',b') = (aa'+bb', ab'+a'b)$ (ensuite on, "transférera" ces opérations au quotient). Vérifions les propriétés suivantes de ces opérations :

- L'addition est commutative : $(a',b')+(a,b) = (a'+a, b'+b)$, ce qui est bien égal à $(a,b)+(a'+b')$.

- La multiplication est commutative : $(a',b')\cdot(a,b) = (a'a+b'b, a'b+b'a)$, bien égal à $(aa'+bb', ab'+a'b)$.

- L'addition est associative : $((a,b)+(a',b'))+(a'',b'') = (a,b)+((a',b')+(a'',b''))$, facile à vérifier.

- La multiplication est associative :

$$((a,b)\cdot(a',b'))\cdot(a'',b'') = (aa'+bb,' ab'+ba')\cdot(a'',b'')$$

$$= (aa'a''+bb'a''+ab'b''+ba'b'', aa'b''+bb'b''+ab'a''+ba'a'')$$

et

$$(a,b)\cdot((a',b')\cdot(a'',b'')) = (a,b)\cdot(a'a''+b'b'', a'b''+b'a'')$$

$$= (aa'a''+ab'b''+ba'b''+bb'a'', aa'b''+ab'a''+ba'a''+bb'b'').$$

- L'addition a un élément neutre, qui est $(0,0)$, facile à vérifier.

- La multiplication a un élément neutre, qui est $(1,0)$: $(a,b)\cdot(1,0) = (a\cdot 1+b\cdot 0, a\cdot 0+b\cdot 1) = (a,b)$.

- Tout élément (a, b) de E n'a pas un opposé, mais à l'équivalence R près, il en a un ; précisément : $(a, b) + (b, a) = (a + b, b + a)R(0, 0)$, car $a + b + 0 = b + a + 0$.

- La multiplication est distributive par rapport à l'addition : $(a, b) \cdot ((a', b') + (a'', b'')) = (a, b) \cdot (a' + a'', b' + b'') = (aa' + aa'' + bb' + bb'', ab' + ab'' + ba' + ba'')$ et $(a, b) \cdot (a', b') + (a, b) \cdot (a'', b'') = (aa' + bb', ab' + ba') + (aa'' + bb'', ab'' + ba'') = (aa' + bb' + aa'' + bb'', ab' + ba' + ab'' + ba'')$.

On définit maintenant l'addition et la multiplication sur le quotient $\mathbb{Z} = \mathbb{N}/R$ de la manière suivante (le transfert dont on parle ci-dessus) : on prend $x, y \in \mathbb{N}/R$, on choisit des représentants de ces classes : $(a, b) \in x, (a', b') \in x'$, c'est-à-dire $x = [(a, b)], x' = [(a', b')]$, et on définit

$$x + x' = [(a, b) + (a', b')], x \cdot x' = [(a, b) \cdot (a', b')].$$

Il faut voir que cette addition et cette multiplication sont bien définies, c'est-à-dire ne dépendent pas des représentants choisis. Pour l'addition, c'est plutôt facile : si $(a, b)R(c, d)$ et $(a', b')R(c', d')$, alors on doit montrer que $[(a, b) + (a', b')] = [(c, d) + (c', d')]$. C'est-à-dire $[(a + a', b + b')] = [(c + c', d + d')] \Leftrightarrow (a + a', b + b')R(c + c', d + d') \Leftrightarrow a + a' + d + d' = b + b' + c + c'$; cette égalité est vraie, car $a + d = b + c$ et $a' + d' = b' + c'$.

Pour voir que la multiplication est bien définie, on procède en deux étapes. Pour montrer que $[(a, b) \cdot (a', b')] = [(c, d) \cdot (c', d')]$, on montre que $[(a, b) \cdot (a', b')] = [(a, b) \cdot (c', d')]$ et que $[(a, b) \cdot (c', d')] = [(c, d) \cdot (c', d')]$. Pour la première égalité, il suffit de montrer que $(a, b) \cdot (a', b')R(a, b) \cdot (c', d')$. Mais on a par hypothèse $a' + d' = b' + c'$; multipliant cette égalité tour à tour par a et b, on obtient $aa' + ad' = ab' + ac'$ et (en échangeant gauche et droite dans l'égalité) $bb' + bc' = ba' + bd'$, et par addition de ces deux dernières égalités, $aa' + ad' + bb' + bc' = ab' + ac' + ba' + bd'$, donc $(aa' + bb', ab' + ba')R(ac' + bd', ad' + bc')$, donc $(a, b) \cdot (a', b')R(a, b) \cdot (c', d')$. L'autre égalité est analogue, et même, on peut la déduire de la première à cause de la commutativité de la multiplication.

La projection canonique $p\mathbb{N} \to \mathbb{N}/R$ définie, rappelons-le, par $p((a, b)) = [(a, b)]$ (la classe d'équivalence de a pour R) préserve l'addition et la multiplication :

$$p((a, b) + (a', b')) = p((a, b)) + p((a', b')), p((a, b) \cdot (a', b')) = p((a, b)) \cdot ((a', b')).$$

Autrement dit :

$$[(a, b) + (a', b')] = [(a, b)] + [(a', b')], [(a, b) \cdot (a', b')] = [(a, b)] \cdot [(a', b')].$$

Cela découle de notre définition de l'addition et de la multiplication.

On vérifie les propriétés usuelles de l'addition et de la multiplication dans $\mathbb{Z}$: commutativité, associativité, élément neutre, opposé, distributivité de la multiplication par rapport à l'addition. Elles se déduisent toutes (sauf pour l'opposé) des propriétés analogues de E, en utilisant la projection canonique $p : \mathbb{N} \to \mathbb{N}/R$. On a par exemple $\forall x, x' \in E/R$, $x \cdot x' = x' \cdot x$; en effet on peut choisir a, a', b, b' dans $\mathbb{N}$ avec $p((a,b)) = x, p((a',b')) = x'$. Alors $x \cdot x' = p((a,b)) \cdot p((a',b')) = p((a,b) \cdot (a',b')) = p((a',b') \cdot (a,b)) = p((a',b')) \cdot p((a,b)) = x' \cdot x$.

L'opposé de $[(a,b)]$ est $[(b,a)]$, car $[(a,b)] + [(b,a)] = [(a+b, a+b)] = [(0,0)]$.

On définit une injection de $\mathbb{N}$ dans $\mathbb{Z}$ par la composition de $\mathbb{N} \to E, n \mapsto (n,0)$ suivie de la projection canonique $E \to E/R$; cette injection préserve l'addition et la multiplication.

8 Les nombres rationnels et les nombres réels

8.1 Rationnels

Un *nombre rationnel* est une *fraction* $\frac{a}{b}$, où a, b sont des nombres entiers relatifs, avec b non nul. L'égalité de deux telles fractions est régie par l'équivalence :

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc,$$

c'est-à-dire l'égalité des *produits croisés*. Tout entier n est identifié à la fraction $\frac{n}{1}$.

Les nombres rationnels s'additionnent et se mutiplient par

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

L'*opposé* d'une fraction et son *inverse* sont donnés par

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

et dans ce dernier cas, on doit avoir $b \neq 0$.

Exercice 115. *Montrer que tout nombre rationnel strictement positif a une factorisation unique $p_1^{n_1} \cdots p_k^{n_k}$, où les p_i sont des nombres premiers distincts et où les exposants n_i sont dans $\mathbb{Z}$.*

Exercice 116. *Montrer que la factorisation en nombres premiers du carré d'un nombre rationnel satisfait à : pour tout i, n_i est pair (notations de l'exercice 115). En déduire que 2 est* irrationnel, *i.e. 2 n'est pas le carré d'un nombre rationnel.*

Exercice 117. ** Soit f la fonction $\mathbb{N}^* \to \mathbb{Q}^*$ définie comme suit : si $n = p_1^{n_1} \cdots p_k^{n_k}$, soit $m_i = n_i/2$ si n_i pair, et $m_i = -(n_i - 1)/2$ si n_i impair ; alors $f(n) = p_1^{m_1} \cdots p_k^{m_k}$. Montrer que f est une bijection. Déterminer $f^{-1}(\mathbb{N}^*)$.*

8.2 Construction mathématique des nombres rationnels

On considère l'ensemble $F = \mathbb{Z} \times \mathbb{Z}^*$ (intuition : F est l'ensemble des fractions, vues comme des couples (a, b), plutôt que $\frac{a}{b}$).

On définit une relation d'équivalence R sur F par : $(a, d)R(a, d)$ si et seulement si $ad = bc$. Alors on définit

$$\mathbb{Q} = E/R.$$

Autrement dit, une fraction est une classe d'équivalence pour R (intuition : un nombre rationnel est l'ensemble des fractions qui le représentent).

On définit l'addition et la multiplication avec les formules usuelles des fractions. On vérifie que cela donne des opérations bien définies sur le quotient E/R. On vérifie que les propriétés usuelles sont satisfaites : commutativité, associativité, élément neutre pour l'addition et la multiplication, opposé et inverse, distributivité de la multiplication par rapport à l'addition.

8.3 Réels

Construire mathématiquement les réels à partir des rationnels est une entreprise plutôt difficile, et il faut pour cela passer par l'analyse mathématique. Nous ne le ferons pas dans ce cours, mais nous énonçons ci-dessous les propriétés fondamentales de $\mathbb{R}$.

Les réels ont les propriétés suivantes :

- $\mathbb{R}$ est muni de l'ordre usuel, qui est un ordre total.

- $\mathbb{Q}$ est *dense* dans $\mathbb{R}$: ceci signifie que pour tous nombres réels a, b avec $a < b$, il existe un rationnel r entre les deux : $a < r < b$.

- Dans $\mathbb{R}$, toute *suite de Cauchy* converge. Une suite de Cauchy est une suite $a_n, n \in \mathbb{N}$ telle que ses éléments sont très proches les uns des autres, pourvu qu'on aille assez loin dans la suite. Précisément : $\forall \epsilon > 0$, $\exists N$ tel que $\forall n, p \geq N$, $|a_n - a_p| < \epsilon$.

On parle souvent de la *droite réelle* parce que $\mathbb{R}$ peut-être vu comme l'ensembles de tous les points d'une droite.

9 Les nombres complexes

Nous construisons ici l'ensemble $\mathbb{C}$ des nombres complexes, à partir de $\mathbb{R}$.

9.1 Introduction : les racines d'une équation du second degré

L'équation du second degré $ax^2 + bx + c = 0$ a pour racines

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Nous supposons ici que a, b, c sont des nombres réels, avec $a \neq 0$, et que $b^2 - 4ac \geq 0$, afin qu'on puisse prendre la racine carrée de Δ.

Que se passe-t-il lorsque $\Delta < 0$? Alors Δ n'a pas de racine carrée dans $\mathbb{R}$. On introduit alors les nombres complexes, dont l'ensemble est noté $\mathbb{C}$. Ils sont faits de telle façon que la racine d'un nombre réel négatif Δ existe : elle vaut $\pm i\sqrt{-\Delta}$, où i est un nombre complexe particulier dont le carré vaut -1. En effet, comme $i^2 = -1$, on a bien $(\pm i\sqrt{-\Delta})^2 = i^2(-\Delta) = \Delta$.

9.2 Construction des nombres complexes

Un nombre complexe est une expression de forme $z = a + bi$, où a, b sont des nombres réels, et i un symbole spécial. La *partie réelle* de z est a, et sa *partie imaginaire* est b (on dit aussi parfois que c'est bi). On les note $a = \Re(z), b = \Im(z)$. Si $z' = a' + b'i$ est un autre nombre complexe, on dira que $z = z'$ si et seulement si $a = a'$ et $b = b'$. Tout nombre réel a est identifié au nombre complexe $a + 0i$, qu'on écrit aussi a ; ainsi $\mathbb{R}$ est contenu dans $\mathbb{C}$, l'ensemble des nombres complexes.

On définit l'addition et la multiplication dans $\mathbb{C}$ par

$$(a+bi)+(a'+b'i) = (a+a')+(b+b')i, (a+bi)(a'+b'i) = (aa'-bb')+(ab'+ba')i.$$

C'est un exercice de routine, de vérifier que ces opérations sont commutatives, associatives, que la multiplication est distributive par rapport à l'addition, que $0 = 0 + 0i$ est élément neutre pour l'addition et que $1 = 1 + 0i$ est élément neutre pour la multiplication.

Ces opérations étendent celles de $\mathbb{R}$.

Par ailleurs, le nombre complexe $0+1i$ est noté simplement i. On a alors par définition de la multiplication

$$i^2 = (0+1i)(0+1i) = (0\cdot 0 - 1\cdot 1) + (0\cdot 1 + 1\cdot 0)i = (-1) + 0i = -1.$$

On définit le *conjugué* $\bar{z}$ de z par $\bar{z} = a - bi = a + (-b)i$. Alors

$$z\bar{z} = (a+bi)(a-bi) = (a^2+b^2) + 0i = a^2 + b^2$$

est un nombre réel. Le *module* de z est $\sqrt{a^2+b^2}$; on le note $|z|$. On a donc

$$|z|^2 = a^2 + b^2.$$

Si z est non nul, c'est-à-dire si a ou b n'est pas nul, alors z admet l'inverse pour la multiplication

$$z^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i = \frac{\bar{z}}{a^2+b^2}.$$

En effet $z\bar{z} = (a+bi)(a-bi) = a^2+b^2+(a(-b)+ba) = a^2+b^2$, donc $z\frac{\bar{z}}{a^2+b^2} = 1$.

Proposition 9.1. *Soient $z = a+bi, z' = a'+b'i \in \mathbb{C}$, alors :*
(i) $z\bar{z} = |z|^2 \in \mathbb{R}$;
(ii) $z + \bar{z} = 2\Re(z)$;
(iii) $z - \bar{z} = 2\Im(z)i$;
(iv) $|zz'| = |z||z'|$ et $|z| = |\bar{z}|$;
(v) $z \in \mathbb{R} \Leftrightarrow \Im(z) = 0 \Leftrightarrow z = \bar{z}$;
(vi) $|z+z'| \leq |z| + |z'|$.

Démonstration. (i) a été vu plus haut ;
(ii) et (iii) : on $z+\bar{z} = (a+bi)+(a-bi) = 2a$ et $z-\bar{z} = (a+bi)-(a-bi) = 2bi$;
(iv) : Comme $zz' = (aa'-bb') + (ab'+ba')i$, on a

$$|zz'|^2 = (aa'-bb')^2+(ab'+ba')^2 = a^2a'^2+b^2b'^2-2aa'bb'+a^2b'^2+b^2a'^2+2ab'ba'$$

$$= a^2a'^2 + b^2b'^2 + a^2b'^2 + b^2a'^2 = (a^2+b^2)(a'^2+b'^2) = (|z||z'|)^2.$$

Comme le module est ≥ 0, on obtient prenant la racine carrée $|zz'| = |z||z'|$. La deuxième égalité découle de $a^2+b^2 = a^2+(-b)^2$.
(v) : $z \in \mathbb{R} \Leftrightarrow b = 0 \Leftrightarrow \Im(z) = 0$ et $b = 0 \Leftrightarrow 2b = 0 \Leftrightarrow z - \bar{z} = 0$.

(vi) : Il suffit de montrer l'inégalité obtenue en élevant au carré, c'est-à-dire : $|z+z'|^2 \leq (|z|+|z'|)^2$. Donc en raisonnant par équivalence :

$$|z+z'|^2 \leq |z|^2 + |z'|^2 + 2|z| \cdot |z'|$$

$$\Leftrightarrow (a+a')^2 + (b+b')^2 \leq a^2 + b^2 + a'^2 + b'^2 + 2\sqrt{a^2+b^2}\sqrt{a'^2+b'^2}$$

$$\Leftrightarrow a^2 + a'^2 + 2aa' + b^2 + b'^2 + 2bb' \leq a^2 + a'^2 + b^2 + b'^2 + 2\sqrt{a^2+b^2}\sqrt{a'^2+b'^2}$$

$$\Leftrightarrow aa' + bb' \leq \sqrt{a^2+b^2}\sqrt{a'^2+b'^2}$$

Si le côté gauche est < 0, l'inégalité est satisfaite. Supposons qu'il soit ≥ 0. Alors notre inégalité est équivalente à celle obtenue en prenant les carrés de chaque côté :

$$(aa' + bb')^2 \leq (a^2+b^2)(a'^2+b'^2) \Leftrightarrow$$

$$a^2a'^2 + b^2b'^2 + 2aa'bb' \leq a^2a'^2 + a^2b'^2 + b^2a'^2 + b^2b'^2$$

$$\Leftrightarrow 2aa'bb' \leq a^2b'^2 + b^2a'^2 \Leftrightarrow 0 \leq (ab' - ba')^2,$$

qui est clairement satisfaite. □

9.3 Calculs avec ls nombres complexes

Addition, Multiplication, formule du binôme.

9.4 Propriétés de la conjugaison complexe

Faire l'exercice 123.

Exercice 118. *Effectuer les opérations suivantes et exprimer le résultat sous la forme $a+bi$.*

a) $(14+3i)+(-5+3i)+(2-3i)+4i+((-15)+(2+3i))$;
b) $1+3i+9i^2+27i^3+81i^4+243i^5$;
d) $(2+i\sqrt{3}+3i\sqrt{2})(4i\sqrt{3}-5i\sqrt{2})$;
c) $(17-2i)-(4-7i)$;
e) $(3i\sqrt{7}-5i\sqrt{2})(3i\sqrt{7}+5i\sqrt{2})$;
f) $\frac{-7-3i}{1+5i}$; *g)* $\frac{4+2i}{4i}$; *h)* $\frac{-7+2i}{2+2i}$; *i)* $\frac{-7+3i}{1+5i}$.

Exercice 119. *Trouver les modules et les arguments des nombres complexes suivants :* $2+3i$, $-3+4i$, $\frac{2+3i}{-3+4i}$, $-7+2i$, $2+2i$, $\frac{-7+2i}{2+2i}$. *(on pourra utiliser une table, ou une calculette).*

Exercice 120. *Montrer que si z est un nombre complexe de module 1, son inverse est $\bar{z}$.*

Exercice 121. *

a) Supposons qu'on ait deux nombres complexes z, z' tels que $z' = az$, avec $a \in \mathbb{R}_+$. Montrer qu'on a égalité dans la proposition 9.1 (vi).

b) On suppose que réciproquement on ait $|z + z'| = \max(|z|, |z'|)$. En suivant la preuve de cette proposition, montrer qu'on doit avoir égalité tout au long, et que d'une part $aa' + bb' \geq 0$, et d'autre part $ab' - ba' = 0$. En déduire la réciproque de a).

Exercice 122. *Soit $\mathbb{K} = \{a + bi \mid a, b \in \mathbb{Q}\}$. Montrer que la somme, le produit et l'inverse d'éléments quelconques de $\mathbb{K}$ est dans $\mathbb{K}$.*

Exercice 123. *Montrer que la fonction $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$, est une bijection qui satisfait à $\overline{z + z'} = \bar{z} + \bar{z}'$ et $\overline{zz'} = \bar{z}\bar{z}'$. En déduire que $\overline{1/z} = 1/\bar{z}$ et que $\overline{z/z'} = \bar{z}/\bar{z}'$. Montrer que $z \in \mathbb{R}$ si et seulement si $z = \bar{z}$, et que $z = -\bar{z}$ si et seulement si $z \in \mathbb{R}i$.*

Exercice 124. *Calculez les nombres complexes*

a) $(1 - 3i)(4 + 21i) + \frac{1}{i}$;

b) $(1 + i)^4$;

c) $i^{1000} + i^{123}$;

9.5 Représentation géométrique

Les nombres complexes admettent une interprétation géométrique : $z = a + bi$ est représenté par le point M de coordonnés (a, b) dans le plan cartésien, comme l'on voit dans la figure 1. On identifie souvent un nombre complexe et sa représentation géométrique ; on dira par exemple que $1 + i$ se trouve sur la droite d'équation $y = x$ du plan cartésien. Conséquemment, on appelle *droite réelle* l'axe des x, et *droite imaginaire* l'axe des y ; en effet, la première correspond aux nombres complexes qui sont en fait réels, et la deuxième à 0 et aux nombres complexes *purement imaginaires*, c'est-à-dire de la forme bi ; remarquez qu'on exclut 0 des nombres purement imaginaires, donc on suppose $b \neq 0$).

La longueur r du segment OM est le module de z. L'*argument* de z est l'angle orienté θ (en radians), comme indiqué sur la figure ; on le note $\arg(z)$. Notez que l'argument est un nombre réel défini modulo 2π, c'est-à-dire qu'on peut ajouter à θ un multiple de 2π ; par exemple, si l'argument est de z est 0, alors son argument est aussi $2\pi, 4\pi, -2\pi, \ldots$.

On a

$$z = a + bi = r(\cos\theta + i\sin\theta),$$

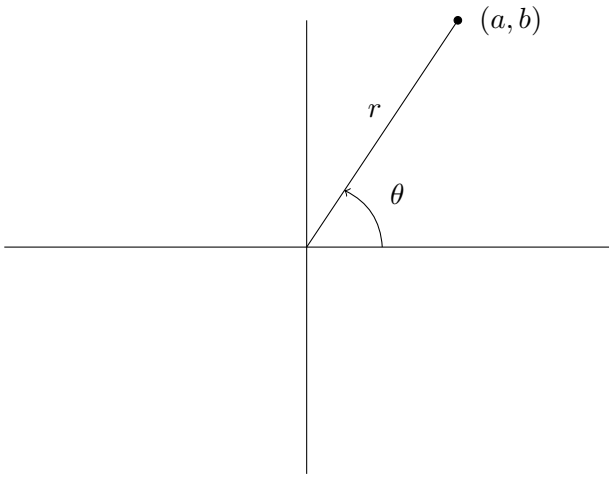

FIGURE 1 – Représentation d'un nombre complexe $z = a + bi$ comme point du plan cartésien

car $a = r\cos\theta, b = r\sin\theta$, comme nous le savons par définition du cosinus et du sinus.

Un nombre complexe de module 1 (i.e. dont le point M correspondant se trouve sur le cercle de centre 0 et de rayon 1) est donc de la forme $\cos\theta + i\sin\theta$, et tout nombre de cette forme est de module 1, car $\cos^2 + \sin^2\theta = 1$. Les nombres complexes de cette forme se multiplient de manière très agréable ; on a en effet :

Proposition 9.2.

$$(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \cos(\theta + \theta') + i\sin(\theta + \theta').$$

Démonstration. Cela découle des formules trigonométriques $\cos(\theta + \theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta'$ et $\sin(\theta + \theta') = \sin\theta\cos\theta' + \cos\theta\sin\theta'$, et de la définition du produit de deux nombres complexes. □

Inversement, ce résultat implique les formules donnant le cosinus et le sinus d'une somme.

Corollaire 9.3. *(formule de Moivre)* $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$.

Démonstration. Pour $n = 0$, le côté gauche est 1, et le droit est $\cos 0 + i\sin 0 = 1$. Supposons la formule vraie pour n et prouvons la pour $n + 1$. On a, en utilisant l'hypothèse de récurrence $(\cos\theta + i\sin\theta)^{n+1} = (\cos\theta +$

$i\sin\theta)^n(\cos\theta+i\sin\theta) = (\cos(n\theta)+i\sin(n\theta))(\cos\theta+i\sin\theta) = \cos((n+1)\theta)+i\sin((n+1)\theta)$, où on a utilisé la proposition 9.2 pour obtenir la dernière égalité. □

Digression : l'exponentielle complexe

Pour tout nombre complexe z on définit $e^z = \exp(z)$ par la formule

$$e^z = \sum_{n\in\mathbb{N}} \frac{z^n}{n!},$$

appelée l'*exponentielle* de z. Le fait que ceci est bien défini (convergence de la série) se prouve dans un cours d'analyse. On montre aussi que l'exponentielle complexe satisfait aux règles usuelles

$$e^{z+z'} = e^z e^{z'}.$$

De plus, on montre que pour tout nombre réel θ

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Les formules de la proposition de celle de Moivre s'écrivent alors naturellement

$$e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'}, (e^{i\theta})^n = e^{in\theta}.$$

Notez que ces formules permettent de retrouver, en utilisant le produit des nombres complexes, les formules trigonométriques utilisées dans la preuve de la proposition 9.2.

Si z est un nombre complexe de module r et d'argument θ, on peut écrire

$$z = re^{i\theta}.$$

On a aussi

$$re^{i\theta}r'e^{i\theta'} = (rr')e^{i(\theta+\theta')}.$$

9.6 Racines n-èmes de 1

Soit n un entier naturel non nul. Considérons les nombres complexes de la forme $\cos(2k\pi/n)+i\sin(2k\pi/n)$, $k = 0,\ldots,n-1$. En utilisant l'exponentielle, on peut écrire

$$\cos(2k\pi/n) + i\sin(2k\pi/n) = e^{2ik\pi/n}.$$

Ce sont des nombres complexes de module 1, donc ils se trouvent sur le *cercle unité* (c'est-à-dire le cercle centré en l'origine et de rayon 1). De plus

leurs arguments étant les angles $0, 2\pi/n, 4\pi/n, \ldots, 2(n-1)\pi/n$, ils forment les n sommets d'un polygone régulier inscrit sur le cercle unité, l'un d'eux étant le point $(1, 0)$. En particulier ils sont au nombre de n.

Par la formule de Moivre, on a

$$\cos(2k\pi/n) + i\sin(2k\pi/n)^n = \cos(2k\pi) + i\sin(2k\pi) = 1,$$

donc la puissance n-ème de chacun de ces n nombres est égale à 1. On appelle ces n nombres les *racines n-èmes de l'unité.*

Exercice 125. *Pour quels n y a-t-il des racines n-èmes de l'unité qui sont réelles, et quelles sont-elles ?*

Exercice 126. *Montrer que si $r > 0$, le nombre complexe $re^{i\theta}$ a n racines n-èmes distinctes, qui forment les sommets d'un polygône régulier à n côtés.*

Exercice 127. *Calculer $(1+i)^{10}$: a) à l'aide du binôme de Newton ; b) à l'aide de la formule de De Moivre.*

Exercice 128. *Montrer que l'ensemble des racines n-èmes de l'unité dans $\mathbb{C}$ est un groupe ave la multiplication (voir Digression en section 7.1). Montrer qu'elles sont toutes puissance de l'une d'entr'elles.*

Exercice 129. *Montrer que $1/2 + i\sqrt{3}/2$ est une racine 6-ème de l'unité et que $\sqrt{2}/2 + i\sqrt{2}/2$ est une racine 8-ème de l'unité.*

Exercice 130. *Écrire sous la forme $a + bi$ les 12 racines douzièmes de l'unité.*

9.7 Théorème fondamental de l'algèbre

Il découle de la section 9.6 que l'équation

$$x^n - 1 = 0$$

a n racines distinctes dans $\mathbb{C}$.

De manière analogue, si $z = re^{i\theta}$ est un nombre complexe, l'équation

$$x^n - z$$

a n solutions distinctes, à savoir les n nombres complexes $\sqrt[n]{r}\omega$, où ω est une racine n-ème de l'unité. En particulier tout nombre complexe non nul a deux racines carrées, opposées l'une de l'autre.

On en déduit que tout polynôme du second degré, avec a, b, c complexes, $a \neq 0$, a deux racines complexes, qui sont données par la même formule que dans le cas réel.

Ceci est un cas très particulier du *théorème fondamental de l'algèbre* : toute équation

$$a_n x^n + a_{n-1} x^n + \cdots + a_1 x + a_0 = 0$$

où les a_i sont dans $\mathbb{C}$ et $a_n \neq 0$, a une solution dans $\mathbb{C}$. La démonstration de ce théorème est au-delà du contenu de ce cours.

Une conséquence est que tout polynôme $P(x)$ de degré $n \geq 1$ à coefficients complexes a *toutes ses racines dans C*, ce qui signifie qu'il peut se factoriser sous la forme

$$z(x - z_1)(x - z_2) \cdots (x - z_n),$$

où $z, z_1, \ldots, z_n \in \mathbb{C}$ et $z \neq 0$.

Digression : les polynômes en une variable

Soit $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. Un polynôme de degré n en la variable x sur $\mathbb{K}$ est une expression de la forme

$$P(x) = a_n x^n + a_{n-1} x^n + \cdots + a_1 x + a_0,$$

où les $a_i \in \mathbb{K}$, avec $a_n \neq 0$. Une racine de $P(x)$ dans $\mathbb{K}$ est un $\alpha \in \mathbb{K}$ tel que

$$P(\alpha) := a_n \alpha^n + a_{n-1} \alpha^n + \cdots + a_1 \alpha + a_0 = 0.$$

Dans ce cas, on peut factoriser

$$P(x) = (x - \alpha) Q(x),$$

où $Q(x)$ est un autre polynôme sur $\mathbb{K}$, de degré $n - 1$ (voir exercice 138).

Digression : les homomorphismes

Il y a tellement d'homomorphismes dans ces notes de cours qu'on ne peut pas passer sous silence leur définition. Soient deux ensembles E, F munis chacun d'une opération, notées respectivement $*$ et $\circ$ (voir la digression en section 7.1 pour la définition de la notion d'opération). Un *homomorphisme* (ou parfois *morphisme*) de E vers F est une fonction $f : E \to F$ telle que pour tous les éléments x, y de E, on ait

$$f(x * y) = f(x) \circ f(y).$$

Un exemple : prenons $E = F = \mathcal{P}(X)$, où X est un ensemble. Prenons sur E les deux opérations union et intersection. Pour $A \in E$, soit $f(A) = X \setminus A$

(complémentaire de A dans X). Alors f est un homomorphisme de E avec l'opération union vers F avec la l'opération intersection. Ce qui signifie

$$f(A \cup B) = f(A) \cap f(B).$$

(voir l'exercice 6). Trouver tous les homomorphismes dans les présentes notes de cours (exercice 140).

Exercice 131. *On veut calculer les racines carrées dans $\mathbb{C}$ du nombre complexe $a+bi$. Si $z = x+iy$ est une telle racine carrée, montrer que $x^2-y^2 = a$, $x^2+y^2 = \sqrt{a^2+b^2}$ et $2xy = b$. En déduire x^2, y^2, puis x et y au signe près. Déterminer les deux racines cherchées en utilisant l'équation $2xy = b$. Appliquer cette méthode au calcul des racines carrées de $3-4i$.*

Exercice 132. *Calculer dans $\mathbb{C}$ les solutions des équations du second degré suivantes.*

a) $x^2 - 1 = 0$ *; b)* $x^2 + 1 = 0$ *; c)* $x^2 - 2 = 0$ *; d)* $x^2 + 2 = 0$ *;*
e) $x^2 - 5x + 6 = 0$ *; f)* $x^2 + x + 1 = 0$ *; g)* $2x^2 + 7x + 1 = 0$ *;*
h) $5x^2 + 3x + 4 = 0$.

Exercice 133. *En utilisant la formule de Moivre, trouver les formules trigonométriques donnant $cos(n\theta)$ et $sin(n\theta)$ en fonction de $cos\theta, sin\theta$, pour $n = 2, 3, 4, 5$.*

Exercice 134. *Trouver les 9 racines neuvièmes de $-i$ dans $\mathbb{C}$, i.e résoudre $z^9 + i = 0$.*

Exercice 135. *Calculer dans $\mathbb{C}$ les solutions des équations suivantes :*

a) $x^4 - 3x^2 + 2 = 0$ *; b)* $x^4 + 4x^2 + 4 = 0$ *;*
c) $x^4 - 5x^2 + 6 = 0$ *; d)* $5x^4 + 3x^2 + 4 = 0$.

Exercice 136. *Trouver l'erreur dans la "preuve" suivante :* $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = i \cdot i = -1$.

Exercice 137. *Avec $a, b, c \in \mathbb{C}$, et $a \neq 0$, trouver α et β tels que $ax^2 + bx + c = a(x+\alpha)^2 + \beta$. Retrouver ainsi les racines de l'équation du second degré, comme rappelées au début du chapitre.*

Exercice 138. *Montrer que si $P(x) = a_n x^n + a_{n-1}x^n + \cdots + a_1 x + a_0$ et si α est racine de P, alors $P(x)$ est un multiple de $x - \alpha$. Indication : écrire $P(x) = P(x) - P(\alpha)$ et utiliser les identités $x^i - \alpha^i = (x-\alpha)(x^{i-1} + x^{i-2}\alpha + \cdots + \alpha^i)$.*

Exercice 139. *Montrer que la fonction*

$$f : a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

est une injection de $\mathbb{C}$ vers les matrices carrées réelles d'ordre 2. Montrer qu'elle permet de représenter les nombres complexes, car elle transforme l'addition et la multiplication complexe en l'addition et la multiplication des matrices ; c'est-à-dire

$$f(z + z') = f(z) + f(z'), f(zz') = f(z)f(z')$$

pour tous nombres complexes z, z'. Quelles sont les opérations sur les matrices qui correspondent à la conjugaison et au carré du module d'un nombre complexe ?

Exercice 140. ** Répertorier tous les homomorphismes dans ces notes de cours. Il faut déterminer les ensembles de départ et d'arrivée, une opération sur chacun de ces ensembles, et la fonction qui est un homomorphisme pour ces opérations*

Troisième partie
Géométrie du plan

10 Triangles et parallélogrammes

10.1 Parallélisme et angles

Angles alterne-internes, alterne-externes, opposés, correspondants.

10.2 Somme des angles

Proposition 10.1. *La somme des (mesures des) trois angles d'un triangle est égale à π radians (en degrés, c'est 180).*

Il est utile de faire un dessin pour chacun des exercices.

Exercice 141. *On considère un polygone régulier à n côtés, dont les sommets sont sur un cercle de centre 0, et trois sommets successifs A, B, C de ce polygone. On veut calculer la mesure de l'angle $x = \widehat{ABC}$. Quelle est-elle pour $n = 3$ et 4 ? Montrer que l'angle $y = \widehat{AOB}$, mesuré en degrés, est égal à $\frac{1}{n} \cdot 360$. Montrer que $x + y = 180$ degrés. En déduire que $x = \frac{n-2}{n} \cdot 180$ degrés. Appliquer cela aux pentagone et hexagone réguliers.*

Exercice 142. *Avec les notations de l'exercice précédent, que peut-on dire du triangle ABC lorsque $n = 6$? En déduire une construction par règle et compas de l'hexagone régulier.*

Exercice 143. *Montrer que la somme des (mesures des) angles d'un polygone convexe à n côtés est $(n-2)\cdot 180$ degrés. Indication : prendre un point O intérieur, et décomposer le polygone en n triangles, chacun d'eux étant déterminé par un côté du polygone, et avec 3ème sommet égal à O.*

10.3 Aire

L'aire d'un rectangle est égale au produit des mesures de deux côtés adjacents.

Comme la surface d'un triangle rectangle peut être vue comme la moitié de la surface d'un rectangle, on obtient : l'aire d'un triangle rectangle est égale au demi-produit des mesures des deux côtés adjacents à l'angle droit.

Il est utile de faire un dessin pour chacun des exercices.

Exercice 144. *Montrer que l'aire d'un triangle est égal au produit d'un de ses côtés par la longueur de la hauteur qui passe par le sommet opposé. Indication : pour un triangle ABC, la hauteur passant par un sommet A est le segment AH où H est la projection orthogonale de A sur BC. Décomposer le triangle en deux triangles rectangles.*

Exercice 145. *Un trapèze est un quadrilatère (polygone à 4 sommets) $ABCD$ tel que AB et CD soient parallèles. Montrer que son aire est égal à la moitié du produit $(AB + CD)\cdot AH$, où H est la projection orthogonale de A sur CD. Indication : décomposer le trapèze en un rectangle et deux triangles rectangles ; il y a deux cas, à traiter tous les deux.*

10.4 Isométrie des triangles

Deux triangles *rectangles* sont isométriques (c'est-à-dire, superposables par une translation et une symétrie au besoin) dès que les côtés correspondants, adjacents à l'angle droit, ont même mesure.

Plus généralement, si deux triangles $ABC, A'B'C'$ satisfont $AC = A'C'$ et $\widehat{CAB} = \widehat{C'A'B'}$ et $\widehat{ACB} = \widehat{A'C'B'}$ (ce qu'on peu abréger en $\hat{A} = \hat{A}'$ et $\hat{C} = \hat{C}'$), alors ces triangles sont isométriques. On appelle ce critère le *second cas d'égalité des triangles.*

Le *premier cas d'égalité des trinagles* : deux triangles $ABC, A'B'C'$ sont isométriques si leurs côtés ont deux à deux même longueur

Er le *troisième cas d'égalité des triangles* est : deux triangles sont égaux s'il ont deux côtés égaux, ainsi que l'angle entre ces deux côtés.

Pour s'en souvenir : premier cas CCC, deuxième cas ACA, troisième cas CAC. Le sigle AAA correspondrait aux triangles semblables (voir plus loin), qui ne sont pas forcément égaux.

Exercice 146. *Que se passe-t-il avec les autres sigles, comme AAC, etc... ? On prendra la convention que les lettres, comme AAC, indiquent aussi la succession dans le triangle des angles et des côtés ; ainsi AAC veut dire qu'il faut considérer deux angles successifs puis le côté qui suit, quand on tourne autour du triangle.*

10.5 Concourance des médiatrices, et des bissectrices

Proposition 10.2. *Les médiatrices (resp. les bissectrices) d'un triangle sont concourantes).*

Démonstration. Dans un triangle ABC, la médiatrice du côté AB est l'ensemble des points qui sont à égale distance de A et B. C'est une droite. Donc la médiatrice de AB et la médiatrice de BC se rencontrent en un point O qui est à égale distance de A, de B et C. Donc O est sur la médiatrice de AC.

Dans un triangle ABC, la bissectrice de l'angle $\widehat{ABC}$ est l'ensemble des points qui sont à égale distance des côtés BA et BC. C'est une droite. Donc la bissectrice de $\widehat{ABC}$ et de $\widehat{BCA}$ se rencontrent en un point P qui est égale distance des côtés BA, $BC = CB$ et CA. Donc P est sur la bissectrice de $\widehat{CAB}$. □

Exercice 147. *L'intersection des médiatrices est le centre du cercle qui passe par les trois sommets du triangle (*cercle circonscrit*). L'intersection des bissectrices est le centre du cercle qui est tangent aux trois côtés (*cercle inscrit*).*

10.6 Parallélogrammes

Un *parallélogramme* est un quadrilatère dont les côtés opposés sont parallèles.

Proposition 10.3. *Soit $ABCD$ un quadrilatère. Les conditions suivantes sont équivalentes :*

(i) $ABCD$ est un parallélogramme ;

(ii) $AB = CD$ et $AD = BC$;
(iii) Les diagonales AC et BD se coupent en leur milieu ;
(iv) $AB = CD$ et AB est parallèle à CD.

Démonstration. (i) implique (ii) : les triangles ABD et BCD sont isométriques. En effet, ils ont un côté commun, qui est BD et les angles adjacents sont égaux deux à deux : $\widehat{ADB} = \widehat{DBC}$ (angles alternes-internes pour les droites parallèles AD et BC et la sécante BC) et $\widehat{ABD} = \widehat{BDC}$.

On en déduit que $BA = DC$ et $AD = CB$.

(ii) implique (i) : par hypothèse, et le premier cas d'égalité, les triangles ABD et CDB sont isométriques. Donc $\widehat{ABD} = \widehat{CDB}$ et par angle-alterne-interne, avec la sécante BD, les droites AB et CD sont parallèles. L'autre parallélisme se prouve de la même façon.

(i) implique (iii) : soit $ABCD$ un parallélogramme et I 'intersection de ses diagonales. On a $AB = CD$, $\widehat{BAI} = \widehat{ICD}$ et $\widehat{ABI} = \widehat{IDC}$. Donc les triangles AIB et DCI sont isométriques. D'où les égalités des côtés correspondants : $IB = ID$, $IA = IC$. Donc les diagonales se coupent en leur milieu.

(iii) implique (ii) : supposons que les diagonales se coupent en leur milieu. On a $AI = IC$, $BI = ID$ et clairement $\widehat{AIB} = \widehat{DIC}$. Donc les traingles AIB et CID sont isométriques et on obtient $AB = CD$. De manière analogue, on a $AD = BC$.

(i) implique (iv) : découle de ce qui précède.

(iv) implique (i) : montrons que les triangles AIB et CID sont isométriques. Ça se prouve comme dans la partie "(i) implique (iii)" en utilisant le 2ème cas d'égalité des triangles. On en déduit que les diagonales se coupent en leur milieu. □

Exercice 148. *Un* rectangle *est un quadrilatère dont tous les angles sont droits. Montrer que les assertions suivantes sont équivalentes, pour un parallélogramme :*
(i) c'est un rectangle ;
(ii) un de ses angles est droit ;
(iii) ses diagonales ont même longueur.
Indications : cas d'égalité des triangles.

Exercice 149. *Montrer qu'un quadrilatère convexe est un parallélogramme si et seulement si les angles opposés sont égaux. Indications : dans un sens utiliser le premier cas d'égalité des triangles. Dans l'autre sens utiliser que la*

somme des angles est 360 degrés, et le critère de parallélisme par les angles alternes-internes.

Exercice 150. *Un* losange *est un parallélogramme dont les quatre côtés on même longueur. Montrer qu'un parallélogramme est un losange si et seulement si ses deux diagonales se coupent sont perpendiculaires. Indication : cas d'égalité des triangles.*

10.7 Concourance des hauteurs et des médianes

Proposition 10.4. *Les trois hauteurs dans un triangle sont concourantes.*

On appelle *orthocentre* leur intersection.

Démonstration. □

Proposition 10.5. *Les trois médianes dans un triangle ABC sont concourantes, et l'intersection G satisfait $AG = \frac{2}{3}AA'$, où A' est le milieu du segment BC, ce qui caractérise G entièrement.*

On appelle G le *centre de gravité* du triangle.

Démonstration. On va utiliser le calcul des vecteurs. La notation $\overrightarrow{AB}$ désigne le *vecteur libre* d'origine A et d'extrémité B. On rappelle la *règle du parallélogramme* : si $ABCD$ sont les sommets d'un parallélogramme, dans cet ordre, alors

$$\overrightarrow{AB} + \overrightarrow{AD} = \overrightarrow{AC};$$

il découle donc de la Proposition 10.3 que si M est le milieu de BD, alors $\overrightarrow{AM} = \frac{1}{2}(\overrightarrow{AB} + \overrightarrow{AD})$. On a aussi la *relation de Chasle* :

$$\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC},$$

pour tous points A, B, C. Enfin, si G, H sont deux points, alors $G = H$ si et seulement si $\overrightarrow{GH} = \overrightarrow{0}$.

Soit maintenant un triangle ABC et A', B', C' les milieux des côtés BC, CA, AB. Soient G le point défini par $\overrightarrow{AG} = \frac{2}{3}\overrightarrow{AA'} = \frac{1}{3}(\overrightarrow{AB} + \overrightarrow{AC})$. De même H le point défini par $\overrightarrow{BH} = \frac{2}{3}\overrightarrow{BB'} = \frac{1}{3}(\overrightarrow{BA} + \overrightarrow{BC})$. Nous allons montrer que $G = H$. Ceci impliquera que les droites AA' et BB' se rencontrent en ce point. Par symétrie (en échangenat B et C ce point sera donc aussi sur la droite CC'. Enfin l'égalité de l'énoncé sera aussi démontré.

Calculons donc $\overrightarrow{GH}$. On a $\overrightarrow{GH} = \overrightarrow{GA} + \overrightarrow{AB} + \overrightarrow{BH} = \frac{1}{3}(-\overrightarrow{AB} - \overrightarrow{AC} + 3\overrightarrow{AB} + \overrightarrow{BA} + \overrightarrow{BC} = \frac{1}{3}(\overrightarrow{CA} + \overrightarrow{AB} + \overrightarrow{BC}) = \frac{1}{3}(\overrightarrow{CB} + \overrightarrow{BC}) = \overrightarrow{0}$. □

Exercice 151. *Dans un triangle équilatéral, que peut-on dire des intersections (médiatrices, bissectrices, hauteurs, médianes) ?*

Exercice 152. *Quel est l'orthocentre d'un triangle rectangle ?*

Exercice 153. *On considère un parallélogramme $ABCD$ et E le point de la droite AC symétrique de A par rapport à E. Montrer que C est le centre de gravité du triangle DEB. Indication : utiliser la caractérisation dans la proposition 10.5.*

10.8 Loi des sinus

$$a/\sin(\alpha) = b/\sin(\beta) = c/\sin(\gamma).$$

Exercice 154. *Démontrer le théorème de Pythagore en utilisant la loi des sinus.*

11 Trois théorèmes antiques

11.1 Théorème de Pythagore

Theorem 11.1. *Soit a, b, c les mesures des côtés d'un triangle rectangle, où c est celle de l'hypoténuse (le côté opposé à l'angle droit). Alors*

$$a^2 + b^2 = c^2.$$

Démonstration. Sur la figure 2, on a représenté un grand carré dont les côtés ont pour longueur $a + b$. Sur chaque côté nous avons indiqué un point à distance a et b des extrémités de ce côté. On obtient ainsi 4 points sur les 4 côtés, et ces points forment un quadrilatère, et nous montrons que c'est un carré.

En effet, les 4 triangles sur la figure sont isométriques : ce sont des triangles rectangles, et les côtés adjacents à l'angle droit ont mesures a et b. Donc leurs hypoténuses ont donc tous la même longueur c. De plus l'angle à chaque sommet de ce quadrilatère vaut 90 degrés : en effet, prenons le sommet du bas de la figure ; on y voit que cet angle, additionné aux deux angles non droits du triangle, donne 180 degrés ; comme la somme des angles de ce triangle vaut 180 degrés, il vaut bien 90 degrés.

On conclut en comparant avec la figure 3. □

Il y a une généralisation du théorème de Pythagore, qui s'appelle *loi des cosinus* ou *théorème d'Al-Kashi* ...

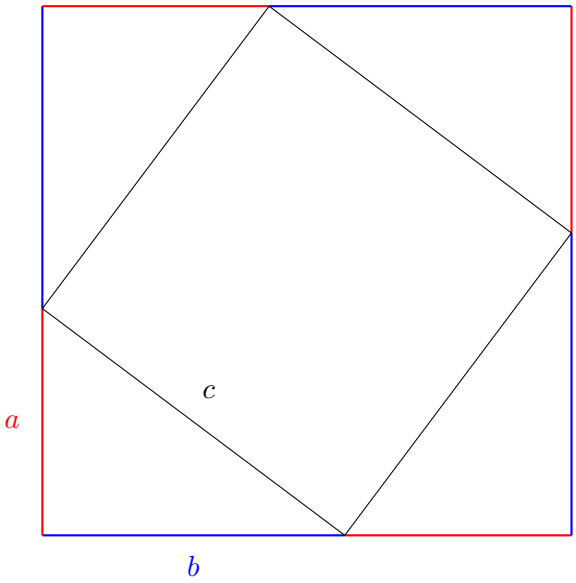

FIGURE 2 – La démonstration du théorème de Pythagore

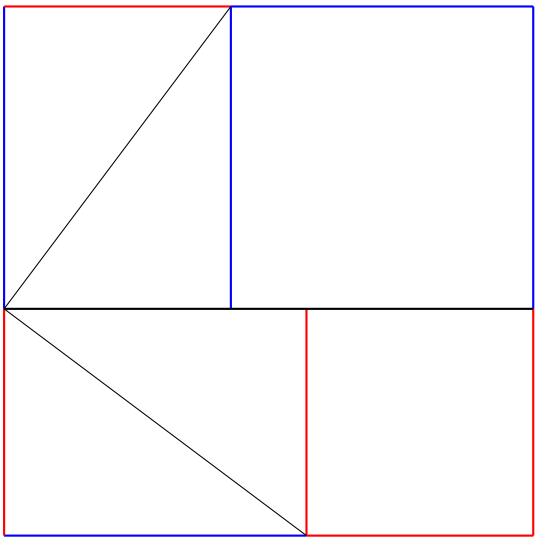

FIGURE 3 – La démonstration du théorème de Pythagore, suite

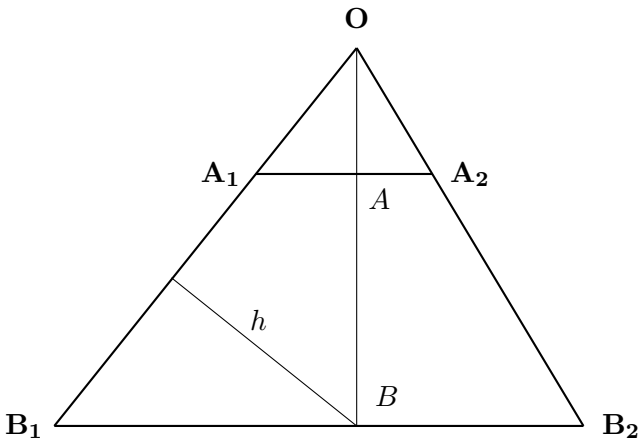

FIGURE 4 – Théorème de Thalès

11.2 Théorème de Thalès

Theorem 11.2. *Dans la figure 4, où A_1A_2 est parallèle à B_1B_2, on a l'égalité des rapports des longueurs de segments*

$$\frac{OB_1}{OA_1} = \frac{B_1B_2}{A_1A_2} = \frac{OB_2}{OA_2}.$$

Nous commençons par un lemme arithmétique.

Lemma 11.3. *Si les nombres b_1, b_2, b_1+b_2 sont non nuls, et si $x = \frac{a_1}{b_1} = \frac{a_2}{b_2}$, alors $x = \frac{a_1+a_2}{b_1+b_2}$.*

Démonstration. On a par hypothèse, $a_1 = xb_1$ et $a_2 = xb_2$. Donc $a_1 + a_2 = x(b_1 + b_2)$, d'où la conclusion. □

Preuve du théorème 11.2. Sur la figure, les points A, B sont tels que la droite contenant O, A, B est perpendiculaire à A_1A_2 et B_1B_2. De plus, h est la longueur de la hauteur issue de B dans le triangle OBB_1.

1. Nous commençons par démontrer le théorème dans le cas particulier des points O, A_1, B_1, A, B, c'est-à-dire nous prouvons que

$$\frac{OB_1}{OA_1} = \frac{OB}{OA} = \frac{BB_1}{AA_1}. \tag{5}$$

Notation : nous notons IJK l'aire du triangle dont les sommets sont les points I, J, K.

Les triangles A_1B_1B et OB_1B ont le sommet commun B, et leurs côtés opposés (A_1B_1 et OB_1 respectivement) sont portés par la même droite. Donc leurs aires sont proportionnelles à ces côtés, et il s'ensuit que

$$\frac{A_1B_1}{OB_1} = \frac{A_1B_1B}{OB_1B}.$$

Les triangles A_1B_1B et AB_1B ont même aire, car ils ont le côté commun B_1B et leurs sommets opposés (A_1 et A repectivement) sont à même distance AB de de côté. Donc $A_1B_1B = AB_1B$; comme $OB_1B = OBB_1$ (c'est le même triangle), on obtient

$$\frac{A_1B_1B}{OB_1B} = \frac{AB_1B}{OBB_1}.$$

Les triangles AB_1B et OBB_1 sont rectangles, avec le côté commun BB_1, adjacent à l'angle droit, et les autres côtés ajacents à l'angle droits sont respectivement AB et OB ; le rapport de leurs aires est donc

$$\frac{AB_1B}{OBB_1} = \frac{AB}{OB}.$$

Mettant ensemble ces trois inégalités, nous trouvons que

$$\frac{A_1B_1}{OB_1} = \frac{AB}{OB}.$$

Par suite

$$\frac{OA_1}{OB_1} = \frac{OB_1 - A_1B_1}{OB_1} = 1 - \frac{A_1B_1}{OB_1} = 1 - \frac{AB}{OB} = \frac{OB - AB}{OB} = \frac{OA}{OB},$$

ce qui implique la première des inégalités dans (5). Pour la deuxième nous évaluons de deux façons l'aire du trapèze rectangle A_1ABB_1. Elle vaut d'une part

$$\frac{1}{2}(B_1B + A_1A) \cdot AB$$

et d'autre part

$$\frac{1}{2}B_1B \cdot OB - \frac{1}{2}A_1A \cdot OA.$$

Nous obtenons donc $B_1B \cdot (OA + AB) - A_1A \cdot OA = B_1B \cdot AB + A_1A \cdot AB$, ce qui implique $B_1B \cdot OA = A_1A \cdot OA + A_1A \cdot AB = A_1A \cdot OB$, d'où la deuxième égalité dans (5).

2. Nous avons par 1., et la propriété symétrique obtenue en remplaçant les indices 1 par les indices 2 :

$$\frac{OB_1}{OA_1} = \frac{OB}{OA} = \frac{OB_2}{OA_2},$$

et

$$\frac{BB_2}{AA_2} = \frac{OB}{OA} = \frac{BB_1}{AA_1},$$

donc par le lemme, ce rapport vaut aussi

$$\frac{BB_2 + BB_1}{AA_2 + AA_1} = \frac{B_1B_2}{A_1A_2}.$$

□

Une conséquence importante du théorème de Thalès est le résultat suivant sur les triangles semblables. Rappelons que deux triangles sont *semblables* si les mesures des trois angles de l'un coïncident avec celles de l'autre triangle.

Corollaire 11.4. *Soient deux triangles semblables ABC et $A'B'C'$ avec $\hat{A} = \hat{A}'$, $\hat{B} = \hat{B}'$ et $\hat{C} = \hat{C}'$. Alors leurs côtés sont proportionnels, précisément :*

$$\frac{AB}{A'B'} = \frac{BC}{B'C'} = \frac{CA}{C'A'}.$$

Démonstration. En déplaçant un des triangles, on peut se ramener à la configuration de la figure 4 : les deux triangles sont alors OA_1A_2 et OB_1B_2. On applique alors le théorème de Thalès. □

Exercice 155. *Montrer que l'intersection des médiatrices d'un triangle rectangle est le milieu de l'hypothénuse. Indication : utiliser le théorème de Thalès.*

Exercice 156. *On considère deux sécantes, trois points A, B, C sur l'une d'elles, et A', B', C' sur l'autre, tels que AA', BB', CC' sont parallèles. Montrer que $AB/BC = A'B'/B'C'$. Indication : exprimer AB et BC en fonction de a, b, OC où O est le point d'intersection des sécantes, et a, b sont les réels tels que $OA = aOC, OB = bOC$; faire de même pour A', B', C', avec les mêmes réels (utiliser le théorème de Thalès).*

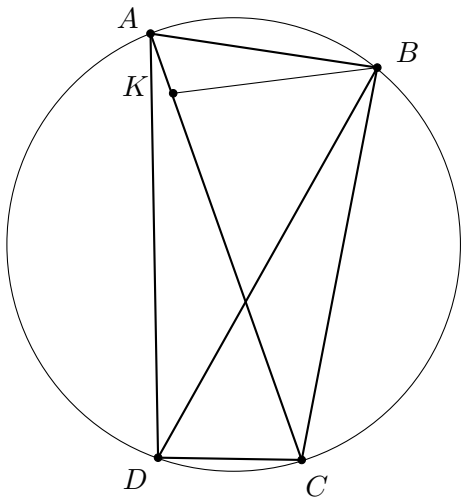

FIGURE 5 – Théorème de Ptolémée

11.3 Théorème de Prolémée

Un polygone est dit *inscriptible dans un cercle* s'il existe un cercle contenant tous ses sommets.

Theorem 11.5. *Dans un quadrilatère convexe inscriptible dans un cercle, le produit des diagonales est égal à la somme des produits des côtés opposés.*

Dans la figure 5, ceci signifie que

$$AC \cdot BD = AB \cdot CD + AD \cdot BC.$$

Proposition 11.6. *(théorème de l'angle inscrit) Etant donné quatre points A, A', B, C sur un cercle, avec A, A' du même côté de la droite BC, les angles $\widehat{BAC}$ et $\widehat{BA'C}$ sont égaux.*

Démonstration. □

Preuve du théorème 11.5. D'après la proposition 11.6, les angles $\widehat{CAB}$ et $\widehat{CDB}$ sont égaux, de même que les angles $\widehat{BDA}$ et $\widehat{BCA}$. Considérons le point K sur la droite AC tel que $\widehat{ABK} = \widehat{DBC}$. On a d'une part $\widehat{KAB} = \widehat{CAB} = \widehat{CDB}$ et $\widehat{BCK} = \widehat{BCA} = \widehat{BDA}$. Et d'autre part $\widehat{ABD} = \widehat{ABK} + \widehat{KBD} = \widehat{DBC} + \widehat{KBD} = \widehat{KBC}$. Nous en déduisons que les triangles ABK et DBC sont semblables, de même que ABD et KBC. Précisément :

- Dans le triangle ABK et DBC : $\widehat{ABK} = \widehat{DBC}$ et $\widehat{KAB} = \widehat{CDB}$, donc ils sont semblables.

- Dans le triangle ABD et KBC : $\widehat{BDA} = \widehat{BCK}$ et $\widehat{ABD} = \widehat{KBC}$, donc ils sont semblables.

Par suite

$$\frac{AK}{AB} = \frac{DC}{DB}\ ,\ \frac{CK}{BC} = \frac{DA}{BD},$$

et $AK \cdot DB = AB \cdot DC$ et $CK \cdot BD = BC \cdot DA$. En additionnant, nous obtenons $(AK+CK)\cdot DB = AB\cdot DC+BC\cdot DA$ et on conclut car $AK+CK = AC$. □

Exercice 157. *Un triangle est-il toujours inscriptible dans un cercle ?*

Exercice 158. *Montrer comment déduire le théorème de Pythagore du théorème de Ptolémée.*

Exercice 159. *On considère un pentagone régulier. Soient c la longueur d'un côté et d la longueur d'une diagonale. En utilisant le théorème de Ptolémée, montrer que $d^2 = cd + c^2$. En déduire que le rapport $x = d/c$ satisfait $x^2 = x + 1$, et puis que $x = \frac{\sqrt{5}+1}{2}$, le* nombre d'or.

12 Nombres complexes et géométrie

On représente chaque point du plan euclidien par un nombre complexe et vice-versa.

12.1 Rotations et translations

Rappelons qu'une *translation*, de *vecteur de translation* V, est une fonction du plan dans lui-même qui associe à tout point X du plan l'unique point Y du plan tel que le vecteur XY soit égal à V.

Si on utilise les coordonnées cartésienne, le plan c'est $\mathbb{R}^2$, le vecteur $V = (v_1, v_2)$, et la translation est la fonction $X = (x_1, x_2) \mapsto (y_1, y_2) = Y = X + (v_1, v_2) = (x_1 + v_1, x_2 + v_2)$.

Représentons maintenant les points du plan par les nombres complexes. Il découle de la définition de l'addition des nombres complexes que de manière équivalente, une *translation* est une fonction $\mathbb{C} \to \mathbb{C}$ de la forme $z \mapsto z + b$, pour un certain b, appelé le *vecteur de translation*.

Nous allons généraliser ces fonctions.

Définition 12.1. *Soient a, b des nombres complexes. Les fonctions $f_{a,b}$ et $\bar{f}_{a,b}$ de $\mathbb{C}$ dans $\mathbb{C}$ sont définies par :*

$$f_{a,b}(z) = az + b, \bar{f}_{a,b}(z) = a\bar{z} + b.$$

Une fonction $f_{a,b}$ est appelée une *fonction affine*. Une translation est donc une fonction de la forme $f_{1,b}$. Une *rotation* est une fonction $f_{a,b}$ telle que $|a| = 1$; l'angle de la rotation est l'angle θ tel que $a = e^{i\theta}$; si $b = 0$, le centre de la rotation est O.

Ces fonctions se composent avec les formules suivantes.

Proposition 12.2.

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b}, f_{a,b} \circ \bar{f}_{c,d} = \bar{f}_{ac,ad+b},$$

$$\bar{f}_{a,b} \circ f_{c,d} = f_{a\bar{c},a\bar{d}+b}, \bar{f}_{a,b} \circ \bar{f}_{c,d} = f_{a\bar{c},a\bar{d}+b}.$$

Exercice 160. *Montrer que $\bar{z}$ est le symétrique de z par rapport à l'axe des x. Montrer que l'argument de $\bar{z}$ est l'opposé de celui de z. Montrer que z est de module 1 si et seulement si $z^{-1} = \bar{z}$.*

Exercice 161. *On considère des fonctions $f_i : z \mapsto a_i z + b_i$. Montrer que $f_1 \circ \cdots \circ f_n$ est la fonction $f(z) = az + b$, avec $a = a_1 \cdots a_n$ et $b = \sum_{1 \leq i \leq n} a_1 \cdots a_{i-1} b_i$.*

Exercice 162. ** On note $j = e^{2i\pi/3}$ ou $j = e^{4i\pi/3}$, une des deux racines cubiques de 1, différente de 1. Montrer que j et j^2 sont racines de $1+x+x^2 = 0$. Soient $z_1, z_2, z_3 \in \mathbb{C}$. Montrer qu'il forment un triangle équilatéral si et seulement si $z_1 + jz_2 + j^2 z_3 = 0$. Indication : noter z le centre du cercle circonscrit au triangle formé par ces trois points. Se ramener au cas au $z = 0$, puis au cas où le cercle est de rayon 1, puis au cas où $z_1 = 1$. Montrer que $1 + jz + j^2 z' = 0$ si et seulement si $z = 1, z' = 1$, ou $z = j, z' = j^2$. Eliminer z' de l'équation et utiliser le fait que $z'^{-1} = \bar{z}', z^{-1} = \bar{z}$, et montrer que l'équation devient $(z-1)(z-j) = 0$.*

12.2 Théorème de Morley (1898)

Etant donné un angle (déterminé par deux demi-droites se coupant en M), on définit les deux *trissectrices* de cette angle comme les deux demi-droites qui découpent cet angle en trois angles égaux.

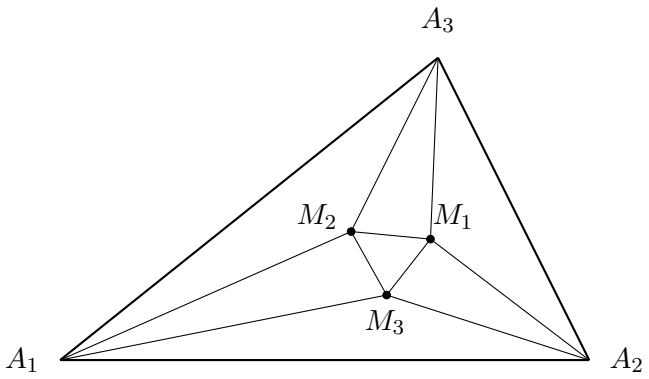

FIGURE 6 – Théorème de Morley

Theorem 12.3. *Soit $A_1A_2A_3$ un triangle, et pour chacun de ses trois angles intérieurs, on considère ses deux trissectrices. On appelle M_1, M_2, M_3 les points obtenus par l'intersection de deux trissectrices voisines, issues de deux sommets voisins (voir Figure 6). Le triangle $M_1M_2M_3$ est équilatéral.*

Démonstration d'après Alain Connes [2]. On note $3\alpha_i$, $i = 1, 2, 3$, la mesure, en radians et dans le sens trigonométrique, de l'angle interne du triangle au sommet A_i. On note f_i la rotation de sommet A_i et d'angle $2\alpha_i$. On peut écrire $f_i(z) = a_i z + b_i$, où $a_i, b_i \in \mathbb{C}$ et $|a_i| = 1$. Précisément a_i est le nombre complexe de module 1 et d'argument $2\alpha_i$.

On note M_3' le point symétrique de M_3 par rapport à la droite A_1A_2. On a $f_2(M_3) = M_3'$ et $f_1(M_3') = M_3$. Donc $f_1 \circ f_2(M_3) = M_3$. Or $M_3 = f_1 \circ f_2(M_3) = a_1(a_2M_3 + b_2) + b_1 = a_1a_2M_3 + a_1b_2 + b_1$, donc $M_3 = \frac{a_1b_2+b_1}{1-a_1a_2}$. On a de même (en permutant cycliquement les indices) $M_1 = \frac{a_2b_3+b_2}{1-a_2a_3}$ et $M_2 = \frac{a_3b_1+b_3}{1-a_3a_1}$.

Montrons maintenant que $f = f_1^3 \circ f_2^3 \circ f_3^3$ est l'identité. Par les résultats de la section 12, on sait que $f(z) = az + b$, où $a = a_1^3a_2^3a_3^3$. Mais a est le nombre complexe de module 1 et d'argument $\sum_i 3(2\alpha_i) = 2\sum_i 3\alpha_i = 2\pi$. Donc $a = 1$, ce qui signifie que f est une translation. Or f_3^3 est la rotation de sommet A_3 et d'angle $6\alpha_3$, donc elle envoie A_1 sur A_1', le symétrique de A_1 par rapport à A_2A_3. Et f_2^3 est la rotation de sommet A_2 et d'angle $6\alpha_2$; donc elle envoie A_1' sur A_1. Enfin f_1^3 envoie A_1 sur A_1. Donc $f(A_1) = A_1$, ce qui implique que f est l'identité et $b = 0$.

Nous avons donc $(a_1a_2a_3)^3 = 1$. De plus, on vérifie en calculant la com-

position $f_1^3 \circ f_2^3 \circ f_3^3$ que

$$(a_1^2 + a_1 + 1)b_1 + a_1^3(a_2^2 + a_2 + 1)b_2 + (a_1a_2)^3(a_3^2 + a_3 + 1)b_3 = 0. \qquad (6)$$

Calculons, avec $c = a_1a_2a_3$, donc $c^3 = 1$:

$$cM_1 + c^2M_2 + c^3M_3 = c\frac{a_2b_3 + b_2}{1 - a_2a_3} + c^2\frac{a_3b_1 + b_3}{1 - a_3a_1} + \frac{a_1b_2 + b_1}{1 - a_1a_2}.$$

En multipliant par le dénominateur commun $D = (1 - a_2a_3)(1 - a_3a_1)(1 - a_1a_2)$, nous obtenons une expression de la forme $H_1b_1 + H_2b_2 + H_3b_3$ où les H_i ne comportent pas de b_i ; on a, en utilisant $c = a_1a_2a_3$, $c^3 = 1$ et $c^2 + c + 1 = 0$:

$$H_1 = c^2a_3(1 - a_2a_3)(1 - a_1a_2) + (1 - a_2a_3)(1 - a_3a_1)$$

$$= (1-a_2a_3)(c^2a_3-c^2a_3a_1a_2+1-a_3a_1) = (1-a_2a_3)(c^2a_3-a_3a_1) = a_3(1-a_2a_3)(c^2-a_1)$$

$$= a_3(c^2 - a_1 - c^2a_2a_3 + a_1a_2a_3) = a_3(-1 - c - a_1 - c^2a_2a_3 + c)$$

$$= \frac{a_3}{a_1}(-a_1 - a_1^2 - 1).$$

De même,

$$H_2 = c\frac{a_1}{a_2}(-a_2 - a_2^2 - 1), H_3 = c^2\frac{a_2}{a_3}(-a_3 - a_3^2 - 1).$$

Finalement

$$-\frac{a_1}{a_3}D(cM_1 + c^2M_2 + c^3M_3)$$

$$= (a_1^2 + a_1 + 1)b_1 + \frac{a_1}{a_3}c\frac{a_1}{a_2}(a_2^2 + a_2 + 1)b_2 + \frac{a_1}{a_3}c^2\frac{a_2}{a_3}(a_3^2 + a_3 + 1)b_3 = 0,$$

d'après (6). On conclut en utilisant l'exercice 162. □

13 Solutionnaire (esquisses)

Exercice 1 $A \times B = \{(1,4),(1,5),(2,4),(2,5),(3,4),(3,5)\}$; $\mathcal{P}(A) = \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\},\}$; $\mathcal{P}(B) = \{\emptyset,\{3\},\{4\},B\}$; $\mathcal{P}(\mathcal{P}(B)) = \{\emptyset,\{\emptyset\},\{\{3\}\},\{\{4\}\},\{B\},\{\{3\},\{4\}\},\{\{3\},B\},\{\{4\},B\},etc...\}$ (16 éléments).
Exercice 3 Tous vrais sauf e) qui est faux.
Exercice 4 C'est l'ensemble des nombres entiers naturels *composés*, c'est-à-dire produit de deux entiers naturels ≥ 2 ; autrement dit, c'est l'ensemble des entiers naturels, distincts de 0 et 1, et qui ne sont pas premiers.

Exercice 5 Soit a un élément de A est $B = A \setminus \{a\}$. Alors $|B| = n-1$ et on peut admettre (hypothèse de récurrence) que la cardinalité de $\mathcal{P}(B)$ est 2^{n-1}. A toute partie E de A, on associe la partie $F = E \cap B$ de B. Pour une partie F de B donnée, il y a exactement deux parties de A qui lui correspondent ainsi ; à savoir F et $F \cup \{a\}$. On en déduit que la cardinalité de $\mathcal{P}(A)$ deux fois celle de $\mathcal{P}(B)$.
Exercice 6 Pour les deux dernière égalités, un dessin peut aider.
Exercice 7
Exercice 8 a) $x \in (A \cup B) \setminus (A \cap B) \Leftrightarrow x \in A \cup B$ et $x \notin A \cap B \Leftrightarrow x$ appartient à l'un des ensembles, mais pas aux deux $\Leftrightarrow x \in A \setminus B$ ou $x \in B \setminus A \Leftrightarrow x \in (A \setminus B) \cup (B \setminus A)$.

b) $x \in A \cap B \Leftrightarrow x \in A$ et $x \in B \Leftrightarrow x \in A$ et $non(x \notin B) \Leftrightarrow x \in A$ et $non(x \in A \setminus B) \Leftrightarrow x \in A \setminus (A \setminus B)$.
Exercice 9 R n'est pas fonctionnelle car $(1,2)$ et $(1,3)$ sont tous deux dans R. L'autre relation est fonctionnelle ; en effet il n'y a pas de a, b, c tels que (a,b) et (a,c) sont dans cette relation et que de plus $b \neq c$.
Exercice 10 Ces égalités découlent de la définition d'une fonction au début de la section 9.
Exercice 11 Faux. On a en effet le contre-exemple suivant $f(1) = f(2) = 1$, $X = \{1,2\}, Y = \{2\}$. Alors $X \setminus Y = \{1\}$, $f(X \setminus Y) = \{1\}$ et $f(X) \setminus f(Y) = \{1\} \setminus \{1\} = \emptyset$.
Exercice 12 Si $z \in g \circ f(X)$, alors il existe $x \in X$ tel que $z = g \circ f(x) = g(f(x)$; alors $y = f(x) \in f(X)$, donc $z = g(y) \in g(f(X))$. Réciproquement, si $z \in= g(f(X)$, alors il existe $y \in f(X)$ tel que $z = g(y)$; alors il existe $x \in X$ tel que $y = g(x)$, donc $z = g(f(x)) = g \circ f(x) \in g \circ f(X)$.

Si $x \in (g \circ f)^{-1}(Y)$, alors $(g \circ f)(x) \in Y$, donc $g(f(x) \in Y$, donc $f(x) \in g^{-1}(Y)$, donc $x \in f^{-1}(g^{-1}(Y))$. Réciproquement, si $x \in f^{-1}(g^{-1}(Y))$, alors $f(x) \in g^{-1}(Y)$, donc $g(f(x)) \in Y$, donc $(g \circ f()x) \in Y$, donc $x \in (g \circ f)^{-1}(Y)$.
Exercice 13 (i) Si $g \circ f(a) = g \circ f(a')$, alors $g(f(a)) = g((a'))$, donc g étant injective $f(a) = f(a')$, donc f étant injective, $a = a'$.

(ii) Si $f(a) = f(a')$, alors $g(f(a)) = g(f(a'))$, donc $g \circ f(a) = g \circ f(a')$, donc $g \circ f$ étant injective $a = a'$.

(iii) Soit $c \in C$; comme $g \circ f$ est injective, il existe $a \in A$ tel que $c = g \circ f(a)$; on a donc $c = g(f(a)$ et c est donc dans l'image de g.
Exercice 14 a) Supposons que $f : A \to B$ soit surjective. Soit $b \in B$; on peut alors choisir $a \in A$ tel que $f(a) = b$, et on pose $h(b) = a$; on obtient alors $f \circ h = \mathrm{id}_B$.

b) Supposons que $f : A \to B$ soit injective. Soit $b \in \mathrm{Im}(f)$; il existe un unique $a \in A$ tel que $b = f(a)$; on pose $g(b) = a$. Soit $b \in B \setminus \mathrm{Im}(f)$; on

pose alors $g(b) = a_0$, où a_0 est un élément fixé dans A. On obtient alors $g \circ f = \mathrm{id}_A$.

Pour les réciproques, on utilise l'exercice 13.

Exercice 15 Si $a \in A$, alors $f(a) \in f(A)$, donc $a \in f^{-1}(f(A))$. Si $b \in f(f^{-1}(B))$, alors il existe $a \in f^{-1}(B)$ tel que $b = f(a)$; alors $f(a) \in B$, donc $b \in B$.

Exercice 16 Supposons que f soit

Exercice 27 a) L'unique élément minimal est 1. Les éléments maximaux sont $6, 7, 8, 9, 10$.

b) Le minimum est 1, et il n'y a pas de maximum (car s'il existe, c'est l'unique élément maximal).

c) Le supremum de $\{2, 3\}$ dans E est 6, et $\{3, 4\}$ n'a pas de supremum dans E, car $\{3, 4\}$ n'a pas de majorant dans E.

Exercice 30 b) La condition est que $R_1 = R_2$ et que R_1 est un ordre total.

Exercice 31 a) Vrai.

b) Faux.

Exercice

Exercice 39 Les classes d'équivalence sont $\{0\}$ et $\{a, -a\}$, $\forall a \in \mathbb{R}_+^*$. Soit $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. On a $f^{-1}(0) = \{0\}$ et $\forall b > 0, f^{-1}(b) = \{a, -a\}$, où $a = \sqrt{b}$.

Exercice 40 Toute classe est l'ensemble des cercles d'un même centre.

Exercice 47 1. Si E est la réunion disjointe des parties $A_i, i = 1, \ldots, n$, alors la réunion des $A_i \times A_i$ est une relation d'équivalence sur E.

2. De 1., on déduit une fonction de l'ensemble des partitions de E dans l'ensemble des relations d'équivalence sur E : c'est la bijection inverse de la fonction déduite du corollaire 5.13.

Exercice 48 a) Pour $n = 0$, $n^2 - n = 0$ et 2 divise 0. Si $n^2 - n$ est divisible par 2, $n^2 - n = 2k$ et alors $(n+1)^2 - (n+1) = n^2 + 2n + 1 - n - 1 = n^2 + n = (n^2 - n) + 2n = 2(k + n)$. Donc $(n + 1)^2 - (n + 1)$ est aussi divisible par 2.

Autre preuve (sans récurrence) : $n^2 - n = (n - 1)n$ est le produit de 2 entiers consécutifs ; comme l'un des deux est pair le produit est pair.

b) $(n+1)^3 - (n+1) - (n^3 - n) = n^3 + 3n^2 + 3n + 1 - n^3 + n = 3(n^2 + n)$ donc : 3 divise $n^3 - n \Rightarrow 3$ divise $(n + 1)^3 - (n + 1)$.

Autre preuve : $n^3 - n = (n-1)n(n+1)$ et comme l'un des trois nombres consécutifs $n - 1, n$ et $n + 1$ est multiple de 3, $n^3 - n$ est divisible par 3.

c) Pour $n = 0, 4^n - 1 = 0$ est divisible par 3. Ensuite, $(4^{n+1} - 1) - (4^n - 1) = 4^n(4 - 1) = 3 \cdot 4n$, donc : 3 divise $4n - 1 \Rightarrow 3$ divise $4^{n+1} - 1$.

Autre preuve : $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1)$; on conclut en posant $x = 4$.

d) Pour $n = 0, 2^{2n+1} + 1 = 3$ est divisible par 3. Puis $(2^{2(n+1)+1} + 1) - (2^{2n+1} + 1) = 2^{2n+1}(2^2 - 1) = 3 \cdot 2^{2n+1}$; donc si 3 divise $2^{2n+1} + 1$, alors 3 divise aussi $2^{2(n+1)+1} + 1$.

Autre preuve : $x^{2n+1} + 1 = (x + 1)(x^{2n} - x^{2n-1} + \cdots + 1)$ donne (avec $x = 2$) $2^{2n+1} + 1 = 3N$.

e) $(9^{n+1} - 8(n + 1) - 1) - (9^n - 8n - 1) = 8 \cdot 9^n - 8 = 8(9n - 1)$. Reste à montrer que 8 divise $9^n - 1$. C'est par récurrence en utilisant $(9^{n+1} - 1) - (9^n - 1) = 8 \cdot 9^n$.

f) $(7^{n+1} - 3^{n+1}) - (7^n - 3^n) = 6 \cdot 7^n - 2 \cdot 3^n = 2(3 \cdot 7^n - 3^n) = 2 \cdot 2 \cdot k = 4k$.

Autre preuve : $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}$ est une identité bien connue ; on pose $x = 7, y = 3$.

g) $2^n > n \Rightarrow 2^{n+1} = 2^n + 2^n > n + 1$, car $2^n \geq 1$.

h). $2^{n-1} \leq n! \Rightarrow 2^n = 2 \cdot 2^{n-1} \leq 2 \cdot n! \leq (n + 1)n! = (n + 1)!$ si $n \geq 1$.

i) $1^2 + \cdots n^2 + (n+1)^2 = n(n+1)(2n+1)/6 + (n+1)^2 = (n+1)(n(2n+1)/6 + n + 1) = (n + 1)(2n^2 + 7n + 6)/ = (n + 1)(n + 2)(2n + 3)/6 = (n + 1)(n + 2)(2(n + 1) + 1)/6$, ce qui est la formule à prouver, avec n rempacé par $n + 1$.

Autre preuve : l'identité $(x + 1)^3 - x^3 = 3x^2 + 3x + 1$. Posons $x = 1, 2, \ldots, n$ et additionnons ces n égalités ; il y a beaucoup de simplifications et on obtient : $(n + 1)^3 - 1^3 = 3(1^2 + 2^2 + \cdots n^2) + 3n(n + 1)/2 + n$. On trouve alors la somme des carrés cherchée.

j) Par hypothèse de récurrence $1+2+\cdots+2^n = 2^{n+1}-1+2^{n+1} = 2^{n+2}-1$. Selon la légende, c'est le nombre de grains de blé reçus par l'inventeur du jeu d'échecs (s'il y avait n cases sur l'échiquier). Ajoutons 1 (grain) à gauche : $1 + (1 + 2 + \cdots + 2^n) = 2 + 2 + 2^2 + \cdots + 2^n = 2^2 + 2^2 + 2^3 + \cdots = 2^{n+1}$, ce qui donne une autre preuve.

k) $0 \cdot 0! + 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! + (n + 1) \cdot (n + 1)! = (n + 1)! - 1 + (n + 1) \cdot (n + 1)! = (n + 2) \cdot (n + 1)! - 1 = (n + 2)! - 1$.

l) $1^3+2^3+\cdots+n^3+(n+1)^3 = (1+2+\cdots+n)^2+(n+1)^3 = (n(n+1)/2)^2+(n+1)^3 = (n+1)^2(n^2/4+n+1) = ((n+1)(n+2)/2)^2 = (1+2+\cdots+(n+1))^2$. On peut aussi écrire : $(x + 1)^4 - x^4 = 4x^3 + 6x^2 + 4x + 1$ et sommer de 1 à n.

Exercice 50 Soit $a \in \mathbb{Z}^*_-$. On a $-a = bq + r, 0 \leq r < b$. Si $r > 0$, $a = b(-q) + (-r) = b(-q - 1) + (b - r) = bq' + r'$, avec $q' = -q - 1$ et $r' = b - r$, $0 \leq r' < b$. Si $r = 0$, $a = bq'' + r''$, avec $q'' = -q$ et $r'' = 0$. L'unicité se prouve comme dans le théorème 7.1.

Exercice 51 Si $b\mathbb{Z} \subset a\mathbb{Z}$, alors $b = b \cdot 1 \in a\mathbb{Z} \Rightarrow a$ divise b. Si a divise b, $b = aq$; alors $\forall x \in b\mathbb{Z}, x = bn = aqn \in a\mathbb{Z}$.

Exercice 52 On utilise l'exercice 51. On a $n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow n\mathbb{Z} \subset m\mathbb{Z}$ et $m\mathbb{Z} \subset n\mathbb{Z} \Leftrightarrow m|n$ et $n|m \Leftrightarrow n = m$.

Exercice 53 a) On montre que $H = \{a_1p_1 + \cdots + a_kp_k \mid p_i \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$. Donc ce sous-groupe est égal à $m\mathbb{Z}$ pour un certain $m \in \mathbb{N}$. Alors m divise chaque a_i, donc $m \leq pgdc(a_1, \ldots, a_k)$. Mais $n = pgdc(a_1, \ldots, a_k)$ divise chaque a_i, donc aussi tout élément de H, donc aussi m. D'où $m = n$.

b)

c) Imiter la preuve du corollaire 7.5.

d) Imiter la preuve du théorème 7.7.

e) On montre que le sous-groupe $\{a_1p_1 + \cdots + a_kp_k \mid p_i \in \mathbb{Z}\}$ de $\mathbb{Z}$ est identique au sous-groupe $\{pgdc(a_1, \ldots, a_{k-1})p + a_kq \mid p, q \in \mathbb{Z}\}$.

f) On calcule $pgdc(a_1, a_2)$ puis $pgdc(pgdc(a1, a2), a3)$ etc...

g) On a $(pgdc(a, b) = c \geq 0$ si et seulement $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$.

Exercice 54 a) $pgdc(233, 144) = 1 = 233 \cdot (-55) + 144 \cdot 89$.

b) $pgdc(4181, 2584) = 1$.

c) $pgdc(2091, 1479) = 3$.

La suite de Fibonacci $(F_n)_{n\geq 0}$ est définie par : $F_0 = F_1 = 1$ et $\forall n \geq 2, Fn = F_{n-1} + Fn - 2$. Les premiers nombres de Fibonacci sont : 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, ... On peut démontrer par récurrence les deux résultats suivants : $\forall n \geq 0, pgdc(F_n, F_{n+1}) = 1$; $F_n^2 - F_{n-1}F_{n+1} = (-1)^n$. Comme $233 = F_{12}$ et $144 = F_{11}$, ceci explique la réponse trouvée en a). Comme $4181 = F_{18}$ et $2584 = F_{17}$, on trouve pour b), $F_{16}F_{18} + (-F_{17})F_{17} = 11$, c'est-à-dire $4181 \cdot 1597 + 2584(-2584) = 1$.

Exercice 55 Par définition d est un diviseur commun de a et b, donc $a = da', b = db', a', b' \in \mathbb{N}$. Si $pgdc(a', b') = d' > 1$, alors dd' serait un diviseur commun de a et b strictement plus grand que d, ce qui est impossible.

Exercice 56 a) On sait que $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$; posons $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Comme $m \in a\mathbb{Z}$ et $m \in b\mathbb{Z}$, m est un multiple de a et de b. Le ppmc de a, b est dans $a\mathbb{Z} \cap b\mathbb{Z}$; donc m divise $ppmc(a, b)$. D'où $m = ppmc(a, b)$.

b) a et b divisent $m \Leftrightarrow m \in a\mathbb{Z} \cap b\mathbb{Z} \Leftrightarrow m \in ppmc(a, b)\mathbb{Z} \Leftrightarrow m$ est un multiple de $ppmc(a, b)$.

c) Puisque a et b divisent ab, la partie b) s'applique.

Exercice 58 On utilise par exemple le théorème 7.4. Ensuite, on a $1 = pgdc(a, b) = pgdc(a - bq, b)$ et on fait une récurrence.

Exercice 59 Si $pgdc(a, c) = d > 1$ (le cas $pgdc(b, c) > 1$ est semblable), alors d divise a et d divise c, donc d divise $a + b$. Donc $d > 1$ divise à la fois a et b. Contradiction.

Exercice 60 $1 = (k+1)+(= 1)k = 1$. Donc $pgdc(k, k+1) = 1$ par le théorème de Bézout.

Exercice 61 $1\cdot(k+2)+(-1)k=2$ montre que $pgdc(k,k+2)$ divise 2. C'est donc 1 ou 2. Ce sera 1 si et seulement si k est impair.
Exercice 61 On a $pgdc(k,k+6)=pgdc(k,6)$. Donc c'est 1 si et seulement si $pgdc(k,6)=1$, i.e. k est de la forme $6l+1$ ou $6l-1$.
Exercice 63 $pgdc(k,2k+1)=pgdc(k,k+1)=1$. La première égalité découle de $pgdc(a,a+b)=pgdc(a,b)$.
Exercice 64 $pgdc(3k+2,5k+3)=pgdc(3k+2,2k+1)=pgdc(k+1,2k+1)=pgdc(k+1,k)=1$.
Exercice 65 Soit $(F_n)_{n\geq 0}$ la suite de Fibonacci définie par $F_0=F_1=1$ et $F_n=F_{n-1}+F_{n-2}$ pour $n>1$. $F_{n+1}k+F_n$ et F_nk+F_{n-1} sont toujours premiers entre eux ($\forall k\geq 0$). Preuve par récurrence.
Exercice 77 $p_{r_1}p_{r_2}\cdots p_{r_k}$ est clairement un diviseur commun de a et b tel que tout diviseur commun de a et b le divise.
Exercice 78 Comme l'exercice 77.
Exercice 79 $\min(n_i,m_i)=\max(n_i,m_i)=n_i+m_i$.
Exercice 80 La réciproque est vraie, i.e. si p est premier et $pgdc(a^2,b^2)=p^2$, alors $pgdc(a,b)=p$. Le résultat est vrai aussi si p n'est pas premier.
Exercice 90 1er cas : $a=2^3p_2^{a_2}\cdots p_k^{a_k}$ et $b=2^{b_1}p_2^{b_2}\cdots p_k^{b_k}$ avec $b_1\geq 3, p_i>2$.

2ème cas : $a=2^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ et $b=2^3p_2^{b_2}\cdots p_k^{b_k}$ avec $a_1>3, p_k>2$. On a $\max(a_i,b_i)=0$ pour $i=2,\cdots,k$.
Exercice 81 $n=2^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ où les p_i sont premiers et $\neq 2$, donc impairs.
Exercice 82 Remarquez qu'on a (voir exercice 79) $ppmc(a,b)=(da')(db')/d=ab/pgdc(a,b)$.
Exercice 83 $\min D(n)=1, \max D(n)=$n. Si n admet deux diviseurs premiers distincts p et q, alors p et q sont dans $D(n)$ et ne sont pas comparables.
Exercice 74 L'ordinateur est bienvenu.
Exercice 91 Chaque facteur $10=2\cdot 5$ fait apparaître un zéro. Dans 10000! $=1\cdot 2\cdot 3\cdots 10000$, il y a un facteur 5 à chaque multiple de 5 (2000 fois) et un facteur $5^2=25$ (400 fois), un facteur $5^3=125$ (80 fois), un facteur $625=5^4$ (16 fois) et un facteur $3125=5^5$ (3 fois). Au total : 2499 zéros. Pour la base 2 on trouve : 9995 zéros !
Exercice 97 $b\in[a]\Leftrightarrow\exists k\in\mathbb{Z}, b-1=nk\Leftrightarrow\exists k\in\mathbb{Z}, b=a+nk\Leftrightarrow b\in a+n\mathbb{Z}$; donc $[a]=a+n\mathbb{Z}$. De plus, $(a+n\mathbb{Z})\cap(b+n\mathbb{Z})\neq\emptyset\Leftrightarrow\exists k_1,k_2, a+nk_1=b+nk_2\Leftrightarrow a-b\in n\mathbb{Z}\Leftrightarrow a\equiv b \mod .n$.
Exercice 98 a) Non ; b) Non ; c) $x=31$; d) Non ; e) $x=21$; f) $x=7$; g) $x=17$.
Exercice 99 $\{x \mid x$ est solution de $ax\equiv 0 \mod n\}=\{x|x$ multiple de $n/pgdc(a,n)\}=n d\mathbb{Z}$, où $d=pgdc(a,n)$. Par exemple $6x\equiv 0 \mod 9$ (resp. $6x\equiv 0 \mod 3$) a comme solutions $3\mathbb{Z}$ (resp. $\mathbb{Z}$).

Exercice 100 Par l'exercice 99, $x_0 + n'\mathbb{Z}$, où $n' = n/pgdc(n,a)$.
Exercice 101 a) $19 + 20k$; b) $11 + 30k$; c) $17 + 35k$; d) $11 + 12k$.
Exercice 102 Plus généralement, on a le *théorème de Wilson* : pour tout nombre premier p, $\Pi_{i=1}^{i=p-1} i \equiv -1 \mod p$.
Exercice 103 On peut démontrer : $\forall n \in \mathbb{Z}, n^p \equiv n \mod p$ si p est premier. Ce résultat s'appelle le *petit théorème de Fermat*.
Exercice 104 Pour $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, x = 2 = 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1$. Réponse : $\{0, 1, 3, 4, 5, 9\}$.
Exercice 115 Factoriser le numérateur et le dénominateur du rationnel.
Exercice 116 Joli.
Exercice 117 On utilise l'exercice 115. La bijection inverse g est définie par : si $x = p_1^{m_1} \cdots p_k^{m_k}$, avec des m_i dans $\mathbb{Z}^*$, soit $n_i = 2m_i$ si $m_i > 0$, $= -2m_i + 1$ si $m_i < 0$; alors $g(x) = p_1^{n_1} \cdots p_k^{n_k}$. On a $f^{-1}(\mathbb{N}^*) = g(\mathbb{N}^*) =$ l'ensemble des carrés de $\mathbb{N}^*$.
Exercice 118 a) $-2 + 10i$; b) $1 + 3i - 9 - 27i + 81 - 243i = 73 - 267i$; c) $13 + 5i$; d) $(5\sqrt{2} - 4\sqrt{3})(3\sqrt{2} + \sqrt{3})$; e) -13 ; f) $-11/13 + 16/13i$; g) $1/2 - i$; h) $-5/4 + 2i$; i) $5/17 + 31/17i$.
Exercice 119 Utiliser $r = \sqrt{a^2 + b^2}$; $\theta = \arctan(b/a)$; $|z_1/z_2| = |z_1|/|z_2|$; $\arg z_1/z_2 = argz_1 - argz_2$.
Exercice 122 On constate que pour $a, b, c, d \in \mathbb{Q}$, $(a+bi)+(c+di) = (a+c)+(b+d)i \in K$, car $a+c, b+d \in \mathbb{Q}$; $(a+bi)(c+di) = (ac-bd)+(bc+ad)i \in K$, car $ac - bd, bc + ad \in \mathbb{Q}$; si $a^2 + b^2 \neq 0$, $(a + bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in K$.
Exercice 126 Les racines sont toutes de même module, soit $\sqrt[n]{r}$, et leurs arguments sont θ/n, $\theta/n + 2\pi/n$, $\theta/n + 2 \cdot 2\pi/n$, ...,$\theta/n + (n-1) \cdot 2\pi/n$.
Exercice 131 Si $z = x + iy$, $z^2 = x^2 - y^2 + 2ixy = a + bi \Rightarrow x^2 - y^2 = a$ et $2xy = b$. De plus $|z^2| = |z|^2 = a^2 + b^2 \Rightarrow |z| = x^2 + y^2 = \sqrt{a^2 + b^2}$. On a donc $x^2 = (1/2)(a + \sqrt{a^2 + b^2}), y^2 = (1/2)(-a + \sqrt{a^2 + b^2})$. Si $b > 0$, alors (à cause de $2xy = b$), x, y ont même signe ; si $b < 0$, x, y sont de signes opposés. Exemple : $a + bi = 3 - 4i$, $b < 0$; $\sqrt{a^2 + b^2} = 5, x + iy = \pm(2 - i)$.
Exercice 132 a) $x = \pm 1$; b) $x = \pm i$; c) $x = \pm\sqrt{2}$; d) $x = \pm i\sqrt{2}$; e) $x = 2, 3$; f) $x = (-1 \pm i\sqrt{3})/2$; g) $x = (-7 \pm \sqrt{41})/2$; h) $x = (-3 \pm i\sqrt{71})/10$.
Exercice 133 Développer $(\cos\theta + i\sin\theta)^n$ avec la formule du binôme. On obtient les formules : $\cos(2\theta) = \cos^2\theta - \sin^2\theta, \sin(2\theta) = 2\sin\theta\cos\theta$; $\cos(3\theta) = \cos^3\theta - 3\cos\theta\sin^2\theta, \sin(3\theta) = 3\cos^2\theta\sin\theta - \sin^3\theta$; $\cos(4\theta) = \cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta, \sin(4\theta) = 4\cos^3\theta\sin\theta - 4\cos\theta)\sin^3\theta$; $\cos(5\theta) = \cos^5\theta - 10\cos^3\theta\sin\theta + 5\cos\theta\sin^4\theta; \sin(5\theta) = 5\cos^4\theta\sin\theta - 10\cos^2\theta\sin^3\theta + \sin 5\theta$.
Exercice 140 Voir exercice 6 (deux exemples) ; proposition 3.2 b), e) f) ; exercice 28 (v), à condition de remplacer $\mathbb{R}$ par $\mathbb{Z}$ pour que le maximum soit

toujours défini ; exercice 53 h) ; la fonction $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, section 7.4 ; proposition 9.1 (iv) ; la conjugaison complexe, exercice 123 ; proposition 9.2 ; l'exponentielle complexe, section 9.5 ; la fonction polynôme, section 9.7 ; exercice 139.

Exercice 146 Le sigle AAC donne un cas d'égalité (le troisième angle est déterminé). Le sigle ACC non : prendre un triangle isocèle ABC de base AB et un point M sur la base qui n'est pas son milieu ; alors les deux triangles CAM et CBM satisfont au critère siglé ACC, mais ne sont pas isométriques, car $BM \neq AM$. Les autres cas sont symétriques de ceux déjà considérés.

Exercice 157 Oui. Le centre du cercle est l'intersection des médiatrices du triangle.

Exercice 158 On considère un rectangle, inscriptible dans un cercle, et le théorème de Ptolémée implique le théorème de Pythagore pour le triangle rectangle dont l'hypoténuse est une diagonale du rectangle.

Exercice 159 Le pentagone est inscriptible dans un cercle. On considère le quadrilatère obtenu en supprimant un des sommets. Le théorème de Ptolémée donne $d^2 = cd + c^2$.

Références

[1] [BH] F. Bergeron, C. Hohlweg, Arithmétique et géométrie classique, disponibles sur les sites des auteurs.

[2] [C] A. Connes, A new proof of Morley's theorem, Publication Mathématiques de l'Institut des hautes études scientifiques, vol. S88, 1998, 43-46. 66

[3] [LR] J. Labelle, C. Reutenauer, cours d'algèbre 1, UQAM. 3