Université Paris 6, Licence FONDNATEXP, UE Maths LG308

`http://www.math.jussieu.fr/~romagny/LG308`

Version de Septembre 2006

Le cours de ce premier semestre est composé de deux parties principales : Arithmétique, et Géométrie. Il est précédé de quelques notions de logique, indispensables pour être en mesure de dépasser l'intuition et pour pouvoir faire des démonstrations. D'ailleurs, le terme de *démonstration* sera l'un des maîtres mots du cours...

Ces notes doivent beaucoup au livre de Daniel Perrin intitulé *Mathématiques d'école : Nombres, mesures et géométrie*, paru aux éditions Cassini. J'ai utilisé également le livre *Geometry : Euclid and beyond* de Robin Hartshorne (éditions Springer). Je remercie vivement Daniel Perrin pour m'avoir (indirectement...) procuré une version de son texte alors qu'il était encore en préparation. Je remercie également Claire Cazes et Frédérique Petit pour leurs relectures et commentaires.

Notations. Rappelons les symboles utilisés pour les ensembles de nombres usuels :

- $\mathbb{N}$ est l'ensemble des nombres entiers naturels,
- $\mathbb{Z}$ est l'ensemble des nombres entiers relatifs,
- $\mathbb{Q}$ est l'ensemble des nombres rationnels (les fractions),
- $\mathbb{R}$ est l'ensemble des nombres réels,
- $\mathbb{C}$ est l'ensemble des nombres complexes.

Préliminaire :
Logique et raisonnement mathématique

Logique et raisonnement mathématique

La logique s'intéresse d'une part aux règles de construction des phrases mathématiques, d'autre part à leur vérité.

Soit X un ensemble. Un *énoncé*, ou une *proposition*, est une phrase mathématique dépendant des éléments de X. Un énoncé peut avoir deux valeurs, dépendant des éléments de X : *vrai* ou *faux* (1 ou 0).

On associe à chaque énoncé P la partie de X des éléments tels que P est vrai.

Exemple : pour l'énoncé « $x \geq 3$ » la partie correspondante de $\mathbb{R}$ est $[3; +\infty[$.

Par définition, si cette partie est X tout entier l'énoncé « $\forall x \in X,\ P(x)$ » est vrai.
De même, si cette partie n'est pas vide, l'énoncé « $\exists x \in X,\ P(x)$ » est vrai.

Correspondance entre connecteurs logiques et opérations ensemblistes :

Logique	Ensemble	Symbole
P		
non P		$\neg P$
P ou Q		$P \vee Q$
P et Q		$P \wedge Q$
P implique Q $=$ (non P) ou Q		$P \Rightarrow Q$ $= \neg P \vee Q$
P équivaut à Q $=$ (P implique Q) et (Q implique P)		$P \Leftrightarrow Q$ $= \ldots$

Complétez par vous-mêmes la deuxième colonne en dessinant l'interprétation ensembliste de chaque connecteur : si la partie de X des éléments tels que P est vrai est notée A, et celle associée de même à Q est notée B, alors la partie associée à P ou Q est...

1 Remarques, exemples

(1) En mathématiques le *ou* est inclusif, c'est-à-dire que (P ou Q) est vraie si et seulement si P est vraie, ou Q est vraie, ou P et Q sont vraies (alors qu'en français, si on dit « prendre fromage ou dessert », ça veut dire qu'on ne prend pas les deux).

(2) On ajoute souvent un indice à une variable quantifiée par $\exists$: « $\exists x_0 \in X$,... » pour insister sur le fait qu'on pointe là un élément *particulier*. A contrario, avec le quantificateur $\forall$ on utilise souvent une lettre neutre (sans indice) : « $\forall x \in X, ...$ » pour souligner que c'est un élément *quelconque*. C'est très utile pour faciliter la compréhension.

(3) Il faut bien faire la différence entre une proposition (qui est une phrase) et sa valeur (qui est l'un des deux qualificatifs « vrai » ou « faux »). Par exemple la proposition dépendant des nombres entiers « $n(n+1)$ est impair » est un énoncé correct du point de vue des règles de logique, bien que faux pour tout $n \in \mathbb{N}$.

Exemples (1) $X = \mathbb{N}$ et $P(n)$: n est pair ou n divise $2n$

(2) $X = \mathbb{N} \times \mathbb{N}$ et $Q(k,n)$: (k divise n) $\iff$ $(\exists n' \in \mathbb{N},\, n = n'k)$

(3) $X = \mathbb{R}$ et $P(x)$: $x^2 + 5x + 1 = 0$

(4) P : $\exists x \in \mathbb{R},\ x^2 + 1 = 0$

(5) $X = \mathbb{N} \times \mathbb{R}$ et $P(n,x)$: $n \geq x$

(6) $X = \mathbb{R}$ et $P(x)$: $\forall n \in \mathbb{N},\ n \geq x$

(7) $\forall n \in \mathbb{N},\ \exists x \in \mathbb{R},\ n \leq x$

(8) $\exists x \in \mathbb{R},\ \forall n \in \mathbb{N},\ n \leq x$

(9) $\forall x \in \mathbb{R},\ \forall n \in \mathbb{N},\ n \leq x$

(10) $\forall x \in \mathbb{R},\ (\forall y \in \mathbb{R},\ x \leq y^2) \Rightarrow x \leq 0$

(11) $\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ (x \leq y^2 \Rightarrow x \leq 0)$

• Un énoncé peut être vrai avec $\exists x \in X$ et faux avec $\forall x \in X$. (3)

• Le choix de l'ensemble des éléments est (bien sûr) très important. (4)

• Un énoncé peut porter aussi sur les éléments de plusieurs ensembles. (5)

• Soit un énoncé P dépendant des éléments de plusieurs ensembles : $P(x,y,z,\dots)$. Alors en écrivant « $\forall x \in X,\ P(x,y,z,\dots)$ » ou « $\exists x_0 \in X,\ P(x,y,z,\dots)$ » on forme un nouvel énoncé $Q(y,z,\dots)$ qui dépend de tous les ensembles de départ *sauf* X. (5 et 6)

• L'ordre des quantificateurs est très important : d'ailleurs une proposition qui est vraie (7) peut être fausse si on le change (8). En revanche, on peut toujours échanger deux quantificateurs identiques (9).

• L'utilisation de parenthèses est parfois nécessaire, et des parenthèses placées différemment donnent des énoncés différents (éventuellement l'un vrai (10) et l'autre faux (11)).

• La négation de $\forall$ est $\exists$ et la négation de $\exists$ est $\forall$. Plus précisément, la négation de $(\forall x \in X,\ P(x))$ est $(\exists x_0 \in X$, non $P(x_0))$. La négation de $(\exists x_0 \in X,\ P(x_0))$ est $(\forall x \in X$, non $P(x))$.

• Dans un énoncé du type « $\forall x \in X,\ P(x)$ » ou « $\exists x \in X,\ P(x)$ », la variable x est muette c'est-à-dire qu'on peut la remplacer par n'importe quelle autre sans changer l'énoncé.

• Si $P \Rightarrow Q$ est vrai on dit que Q est une *condition nécessaire* de P, ou que P est une *condition suffisante* de Q. Si $P \iff Q$ on dit que P est une *condition nécessaire et suffisante* de Q (ou l'inverse).

2 Techniques de démonstration

Voici un petit résumé des différentes techniques de démonstration à notre disposition.

Lorsqu'on doit montrer...	Les techniques de démonstration sont...
une implication $P \Rightarrow Q$	raisonnement ordinaire raisonnement par contraposée : on montre que $\urcorner Q \Rightarrow \urcorner P$. raisonnement par l'absurde : on suppose P et $\urcorner Q$ et on arrive à une contradiction.
une équivalence $P \Leftrightarrow Q$	raisonnement par double implication : $P \Rightarrow Q$ et $Q \Rightarrow P$
une égalité d'ensembles $A = B$	raisonnement par double inclusion : $A \subset B$ et $B \subset A$
qu'une proposition P est fausse	on montre que non P est vraie
une propriété $P(n)$ dépendant des entiers naturels	raisonnement par récurrence

Enfin voici un *truc* de rédaction vraiment très utile : quand on doit montrer que « $\forall x \in X$,... » on commence par écrire : « Soit $x \in X$ ».

3 Logique et langue courante

Voici diverses formulations en français du quantificateur $\forall$:

Pour tout $x \in \mathbb{R}$, x^2 est positif.
Soit x réel. On a...
Tout réel x vérifie...
Quel que soit $x \in \mathbb{R}$,...
Un (quelconque) nombre réel x a son carré positif.

Diverses formulations en français du quantificateur $\exists$:

Il existe $x_0 \in X$ tel que...
Il y a un $x_0 \in X$ tel que...
Trouvez/on a trouvé x_0 dans X tel que...
« Le nombre entier n est de la forme $2k$ »
pour dire « il existe k tel que $n = 2k$ »... c'est-à-dire simplement « n est pair » !

Diverses formulations en français de l'implication :

Si $x \geq 0$ alors...
Quand (dès que, lorsque) $x \geq 0$, on a...
Soit on a $x < 0$, soit...
(c'est le « soit... soit » qui exprime une alternative, comme « ou bien... ou bien »)
Soit $x \geq 0$. Alors...
(c'est le « soit » qui sert à se donner un élément : il est complètement différent !)
Puisque $x \geq 0$, alors...
On a ... car $x \geq 0$
Il suffit que $x \geq 0$ pour que...
... est nécessaire pour que $x \geq 0$.

Diverses formulations en français de l'équivalence :

P si et seulement si Q
P c'est-à-dire Q
P i.e. Q
On a P exactement lorsqu'on a Q

4 Exercices

Exercice Log.1 Montrez que

(a) $P \Rightarrow (Q$ ou $R)$ est la même chose que $(P$ et (non $Q)) \Rightarrow R$.

(b) $P \Rightarrow Q$ est la même chose que (non $Q \Rightarrow$ non P).
On appelle cette dernière l'*implication contraposée* de $P \Rightarrow Q$.

(c) $P \iff Q$ est la même chose que (non $P \iff$ non Q).

Exercice Log.2 Écrivez les énoncés suivants sous forme de proposition mathématique avec des quantificateurs (sans autre mot de français que les connecteurs « ou, et »). On rappelle que $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ désignent l'ensemble des nombres rationnels, réels, complexes.

(a) Tout entier relatif est la différence de deux entiers naturels.

(b) La fonction f n'est pas strictement positive sur $\mathbb{R}$ tout entier.

(c) Le module d'un nombre complexe est un nombre réel.

(d) Il n'existe pas de nombre rationnel dont le carré vaut deux.

(e) Les seuls nombres entiers naturels pairs sont 2, 8 et 44.

Exercice Log.3 Maman dit à Nicolas : « Si tu ne ranges pas ta chambre, tu n'auras pas de chocolat ». Nicolas range sa chambre, mais Maman ne lui donne pas de chocolat. Pourquoi ?

Avertissement pour la suite

Dans la suite du cours, contrairement à ce qui est le cas en Logique, on ne s'intéresse qu'aux énoncés justes. En conséquence, dans la suite du cours, on notera simplement « P » au lieu de « P est vraie ». Par exemple on notera : $\forall x \in \mathbb{R}$, $x^2 \geq 0$ et il ne viendra à l'idée de personne d'écrire :

« $\forall x \in \mathbb{R}$, $x^2 \geq 0$ est vrai »...

Arithmétique

Arithmétique

En guise d'introduction rappelons que les *nombres* : un, deux, trois... sont utilisés pour compter les éléments d'un ensemble d'objets. Le zéro est utilisé pour désigner l'absence d'objet dans un ensemble. Il a été introduit (seulement) au V$^{\text{ème}}$ siècle après J.C. par les indiens : c'était un concept plus difficile à créer tout simplement parce qu'à l'époque on ne comptait pas les éléments d'ensembles qui n'en avaient pas. L'Arithmétique est l'étude des nombres entiers.

Rappelons aussi que les *chiffres* : 0, 1, ..., 9 sont les symboles des dix premiers nombres. Dans la notation décimale, ils servent à écrire tous les nombres.

1 Les entiers

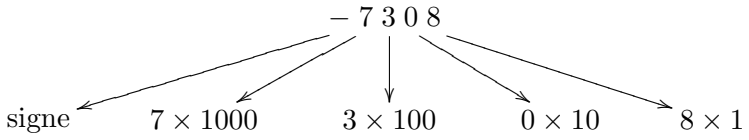
1.1 Entiers naturels et entiers relatifs

Les *entiers naturels* sont les nombres de l'ensemble

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

Les *entiers relatifs* sont les nombres de l'ensemble $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ c'est-à-dire les entiers naturels et leurs *opposés* ([1]).

La notation décimale d'un entier relatif utilise les symboles +, - et les chiffres de la façon suivante : « moins sept mille trois cent huit » est noté



1.2 Ordre et opérations sur les entiers

Il existe une relation d'*ordre* entre les entiers relatifs. On utilise la notation habituelle $m \leq n$ pour « m est inférieur ou égal à n » ainsi que les notations parentes $m < n$, $n \geq m$, $n > m$.

Les opérations de base sur les entiers sont l'*addition* et la *multiplication*. Soient m et n deux entiers relatifs avec $n > 0$. Une autre façon de voir le produit mn est de dire que c'est le multiple n-uple de m c'est-à-dire la répétition n fois de l'addition, i.e. $mn = m + \cdots + m$ (n termes). De même si on répète n fois la multiplication de m par lui-même on obtient la *puissance* $n^{\text{ème}}$ *de* m notée m^n : $m^n = m \times \cdots \times m$ (n termes). Cette opération a aussi un sens pour tout $m \in \mathbb{Z}$; enfin rappelons que par convention on pose $m^0 = 1$ si $m \neq 0$.

Nous supposons connues les propriétés élémentaires de ces opérations. Rappelons simplement une propriété essentielle qui est que ces opérations sont *compatibles* avec la relation d'ordre. Pour l'addition cela veut dire que pour tous entiers relatifs m, n, p, q on a

$$(m \leq n \quad \text{et} \quad p \leq q) \quad \Rightarrow \quad m + p \leq n + q$$

On déduit facilement une compatiblité similaire pour la multiplication mais soyez méfiants car pour l'écrire correctement il faut tenir compte du signe des entiers.

[1] On utilise les lettres $\mathbb{N}$ et $\mathbb{Z}$ pour les mots allemands *Nummer* et *Zahl*.

Exercice 1.2.1 Rappelons que pour tout entier naturel n, on appelle *factorielle de n* le nombre entier défini ([2]) par $n! \stackrel{\text{déf}}{=} 1 \times 2 \times \cdots \times n$ si $n \geq 1$, et $0! = 1$. Soient deux entiers $0 \leq k \leq n$. Le coefficient binômial C_n^k est défini par

$$\mathrm{C}_n^k \stackrel{\text{déf}}{=} \frac{n!}{k!(n-k)!}$$

On verra plus loin que, bien que cela ne soit pas évident, c'est bien un nombre entier.

(a) Démontrez que $\mathrm{C}_n^{n-k} = \mathrm{C}_n^k$ et que si $1 \leq k \leq n$, on a $k\mathrm{C}_n^k = n\mathrm{C}_{n-1}^{k-1}$.

(b) Démontrez que si $0 \leq k \leq n-1$ on a $\mathrm{C}_n^k + \mathrm{C}_n^{k+1} = \mathrm{C}_{n+1}^{k+1}$.

1.3 Le principe de récurrence

L'ensemble des entiers naturels $\mathbb{N}$ possède une propriété très intuitive qui a deux énoncés équivalents, contenus dans les propositions 1.3.1 et 1.3.2 qui suivent. Nous ne les démontrons pas : ce sont notre point de départ intuitif pour raisonner sur les nombres entiers. (Le fait qu'elles sont équivalentes est démontré en exercice.)

Proposition 1.3.1 *Tout ensemble non vide d'entiers naturels contient un entier inférieur ou égal à tous les autres.*

Cette popriété est équivalente à la suivante qui est le *principe de récurrence* :

Proposition 1.3.2 *Soit $n_0 \geq 0$ un entier. Soit $P(n)$ une propriété dépendant d'un nombre entier $n \geq n_0$. Supposons que*

(i) *$P(n_0)$ est vraie (P est initialisée), et*

(ii) *$P(n) \Rightarrow P(n+1)$ pour tout $n \geq n_0$ (P est héréditaire).*

Alors la propriété $P(n)$ est vraie pour tout $n \geq n_0$.

Donnons des exemples d'application.

Exemple 1.3.3 Comme application de la proposition 1.3.1, démontrons que tout nombre entier $n \geq 2$ est divisible par un nombre premier (un nombre premier est un nombre $p \geq 2$ qui n'a pour diviseurs positifs que 1 et lui-même). Soit donc $n \geq 2$ et soit E l'ensemble des entiers naturels $k \geq 2$ qui divisent n. On a $n \in E$ donc E n'est pas vide : d'après la proposition 1.3.1 il possède donc un plus petit élément p. Ce nombre p est forcément premier car si r est un de ses diviseurs on a soit $r = 1$, soit $r \in E$. Or lorsque $r \in E$ on a $p \leq r$ (car p est plus petit que tous les éléments de E) et $r \leq p$ (car r divise p) donc $r = p$.

Exercice 1.3.4 Montrer par récurrence que les coefficients binomiaux C_n^k sont entiers.
(*Indication* : prendre pour $P(n)$: « pour tout k tel que $0 \leq k \leq n$ on a $\mathrm{C}_n^k \in \mathbb{N}$ ».)

Exemple 1.3.5 Démontrons par récurrence la formule du *binôme de Newton* : pour tout $n \geq 1$ et tout couple (x, y) de nombres entiers, réels ou même complexes on a

$$(x+y)^n = \sum_{k=0}^{n} \mathrm{C}_n^k x^k y^{n-k} \ .$$

[2] Une remarque de notation : lorsqu'on utilise le signe « = » pour définir un objet mathématique il est parfois préférable d'utiliser le signe « $\stackrel{\text{déf}}{=}$ » pour ne pas confondre avec le « = » utilisé pour noter une *égalité*.

(On rappelle que $\sum_{k=0}^{n} a_k$ désigne la somme $a_0 + a_1 + \cdots + a_n$.)
Initialisation : pour $n = 1$ l'égalité est claire.
Hérédité : si la propriété est vraie pour un entier $n \geq 1$ alors

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n} \mathrm{C}_n^k x^k y^{n-k} \\ &= x(\mathrm{C}_n^0 x^0 y^n + \cdots + \mathrm{C}_n^n x^n y^0) + y(\mathrm{C}_n^0 x^0 y^n + \cdots + \mathrm{C}_n^n x^n y^0) \\ &= (0 + \mathrm{C}_n^0)x^0 y^{n+1} + \cdots + (\underbrace{\mathrm{C}_n^{k-1} + \mathrm{C}_n^k}_{\mathrm{C}_{n+1}^k})x^k y^{n+1-k} + \cdots + (\mathrm{C}_n^n + 0)x^{n+1}y^0 \\ &= \sum_{k=0}^{n+1} \mathrm{C}_{n+1}^k x^k y^{n+1-k}\ .\end{aligned}$$

Conclusion : la propriété est initialisée à $n = 1$ et héréditaire, donc par le principe de récurrence elle est vraie pour tout $n \geq 1$.

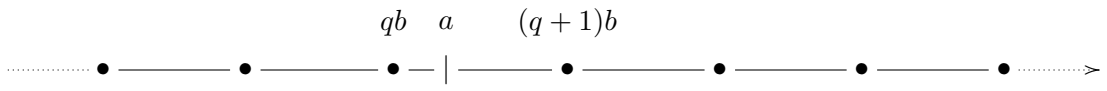
2 La division euclidienne

La division euclidienne est l'un des piliers de l'arithmétique. Comme nous allons le voir, elle est à la base du système de numération en base dix utilisé aujourd'hui.

On sait peu de choses sur Euclide. Il vécut aux alentours de -300, enseigna et écrivit au Musée et à la Bibliothèque d'Alexandrie. Son traité *Les Éléments*, composé de treize *livres*, a un style et une profondeur qui en font l'un des textes mathématiques les plus importants de tous les temps. La division euclidienne (connue en fait bien avant Euclide) est démontrée dans le *Livre VII*.

2.1 Le théorème de division euclidienne

Soient a et b deux entiers naturels, avec $b \neq 0$. Si a est un multiple de b on a $a = bq$ pour un certain entier q. Si ce n'est pas le cas, on peut essayer d'approcher a à l'aide de multiples de b. Pour faire cela, on place a ainsi que tous les multiples de b sur l'axe des nombres entiers, et on constate que a est situé *entre deux de ces multiples, bien déterminés* :



(si a est un multiple de b on choisit l'intervalle qui est à sa droite). Ceci explique le théorème suivant :

Théorème 2.1.1 *Soient deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}$ avec $b > 0$. Alors, il existe un unique couple d'entiers $(q, r) \in \mathbb{Z}^2$, tel que*

(i) $a = bq + r$

(ii) $0 \leq r < b$.

Cette écriture s'appelle la division euclidienne *de a par b. On dit que a est le* dividende*, b le* diviseur*, q le* quotient *et r le* reste*.*

Pour démontrer cela l'idée est de chercher d'abord q, et pour cela de regarder l'ensemble de tous les multiples de b qui sont plus grands que a. Précisément :

Démonstration : Pour simplifier la démonstration, on suppose que $a \geq 0$. Soit alors $E \overset{\text{déf}}{=} \{\, k \in \mathbb{N}\,,\ kb > a \,\}$. Cet ensemble est non vide, en effet, en utilisant le fait que $b \geq 1$ on voit que $a+1 \in E$. Donc d'après 1.3.1 il possède un plus petit élément u. Soit $q = u-1$. Comme $q \notin E$ et $q+1 \in E$ on a $qb \leq a < (q+1)b$. Donc $r = a - bq$ vérifie : $0 \leq r < b$.

Montrons maintenant que ce couple (q, r) qui a les propriétés requises, est unique. Supposons qu'on ait deux écritures $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$. On a alors $|r' - r| < b$ et simultanément $r' - r$ est un multiple de b car $r' - r = b(q - q')$. Donc nécessairement $r' - r = 0$ et par conséquent $q' - q = 0$ également. □

En pratique, comme vous le savez, on pose la division ainsi :

dividende →	381	7	← diviseur
	-350	54	← quotient
	31		
	-28		
reste →	3		

Exercice 2.1.2 Samy range 461 pots de yaourt dans des caisses. Il ne commence pas une caisse avant d'avoir fini la précédente. À la fin il a rangé les pots dans 14 caisses. Combien de pots contiennent les caisses pleines ? Combien de pots contient la dernière caisse ?

L'application la plus importante du théorème de division euclidienne est l'écriture en base b qui permet d'écrire tous les nombres avec un nombre fini de symboles.

2.2 Écriture d'un entier en base b

Regardons le cas de la base $b = 10$ qui nous est familier. On effectue successivement les divisions euclidiennes par 10 de $a = 7308$ puis des quotients qui apparaissent :

$$\begin{array}{rcrll} 7308 & = & 730 \times 10 + 8 & \text{on pose} & a_1 \overset{\text{déf}}{=} 730 \quad \text{(c'est le quotient)} \\ 730 & = & 73 \times 10 + 0 & \text{〃} & a_2 \overset{\text{déf}}{=} 73 \\ 73 & = & 7 \times 10 + 3 & \text{〃} & a_3 \overset{\text{déf}}{=} 7 \\ 7 & = & 0 \times 10 + 7 & \text{et on a} & a_4 \overset{\text{déf}}{=} 0 \end{array}$$

On voit que les restes r_0, r_1, r_2, r_3 de ces divisions euclidiennes donnent la suite des chiffres de l'écriture en base dix du nombre $a = 7308$ à savoir $7308 = 7 \times 10^3 + 3 \times 10^2 + 0 \times 10^1 + 8$. Plus généralement :

Théorème 2.2.1 *Soit $b \geq 2$ un entier. Alors pour tout entier $a \geq 1$ il existe un unique n et d'uniques entiers $r_0, \ldots, r_n$ tels que*

(i) $a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$ *avec $r_n \neq 0$, et*

(ii) $0 \leq r_i < b$ *pour tout i.*

*Cette écriture est appelée l'*écriture de a en base b*, et les r_i sont ses* chiffres*.*

Démonstration : Montrons d'abord l'unicité. Supposons qu'existe une écriture $a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$ avec la condition (ii). Alors r_0 est le reste de la division euclidienne de a par b, qui est unique d'après le théorème de division euclidienne. Posons $a_0 \overset{\text{déf}}{=} a$ et $a_1 \overset{\text{déf}}{=} \frac{a_0 - r_0}{b}$ qui est égal à $r_n b^{n-1} + r_{n-1} b^{n-2} + \cdots + r_1$. Alors r_1 est le reste de la division euclidienne de a_1 par b. On continue en définissant par récurrence $a_i \overset{\text{déf}}{=} \frac{a_{i-1} - r_{i-1}}{b}$. On voit que $a_i = r_n b^{n-i} + \cdots + r_i$ et donc r_i est le reste de la division euclidienne de a_i par b, unique donc. Enfin le nombre n est bien déterminé comme étant le premier instant i du processus où $a_i = r_i$. On a montré que les nombres n et $r_0, \ldots, r_n$ s'ils existent, sont uniquement déterminés.

Montrons maintenant l'existence. Vu ce qui précède on sait comment faire : on effectue des divisions euclidiennes successives (en notant a_i les quotients et r_i les restes) :

$$\begin{array}{rcll} a & = & ba_1 + r_0 & (0 \leq r_0 < b) \\ a_1 & = & ba_2 + r_1 & (0 \leq r_1 < b) \\ & \vdots & & \\ a_k & = & ba_{k+1} + r_k & (0 \leq r_k < b) \\ & \vdots & & \end{array}$$

Comme $b \geq 2$, les a_k sont de plus en plus petits : $a_{k+1} \leq \frac{1}{b} a_k < a_k$. Donc il vient un instant où $a_n < b$ c'est-à-dire $a_n = r_n$ et $a_{n+1} = 0$. En remplaçant successivement a, a_1, $a_2 \ldots$ par leurs expressions ci-dessus on a

$$\begin{aligned} a &= a_1 b + r_0 = a_2 b^2 + r_1 b + r_0 = a_3 b^3 + r_2 b^2 + r_1 b + r_0 = \ldots \\ &= r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0 \end{aligned}$$

ce qui est l'écriture recherchée. □

Le nombre 0, quant à lui, s'écrit 0 dans toutes les bases (son écriture en base b a cependant cela de particulier qu'elle ne vérifie pas la condition $r_n \neq 0$).

2.3 Notation de l'écriture en base b et exemples de bases

Pour noter un nombre a à l'aide de ses chiffres en base b on écrira $a = \overline{r_n r_{n-1} \ldots r_0}_{(b)}$. Cela veut dire exactement que $a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$. Dans le cas de la base $b = 10$, quand ça ne risquera pas de prêter à confusion on notera comme d'habitude $r_n r_{n-1} \ldots r_0$ plutôt que $\overline{r_n r_{n-1} \ldots r_0}_{(\text{dix})}$.

Exemple 2.3.1 Le théorème 2.2.1 nous apprend qu'on peut représenter tous les entiers déjà à l'aide de $b = 2$. On parle d'écriture *binaire*. Ce choix de base est particulièrement adapté aux ordinateurs : la tension aux bornes de leurs circuits physiques (des transistors utilisés comme interrupteurs) ne peut prendre que deux valeurs qu'on note 0 et 1. Toute information est codée dans un ordinateur à l'aide de 0 et de 1. Ce sont ces deux symboles qu'on utilise pour écrire les nombres en binaire. Par exemple le nombre $17 = 2^4 + 1$ s'écrit 10001 en binaire.

Voici, en exemple, comment écrire 13 en binaire. La première division euclidienne s'écrit $13 = 6 \times 2 + 1$ et donc le chiffre des unités est 1. La deuxième division euclidienne (celle du quotient, 6, par le diviseur qui est toujours 2) est $6 = 3 \times 2 + 0$ donc le chiffre des dizaines est 0. La troisième division euclidienne est $3 = 1 \times 2 + 1$ donc le chiffre des centaines est 1. La quatrième division euclidienne est $1 = 2 \times 0 + 1$ donc le chiffre des

milliers est 1. Et ici, le quotient est 0 donc c'est fini ! Ainsi, le nombre 13 s'écrit 1101 en base 2, c'est-à-dire

$$\overline{13}_{(\text{dix})} = \overline{1101}_{(\text{deux})}$$

Remarquons que les nombres qui remplacent 10, 100, 1000, ... sont ici 2, 4, 8, ... et donc on devrait dire les *deuzaines*, les *quatraines*, les *huitaines* au lieu des *dizaines*, *centaines*, *milliers*. Un autre problème de notation est que si la base b est grande, pour écrire les nombres en base b il faut avoir fait un choix de b symboles pour désigner $0, 1, \ldots, b-1$. Si $b > 10$ comme dans l'exemple suivant, on n'a pas de symbole évident à disposition !

Exemple 2.3.2 Une autre base utilisée parfois est $b = 16$. On parle d'écriture *hexadécimale*. La raison de son utilisation est aussi liée à l'ordinateur et à la base 2. Ses chiffres sont $0, 1, \ldots, 9, A, B, C, D, E, F$ qui désignent les 16 premiers entiers (A pour 10, etc). Ainsi, en hexadécimal $1B2$ représente le nombre $1 \times 16^2 + 11 \times 16 + 2 = 434$ (en base dix) et $\overline{45}_{(\text{dix})}$ s'écrit $2D$ en hexadécimal.

2.4 Repères historiques sur la numération

À l'aube de l'Humanité. La nécessité de compter s'est faite ressentir très tôt : par exemple un berger devait pouvoir compter les brebis de son troupeau, et clairement les mains ne suffisent pas très longtemps pour faire cela.

Égyptiens et Babyloniens. L'Homme a su compter avant de savoir écrire : dès -3000 les Égyptiens écrivirent les nombres en les notant sous forme de hiéroglyphes. Les Babyloniens écrivirent les nombres avec leur écriture cunéiforme ([3]). Pour les calculs les Babyloniens avaient déjà un système à base ; la base utilisée était 60 ce qui a laissé quelques traces dans les systèmes de numération que l'on utilise aujourd'hui (minutes, secondes).

En Extrême-Orient. Les Chinois et les Indiens aussi ont compté très tôt mais on a moins de traces de leurs mathématiques avant le Moyen-Âge. Les Chinois avaient des symboles pour les nombres de 1 à 9 et pour les puissances de 10. Faute de pouvoir manipuler des dessins chinois, notons ♯ à la place du symbole que les chinois utilisaient pour 10 et ♠ pour 100 : le nombre 729 était noté 7♠2♯9. Observez que c'est très similaire à notre numération *parlée* : les puissances de dix n'ont de nom que jusqu'à une certaine taille, dans tous les langages ([4])... On peut cependant nommer des nombres très grands, ainsi, sur le site internet donné en note de bas de page, on indique que le nombre 14 526 329 784 152 563 412 741 se prononce « 14 mille 526 trillions 329 mille 784 billions 152 mille 563 millions 412 mille 741 unités ». Son ordre de grandeur est 10^{22}.

Les romains. Ils avaient des symboles pour les puissances de 10 seulement, et ils les juxtaposaient pour écrire tous les nombres. C'est donc un système de numération additif. Les symboles de 1, 10, 100, 1000 sont I, X, C, M. Par la suite le système fut rafiné avec l'introduction d'un symbole pour 5 (V) et ses décuples 50 (L), 500 (D).

Le système à base dix utilisée aujourd'hui. Dans ce système, les chiffres n'ont pas la même siginification selon leur place dans l'écriture du nombre (729 et 297 ne sont pas le même nombre !). Pour cette raison, on dit que c'est un système de numération *positionnel à base dix*. Par opposition, les systèmes tels que la numération romaine ou égyptienne sont dits *systèmes de numération non positionnels additifs*. Les systèmes positionnels permettent d'écrire des nombres aussi grands qu'on veut, et par ailleurs, ils facilitent grandement le traitement des opérations (addition-soustraction, multiplication-division).

[3] Voir http://classes.bnf.fr/dossiecr/in-cunei.htm

[4] Voir http://perso.club-internet.fr/petrequin/mathema/traites/gnombres/gn_nombres.html

3 Divisibilité et congruences

3.1 Premières propriétés

Définition 3.1.1 Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On dit que b *divise* a lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = qb$. On note alors $b|a$. On dit aussi que a *est multiple de* b, ou que b *est un diviseur de* a.

Par exemple, 1 divise tout entier ; tout entier divise 0 ; et l'ensemble des diviseurs de 25 est $\{-25, -5, -1, 1, 5, 25\}$. Souvent on ne mentionnera que l'ensemble des diviseurs dans $\mathbb{N}$; pour 25 c'est $\{1, 5, 25\}$. Il est clair que si a_1 et a_2 sont multiples de b alors il en est de même pour $a_1 + a_2$, $a_1 - a_2$ et aussi na_1 pour tout entier n.

Définition 3.1.2 Soit $n > 0$ un entier naturel. On dit que deux entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ sont *congrus entre eux modulo* n lorsque n divise $a - b$. Plusieurs notations sont utilisées :

$$a \equiv b \bmod n \quad \text{ou} \quad a \equiv b \pmod{n} \quad \text{ou parfois} \quad a \equiv b\,(n)$$

Un entier $a \geq 1$ est congru modulo n à exactement *un* entier compris entre 0 et $n - 1$, qui n'est rien d'autre que le reste de la division euclidienne de a par n. En particulier :

Remarque 3.1.3 (cruciale) C'est la même chose de dire « n divise a » ou « $a \equiv 0\,(n)$ ».

La relation de congruence modulo n est vraiment très importante du fait qu'elle se comporte comme une égalité à bien des égards :

Proposition 3.1.4 *Soit a, a', b, b', c des entiers relatifs, et $k \in \mathbb{N}$. Alors on a :*

(1)	$a \equiv a\,(n)$	(réflexivité)
(2)	*si* $a \equiv b\,(n)$ *alors* $b \equiv a\,(n)$	(symétrie)
(3)	*si* $a \equiv b\,(n)$ *et* $b \equiv c\,(n)$ *alors* $a \equiv c\,(n)$	(transitivité)
(4)	*si* $a \equiv b\,(n)$ *et* $a' \equiv b'\,(n)$ *alors* $a + a' \equiv b + b'\,(n)$	(compatibilité avec $+$)
(5)	*si* $a \equiv b\,(n)$ *alors* $-a \equiv -b\,(n)$	(compatibilité avec $-$)
(6)	*si* $a \equiv b\,(n)$ *et* $a' \equiv b'\,(n)$ *alors* $aa' \equiv bb'\,(n)$	(compatibilité avec $\times$)
(7)	*si* $a \equiv b\,(n)$ *alors* $a^k \equiv b^k\,(n)$	(comp. avec les puissances)

Démonstration : D'abord (1), (2) et (5) sont évidentes. Ensuite :

(3) découle du fait que si $a - b = nq_1$ et $b - c = nq_2$ alors $a - c = n(q_1 + q_2)$.

(4) découle du fait que si $a - b = nq_1$ et $a' - b' = nq_2$ alors $(a + a') - (b + b') = n(q_1 + q_2)$.

(6) découle du fait que si $a - b = nq_1$ et $a' - b' = nq_2$ alors

$$aa' - bb' = a(a' - b') + (a - b)b' = anq_2 + b'nq_1 = n(aq_2 + b'q_1)$$

(on fait apparaître « de force » les différences $a - b$ et $a' - b'$ qui nous intéressent).

(7) se déduit de (6) par récurrence, ou bien directement, car si $a - b = nq_1$ alors

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}) = nq_1(a^{k-1} + \cdots + b^{k-1})\,.$$

□

En revanche, on se méfiera du fait que cela n'a pas de sens en général de vouloir utiliser la relation d'ordre avec les congruences. Par exemple on voit bien que l'inégalité $8 \leq 12$ ne « passe pas » modulo 5 puisque $8 \equiv 3\,(5)$ et $12 \equiv 2\,(5)$. Mais comme le dit la proposition, l'addition « passe » modulo 5. Ainsi, dans ce cas particulier, on a $8 + 12 \equiv 20 \equiv 0\,(5)$ et on a bien $3 + 2 \equiv 5 \equiv 0\,(5)$.

3.2 Calcul modulo n

À l'école primaire, on a appris les tables d'addition et de multiplication des nombres entiers, qui sont des tables infinies (on n'en a appris que le début). Le résultat de la proposition précédente nous permet de faire pareil avec les *restes modulo* n, c'est-à-dire les restes des divisions euclidiennes par n : les nombres 0, 1, ..., $n-1$. En effet, la proposition nous dit que les calculs arithmétiques usuels (addition, soustraction, multiplication, puissances) sont compatibles à la congruence modulo n. On obtient des tables finies, qui n'ont que n lignes et n colonnes. Voici un exemple, celui du calcul modulo 5.

Table d'addition modulo 5 : dans les cases du tableau, on lit $a+b$ modulo 5, c'est-à-dire le reste de la division euclidienne de $a+b$ par 5.

a \b	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table de multiplication modulo 5 : dans les cases du tableau, on lit $a \times b$ modulo 5, c'est-à-dire le reste de la division euclidienne de $a \times b$ par 5.

a \b	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table des carrés modulo 5 : on lit a^2 modulo 5, reste de la division euclidienne de a^2 par 5.

a	0	1	2	3	4
a^2	0	1	4	4	1

3.3 Critères de divisibilité

Une application immédiate de la notion de congruence est de démontrer les critères classiques de divisibilité ([5]). Soit a un entier, écrit $r_n r_{n-1} \dots r_1 r_0$ en base dix. Les principaux critères à connaître sont les suivants :

2, 5 et 10

- a est divisible par 2 si et seulement si son dernier chiffre r_0 est divisible par 2.
- a est divisible par 5 si et seulement si son dernier chiffre r_0 est divisible par 5.
- a est divisible par 10 si et seulement si son dernier chiffre r_0 est nul.

4 et 25

- a est divisible par 4 si et seulement si le nombre $r_1 r_0$ (en base dix) formé par ses deux derniers chiffres, est divisible par 4.
- a est divisible par 25 si et seulement si le nombre $r_1 r_0$ (en base dix) formé par ses deux derniers chiffres, est divisible par 25.

3 et 9

- a est divisible par 3 si et seulement si la somme des chiffres de son écriture décimale $r_n + \dots + r_0$ est divisible par 3.

[5] Un critère est une condition *suffisante*. Souvent le mot est utilisé aussi (c'est un léger abus) pour signifier une condition *nécessaire et suffisante*. C'est le cas ici.

• a est divisible par 9 si et seulement si la somme des chiffres de son écriture décimale $r_n + \cdots + r_0$ est divisible par 9.

Démonstration : Démontrons seulement les critères de divisibilité par 2 et 9.

Étant donnée l'écriture en base dix $a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$ on voit que $a \equiv r_0\,(2)$. Donc $a \equiv 0\,(2)$ si et seulement si $r_0 \equiv 0\,(2)$ qui est le critère recherché pour la divisibilité par 2.

Pour 9 il suffit de remarquer que $10 \equiv 1(9)$ donc $10^k \equiv 1^k \equiv 1(9)$ pour tout $k \geq 0$. Donc $a \equiv r_n + r_{n-1} + \cdots + r_1 + r_0(9)$. Donc $a \equiv 0(9)$ si et seulement si $r_n + r_{n-1} + \cdots + r_1 + r_0 \equiv 0(9)$.

Prouvez les autres critères en exercice. □

4 Plus grand commun diviseur, plus petit commun multiple

4.1 Le pgcd

Proposition et définition 4.1.1 *Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}$, non tous les deux nuls. L'ensemble des diviseurs communs de a et b dans $\mathbb{N}$ est fini et non vide. Il a un plus grand élément qu'on appelle leur* plus grand commun diviseur *noté* $\mathrm{pgcd}(a, b)$.

Démonstration : Par hypothèse a ou b est non nul, disons a. Alors les diviseurs de a et b dans $\mathbb{N}$ sont inférieurs à a, donc ils forment un ensemble fini, non vide car 1 en fait partie. Cet ensemble a donc un plus grand élément. □

Définition 4.1.2 On dit que a et b sont *premiers entre eux* ssi $\mathrm{pgcd}(a, b) = 1$.

Voici quelques exemples. On ne regarde que les diviseurs dans $\mathbb{N}$.

(a) Les diviseurs communs de 24 et 30 sont $1, 2, 3, 6$ et leur pgcd est donc 6.

(b) Le seul diviseur commun de 24 et 25 est 1 donc leur pgcd est 1. Ils sont premiers entre eux.

(c) Si $b|a$ alors $\mathrm{pgcd}(a, b) = b$. Par exemple $\mathrm{pgcd}(a, 1) = 1$.

4.2 Algorithme d'Euclide et théorème de Bézout

Proposition 4.2.1 *Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}$, non tous les deux nuls. Effectuons la division euclidienne de a par b, soit $a = bq + r$ avec $0 \leq r < b$. Alors les diviseurs communs de a et b sont les mêmes que ceux de b et r, en particulier,* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.

Démonstration : Comme $r = a - bq$ il est clair qu'un diviseur commun de a et b divise b et r. De même comme $a = bq + r$ un diviseur commun de b et r divise a et b. □

Supposons que $b < a$. En changeant a et b par b et r on ne change pas le pgcd. Ce qui est très utile là-dedans, c'est que les nombres considérés maintenant sont moins grands et on peut itérer le processus : b devient le nouveau dividende, r devient le nouveau diviseur et on peut refaire une division euclidienne. Ainsi pour 490 et 154,

$$\begin{aligned} 490 &= 3 \times 154 + 28 \\ 154 &= 5 \times 28 + 14 \\ 28 &= 2 \times 14 + 0 \end{aligned}$$

Tant que les restes des divisions euclidiennes effectuées sont non nuls ils sont strictement décroissants : $154 > 28 > 14 > \dots$ Donc ils finissent par s'annuler, ce qui met fin au processus. À ce moment-là on calcule $\text{pgcd}(490, 154) = \text{pgcd}(154, 28) = \text{pgcd}(28, 14) = 14$. On voit que le pgcd est le dernier reste non nul du processus de divisions euclidiennes par les restes successifs.

Le résultat général est le suivant :

Théorème 4.2.2 (Algorithme d'Euclide) *Soient $a \in \mathbb{N}$, $b \in \mathbb{N}$ avec $b < a$. On pose $r_0 \overset{\text{déf}}{=} a$ et $r_1 \overset{\text{déf}}{=} b$. Par récurrence, tant que $r_k \neq 0$ on définit r_{k+1} comme étant le reste de la division euclidienne de r_{k-1} par r_k :*

$$r_{k-1} = r_k q_k + r_{k+1} \qquad \text{avec} \quad 0 \leq r_{k+1} < r_k$$

Le pgcd *de a et b est le dernier reste non nul de cet algorithme.*

Démonstration : On a une suite strictement décroissante $r_0 > r_1 > r_2 > \dots$ constituée par les restes non nuls successifs. Elle forme un sous-ensemble non vide de $\mathbb{N}$ donc elle a un plus petit élément (prop. 1.3.1) noté r_n. On a donc $r_{n+1} = 0$ (car sinon il serait strictement inférieur à r_n) c'est-à-dire $r_n | r_{n-1}$. D'après la proposition 4.2.1 on a :

$$\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$$

c'est ce que l'on voulait. □

Le mot *algorithme* vient du nom d'un grand mathématicien arabe, Al-Khwārizmī (780-850). Le mot algèbre vient du mot arabe *al-jabr* que l'on peut traduire par *restaurer* (pour les mathématiciens arabes, *al-jabr* signifiait faire passer de l'autre côté d'une équation une quantité qui était « soustraite » pour la transformer en quantité « ajoutée »). Les mots *chiffre* et *zéro* dérivent tous les deux du mot arabe *sifr*, lui-même provenant du sanscrit *sūnyā* qui signifiait *vide*.

Théorème 4.2.3 (Bézout) *Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}$, non tous les deux nuls, et notons $d = \text{pgcd}(a, b)$. Alors,*

(1) *Il existe $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$ tels que $d = \lambda a + \mu b$.*

(2) *a et b sont premiers entre eux si et seulement s'il existe $\lambda, \mu \in \mathbb{Z}$ tels que $1 = \lambda a + \mu b$.*

Démonstration : En fait la propriété (1) est vraie pour tous les restes de l'algorithme d'Euclide, pas seulement le dernier : pour tout $k \geq 0$ il existe λ_k, μ_k tels que $r_k = \lambda_k a + \mu_k b$. Pour $k = 0$ et $k = 1$ c'est clair car $r_0 = a$ (prendre $\lambda = 1$, $\mu = 0$) et $r_1 = b$ ($\lambda = 0$, $\mu = 1$). Par récurrence il suffit maintenant de prouver que cette propriété ([6]) est héréditaire. Or d'après la division euclidienne $r_{k-1} = r_k q_k + r_{k+1}$ on a

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k = (\lambda_{k-1} a + \mu_{k-1} b) - (\lambda_k a + \mu_k b) q_k \\ &= (\lambda_{k-1} - \lambda_k q_k) a + (\mu_{k-1} - \mu_k q_k) b \end{aligned}$$

d'où le résultat découle en posant $\lambda_{k+1} \overset{\text{déf}}{=} \lambda_{k-1} - \lambda_k q_k$ et $\mu_{k+1} \overset{\text{déf}}{=} \mu_{k-1} - \mu_k q_k$.

Passons à (2). Si a et b sont premiers entre eux on a $d = 1$ donc il existe $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$ tels que $1 = \lambda a + \mu b$ d'après (1). Réciproquement si $1 = \lambda a + \mu b$ alors soit d un diviseur commun de a et b dans $\mathbb{N}$, il divise $\lambda a + \mu b$, donc divise 1, donc $d = 1$. □

[6] Quelle propriété $P(k)$ doit-on prendre exactement pour faire fonctionner la récurrence ?

Étienne Bézout (1730-1783) est un mathématicien français né à Nemours. Il laissa son nom au théorème qui est dans notre cours ainsi qu'à un théorème de Géométrie Algébrique qui compte le nombre de points d'intersection de deux courbes planes définies par des polynômes (en deux variables x, y) de degrés m et n.

L'algorithme d'Euclide donne un moyen de *déterminer pratiquement* (algorithmiquement) *une relation de Bézout*. La règle est la suivante. Les divisions euclidiennes de l'algorithme d'Euclide s'écrivent $r_{k-1} = r_k q_k + r_{k+1}$ (avec $0 \leq r_{k+1} < r_k$). On les « renverse » :

$$r_{k+1} = r_{k-1} - r_k q_k$$

et on remonte le calcul en partant du pgcd : $d = r_n = r_{n-2} - r_{n-1}q_{n-1} = \dots$ en remplaçant successivement les restes.

Exemple 4.2.4 Traitons en exemple le cas $a = 1197$ et $b = 210$. L'algorithme d'Euclide donne

$$\begin{aligned} 1197 &= 5 \times 210 + 147 \\ 210 &= 1 \times 147 + 63 \\ 147 &= 2 \times 63 + 21 \\ 63 &= 3 \times 21 \end{aligned}$$

Donc $\text{pgcd}(1197, 210) = 21$ et en remontant les divisions :

$$\begin{aligned} 21 = &\ 147 - 2 \times 63 = 147 - 2 \times (210 - 147) = 3 \times 147 - 2 \times 210 \\ = &\ 3 \times (1197 - 5 \times 210) - 2 \times 210 = 3 \times 1197 - 17 \times 210 \end{aligned}$$

C'est une relation de Bézout.

Exercice 4.2.5 (1) Soient a, b, c des entiers naturels non nuls. On suppose que a est premier avec b et premier avec c. Montrez qu'il est premier avec bc. (*Indic : écrivez deux relations de Bézout et multipliez-les entre elles.*)

(2) Soient a, b, m, n des entiers naturels non nuls. Montrez que a est premier avec b ssi a^m est premier avec b^n. (*Indic : un sens est facile. Pour l'autre sens, écrivez une relation de Bézout et élevez-la à la puissance $m+n-1$. Utilisez la formule du binôme de Newton 1.3.5 et, dans la somme obtenue, montrez que pour chaque valeur de l'indice k, soit l'exposant de a est $\geq m$, soit l'exposant de b est $\geq n$.*)

4.3 Propriétés importantes du pgcd

Lemme 4.3.1 (Lemme de Gauß) *Soient a, b, c des entiers naturels avec* $\text{pgcd}(a, b) = 1$. *Si $a|bc$ alors $a|c$.*

Démonstration : Comme $\text{pgcd}(a, b) = 1$, il existe $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$ tels que $1 = \lambda a + \mu b$. Si a divise bc alors a divise $\lambda ac + \mu bc = c$. □

Karl Friedrich Gauß (1777-1855) est né dans une famille de paysans ruinés venus s'installer dans la ville de Brunswick. Son génie mathématique se manifesta très tôt : en 1791, le Duc de Brunswick lui donna une bourse pour recevoir le meilleur enseignement possible. Il publia à 24 ans ses travaux en Arithmétique, les *Disquisitiones Arithmeticæ*. En 1807 il obtint un poste à l'Université de Göttingen où il resta jusqu'à la fin de sa vie. Gauß publia peu car il n'était jamais entièrement satisfait de ce qu'il avait écrit. Ses travaux couvrent aussi l'astronomie, l'électricité, l'électromagnétisme...
Plus de détails sont sur http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html

Proposition 4.3.2 *Soient $a \in \mathbb{N}$, $b \in \mathbb{N}$ non tous les deux nuls et $d = \text{pgcd}(a, b)$. Tout diviseur commun de a et b divise d.*

Démonstration : D'après le théorème de Bézout, il existe $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$ tels que $\lambda a + \mu b = d$. Si e divise a et b, il divise $\lambda a + \mu b$ c'est-à-dire d. □

Voici un résultat très utile lorsqu'on manipule des pgcd :

Proposition 4.3.3 *Soient a, b des entiers naturels, non tous deux nuls. Soit $d \in \mathbb{N}$. Alors $d = \text{pgcd}(a, b)$ si et seulement s'il existe des entiers naturels a' et b' tels que $a = da'$, $b = db'$ avec $\text{pgcd}(a', b') = 1$.*

Démonstration : Si $d = \text{pgcd}(a, b)$ alors il existe des entiers naturels a', b' tels que $a = da'$ et $b = db'$. De plus, si e est un diviseur commun de a' et b' alors de divise a et b donc $de \leq \text{pgcd}(a, b) = d$, donc $e = 1$.

Réciproquement supposons que $a = da'$ et $b = db'$ avec $\text{pgcd}(a', b') = 1$. On a une relation de Bézout $\lambda a' + \mu b' = 1$ donc $\lambda a + \mu b = d$. Ceci montre que si e est un diviseur commun de a et b il divise d. En particulier, $e \leq d$ donc $d = \text{pgcd}(a, b)$. □

Exercice 4.3.4 Cet exercice est la suite de l'exercice 4.2.5.

(1) Soient a, b entiers naturels non nuls et $d \overset{\text{déf}}{=} \text{pgcd}(a, b)$. Montrez que $\text{pgcd}(a^n, b^n) = d^n$. (*Indic : utilisez la proposition 4.3.3 et l'exercice 4.2.5(2).*)

(2) Soient a, b, n entiers naturels non nuls. Montrez que $a^n | b^n$ si et seulement si $a | b$. (*Indic : utilisez le fait que $x | y$ ssi $\text{pgcd}(x, y) = x$, ainsi que la question précédente.*)

(3) Soient a, b, n entiers naturels non nuls. On suppose que a et b sont premiers entre eux. Montrez que si ab est une puissance n-ième, alors a et b sont des puissances n-ièmes. (*Indic : écrivez $ab = r^n$ et posez $i = \text{pgcd}(a, r)$, $j = \text{pgcd}(b, r)$. Calculez i^n et j^n en utilisant la question (1).*)

4.4 Le ppcm

Le ppcm est le pendant du pgcd, pour les multiples au lieu des diviseurs. Étant donnés deux entiers naturels a et b non nuls, l'ensemble des multiples communs non nuls de a et b dans $\mathbb{N}$ est non vide car il contient ab. D'après la proposition 1.3.1 il contient un plus petit élément, ce qui justifie la définition suivante :

Définition 4.4.1 Soient a et b entiers naturels non nuls. L'ensemble des multiples communs non nuls de a et b dans $\mathbb{N}$ a un plus petit élément qu'on appelle leur *plus petit commun multiple* noté $\text{ppcm}(a, b)$. Si a ou b est nul on peut encore définir leur ppcm par $\text{ppcm}(a, b) = 0$.

Exemples 4.4.2 Pour les exemples situés après la définition 4.1.2, vérifiez que les ppcm sont (a) 120 (b) 600 (c) a.

Le lien entre pgcd et ppcm peut être précisé comme suit :

Proposition 4.4.3 *Soient a, b entiers naturels non tous les deux nuls. Soient $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$. On a alors : $ab = dm$.*

Démonstration : On écrit $a = da'$, $b = db'$ avec $\text{pgcd}(a', b') = 1$. On va montrer que $m = da'b'$. Tout d'abord il est clair que $da'b' = ab' = a'b$ est un multiple commun de a et b. Étant donné un autre multiple commun n on va montrer que $da'b' \leq n$, et même que $da'b'|n$. En effet, par hypothèse il existe n_1, n_2 tels que $n = an_1 = bn_2$. Divisant par d on obtient $a'n_1 = b'n_2$. En particulier $a'|b'n_2$ donc d'après le lemme de Gauß il existe n_3 tel que $n_2 = a'n_3$. Par conséquent $n = ba'n_3 = da'b'n_3$.

En conclusion $ab = da'db' = dm$. □

Remarquons que la démonstration a prouvé l'équivalent de la propriété de 4.3.2 pour le ppcm : *tout multiple commun de a et b est divisible par leur* ppcm. En particulier :

Proposition 4.4.4 *Soient $a_1, \ldots, a_k$ des entiers strictement positifs et premiers entre eux deux à deux (c'est-à-dire* $\text{pgcd}(a_i, a_j) = 1$ *pour deux quelconques d'entre eux). Soit $n \in \mathbb{N}$. Si tous les a_i divisent n alors leur produit divise n.*

Démonstration : Pour $k = 2$: soit $m = \text{ppcm}(a_1, a_2)$, d'après ce qui précède on a $m|n$, or $m = a_1a_2$ par 4.4.3. Pour $k > 2$ c'est identique par récurrence sur k (il faut utiliser le résultat de l'exercice 4.2.5(1)). □

Évidemment, l'hypothèse que les entiers a_i soient premiers entre eux deux à deux est essentielle. Déjà pour $k = 2$, on peut trouver un contre-exemple à la proposition si cette hypothèse n'est pas vérifiée : on prend $a_1 = 6$, $a_2 = 10$, et $n = 30$.

5 Nombres premiers

5.1 Définition et propriétés importantes

Définition 5.1.1 Soit un nombre entier $p \geq 2$. On dit que p est un *nombre premier* si ses seuls diviseurs positifs sont 1 et lui-même. Un nombre $n \geq 2$ qui n'est pas premier est dit *composé*.

Remarques 5.1.2

(i) Dire que n est composé signifie que $n = rs$ avec $1 < r < n$ et $1 < s < n$.

(ii) Les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43...

(iii) Soit deux premiers distincts $p \neq q$, alors pour tous $m, n \geq 1$, $\text{pgcd}(p^m, q^n) = 1$.

Les nombres premiers sont à la fois des nombres fondamentaux et très mystérieux. Ils sont fondamentaux à cause du théorème suivant :

Théorème 5.1.3 (Décomposition en facteurs premiers) *Tout entier $n \geq 2$ s'écrit comme un produit de nombres premiers, de façon unique à l'ordre près des facteurs. Une telle écriture est donc de la forme*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

avec $r \geq 1$ un entier déterminé, $p_1 < \cdots < p_r$ des entiers premiers distincts, et $\alpha_1, \ldots, \alpha_r$ des exposants (entiers) non nuls.

Dans l'énoncé du théorème, l'unicité signifie la chose suivante. Soient deux décompositions en facteurs premiers d'un entier $n \geq 2$, à r, respectivement s facteurs,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

avec $p_1 < \dots < p_r$ entiers premiers distincts, $q_1 < \dots < q_s$ entiers premiers distincts, et $\alpha_1, \dots, \alpha_r$, $\beta_1, \dots, \beta_s$ des exposants non nuls. Alors ces deux décompositions sont les mêmes, c'est-à-dire que $r = s$, $p_1 = q_1$, ..., $p_r = q_r$, $\alpha_1 = \beta_1$, ..., $\alpha_r = \beta_r$.

Démonstration : Soit E l'ensemble des nombres premiers qui divisent n. D'après l'exemple 1.3.3 il existe un tel nombre premier, c'est-à-dire que E est non vide. Choisissons N tel que $n < 2^N$ ([7]) et montrons que E est fini avec moins de N éléments. En effet, prenons des éléments distincts $p_1, \dots, p_k$ dans E. Comme $p_1, \dots, p_k$ sont premiers entre eux deux à deux on a $p_1 p_2 \dots p_k \mid n$ d'après la proposition 4.4.4. En particulier, $2^k \leq p_1 p_2 \dots p_k \leq n < 2^N$ donc $k < N$. Donc E est fini et $E = \{p_1, \dots, p_r\}$ avec $r < N$.

Pour chaque indice i il y a un nombre $\alpha_i \geq 1$ maximal tel que $p_i^{\alpha_i}$ divise n. En appliquant encore la proposition 4.4.4 pour les nombres $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ on obtient que $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ divise n, c'est-à-dire qu'il existe un entier m tel que $n = m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Si $m > 1$ il a un facteur premier p_u qui doit être dans E, pour un certain indice u. Donc $p_u \times p_u^{\alpha_u}$ divise n. C'est impossible car α_u a été choisi maximal, donc $m = 1$ et $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. □

Remarque 5.1.4 Plus ou moins par leur définition même, les entiers naturels s'obtiennent à partir du nombre 1 par des additions successives. Le théorème 5.1.3 nous dit que, si on veut obtenir tous les entiers par des *multiplications* successives, alors un seul nombre ne suffit pas et il faut prendre l'ensemble des nombres premiers. En d'autres termes, les nombres premiers sont les « atomes » de base de l'écriture multiplicative de tous les entiers. Pour cette raison, on ne considère pas que 1 est un nombre premier : il est inutile dans les écritures multiplicatives ([8]).

Nous traiterons un exemple de décomposition en facteurs premiers à la fin de ce paragraphe, après la proposition 5.1.6. Voici maintenant quelques faits qui montrent que les nombres premiers sont beaux et mystérieux. D'abord, on doit à Euclide (encore lui !) la démonstration du fait suivant :

Proposition 5.1.5 *Il y a une infinité de nombres premiers.*

Démonstration : En raisonnant par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, \dots, p_r$. Considérons le nombre $N \overset{\text{déf}}{=} p_1 \dots p_r + 1$. Ce nombre est > 1 donc il admet un diviseur premier qui est donc l'un des r nombres premiers, p_u ($1 \leq u \leq r$). Comme $p_u | N$ et $p_u | p_1 \dots p_r$ on en déduit que p_u divise 1 ce qui est absurde. Donc, il y a une infinité de nombres premiers. □

Les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53... et après ? On ne connaît pas de formule donnant tous les nombres premiers. Certes, connaissant les r premiers, la proposition donne une façon d'en trouver un autre, en regardant un facteur premier de $N = p_1 \dots p_r + 1$. Malheureusement, *primo* ces nombres grandissent trop vite, et *secundo* la méthode demande de savoir trouver des facteurs premiers d'un entier, ce qui est aussi compliqué que de trouver les nombres premiers eux-mêmes...

[7] Par exemple on peut prendre N égal au nombre de chiffres de l'écriture en base 2 de n (vérifiez-le).

[8] Et, étant donné un nombre premier p, le nombre de facteurs premiers dans p^k est k. Donc si $k = 0$ on a envie de dire qu'il n'y a aucun facteur premier dans $p^0 = 1$...

Un autre problème très difficile est de savoir si un nombre donné n est premier. Pour cela il faut tester s'il est divisible par tous les nombres premiers $\leq n$, qu'en général on ne connaît pas très bien. La seule amélioration de cette méthode est :

Proposition 5.1.6 *Pour tester si un entier $n \geq 2$ est premier, il suffit de tester s'il est divisible par les nombres premiers $p \leq \sqrt{n}$.*

Démonstration : Si n n'est pas premier il s'écrit $n = ab$ avec $1 < a \leq b < n$. Donc $a^2 \leq n$ de sorte que si p est un facteur premier de a, on a $p \leq \sqrt{n}$. Par contraposée, si n n'est divisible par aucun des nombres premiers $p \leq \sqrt{n}$, alors il est premier. □

Voici l'exemple de $n = 2005$. On a $n = 5 \times 401$ et il nous reste à décomposer 401. L'utilisation des critères de divisibilité montre qu'il n'est pas divisible par 2, ni par 3, ni par 5. Il n'existe pas de critère pour 7 mais on vérifie facilement que 401 n'est pas divisible par 7. Et ensuite ?... La proposition 5.1.6 montre qu'il suffit de tester la divisibilité par les nombres premiers $p \leq \sqrt{401}$, or $\sqrt{401} \approx 20,02$.

Exercice 5.1.7 Vérifiez que 401 n'est divisible par aucun des nombres premiers 7, 11, 13, 17 et 19. Il en résulte que la décomposition en facteurs premiers de 2005 est $2005 = 5 \times 401$.

Exercice 5.1.8 Donnez la décomposition en facteurs premiers de 2006 et 2007.

5.2 Exemples de nombres premiers et composés

Aujourd'hui il faut d'énormes ordinateurs pour trouver des grands nombres premiers (de temps en temps, le record du plus grand premier connu tombe). Souvent on en trouve parmi les nombres de Mersenne, nombres de la forme $2^p - 1$ avec p premier.

Marin Mersenne (1588-1648) voulait trouver une formule pour représenter tous les nombres premiers, ce que l'on ne connaît toujours pas. Il étudia les nombres de la forme $2^p - 1$ (p premier) qu'il affirma premiers si $p = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127 et 257 et composés pour les 44 autres premiers inférieurs à 257. Par la suite on montra qu'il s'était trompé pour 67 et 257 ainsi que 61, 89, 107. Leonhard Euler (1707-1783) est un génie mathématique de la taille de Gauß. Je n'ai pas le courage de résumer sa vie si intense ! Les curieux sont encouragés à aller voir sur le site :
http://www-gap.dcs.st-and.ac.uk/∼history/BiogIndex.html

Proposition 5.2.1 *Le plus grand nombre premier connu (en octobre 2006) est le nombre de Mersenne $2^{32582657} - 1$. Son écriture décimale a près de 10 millions de chiffres.*

Démonstration : Il n'y a pas d'autre moyen que la vérification par ordinateur en utilisant la proposition 5.1.6 ! Ces calculs durent en général plusieurs semaines... □

Fermat pensait que les nombres $F_k \stackrel{\text{déf}}{=} 2^{2^k} + 1$ étaient tous premiers mais Euler a montré que ce n'était pas vrai pour F_5.

Proposition 5.2.2 (Euler) *Le nombre de Fermat $F_5 \stackrel{\text{déf}}{=} 2^{32} + 1$ est composé, plus précisément il est divisible par* 641.

Démonstration : L'astuce (double) est de voir que $641 = 640 + 1 = 5 \times 2^7 + 1$ et $641 = 625 + 16 = 5^4 + 2^4$. Modulo 641, la première relation donne $5 \times 2^7 \equiv -1$ donc $5^4 \times 2^{28} \equiv (-1)^4 \equiv 1$. La deuxième donne $5^4 \equiv -2^4$. En remplaçant, on obtient $-2^4 \times 2^{28} \equiv 1$ c'est-à-dire que $2^{32} + 1 \equiv 0 \bmod 641$, c'est ce que l'on voulait. □

Pierre Fermat (1601-1665), juriste de métier, était aussi mathématicien amateur et soumettait ses questions et découvertes à des grands mathématiciens. Il lut l'*Arithmetica* de Diophante où est résolue l'équation en nombres entiers $x^2 + y^2 = z^2$. Ceci le mena à s'intéresser à l'équation $x^n + y^n = z^n$ avec $n \geq 3$.

Le « dernier théorème de Fermat » affirme que cette équation n'a pas de solution avec x, y, z entiers non nuls. C'est resté une énigme pour les mathématiciens pendant 350 ans, jusqu'en 1993, date à laquelle l'anglais Andrew Wiles (1953-) l'a démontré.

5.3 Application au pgcd et au ppcm

Soient a, b deux entiers naturels non nuls. Soit r le nombre de facteurs premiers de a, et s le nombre de facteurs premiers de b, voir théorème 5.1.3. Soient $p_1, \ldots, p_t$ les nombres premiers qui interviennent dans l'une ou l'autre des décompositions : on a donc $r \leq t$ et $s \leq t$. On peut alors écrire

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$$

quitte à mettre un exposant $\alpha_i = 0$ si le facteur p_i n'apparaît pas dans la décomposition de a, c'est-à-dire si $p_i | b$ mais $p_i \not| a$. De même on écrit $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}$.

Exemple 5.3.1 Soient $a = 12740$ et $b = 168$. On écrit

$$a = 2^2 \times 5^1 \times 7^2 \times 13^1 \qquad \text{et} \quad b = 2^3 \times 3^1 \times 7^1$$

En incluant dans les deux écritures les facteurs premiers $2, 3, 5, 7, 13$ on a :

$$a = 2^2 \times 3^0 \times 5^1 \times 7^2 \times 13^1 \qquad \text{et} \quad b = 2^3 \times 3^1 \times 5^0 \times 7^1 \times 13^0$$

Étant donnés a et b avec une écriture comme ci-dessus, il est facile de vérifier que b divise a si et seulement si $\beta_i \leq \alpha_i$ pour tout i. En particulier, ceci dit que si b divise a, alors l'écriture en facteurs premiers de b ne peut contenir d'autres facteurs premiers que ceux de a. On utilise cette remarque pour démontrer :

Proposition 5.3.2 *Soient a, b entiers naturels non nuls, écrits comme ci-dessus :*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t} \qquad et \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}$$

Soient $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$. Alors on a

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t} \qquad et \quad m = p_1^{\delta_1} p_2^{\delta_2} \ldots p_t^{\delta_t}$$

avec $\gamma_i \overset{\text{déf}}{=} \min(\alpha_i, \beta_i)$ et $\delta_i \overset{\text{déf}}{=} \max(\alpha_i, \beta_i)$.

Démonstration : Soit $e \overset{\text{déf}}{=} p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t}$, on doit donc montrer que $e = d$. Écrivons la décomposition en facteurs premiers de d sous la forme $d = p_1^{\gamma'_1} p_2^{\gamma'_2} \ldots p_t^{\gamma'_t}$.

Comme $\gamma_i \leq \alpha_i$ et $\gamma_i \leq \beta_i$ pour tout i, il est clair que e divise a et b. Donc il divise leur pgcd, d. Réciproquement, comme d divise a et b on a $\gamma'_i \leq \alpha_i$ et $\gamma'_i \leq \beta_i$ pour tout i, donc $\gamma'_i \leq \min(\alpha_i, \beta_i) = \gamma_i$. C'est fini.

Pour le ppcm la démonstration est identique. On peut aussi donner une autre démonstration en utilisant le fait que $ab = dm$ et $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$. □

Exemple 5.3.3 Calculons le pgcd de $a = 12740$ et $b = 168$. D'après l'écriture ci-dessus on trouve immédiatement $d = 2^2 \times 7 = 28$ et $m = 2^3 \times 3 \times 5 \times 7^2 \times 13 = 76440$.

Géométrie plane

Note importante. En Géométrie, les dessins sont omniprésents. Pour avoir une bonne intuition des situations rencontrées, on ne peut pas en faire l'économie. Pour des questions de place, j'ai choisi de ne pas inclure les dessins dans le polycopié. C'est donc un passage obligé pour le lecteur que de dessiner, à côté de chaque énoncé, remarque, théorème,... la figure correspondante. C'est aussi un excellent exercice, car faire de bons dessins n'est pas aussi facile que ce que l'on peut croire !

Géométrie plane

Cette partie du cours a pour but de revoir ainsi que d'approfondir certains résultats connus. Une de nos préoccupations, au cours du chemin, sera de faire la part entre

- des énoncés de départ non démontrés. Du point de vue du Professeur des Écoles, on peut considérer que ce sont des choses basiques que doit s'approprier un enfant comme évidentes, lorsqu'il joue avec des couleurs, des formes géométriques, compare leurs longueurs... C'est l'apprentissage de la perception, de l'intuition. Dans le vocabulaire du mathématicien, ces énoncés sont les *axiomes*.
- les résultats qui s'en déduisent. On verra qu'on peut démontrer la plupart des résultats classiques de Géométrie (théorèmes de Pythagore, Thalès ; calculs de longueurs et d'aires de figures usuelles). Du point de vue du Professeur des Écoles, pour ses élèves c'est l'apprentissage du raisonnement. Du point de vue du mathématicien, c'est simplement le développement de la théorie.

1 Géométrie d'Euclide, Géométrie d'aujourd'hui

L'un des buts de la Géométrie est d'arriver à mieux percevoir et décrire les objets qui se trouvent autour de nous, et pour commencer, les plus simples d'entre eux : en dimension 2, droites, cercles, polygones ; en dimension 3, sphères, boules, cubes, polyèdres...

1.1 La Géométrie d'Euclide. Une façon de décrire les objets géométriques est d'adopter un point de vue qualitatif : c'est à cela que servent les notions de parallélisme ou d'incidence de deux droites, de convexité ou de concavité d'un polygone, d'angles aigus ou obtus, d'intérieur d'une figure, etc. Ainsi Euclide développa-t-il la Géométrie du plan sans recours explicite à des longueurs ou des angles en tant que nombres. (Par ailleurs, du temps des Grecs anciens les nombres réels n'avaient pas été inventés — voir encadré ci-dessous — donc il aurait été bien difficile de décider quel genre de quantité une longueur doit être). De cette manière il établit presque tous les résultats dont nous allons parler. Signalons que certains des raisonnement d'Euclide ne seraient pas considérés comme valables aujourd'hui, mais Hilbert a repris tout le travail d'Euclide en 1899 (plus de vingt siècles plus tard !) pour le rendre correct.

David Hilbert (1862-1943) naquit et étudia à Königsberg (à l'époque en Prusse). En 1895 il fut nommé professeur à Göttingen (presque un siècle après Gauß), où il s'installa jusqu'à la fin de sa vie. Hilbert apporta d'immenses contributions à de nombreuses branches des mathématiques. En 1899 il publia les résultats de ses travaux (les *Grundlagen der Geometrie*, fondations de la Géométrie) visant à donner des fondements axiomatiques rigoureux à la géométrie d'Euclide. Au Congrès International des Mathématiciens de 1900 à Paris, il posa une liste de 23 problèmes ouverts qui ont été l'objet de recherches incessantes depuis lors (beaucoup ont été résolus).

1.2 La Géométrie d'aujourd'hui. Le point de vue quantitatif consiste à associer des nombres aux objets géométriques : on cherche alors à mesurer des grandeurs telles que

la longueur d'une courbe, l'aire d'une figure du plan ou de l'espace, ou l'angle entre deux droites. Tous les nombres en question seront des nombres réels. C'est la principale chose qui diffère de la Géométrie telle que la pratiquait Euclide (mais la différence est de taille !).

~ Une courte histoire des nombres ~

Les ensembles de nombres que nous manipulons sont $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (entiers naturels, entiers relatifs, nombres rationnels, réels, complexes). Ils sont inclus les uns dans les autres. Ce que les Grecs appelaient *nombres* correspond à ce que nous appelons nombres rationnels (les fractions a/b de nombres entiers relatifs). Ils connaissaient donc $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ mais avaient remarqué que certaines quantités naturelles (telle que la diagonale du carré de côté 1, qui vaut $\sqrt{2}$) n'étaient pas des fractions.
Au Moyen-Âge, les mathématiciens arabes et chinois étudièrent les équations polynômiales ; à la Renaissance, les mathématiciens italiens résolurent plus particulièrement les équations du troisième degré. Cela amena à considérer les solutions de ces équations (par exemple $\sqrt{2}$ racine de $X^2-2=0$, ou i racine de $X^2+1=0$...) comme des nombres à part entière. Les premiers nombres construits avec i furent appelés *imaginaires*. Il faut remarquer qu'on ne connaissait de nombres complexes que ceux qui étaient racines de polynômes. Par exemple, le nombre π (demi-périmètre du cercle de rayon 1) ou le nombre e (base des logarithmes népériens) étaient connus mais incompris.
Vers la fin du XIX-ième siècle, le mathématicien allemand Richard Dedekind (1831-1916) donna une (très élégante) construction de l'ensemble des réels, aujourd'hui indispensables à la Géométrie. Sa construction introduit les réels comme des « coupures » dans l'ensemble des rationnels.
J'en profite pour vous rappeler l'excellente adresse internet où on peut consulter la biographie de Dedekind et de beaucoup d'autres : http://www-gap.dcs.st-and.ac.uk/~history/BiogIndex.html

La définition des nombres réels sera reprise au second semestre, mais nous la présentons brièvement car elle nous sera utile bientôt. Rappelons que deux suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont dites *adjacentes* lorsque $(u_n)_{n\in\mathbb{N}}$ est croissante, $(v_n)_{n\in\mathbb{N}}$ est décroissante et $(v_n-u_n)_{n\in\mathbb{N}}$ tend vers 0 quand n tend vers l'infini. L'ensemble $\mathbb{R}$ des nombres réels est l'unique ensemble satisfaisant les propriétés suivantes :

(i) $\mathbb{R}$ contient $\mathbb{Q}$ et est muni d'une addition et d'une multiplication qui étendent celles de $\mathbb{Q}$ et ont les mêmes propriétés usuelles.

(ii) Il y a une relation d'ordre « $\leq$ » sur $\mathbb{R}$ qui étend celle de $\mathbb{Q}$.

(iii) Des suites adjacentes $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ ont toujours une limite dans $\mathbb{R}$, lorsque n tend vers $+\infty$.

Remarque 1.3 Soit a un nombre réel, disons positif pour simplifier. Alors pour tout $n\geq 0$, il existe un unique nombre rationnel $a_n=\frac{q_n}{10^n}$ (avec $q_n\in\mathbb{N}$) tel que $a_n\leq a<a_n+\frac{1}{10^n}$. En effet, ces conditions sont équivalentes à $10^n a_n\leq 10^n a<10^n a_n+1$ donc q_n est la partie entière de $10^n a$. Posons $a'_n=a_n+\frac{1}{10^n}$. On appelle a_n, resp. a'_n, la n-ième approximation décimale inférieure, resp. supérieure, de a. Les suites de termes a_n et a'_n sont adjacentes et convergent vers a lorsque n tend vers $+\infty$.

Par exemple si $a=\pi$, les approximations décimales inférieures sont

$$a_0=3\ ;\ a_1=3,1\ ;\ a_2=3,14\ ;\ a_3=3,141\ ;\ a_4=3,1415\ ;\ a_5=3,14159\ldots$$

et les approximations décimales supérieures sont

$$a'_0=4\ ;\ a'_1=3,2\ ;\ a'_2=3,15\ ;\ a'_3=3,142\ ;\ a'_4=3,1416\ ;\ a'_5=3,14160\ldots$$

Exercice 1.4 Montrez que $\sqrt{2}$ n'est pas un nombre rationnel. (*Indic : supposez que $\sqrt{2}=a/b$. Élevez au carré puis utilisez la décomposition en facteurs premiers de a et b*)

1.5 La Géométrie emprunte aux deux approches : qualitative et quantitative. Naturellement c'est la première approche qui convient le mieux aux enfants, car ils y voient un terrain d'expression de leur intuition (et aussi car ils ne maîtrisent pas encore les nombres !).

Pour cette raison, nous essaierons d'aller le plus loin possible dans le développement du cours sans utiliser de nombres réels([9]).

[9]Mais nous en passer complètement, comme le fit Euclide, nous écarterait de l'un de nos objectifs :

2 Quelques définitions dans l'esprit d'Euclide

Posez-vous les questions « Qu'est-ce qu'une droite ? » ou « Qu'est ce que la longueur d'un morceau de courbe tracé sur le tableau ? » et vous verrez qu'il n'est pas simple ne serait-ce que de définir les objets de la Géométrie et leurs grandeurs caractéristiques ([10]). Le concept même de *grandeur* n'est pas facile à définir ; il est souvent confondu avec celui de *mesure* alors que les deux sont bien distincts. Pour avoir un petit rafraîchissement sur ces notions, et leur lien avec les Sciences Physiques, je recommande au lecteur arrivé ici de lire l'Annexe D.

Pour résoudre ces problèmes délicats, l'approche d'Euclide revient à *ne pas définir* les concepts les plus intuitifs comme les points et les droites, mais *supposer qu'ils existent* en acceptant leurs propriétés de base, qu'on doit énoncer.

2.1 Points et droites

On postule ([11]) l'existence d'un ensemble E appelé *plan euclidien* et dont les éléments s'appellent les . Cet ensemble possède des parties d'intérêt particulier appelées les , qui vérifient les propriétés suivantes, nommées *axiomes d'incidence* :

(I1) Par deux points distincts A et B passe une et une seule notée (AB).

(I2) Toute contient au moins deux points.

(I3) Il existe trois points non alignés.

En conséquence, deux distinctes ont au plus un point commun.

Définition 2.1.1 Deux droites sans point commun sont dites . On dit alors qu'elles définissent la même (si on préfère, une est donc un ensemble de droites parallèles à une droite fixée). Deux droites distinctes qui se coupent sont dites . Trois (ou plus) droites distinctes qui passent par un même point sont dites .

On suppose aussi vérifiée la propriété :

(P) Par un point M non situé sur la droite $\mathcal{D}$ passe une droite parallèle à $\mathcal{D}$ et une seule.

2.2 Ordre des points

On suppose qu'il existe une relation d'ordre entre les points de chaque droite $\mathcal{D}$ du plan (on l'écrit : « C est entre A et B »), qui vérifie :

---

présenter la Géométrie du plan de manière à la fois intuitive (pour pouvoir être enseignée), moderne et efficace (pour pouvoir calculer des longueurs et des aires, par exemple). Donc nous présenterons aussi les coordonnées dans $\mathbb{R}^2$, le moment venu.

[10] Malheureusement le dictionnaire risque de ne pas vous satisfaire beaucoup sur ces questions... Allez voir ce qu'il dit !

[11] « On postule », « on suppose »... : ces locutions indiquent qu'on introduit là des objets dont l'existence et les propriétés sont admises (les fameux axiomes).

(O) Étant donnés trois points A, B, C sur $\mathcal{D}$, si B est entre A et C, B est entre C et A. De plus, s'ils sont tous distincts, alors un et un seul d'entre eux est entre les deux autres.

La relation d'ordre permet de définir différents concepts usuels.

Définitions 2.2.1 (1) Soient A et B deux points du plan. Le *d'extrémités A et B* est l'ensemble des points situés entre A et B (on considère que « A est entre A et B » de sorte que les extrémités appartiennent au segment). On le note $[AB]$.

(2) La *d'origine A et contenant B* est l'ensemble des points M tels que M est situé entre A et B, ou B est situé entre A et M. On la note $[AB)$. On appelle parfois demi-droite à $[AB)$ l'ensemble des points M tels que A est entre M et B. Un sur la droite (AB) est le choix d'une des deux demi-droites : $[AB)$ ou son opposée.

(3) Le *délimité par la droite $\mathcal{D}$ et contenant le point A* (avec $A \notin \mathcal{D}$) est l'ensemble des points M du plan tels que : $M \in \mathcal{D}$ ou le segment $[AM]$ ne rencontre pas $\mathcal{D}$.

(4) Le *de sommets A, B, C* est la réunion des trois segments $[AB]$, $[BC]$ et $[AC]$. On le note ABC. Son est l'intersection des trois demi-plans ouverts délimités par (AB) (resp. (BC), (AC)) contenant C (resp. A, B).

Chacun de ces concepts possède une variante *ouverte* et une variante *fermée* : par exemple, le segment semi-ouvert $]AB]$, la demi-droite ouverte $]AB)$.

2.3 Secteurs angulaires

Définition 2.3.1 Soit O un point du plan et $[OA)$, $[OB)$ deux demi-droites issues de O.

(i) Supposons d'abord O, A, B non alignés. Soit H_A^+ (resp. H_A^-) le demi-plan fermé délimité par (OA) et contenant B (resp. ne contenant pas B). Les demi-droites $[OA)$ et $[OB)$ délimitent

- le *secteur angulaire* $\widehat{[AOB]}$: par définition c'est $H_A^+ \cap H_B^+$.
- le *secteur angulaire* $[AOB]^\vee$: par définition c'est $H_A^- \cup H_B^-$.

(ii) Supposons O, A, B alignés et $[OA) = [OB)$. Alors le secteur angulaire saillant est réduit à $[OA)$, on l'appelle un secteur . Le secteur angulaire rentrant est le plan tout entier, on l'appelle un secteur .

(iii) Supposons O, A, B alignés et les demi-droites opposées. Alors les deux secteurs angulaires (saillants ou rentrants tous deux) sont les demi-plans délimités par (OA). On les appelle des secteurs .

Si les demi-droites sont notées δ_1 et δ_2, on utilise aussi les notations $\widehat{[\delta_1, \delta_2]}$ et $[\delta_1, \delta_2]^\vee$ pour désigner les secteurs angulaires, ou même $[\delta_1, \delta_2]$ si on ne précise pas saillant/rentrant.

2.4 Longueurs

On suppose qu'il existe une *mesure des longueurs* des segments du plan, c'est-à-dire une fonction ℓ qui à un segment $[AB]$ associe un nombre positif noté $\ell([AB])$ ou plus simplement AB, et que cette fonction vérifie les propriétés suivantes :

(L1) $AB = 0$ si et seulement si $A = B$.

(L2) $AB = BA$.

(L3) Si A, B et C sont alignés alors $AB \leq AC + CB$, avec égalité ssi $C \in [AB]$.

Il s'agit ici d'une adaptation de la formulation d'Euclide. En fait, comme nous l'avons dit, Euclide ne parlait pas du tout de « nombre » (je suis resté volontairement vague ci-dessus) et, en remplacement, comparait les segments de manière astucieuse pour pouvoir éviter ces mêmes nombres. Ainsi, l'addition de deux longueurs était remplacée par la « mise bout à bout » de deux segments.

Une variante de la longueur est parfois utile, la notion de :

Définition 2.4.1 Soit δ une demi-droite d'origine O et $\mathcal{D}$ la droite qui la supporte. Alors on appelle *d'un point M sur la droite $\mathcal{D}$ dans le repère formé par δ*, le nombre $\overline{OM}$ défini par : $\overline{OM} = OM$ si $M \in \delta$, et $\overline{OM} = -OM$ si $M \notin \delta$.

2.5 Angles

Nous allons définir la *mesure des angles* des secteurs angulaires à partir de la longueur. Une définition plus complète de la longueur sera donnée au second semestre. D'ici là, nous admettrons qu'on peut mesurer les longueurs de figures plus compliquées que des segments, comme les cercles dont nous rappelons la définition :

Définitions 2.5.1 Soient r un nombre réel et O, A des points du plan.

(1) Le de centre O et de rayon r est l'ensemble des points M tels que $OM = r$. Il est noté $\mathcal{C}(O, r)$.

(2) On appelle le nombre égal à la demi-longueur du cercle $\mathcal{C}(O, 1)$.

(3) On considère un secteur angulaire de sommet A. Pour définir la mesure de son angle, on trace le cercle $\mathcal{C}(A, 1)$ et on appelle B et C les points d'intersection du cercle avec les demi-droites qui délimitent le secteur angulaire. Alors, la longueur de l'arc $\overset{\frown}{BC}$ est appelée *mesure* en *de l'angle du secteur angulaire.*

Remarque 2.5.2 Comme l'arc correspondant à un secteur saillant est contenu dans un demi-cercle, l'angle correspondant est $\leq \pi$. Au contraire, un angle rentrant est $> \pi$. Précisément, si l'angle du secteur saillant $[\widehat{AOB}]$ vaut θ, celui du secteur rentrant $[AOB]^\vee$ vaut $2\pi - \theta$.

On admet que la mesure des angles vérifie l'axiome suivant, appelé *premier cas d'égalité des triangles* et baptisé CAC pour « côté-angle-côté » :

(CAC) Supposons que deux triangles ont deux de leurs côtés « égaux » (c'est-à-dire, de longueurs égales) et les angles compris entre ces côtés égaux. Alors tous les côtés et tous les angles des triangles sont égaux (les triangles sont).

Exemple 2.5.3 Soient C, O, B trois points alignés, dans cet ordre. Soit A un point n'appartenant pas à la droite (OB). Si les deux secteurs $[\widehat{COA}]$ et $[\widehat{AOB}]$ ont même mesure, on dit que ce sont des secteurs angulaires . Cela revient au même de dire que leur mesure en radians est égale à $\pi/2$. On dit aussi que l'angle $\widehat{AOB}$ est droit, et que les droites (OB) et (OA) sont ou .

On a une propriété analogue à la propriété (P) (paragraphe 2.1) avec les droites perpendiculaires : « par tout point M passe une droite perpendiculaire à la droite $\mathcal{D}$ et une seule ». En particulier on peut définir la notion de :

Définition 2.5.4 Soit $\mathcal{D}$ une droite du plan E. Pour tout point $M \in E$, notons M' le point intersection de la droite $\mathcal{D}$ avec la perpendiculaire à $\mathcal{D}$ passant par M. On définit la *sur* $\mathcal{D}$ notée $\pi_{\mathcal{D}}$ par $\pi_{\mathcal{D}}(M) \overset{\text{déf}}{=} M'$.

Nous n'insistons pas sur les notions classiques d'angles supplémentaires, complémentaires, opposés, alternes-internes (etc.) car elles nous serviront peu ([12]).

2.6 Aires

Fixons maintenant deux points distincts O, I qui définissent donc une *de longueur* OI (voir D.2 et 2.4). (Si on note $m \overset{\text{déf}}{=} OI$ cette , pour faire penser au *mètre*, on a vu dans D.2 que l'unité d'aire doit être $m^2 = OI^2$, le *mètre carré*.) On appelle *carré unité* le carré construit sur le côté $[OI]$, et on le note $\mathcal{C}$.

La définition précise d'un *polygone* est rappelée dans l'Annexe A. On suppose qu'il existe une *mesure des* , c'est-à-dire une fonction $\mathcal{A}$ qui associe aux polygones du plan un nombre positif noté $\mathcal{A}(\mathcal{P})$, qui est *unique* et vérifiant les propriétés suivantes :

($\mathcal{A}1$) L' du carré unité $\mathcal{C}$ est égale à une unité : $\mathcal{A}(\mathcal{C}) = 1$ ([13]).

($\mathcal{A}2$) L' de la réunion de deux polygones disjoints $\mathcal{P}$ et $\mathcal{Q}$ (c'est-à-dire tels que $\mathcal{P} \cap \mathcal{Q} = \emptyset$) est la somme des des deux polygones : $\mathcal{A}(\mathcal{P} \cup \mathcal{Q}) = \mathcal{A}(\mathcal{P}) + \mathcal{A}(\mathcal{Q})$.

[12] Pour être complet, rappelons-les tout de même ici :

Définitions 2.5.5 Soient C, O, B trois point alignés, dans cet ordre. Soit A un point n'appartenant pas à la droite (OB). On dit que les deux secteurs $[\widehat{COA}]$ et $[\widehat{AOB}]$ sont *supplémentaires*. (Cela veut dire que la somme de leurs angles est égale à l'angle plat π.)

Soit $[\widehat{AOB}]$ un secteur angulaire droit et soit C un point situé à l'intérieur du secteur angulaire. On dit que les deux secteurs $[\widehat{AOC}]$ et $[\widehat{COB}]$ sont *complémentaires*. (Cela veut dire que la somme de leurs angles est égale à l'angle droit $\pi/2$.)

Définitions 2.5.6 Soient $\mathcal{D}$ et $\mathcal{D}'$ deux droites parallèles, soit Δ une droite les coupant. On appelle O et O' les points d'intersection de Δ avec $\mathcal{D}$ et $\mathcal{D}'$. Soient A et B des points de $\mathcal{D}$ tels que O est situé entre A et B (et A', B' points de $\mathcal{D}'$ idem). On suppose que A et A' sont du même côté de Δ. Enfin, soient C et C' des points de Δ tels que C est situé de l'autre côté de $\mathcal{D}$ que O' et C' est situé de l'autre côté de $\mathcal{D}'$ que O. Alors :
(1) On dit que les secteurs $[\widehat{AOC}]$ et $[\widehat{BOO'}]$ sont *opposés*.
(2) On dit que les secteurs $[\widehat{BOO'}]$ et $[\widehat{A'O'O}]$ sont *alternes-internes*.
(3) On dit que les secteurs $[\widehat{AOC}]$ et $[\widehat{C'O'B'}]$ sont *alternes-externes*.
(4) On dit que les secteurs $[\widehat{BOO'}]$ et $[\widehat{B'O'C'}]$ sont *correspondants*.

($\mathcal{A}3$) L'[redacted] est invariante par isométrie : si $\mathcal{P}$ est un polygone et u est une isométrie, on a $\mathcal{A}(u(\mathcal{P})) = \mathcal{A}(\mathcal{P})$.

Les axiomes ($\mathcal{A}2$) et ($\mathcal{A}3$) sont fondamentaux : ils sont à la base de la méthode de calcul des aires *par découpage et recollement* qui consiste, comme son nom l'indique, à calculer les aires de figures en les découpant en figures plus simples (on utilise ($\mathcal{A}2$)) et en recollant éventuellement les morceaux autrement (on peut déplacer les morceaux comme on veut grâce à ($\mathcal{A}3$), par translations et rotations). C'est la technique de base qu'utilisait Euclide.

Lemme 2.6.1 *Un point et un segment ont une aire* [redacted].

Démonstration : Comme tout point est inclus dans un segment, l'aire d'un point est inférieure à celle d'un segment donc il suffit de montrer que l'aire d'un segment est nulle.

D'après l'axiome ($\mathcal{A}3$) tous les segments de longueur 1 ont même aire puisqu'ils sont isométriques. Soit donc α leur aire commune. Pour tout entier n on peut considérer n segments « horizontaux », disjoints, inclus dans le carré unité $\mathcal{C}$ et parallèles à un de ses côtés. Comme ils sont disjoints leur aire totale est égale à $n\alpha$. Par ailleurs elle est inférieure à l'aire de $\mathcal{C}$, donc $n\alpha \leq 1$. Ainsi $0 \leq \alpha \leq 1/n$ donc en faisant tendre n vers l'infini on obtient $\alpha = 0$. □

Une conséquence très importante de ce lemme est que l'aire d'un polygone privé de certaines parties de sa frontière (des bouts de segments) est égale à l'aire du polygone lui-même. Dit autrement on peut renforcer la propriété ($\mathcal{A}2$) en :

($\mathcal{A}2'$) Si deux polygones ont pour intersection une réunion finie de points et de segments, alors on a $\mathcal{A}(\mathcal{P} \cup \mathcal{Q}) = \mathcal{A}(\mathcal{P}) + \mathcal{A}(\mathcal{Q})$.

Cela nous permet le calcul élémentaire que voici.

Proposition 2.6.2 *L'aire d'un rectangle R de côtés de longueurs a et b est égale à ab.*

Démonstration : Supposons d'abord que les côtés sont des nombres rationnels $a = p/q$ et $b = r/s$. Considérons un grand rectangle R' de côtés p et r. Comme R' a des côtés entiers, en le découpant en pr carrés unité, on a $\mathcal{A}(R') = pr$, d'après les axiomes ($\mathcal{A}1$) et ($\mathcal{A}2'$). D'autre part en découpant en q parts égales le côté p et en s parts égales le côté r on recouvre R' par qs rectangles de côtés a et b, c'est-à-dire des exemplaires du rectangle R. Donc $\mathcal{A}(R') = qs\mathcal{A}(R)$. Finalement $\mathcal{A}(R) = pr/qs = ab$.

Dans le cas où a et b sont des nombres réels quelconques, on considère des rectangles R_n et R'_n tels que $R_n \subset R \subset R'_n$, dont les côtés ont pour valeur les approximations décimales inférieures a_n, b_n et supérieures a'_n, b'_n (voir 1.3). On a alors

$$a_n b_n = \mathcal{A}(R_n) \leq \mathcal{A}(R) \leq \mathcal{A}(R'_n) = a'_n b'_n$$

car les rectangles R_n et R'_n ont des côtés rationnels. Les suites de termes $a_n b_n$ et $a'_n b'_n$ sont adjacentes de limite ab. En passant à la limite on obtient $\mathcal{A}(R) = ab$. □

Exercice 2.6.3 Soit ABC un triangle et AH la hauteur issue de A. Montrez que son aire vaut $\mathcal{A}(ABC) = \frac{1}{2} BC \times AH$. (*Indic : découpage et recollement, axiomes* ($\mathcal{A}2'$) *et* ($\mathcal{A}3$).)

[13] Ou si on préfère, $\mathcal{A}(C) = 1 \times OI^2$, l'unité étant OI^2.

2.7 Vecteurs

Il y a un lien très étroit entre les parallélogrammes et d'autres objets géométriques qui sont les *vecteurs*. Rappelons que :

Définition 2.7.1 On dit qu'un quadrilatère est un si ses côtés opposés sont parallèles.

Il y a d'autres définitions classiques d'un parallélogramme (les côtés opposés ont même longeur ; ou, les angles des sommets opposés sont égaux ; ou, les diagonales se coupent en leur milieu) mais le théorème de Thalès (paragraphe suivant) est nécessaire pour montrer qu'elles sont toutes équivalentes. Nous renvoyons à l'Annexe A pour des détails à ce sujet.

Définition 2.7.2 Un *vecteur non nul* $\vec{v}$ est un triplet constitué de : une direction (déf. 2.1.1), un sens (déf. 2.2.1) et une strictement positive (notée $\|\vec{v}\|$). Le *vecteur nul* noté $\vec{0}$ n'a ni direction ni sens, et a une nulle : $\|\vec{0}\| = 0$.

Deux points A et B définissent un unique vecteur noté $\overrightarrow{AB}$. De plus on a $\overrightarrow{AB} = \overrightarrow{CD}$ ssi le quadrilatère $ABDC$ est un parallélogramme.

Étant donné un vecteur $\vec{v}$ et un point A, on peut tracer la demi-droite δ d'origine A déterminée par la direction et le sens de $\vec{v}$. En reportant sur δ le point B tel que AB soit égal à $\|\vec{v}\|$, on obtient $\vec{v} = \overrightarrow{AB}$. Un point B vérifiant cela est alors unique.

Il y a deux opérations importantes qu'on peut faire avec les vecteurs :

- étant donné un vecteur $\vec{v}$ et un nombre réel λ, on définit le vecteur $\lambda\vec{v}$ comme suit. Si $\lambda = 0$ on pose $\lambda\vec{v} \overset{\text{déf}}{=} \vec{0}$. Sinon, le vecteur $\lambda\vec{v}$ a même direction que $\vec{v}$ et $\|\lambda\vec{v}\| = |\lambda| \, \|\vec{v}\|$. Enfin son sens est le même que celui de $\vec{v}$ ou le sens opposé, selon que $\lambda > 0$ ou $\lambda < 0$.
- étant donnés deux vecteurs $\vec{v}$ et $\vec{w}$, on peut définir le vecteur $\vec{v} + \vec{w}$. Pour cela on choisit trois points A, B, C tels que $\vec{v} = \overrightarrow{AB}$ et $\vec{w} = \overrightarrow{AC}$. Soit D l'unique point tel que $ABDC$ est un parallélogramme, on définit $\vec{v} + \vec{w} \overset{\text{déf}}{=} \overrightarrow{AD}$.

Remarque 2.7.3 Par définition de la somme des vecteurs, la célèbre *relation de Chasles* $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$ est vérifiée.

Une dernière utilisation des vecteurs est de pouvoir définir une demi-droite à l'aide d'un point base O et d'un vecteur $\vec{u}$: c'est l'ensemble des points M tels que $\overrightarrow{OM} = \lambda\vec{u}$ avec $\lambda \geq 0$. Nous noterons $(O, \vec{u})$ la demi-droite ainsi définie.

3 Les théorèmes de Pythagore et Thalès

3.1 Le théorème de Pythagore

Théorème 3.1.1 (Pythagore) *Soit ABC un triangle rectangle en A. Alors on a :*

$$AB^2 + AC^2 = BC^2 \, .$$

Démonstration : Soient $a \overset{\text{déf}}{=} BC$, $b \overset{\text{déf}}{=} AC$, $c \overset{\text{déf}}{=} AB$. Soit $A_1A_2A_3A_4$ un carré de côté égal à $b + c$ et de centre O, et $B_1 \in [A_1A_2]$, $B_2 \in [A_2A_3]$,... tels que $A_iB_i = AB$ pour $i = 1, 2, 3, 4$. Il est clair que les quatre triangles $A_1B_1B_4$, $A_2B_2B_1$,... sont tous isométriques

à ABC. D'autre part, en utilisant la somme des angles d'un triangle, c'est un exercice facile que de voir que $B_1B_2B_3B_4$ est un carré de côté a. En calculant l'aire de $A_1A_2A_3A_4$ par découpage on a

$$(b+c)^2 = a^2 + 2bc$$

dont on déduit que $a = b^2 + c^2$. □

Voilà, sous forme d'exercice, une première application du théorème de Pythagore, pour décrire la médiatrice d'un segment.

Définition 3.1.2 Soient A, B deux points distincts. On appelle *milieu* du segment $[AB]$ l'unique point $I \in [AB]$ tel que $AI = IB$. On appelle *médiatrice de* $[AB]$ la droite Δ perpendiculaire à (AB) passant par I.

Exercice 3.1.3 Montrez que la médiatrice d'un segment $[AB]$ est l'ensemble des points à égale distance de A et B.

Exercice 3.1.4 On dit qu'une partie D du plan est *convexe* si pour chaque couple de points A, B de D, le segment $[AB]$ tout entier est inclus dans D. À l'aide du théorème de Pythagore, montrez qu'un disque est convexe.

3.2 Le théorème de Thalès

Nous allons maintenant démontrer le théorème de Thalès qui établit un lien étroit entre paralélisme et proportions. L'exercice facile suivant sera utile.

Exercice 3.2.1 Soient x_1, y_1, x_2, y_2 des nombres réels tels que y_1, y_2 et $y_1 + y_2$ sont non nuls. Montrez que si $\frac{x_1}{y_1} = \frac{x_2}{y_2}$ alors c'est aussi égal à $\frac{x_1+x_2}{y_1+y_2}$.

Pour démontrer le théorème de Thalès on le démontre d'abord dans un cas particulier :

Lemme 3.2.2 *Soit ABC un triangle rectangle en B. Soient $B' \in (AB)$, $C' \in (AC)$ tels que $(B'C')$ est parallèle à (BC). Alors on a*

$$\frac{\overline{AB'}}{\overline{AB}} = \frac{\overline{AC'}}{\overline{AC}} = \frac{\overline{B'C'}}{\overline{BC}} .$$

Démonstration : Supposons qu'on est dans le cas où $B' \in [AB]$ et $C' \in [AC]$, dans ce cas les mesures algébriques qui interviennent dans l'énoncé sont toutes positives, ce qui nous facilitera la tâche. Le raisonnement dans les autres cas est tout à fait similaire.

Nous allons montrer d'abord que $AB'/AB = B'C'/BC$. La parallèle à (BC) passant par A et la parallèle à (AB) passant par C se coupent en un point D. La parallèle à (AB) passant par C' coupe (AD) en E et (BC) en F. Enfin appelons G l'intersection de $(B'C')$ et (CD). Ainsi le quadrilatère $ADCB$ est un rectangle. Les triangles suivants sont isométriques : FCC' et GCC'; AEC' et $AB'C'$; et bien sûr ABC et ADC. Donc

$$\mathcal{A}(BFC'B') + \mathcal{A}(FCC') + \mathcal{A}(AB'C') = \mathcal{A}(EDGC') + \mathcal{A}(GCC') + \mathcal{A}(AEC')$$

d'où $\mathcal{A}(BFC'B') = \mathcal{A}(EDGC')$. En ajoutant l'aire du rectangle $AEC'B'$ on a $\mathcal{A}(AEFB) = \mathcal{A}(ADGB')$, donc $AB \times B'C' = AB' \times BC$, c'est ce qu'on voulait. Montrons maintenant qu'on a aussi $AC'/AC = AB'/AB$. D'après ce qu'on vient de montrer et l'exercice 3.2.1,

$$\frac{(AB')^2}{AB^2} = \frac{(B'C')^2}{BC^2} = \frac{(AB')^2 + (B'C')^2}{AB^2 + BC^2} = \frac{(AC')^2}{AC^2}$$

en utilisant Pythagore. En prenant la racine carrée on obtient le résultat. □

Théorème 3.2.3 (Thalès) *Soit ABC un triangle. Soient deux points $B' \in (AB)$ et $C' \in (AC)$. Alors,*

(1) *Si $(B'C')$ est parallèle à (BC), on a* $\dfrac{\overline{AB'}}{\overline{AB}} = \dfrac{\overline{AC'}}{\overline{AC}} = \dfrac{\overline{B'C'}}{\overline{BC}}$.

(2) *Réciproquement, si* $\dfrac{\overline{AB'}}{\overline{AB}} = \dfrac{\overline{AC'}}{\overline{AC}}$ *alors $(B'C')$ est parallèle à (BC).*

Démonstration : Montrons d'abord (1). Comme dans la démonstration du lemme 3.2.2, on suppose que $B' \in [AB]$ et $C' \in [AC]$ pour ne pas nous ennuyer avec les signes. On trace la hauteur issue de A et on appelle D, D' ses points d'intersection avec (BC) et $(B'C')$. Supposons que ces points D, D' sont intérieurs au triangle (dans le cas contraire, le raisonnement serait analogue). D'après le lemme 3.2.2, utilisé dans les triangles rectangles ADB et ACD,

$$\frac{AB'}{AB} = \frac{AD'}{AD} = \frac{AC'}{AC}$$

et d'autre part (utilisant l'exercice 3.2.1)

$$\frac{AD'}{AD} = \frac{B'D'}{BD} = \frac{D'C}{DC} = \frac{B'D' + D'C}{BD + DC} = \frac{B'C'}{BC} \ .$$

Montrons maintenant (2). On suppose que $\overline{AB'}/\overline{AB} = \overline{AC'}/\overline{AC}$. Soit C^* le point d'intersection de la parallèle à (BC) passant par B'. D'après le point (1) déjà démontré, on a $\overline{AB'}/\overline{AB} = \overline{AC^*}/\overline{AC}$. Il s'ensuit que $\overline{AC^*} = \overline{AC'}$, donc $C^* = C'$, donc $(B'C')$ est parallèle à (BC). □

Remarque 3.2.4 Attention à l'énoncé du sens réciproque du théorème (le point (2)). Il n'est pas vrai en général que si $\overline{AC'}/\overline{AC} = \overline{B'C'}/\overline{BC}$, alors $(B'C')$ est parallèle à (BC).

4 Angles orientés

4.1 Orientation du plan

La notion d'*orientation* reflète une propriété remarquable des déplacements (i.e. les rotations et translations, voir 5.1.5). Au risque de faire une légère entorse au bon ordre de présentation des concepts, nous définirons ce qu'est l'*orientation* avant de présenter les isométries (l'orientation étant définie à l'aide des rotations). Le lecteur courageux ou simplement curieux, souhaitant éviter de faire cette entorse, trouvera que c'est maintenant le bon moment pour lire l'Annexe B. Il y est démontré que les déplacements vérifient la propriété fondamentale suivante (voir corollaire B.10) :

Proposition 4.1.1 *Soient δ et δ' deux demi-droites, distinctes ou non, d'origines O et O'. Alors il existe un unique déplacement d tel que $d(\delta) = \delta'$.* □

Dit de manière intuitive, cela va nous permettre de caler tous les secteurs angulaires sur un même demi-axe fixé pour pouvoir comparer les sens dans lesquels ils tournent, comme dans la définition qui suit.

Définitions 4.1.2 (i) Un secteur angulaire *orienté* $S = [\delta_1, \delta_2]$ est donné par un secteur angulaire et un ordre entre les demi-droites δ_1, δ_2 qui le délimitent. L'angle du secteur orienté est noté (δ_1, δ_2).

(ii) L'angle *opposé* de (δ_1, δ_2) est égal par définition à (δ_2, δ_1). Il est noté $-(\delta_1, \delta_2)$.

(iii) Soient $S = [\delta_1, \delta_2]$ et $S' = [\delta'_1, \delta'_2]$ deux secteurs orientés. D'après 4.1.1 il y a un unique déplacement d tel que $d(\delta_1) = \delta'_1$. Alors on dit que les secteurs ont *la même orientation* si $d(S) \subset S'$ ou $S' \subset d(S)$.

(iii) Une *orientation du plan* est définie par le choix d'un secteur orienté $S = [\delta_1, \delta_2]$ avec $\delta_1 \neq \delta_2$. Plaçant un cadran de montre dans le plan, le *sens trigonométrique* est le sens inverse des aiguilles d'une montre (donné par le secteur orienté depuis « 1 heure » vers « midi »). □

Dans toute la suite, on fixe une fois pour toutes l'orientation du plan donnée par le sens trigonométrique. On la qualifie d'orientation *positive*. De plus nous conservons le choix du radian comme unité d'angle : cela veut dire que la mesure de l'angle plein (tour complet) est 2π (si on choisissait le degré comme unité, l'angle plein mesurerait 360^o).

4.2 Angles de vecteurs

Définition 4.2.1 Soient deux vecteurs non nuls $\vec{u}$ et $\vec{u}\,'$. Soient O un point quelconque du plan, $\delta \overset{\text{déf}}{=} (O, \vec{u})$ et $\delta' \overset{\text{déf}}{=} (O, \vec{u}\,')$. L'angle de vecteurs $(\vec{u}, \vec{u}\,')$ est par définition l'angle orienté (δ, δ').

On mesure les angles de vecteurs par des nombres réels, *avec la restriction que deux réels θ, θ' qui diffèrent d'un multiple de 2π mesurent le même angle*. On dit que θ et θ' sont *congrus* (ou parfois simplement *égaux*) modulo 2π et on note

$\theta = \theta'\ [2\pi]$ ce qui veut dire par définition : il existe $k \in \mathbb{Z}$ tel que $\theta = \theta' + k \times 2\pi$.

En résumé les propriétés principales vérifiées par les angles orientés sont :

(1) l'angle opposé $-(\vec{u}, \vec{v})$ est par définition l'angle $(\vec{v}, \vec{u})$

(2) $(\vec{u}, \vec{u}) = 0\ [2\pi]$

(3) $(-\vec{u}, \vec{u}) = \pi\ [2\pi]$

(4) $(\vec{u}, \vec{v}) + (\vec{v}, \vec{w}) = (\vec{u}, \vec{w})\ [2\pi]$ (relation de Chasles)

La relation de Chasles est une simple traduction de l'axiome (A2) sur les angles (voir § 2.5).

4.3 Angles de droites

On souhaite maintenant donner une définition raisonnable des angles de droites ; *raisonnable* veut dire en particulier qu'on aimerait que si $\mathcal{D}_1$, $\mathcal{D}_2$ et $\mathcal{D}_3$ sont trois droites du plan, alors

- $(\mathcal{D}_1, \mathcal{D}_1) = 0$,
- $(\mathcal{D}_1, \mathcal{D}_2) + (\mathcal{D}_2, \mathcal{D}_3) = (\mathcal{D}_1, \mathcal{D}_3)$.

(La deuxième relation est une relation de Chasles.) Il se trouve que donner une telle définition n'est pas si simple que cela en a l'air, à cause de la nécessité de choisir un *sens* sur les droites. En effet, dessinons deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ sécantes en O. Choisissons des vecteurs directeurs $\vec{u}_1$ et $\vec{u}_2$ sur ces droites. Soit l'angle de vecteurs $\theta = (\vec{u}_1, \vec{u}_2)$. On a envie de dire que $(\mathcal{D}_1, \mathcal{D}_2) = \theta$ et $(\mathcal{D}_2, \mathcal{D}_1) = \pi - \theta$. Mais alors,

$$(\mathcal{D}_1, \mathcal{D}_1) = (\mathcal{D}_1, \mathcal{D}_2) + (\mathcal{D}_2, \mathcal{D}_1) = \theta + (\pi - \theta) = \pi$$

Or $(\mathcal{D}_1, \mathcal{D}_1) = 0$! On voit que ce problème disparaît si on définit les angles de droites *modulo* π, ce qui donne mène en effet à une définition correcte :

Définition 4.3.1 Soient deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ passant par un point O. Choisissons des vecteurs directeurs $\vec{u}_1$ et $\vec{u}_2$ sur ces droites. On pose par définition $(\mathcal{D}_1, \mathcal{D}_2) \stackrel{\text{déf}}{=} (\vec{u}_1, \vec{u}_2)$ $[\pi]$. Cela veut dire que deux réels θ, θ' qui mesurent l'angle orienté de droites $(\mathcal{D}_1, \mathcal{D}_2)$ diffèrent d'un multiple de π (il existe $k \in \mathbb{Z}$ tel que $\theta = \theta' + k\pi$).

Si on choisit $-\vec{u}_1$ plutôt que $\vec{u}_1$ pour vecteur directeur, alors on change l'angle orienté $(\vec{u}_1, \vec{u}_2)$. Cependant on voit que, modulo π, c'est bien la même chose puisque $(-\vec{u}_1, \vec{u}_2) = (-\vec{u}_1, \vec{u}_1) + (\vec{u}_1, \vec{u}_2) = \pi + (\vec{u}_1, \vec{u}_2)$ $[2\pi]$. Ceci étant dit, pour les angles de droites on a aussi une relation de Chasles :

$$(\mathcal{D}_1, \mathcal{D}_2) + (\mathcal{D}_2, \mathcal{D}_3) = (\mathcal{D}_1, \mathcal{D}_3) \ [\pi] \ .$$

Remarque 4.3.2 Vérifiez qu'il ne se passe rien de nouveau si on change $\vec{u}_2$ en $-\vec{u}_2$: les quatre angles $(\vec{u}_1, \vec{u}_2)$, $(-\vec{u}_1, \vec{u}_2)$, $(\vec{u}_1, -\vec{u}_2)$ et $(-\vec{u}_1, -\vec{u}_2)$ sont égaux modulo π.

Notons qu'on peut ramener une égalité du type $\theta = \theta'$ $[\pi]$ à des égalités modulo 2π :

Lemme 4.3.3 *« $\theta = \theta'$ $[\pi]$ » équivaut à « $\theta = \theta'$ $[2\pi]$ ou $\theta = \theta' + \pi$ $[2\pi]$ ».*

Démonstration : (Idée) En effet, si $\theta = \theta' + k\pi$ on écrit la division euclidienne de k par 2 : $k = 2k' + r$ avec un reste r qui vaut 0 ou 1. On a donc $\theta = \theta' + r\pi + 2k'\pi$. □

4.4 Bissectrices

Voici les subtilités, liées aux discussions qui précèdent, des notions de bissectrices :

Définition 4.4.1 Soient δ_1 et δ_2 deux demi-droites d'origine O. Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ deux droites passant par O.

(i) On appelle *demi-droite bissectrice* du secteur $[\delta_1, \delta_2]$ la demi-droite β située à l'intérieur du secteur et telle que $(\delta_1, \beta) = (\beta, \delta_2)$ $[2\pi]$. On appelle *droite bissectrice* du secteur $[\delta_1, \delta_2]$ la droite réunion des deux demi-droites vérifiant $(\delta_1, \beta) = (\beta, \delta_2)$ $[2\pi]$, c'est-à-dire β et $-\beta$.

(ii) On appelle *bissectrice* de l'angle de droites $(\mathcal{D}_1, \mathcal{D}_2)$ une droite $\mathcal{B}$ passant par O et telle que $(\mathcal{D}_1, \mathcal{B}) = (\mathcal{B}, \mathcal{D}_2)$ $[\pi]$. Un angle de droites a deux bissectrices, dites *intérieure* et *extérieure* ; elles sont perpendiculaires entre elles.

Dans n'importe lequel de ces cas, on construit une bissectrice comme médiatrice de $[A_1A_2]$, où A_1 et A_2 sont deux points choisis sur les (demi-)droites appropriées et tels que $OA_1 = OA_2 > 0$. Pour justifier le point (ii) de la définition 4.4.1, montrons comment on trouve deux bissectrices pour un angle de droites. Une bissectrice $\mathcal{B}$ doit vérifier

$$(\mathcal{D}_1, \mathcal{B}) + (\mathcal{B}, \mathcal{D}_2) = 2(\mathcal{D}_1, \mathcal{B}) = \theta \ [\pi] \ .$$

Utilisant le lemme 4.3.3, on peut écrire de manière équivalente : $2(\mathcal{D}_1, \mathcal{B}) = \theta$ $[2\pi]$ ou $2(\mathcal{D}_1, \mathcal{B}) = \theta + \pi$ $[2\pi]$. C'est équivalent à

$$(\mathcal{D}_1, \mathcal{B}) = \tfrac{\theta}{2} \ [\pi] \quad \text{ou} \quad (\mathcal{D}_1, \mathcal{B}) = \tfrac{\theta}{2} + \tfrac{\pi}{2} \ [\pi] \ .$$

On voit qu'on obtient deux droites et qu'elles sont perpendiculaires entre elles.

4.5 Trigonométrie des angles

Le théorème de Thalès permet de définir diverses quantités trigonométriques associées aux angles. Soient $\vec{u}$ et $\vec{v}$ deux vecteurs non nuls. Considérons un point origine O et un vecteur $\vec{w} \neq \vec{0}$ tel que $(\vec{u}, \vec{w}) = \pi/2\ [2\pi]$. On note $\mathcal{D}_u$, $\mathcal{D}_w$ les droites passant par O et dirigées par $\vec{u}$, $\vec{w}$ (ces vecteurs donnent une orientation pour les mesures algébriques).

Étant donné un réel quelconque $R > 0$ on peut considérer le point M_R de la demi-droite $(O, \vec{v})$ tel que $OM_R = R$. Soit C_R et S_R ses projetés orthogonaux sur $\mathcal{D}_u$ et $\mathcal{D}_w$.

Définition 4.5.1 Avec les notations ci-dessus, on définit

(1) le *cosinus* $\cos(\vec{u}, \vec{v}) \stackrel{\text{déf}}{=} \overline{OC}_R / \overline{OM}_R$

(2) le *sinus* $\sin(\vec{u}, \vec{v}) \stackrel{\text{déf}}{=} \overline{OS}_R / \overline{OM}_R$

(3) la *tangente* $\tan(\vec{u}, \vec{v}) \stackrel{\text{déf}}{=} \overline{OS}_R / \overline{OC}_R$ est définie lorsque $C_R \neq O$.

(4) la *cotangente* $\operatorname{cotan}(\vec{u}, \vec{v}) \stackrel{\text{déf}}{=} \overline{OC}_R / \overline{OS}_R$ est définie lorsque $S_R \neq O$.

Le théorème de Thalès permet de montrer que ces quantités sont indépendantes de R. Le plus souvent on les calcule donc en utilisant le cercle de rayon 1. Le théorème de Pythagore n'est pas absent de l'histoire : il fournit la fameuse relation $\cos^2(\theta) + \sin^2(\theta) = 1$. Les formules usuelles de trigonométrie peuvent être démontrées par voie géométrique ; nous donnons un exemple dans l'exercice suivant.

Exercice 4.5.2 Démontrez la formule $\cos(a + b) = \cos a \cos b - \sin a \sin b$.

Définition 4.5.3 Le *produit scalaire* de deux vecteurs $\vec{u}$ et $\vec{v}$ est le nombre réel défini par

- $\vec{u}.\vec{v} \stackrel{\text{déf}}{=} \|\vec{u}\| \|\vec{v}\| \cos(\vec{u}, \vec{v})$ si aucun des deux vecteurs n'est nul,
- $\vec{u}.\vec{v} \stackrel{\text{déf}}{=} 0$ sinon (l'angle orienté $(\vec{u}, \vec{v})$ n'est alors pas défini.)

On peut donner une autre description du produit scalaire : lorsque $\vec{u} = \overrightarrow{MA}$ et $\vec{v} = \overrightarrow{MB}$, appelons H le projeté orthogonal de B sur la droite (MA). Il est facile de voir que

$$\overrightarrow{MA}.\overrightarrow{MB} = \overline{MA} \times \overline{MH}\ .$$

Proposition 4.5.4 *Le produit scalaire vérifie : pour tous vecteurs $\vec{u}$, $\vec{v}$, $\vec{w}$ et tout $\lambda \in \mathbb{R}$,*

(i) $(\lambda\vec{u}).\vec{v} = \lambda(\vec{u}.\vec{v})$

(ii) $(\vec{u} + \vec{v}).\vec{w} = \vec{u}.\vec{w} + \vec{v}.\vec{w}$

(iii) $\vec{u}.\vec{v} = 0$ *ssi* $\vec{u}$ *et* $\vec{v}$ *sont orthogonaux.*

Démonstration : Les propriétés sont relativement évidentes, sauf peut-être la deuxième. Pour la démontrer choisissons des points A, B, C, E tels que $\vec{u} = \overrightarrow{AB}$, $\vec{v} = \overrightarrow{AC}$ et $\vec{w} = \overrightarrow{AE}$. Alors $\vec{u}+\vec{v}$ est égal au vecteur $\overrightarrow{AD}$, où D est le point tel que $ACDB$ est un parallélogramme. Appelons H, K, L les projetés orthogonaux de B, C, D sur (AE). Comme $ACDB$ est un parallélogramme on vérifie facilement que $\overline{AH} = \overline{KL}$. Il en découle que

$$\overline{AD} \times \overline{AL} = \overline{AD} \times (\overline{AK} + \overline{KL}) = \overline{AD} \times \overline{AK} + \overline{AD} \times \overline{AH}$$

c'est-à-dire exactement $(\vec{u} + \vec{v}).\vec{w} = \vec{u}.\vec{w} + \vec{v}.\vec{w}$. □

Exercice 4.5.5 Soit ABC un triangle. Montrez que la hauteur issue de A est l'ensemble des points M du plan tels que $\overrightarrow{MA}.\overrightarrow{MB} = \overrightarrow{MA}.\overrightarrow{MC}$.

Exercice 4.5.6 Rappelons que la *distance d'un point M à une droite* (AB) est la longueur MH, où H est le projeté orthogonal de M sur la droite (AB). C'est la plus petite des longueurs MC lorsque $C \in (AB)$, car on a $MC = \sqrt{MH^2 + HC^2} \geq MH$ d'après le théorème de Pythagore. Montrez que l'ensemble des points à égale distance de deux droites sécantes $\mathcal{D}_1$ et $\mathcal{D}_2$ est la réunion de leurs deux bissectrices.

5 Transformations du plan

Dans ce paragraphe nous étudions les principales transformations du plan utilisées en géométrie euclidienne. L'*identité* id_E définie par $\mathrm{id}_E(M) = M$ est la plus simple d'entre elles. En guise de préambule rappelons que, étant données deux applications $f\colon E \to E$ et $g\colon E \to E$, on définit leur *composée* comme étant l'application notée $g \circ f\colon E \to E$ et définie par $(g \circ f)(M) \overset{\text{déf}}{=} g(f(M))$. C'est l'action successive de f sur le point M, puis de g sur le point $f(M)$. Méfiez-vous du fait que, chronologiquement, on applique f puis g, alors que la notation $g \circ f$ semble refléter l'ordre inverse.

Certaines applications $f\colon E \to E$ ont une *réciproque* (on dit aussi une *inverse*), c'est-à-dire une application $g\colon E \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_E$. La réciproque est notée f^{-1}, mais attention, cette notation ne doit pas induire de confusion avec l'inverse d'un nombre réel... Si f a une réciproque, on dit qu'elle est *bijective*. Une *transformation du plan* est par définition une application bijective $f\colon E \to E$.

5.1 Isométries

Définition 5.1.1 Une *isométrie du plan* est une transformation du plan $u\colon E \to E$ qui préserve la longueur, c.-à-d. que pour tous points A, B d'images A', B' on a $A'B' = AB$.

L'isométrie la plus simple est l'identité id_E. Rappelons sans démonstration les propriétés générales des isométries :

Proposition 5.1.2 *Une isométrie conserve les les milieux, l'alignement, le parallélisme, l'orthogonalité, les angles non orientés.* □

Nous montrerons (théorème 5.1.5) qu'il y a exactement quatre types d'isométries :

Définitions 5.1.3

(i) *Réflexions.* Soit $\mathcal{D}$ une droite. Pour tout point M du plan, on considère H le projeté orthogonal de M sur $\mathcal{D}$, et le point M' tel que $\overrightarrow{HM'} = -\overrightarrow{HM}$. On pose $s_{\mathcal{D}}(M) \overset{\text{déf}}{=} M'$ ce qui définit la réflexion (ou symétrie) d'axe $\mathcal{D}$.

(ii) *Translations.* Soit $\vec{v}$ un vecteur. Pour tout point M du plan, on considère le point M' tel que $\overrightarrow{MM'} = \vec{v}$. On pose $t_{\vec{v}}(M) \overset{\text{déf}}{=} M'$ ce qui définit la translation de vecteur $\vec{v}$.

(iii) *Symétries glissées.* Soient $\vec{v}$ un vecteur et $\mathcal{D}$ une droite parallèle à la direction de $\vec{v}$. On pose $\sigma_{\vec{v},\mathcal{D}} \overset{\text{déf}}{=} t_{\vec{v}} \circ s_{\mathcal{D}}$ ce qui définit la symétrie glissée de vecteur $\vec{v}$ et d'axe $\mathcal{D}$.

(iv) *Rotations.* Soit $\theta \in \mathbb{R}$ et O un point. Pour tout point M du plan, on considère le point M' tel que $OM' = OM$ et $(\overrightarrow{OM}, \overrightarrow{OM'}) = \theta\ [2\pi]$. On pose $r_{O,\theta}(M) = M'$ ce qui définit la rotation de centre O et d'angle θ.

Les *éléments caractéristiques* d'une isométrie sont ceux qui la déterminent exactement. Pour une réflexion il s'agit donc de son axe $\mathcal{D}$, pour une translation son vecteur $\vec{v}$, pour une symétrie glissée son vecteur $\vec{v}$ et son axe $\mathcal{D}$, enfin, pour une rotation, son centre O et son angle θ. Pour les symétries glissées, il n'est pas tout à fait immédiat de trouver les éléments caractéristiques ; à bien y réfléchir il n'est même pas évident que deux couples vecteur-axe $(\vec{v}, \mathcal{D})$ différents ne puissent pas définir la même symétrie glissée. Aussi, attirons l'attention sur le fait suivant :

Lemme 5.1.4 *Le vecteur $\vec{v}$ d'une symétrie glissée σ est déterminé par le fait que $\sigma \circ \sigma$ est une translation de vecteur $2\vec{v}$. Son axe $\mathcal{D}$, par le fait que $\sigma \circ t_{-\vec{v}}$ est la réflexion d'axe $\mathcal{D}$.*

Démonstration : Il est facile de vérifier que, $\vec{v}$ et $\mathcal{D}$ étant parallèles, on a $t_{\vec{v}} \circ s_{\mathcal{D}} = s_{\mathcal{D}} \circ t_{\vec{v}}$. Il en résulte que $\sigma \circ \sigma = t_{\vec{v}} \circ s_{\mathcal{D}} \circ t_{\vec{v}} \circ s_{\mathcal{D}} = t_{\vec{v}} \circ t_{\vec{v}} \circ s_{\mathcal{D}} \circ s_{\mathcal{D}} = t_{2\vec{v}}$. Le reste est clair. □

Le théorème de classification nous dit que ce sont là les seules isométries :

Théorème 5.1.5 *Toute isométrie du plan est de l'une des formes suivantes :*

(1) *un* déplacement *: translation ou rotation, si elle préserve l'orientation,*

(2) *un* antidéplacement *: réflexion ou symétrie glissée, si elle change l'orientation.*

En particulier toute isométrie est une composée de réflexions : les translations et les rotations sont composées de 2 réflexions, et les symétries glissées sont composées de 3 réflexions.

La démonstration est donnée dans l'Annexe B. En regardant les points fixes des isométries on obtient une autre façon de les classer :

(a) une isométrie sans point fixe est une translation ou une symétrie glissée,

(b) une isométrie avec un seul point fixe est une rotation,

(c) une isométrie avec une droite de points fixes est une réflexion.

5.2 Homothéties et homogénéité de l'aire

Définition 5.2.1 Soit O un point et $\lambda \in \mathbb{R}$. L'*homothétie de centre O et de rapport λ* est la transformation du plan $h_{O,\lambda}$ définie comme suit : pour tout point M du plan, on considère le point M' tel que $\overrightarrow{OM'} = \lambda \overrightarrow{OM}$. On pose $h_{O,\lambda}(M) \overset{\text{déf}}{=} M'$.

Cas particuliers 5.2.2 (i) Si $\lambda = 1$ l'homothétie est juste l'identité.

(ii) Si $\lambda = -1$ l'homothétie est la *symétrie centrale de centre O*.

(iii) Si $\lambda = 0$ la transformation envoie tous les points sur le point O. Souvent on ne considère pas ce cas particulier comme une homothétie.

Il découle directement du théorème de Thalès qu'une homothétie de rapport λ multiplie toutes les longueurs par $|\lambda|$. Donc les seules homothéties qui sont des isométries sont l'identité et les symétrie centrales ($\lambda = -1$). En conséquence :

Lemme 5.2.3 *Soit h une homothétie de rapport $\lambda \neq 0$ et u une isométrie. Alors $h \circ u \circ h^{-1}$ est une isométrie.*

Démonstration : Appliquant successivement h^{-1}, puis u, puis h, la longueur d'un segment est multipliée par $1/|\lambda|$, puis inchangée, puis multipliée par $|\lambda|$. Au total elle est donc inchangée. □

Théorème 5.2.4 *L'aire est* homogène*, c'est-à-dire que pour toute homothétie h de rapport λ et pour tout polygone $\mathcal{P}$, on a $\mathcal{A}(h(\mathcal{P})) = \lambda^2\mathcal{A}(\mathcal{P})$.*

Démonstration : Fixons une homothétie h de rapport $\lambda \neq 0$ (si $\lambda = 0$ le résultat est évident). Considérons la fonction $\mathcal{A}'$ qui associe la quantité $\mathcal{A}'(\mathcal{P}) \overset{\text{déf}}{=} \frac{1}{\lambda^2}\mathcal{A}(h(\mathcal{P}))$ à un polygone $\mathcal{P}$. On va démontrer qu'elle vérifie les trois propriétés $(\mathcal{A}1)$, $(\mathcal{A}2)$ et $(\mathcal{A}3)$ du paragraphe 2.6.

La propriété $(\mathcal{A}1)$ est conséquence de la proposition 2.6.2, appliquée pour le rectangle de côtés $a = b = \lambda$. Notons que c'est là que le facteur $1/\lambda^2$ est crucial pour avoir $\mathcal{A}'(C) = 1$.

Pour vérifier $(\mathcal{A}2)$, soient $\mathcal{P}$ et $\mathcal{Q}$ deux polygones disjoints. Alors $h(\mathcal{P})$ et $h(\mathcal{Q})$ sont deux polygones disjoints, donc on a $\mathcal{A}(h(\mathcal{P}) \cup h(\mathcal{Q})) = \mathcal{A}(h(\mathcal{P})) + \mathcal{A}(h(\mathcal{Q}))$. En divisant par λ^2 on en déduit $\mathcal{A}'(\mathcal{P} \cup \mathcal{Q}) = \mathcal{A}'(\mathcal{P}) + \mathcal{A}'(\mathcal{Q})$, c'est ce qu'on voulait.

On doit enfin vérifier l'invariance par isométrie. Soit u une isométrie, d'après le lemme on a une isométrie $v \overset{\text{déf}}{=} h \circ u \circ h^{-1}$ ou encore $h \circ u = v \circ h$. On n'a plus qu'à faire le calcul

$$\mathcal{A}'(u(\mathcal{P})) = \frac{1}{\lambda^2}\mathcal{A}\big(h(u(\mathcal{P}))\big) = \frac{1}{\lambda^2}\mathcal{A}\big(v(h(\mathcal{P}))\big) = \frac{1}{\lambda^2}\mathcal{A}\big(h(\mathcal{P})\big) = \mathcal{A}'(\mathcal{P})$$

(on a utilisé l'invariance de $\mathcal{A}$ par l'isométrie v). Il en résulte bien que $\mathcal{A}'$ vérifie $(\mathcal{A}3)$.

Il n'y a qu'une fonction vérifiant les propriétés $(\mathcal{A}1)$ à $(\mathcal{A}3)$ (on l'a admis, *cf* § 2.6), donc $\mathcal{A}' = \mathcal{A}$. Cela signifie exactement que $\mathcal{A}(h(\mathcal{P})) = \lambda^2\mathcal{A}(\mathcal{P})$, pour tout polygone $\mathcal{P}$. □

6 Droites remarquables dans les triangles

Rappelons, s'il le fallait, que les *hauteurs* d'un triangle sont les droites passant par un sommet et perpendiculaires au côté opposé. Les *médianes* sont les droites passant par un sommet et le milieu du côté opposé. Dans ce paragraphe nous démontrons les théorèmes classiques qui affirment que ces droites sont concourantes.

Proposition 6.1 *Les trois médiatrices d'un triangle sont concourantes en un point O appelé* centre du cercle circonscrit *du triangle.*

Démonstration : On utilise la description des médiatrices donnée dans 3.1.3. Soient A, B, C les sommets du triangle et $\mathcal{D}_A$, $\mathcal{D}_B$, $\mathcal{D}_C$ les médiatrices (resp. de $[BC]$, $[AC]$, $[AB]$). Soit O l'intersection de $\mathcal{D}_A$ et $\mathcal{D}_B$. On a donc $OB = OC$ et $OC = OA$. Donc $OB = OA$ c'est-à-dire que $O \in \mathcal{D}_C$. Remarque : le cercle circonscrit au triangle est le cercle de centre O et de rayon $R = OA = OB = OC$. □

Proposition 6.2 *Les trois bissectrices intérieures d'un triangle sont concourantes en un point I appelé* centre du cercle inscrit *du triangle.*

Remarquons que le sens du mot *intérieur* est différent de celui de la définition 4.4.1(ii) : la « bissectrice intérieure » en le sommet A est ici celle des deux bissectrices de $((AB), (AC))$ qui traverse l'intérieur du triangle.

Démonstration : Soient A, B, C les sommets du triangle et $\mathcal{B}_A$, $\mathcal{B}_B$, $\mathcal{B}_C$ les bissectrices intérieures en A, B, C. Utilisons 4.5.6 : l'ensemble des points situés à égale distance de (AB) et (AC) est constitué de deux droites et $\mathcal{B}_A$ est celle des deux qui traverse l'intérieur du triangle. Donc, le point I d'intersection de $\mathcal{B}_A$ et $\mathcal{B}_B$ est à égale distance de (AB) et (AC) d'une part, et de (AB) et (BC), d'autre part. Donc I est à égale distance de (AC) et (BC), comme il est intérieur au triangle, $I \in \mathcal{B}_C$. □

Remarques 6.3 (1) Le cercle inscrit dans le triangle est le cercle de centre I et de rayon $r = d(I,(AB)) = d(I,(BC)) = d(I,(AC))$.

(2) Si on ne considère pas seulement les bissectrices intérieures mais toutes les bissectrices, la même preuve que celle donnée montre que deux quelconques des bissectrices extérieures, et la troisième bissectrice intérieure, sont concourantes. On obtient ainsi trois nouveaux cercles inscrits, situés à l'extérieur du triangle.

Proposition 6.4 *Soit $\mathcal{T} = ABC$ un triangle. On nomme A^* (resp. B^*, C^*) l'intersection des deux droites parallèles aux côtés contenant A (resp. B, C) et passant par les sommets opposés. On associe ainsi à $\mathcal{T}$ un nouveau triangle $\mathcal{T}^* = A^*B^*C^*$.*

(1) *Les médianes de $\mathcal{T}$ et celles de $\mathcal{T}^*$ sont les mêmes.*

(2) *Les hauteurs de $\mathcal{T}$ sont les médiatrices de $\mathcal{T}^*$.*

Démonstration : On observe que comme $ACBC^*$, AB^*CB, ACA^*B sont des parallélogrammes, leurs diagonales se coupent en leur milieu donc les droites (AA^*), (BB^*), (CC^*) sont les médianes de $\mathcal{T}$. D'autre part utilisant les mêmes parallélogrammes on a $C^*A = BC = AB^*$, et de même sur les autres côtés de $\mathcal{T}^*$. Ainsi A est le milieu de $[B^*C^*]$, B est le milieu de $[A^*C^*]$, C est le milieu de $[A^*B^*]$. Donc les droites (AA^*), (BB^*), (CC^*) sont aussi les médianes de $\mathcal{T}^*$.

Il est alors clair que la hauteur de $\mathcal{T}$ issue de A est la médiatrice de $[B^*C^*]$, et idem sur les autres côtés de $\mathcal{T}^*$. Ceci prouve (1) et (2). □

Proposition 6.5 *Les trois médianes d'un triangle sont concourantes en un point G appelé* centre de gravité *du triangle. Ce point est situé aux $2/3$ sur chaque médiane, par exemple, si (AA') est la médiane en un sommet A on a : $AG = \frac{2}{3}AA'$.*

Démonstration : Soit $\mathcal{T} = ABC$ un triangle et considérons le triangle $\mathcal{T}^*$ de la proposition 6.4. Soit G l'intersection de (AA^*) et (BB^*), deux des médianes de $\mathcal{T}$. D'après le théorème de Thalès on a

$$\frac{\overline{GA^*}}{\overline{GA}} = \frac{\overline{GB^*}}{\overline{GB}} = \frac{\overline{A^*B^*}}{\overline{AB}} = -2\,.$$

On introduit l'homothétie h de centre G et de rapport -2, de sorte que $h(A) = A^*$ et $h(B) = B^*$. L'image par h de (BC) est une parallèle à (BC) et passant par $h(B) = B^*$, donc c'est (B^*C^*). De même l'image par h de (AC) est une parallèle à (AC) et passant par $h(A) = A^*$, donc c'est (A^*C^*). Donc l'image de $(BC) \cap (AC)$ est $(B^*C^*) \cap (A^*C^*)$, i.e. $h(C) = C^*$. En particulier G, C et C^* sont alignés, donc G est situé sur la troisième médiane. Enfin soit A' le milieu de $[BC]$, utilisant le fait que $h(A) = A^*$ on déduit que $\overrightarrow{AA^*} = 3\overrightarrow{AG} = 2\overrightarrow{AA'}$ d'où la propriété des $2/3$. □

Proposition 6.6 *Les trois hauteurs d'un triangle sont concourantes en un point H appelé* orthocentre *du triangle.*

Démonstration : Soit $\mathcal{T} = ABC$ un triangle. D'après la proposition 6.4 les trois hauteurs de $\mathcal{T}$ sont les trois médiatrices de $\mathcal{T}^*$, et donc d'après 6.1 elles sont concourantes. □

Théorème 6.7 (Droite d'Euler) *Dans un triangle, le centre du cercle circonscrit O, le centre de gravité G et l'orthocentre H sont alignés sur une droite appelée la* droite d'Euler *du tiangle. De plus on a $\overrightarrow{GH} = -2\overrightarrow{GO}$.*

Démonstration : On reprend les notations $\mathcal{T} = ABC$, $\mathcal{T}^* = A^*B^*C^*$ et h l'homothétie h de centre G et de rapport -2. Celle-ci envoie les médiatrices de $\mathcal{T}$ sur les médiatrices de $\mathcal{T}^*$, donc envoie le centre du cercle circonscrit O sur le centre du cercle circonscrit O^* de $\mathcal{T}^*$. Comme les médiatrices de $\mathcal{T}^*$ sont les hauteurs de $\mathcal{T}$ (proposition 6.4) on a $O^* = H$. Donc $h(O) = H$, on en déduit que G, H, O sont alignés et que $GH = 2GO$. □

Annexe A : Triangles et quadrilatères

A.1 Triangles

Définition A.1.1 Soit ABC un triangle. On dit qu'il est *isocèle* s'il a au moins deux côtés de même longueur. On dit qu'il est *rectangle* s'il a un angle droit. On dit qu'il est *équilatéral* si ses trois côtés sont de même longueur. On dit qu'il est *rectangle isocèle* s'il est rectangle et isocèle.

Exercice A.1.2 Montrez qu'un triangle est isocèle si et seulement s'il a au moins deux angles égaux. Montrez que dans un triangle équilatéral tous les angles valent $\pi/3$. Que valent les angles d'un triangle rectangle isocèle ?

Exercice A.1.3 Soit ABC un triangle. Soit (AI) la médiane issue de A. Montrez que ABC est un triangle rectangle en A ssi $AI = BI = CI$.

La propriété suivante est très classique. Pour la démontrer nous utiliserons des propriétés des parallélogrammes, et donc nous attendrons le paragraphe suivant.

Proposition A.1.4 *La somme des angles (non orientés) d'un triangle est égale à π.*

A.2 Quadrilatères

Un quadrilatère est un polygone à quatre côtés. On distingue les quadrilatères convexes, les quadrilatères *croisés* pour lesquels deux côtés se coupent en un point autre qu'un sommet, et les quadrilatères *convexes* qui sont les autres (ni convexes ni croisés).

Définition A.2.1 Soit $ABCD$ un quadrilatère convexe.

(i) On dit que c'est un *trapèze* s'il a deux côtés opposés parallèles.

(ii) On dit que c'est un *parallélogramme* si ses côtés opposés sont parallèles 2 à 2. C'est la même chose de dire que ses côtés opposés sont égaux 2 à 2, ou encore, que les angles aux sommets opposés sont égaux 2 à 2, ou encore, que les diagonales se coupent en leur milieu.

(iii) On dit que c'est un *rectangle* si c'est un quadrilatère avec 4 angles droits. C'est la même chose de dire que c'est un parallélogramme avec un angle droit, ou encore, un parallélogramme dont les diagonales ont même longueur.

(iv) On dit que c'est un *losange* si c'est un quadrilatère avec 4 côtés égaux. C'est la même chose de dire que c'est un parallélogramme avec des diagonales perpendiculaires.

(v) On dit que c'est un *carré* si c'est un rectangle et un losange.

Exercice A.2.2 Démontrez que les différentes définitions d'un parallélogramme sont équivalentes : côtés opposés parallèles, ou côtés opposés égaux, ou angles aux sommets opposés, ou diagonales se coupant en leur milieu.

Remarque A.2.3 On peut maintenant démontrer que la somme des angles (non orientés) d'un triangle est égale à π (proposition A.1.4). En effet, soit ABC un triangle et α, β, γ les angles en A, B, C. Soient I et J les milieux de $[AB]$ et $[AC]$. Soit C' (resp. B') symétrique de C (resp. B) par rapport à I (resp. J). Les propriétés de la symétrie montrent que (AC') est parallèle à (BC), et (BC') parallèle à (AC). Donc $AC'BC$ est un parallélogramme, ainsi, $\widehat{AC'B} = \widehat{ACB}$. On en déduit que $\widehat{B'AC} = \widehat{AC'B} = \widehat{ACB} = \gamma$.

On montre de la même façon que $\widehat{C'AB} = \widehat{ABC} = \beta$. Il en découle que

$$\pi = \widehat{B'AC} + \widehat{CAB} + \widehat{C'AB} = \gamma + \alpha + \beta \, .$$

C'est exactement dire que la somme des angles est égale à π.

A.3 Polygones généraux

Définition A.3.1 Soit $n \geq 2$ un entier et $A_0, A_1, \ldots, A_n$ des points du plan E tels que trois points consécutifs ne sont pas alignés. La *ligne polygonale de sommets A_i et de côtés* $[A_iA_{i+1}]$, notée $\mathcal{L} = (A_0A_1 \ldots A_n)$ est la suite des n segments $[A_0A_1]$, $[A_1A_2]$,... $[A_{n-1}A_n]$, pris dans cet ordre. On dit que $\mathcal{L}$ est *fermée* si $A_n = A_0$.

Définition A.3.2 On dit qu'une ligne polygonale $\mathcal{L}$ est *simple* si elle vérifie la propriété suivante : si deux côtés de $\mathcal{L}$ ont un point d'intersection, alors ce sont deux côtés consécutifs $[A_{i-1}A_i]$ et $[A_iA_{i+1}]$ et leur intersection est réduite à leur sommet commun A_i.

Un *polygone* est une ligne polygonale fermée simple.

Définition A.3.3 On appelle *diagonale* d'un polygone $\mathcal{P}$ un segment $[A_iA_j]$ entre deux sommets, qui n'est pas un côté.

Dans le cas particulier où le nombre de sommets est $n = 3$ on obtient une définition du triangle équivalente à celle déjà donnée (2.2.1(4)). Le cas du triangle est très particulier car si A, B, C ne sont pas alignés alors une ligne polygonale entre ces points est forcément simple. Une autre particularité des triangles est qu'ils n'ont pas de diagonale.

En général la définition de l'intérieur donnée dans 2.2.1(4) n'a pas de sens pour les polygones quelconques (essayez d'adapter la définition et testez-la sur des exemples pour voir que ce n'est pas simple !). Ceux pour lesquels elle fonctionne encore sont appelés des polygones *convexes* :

Définition A.3.4 On dit qu'un polygone $\mathcal{P}$ est *convexe* si pour chaque côté $[A_iA_{i+1}]$, l'un des demi-plans fermés délimités par le côté (plus exactement par la droite (A_iA_{i+1})) contient $\mathcal{P}$.

On peut définir en toute généralité l'*intérieur* (et donc l'*extérieur*) d'un polygone quelconque. Ces deux zones recouvrent le plan et vérifient les propriétés qu'on en attend : on peut rejoindre deux points de l'intérieur (ou de l'extérieur) par une courbe ou une ligne polygonale, sans franchir $\mathcal{P}$. Par contre on est obligé de franchir $\mathcal{P}$ pour joindre un point intérieur et un point extérieur.

Voici une définition précise de ces zones : soit M un point du plan n'appartenant pas à $\mathcal{P}$. Soit δ une demi-droite d'origine M ne rencontrant aucun sommet de $\mathcal{P}$, et $\nu(M, \delta)$ le nombre de côtés de $\mathcal{P}$ que coupe δ. On montre que la parité de $\nu(M, \delta)$ est indépendante de δ.

Définition A.3.5 On dit que M est *intérieur* à un polygone $\mathcal{P}$ ssi $\nu(M, \delta)$ est impair, et *extérieur* à $\mathcal{P}$ ssi $\nu(M, \delta)$ est pair.

Remarque A.3.6 Il est fréquent qu'on utilise le terme « polygone » pour désigner à la fois le polygone en tant que ligne comme nous l'avons défini, ou la réunion de cette ligne (la frontière) et de l'intérieur. Le contexte ou l'énoncé permet toujours de distinguer quel sens est utilisé.

Soit $\mathcal{P}$ un polygone et $\mathcal{P}^+$ la réunion du polygone et de son intérieur. On peut montrer que les conditions suivantes sont équivalentes :

(1) $\mathcal{P}$ est convexe ;

(2) pour chaque paire de points A et B sur $\mathcal{P}$, on a $[AB] \subset \mathcal{P}^+$;

(3) pour chaque paire de sommets A_i et A_j, on a $[A_iA_j] \subset \mathcal{P}^+$;

(4) pour chaque point M dans l'intérieur de $\mathcal{P}$, toute demi-droite δ d'origine M coupe $\mathcal{P}$ en un unique point ;

(5) les angles de $\mathcal{P}$ sont tous saillants.

Proposition A.3.7 *La somme des angles d'un polygone convexe à n côtés est égale à $(n-2)\pi$.*

Démonstration : Considérons un point O intérieur au polygone, et traçons les n segments qui le relient aux sommets. On obtient un découpage du polygone en n triangles. La somme des angles de ces triangles (soit $n\pi$ d'après la proposition A.1.4) est égale à la somme des angles du polygone, plus la somme des angles de sommet O, égale à 2π (un angle plein). Finalement la somme des angles du polygone est égale à $(n-2)\pi$. □

Annexe B : classification des isométries

Définition B.1 Une *isométrie du plan* est une transformation du plan $u\colon E \to E$ qui préserve la longueur, c.-à-d. que pour tous points A, B d'images A', B' on a $A'B' = AB$.

Dans cette Annexe, nous allons étudier et classer les isométries. Nous mettrons en évidence une propriété importante des rotations et des déplacements (voir B.10) qui permettra de définir ce qu'est l'*orientation*. Tant que ceci ne sera pas fait, nous ne pouvons pas utiliser la définition des rotations donnée dans 5.1.3. Provisoirement, nous dirons qu'une rotation est une composée de deux réflexions d'axes sécants.

Définitions B.2 (i) Soit $\mathcal{D}$ une droite. La *réflexion (ou symétrie) d'axe* $\mathcal{D}$ notée $s_{\mathcal{D}}$ est définie ainsi. Soit M un point du plan et H son projeté orthogonal sur $\mathcal{D}$. On considère le point M' tel que $\overrightarrow{HM'} = -\overrightarrow{HM}$ et on pose $s_{\mathcal{D}}(M) \overset{\text{déf}}{=} M'$.

(ii) Soit $\vec{v}$ un vecteur. La *translation de vecteur* $\vec{v}$ notée $t_{\vec{v}}$ est définie ainsi. Soit M un point, on considère le point M' tel que $\overrightarrow{MM'} = \vec{v}$ et on pose $t_{\vec{v}}(M) \overset{\text{déf}}{=} M'$.

(iii) Soient $\vec{v}$ un vecteur et $\mathcal{D}$ une droite parallèle à la direction de $\vec{v}$. La *symétrie glissée de vecteur* $\vec{v}$ *et d'axe* $\mathcal{D}$ est définie par $\sigma_{\vec{v},\mathcal{D}} \overset{\text{déf}}{=} t_{\vec{v}} \circ s_{\mathcal{D}}$.

(iv) Soit O un point. Une *rotation de centre* O est une isométrie composée de deux réflexions d'axes passant par O.

Le théorème que nous voulons démontrer est le suivant :

Théorème B.3 *Toute isométrie est de l'une des formes suivantes :*

(1) *un* déplacement *: translation ou rotation,*

(2) *un* antidéplacement *: réflexion ou symétrie glissée.*

En particulier toute isométrie est une composée de réflexions (en nombre ≤ 3*).*

Passons à la démonstration, qui se fera en plusieurs étapes. Comme on l'a déjà dit, pour définir une rotation en « tournant » d'un angle θ autour du point O (comme on en a l'habitude) il nous manque le concept d'*orientation* (donc on ne sait pas « dans quel sens tourner »). On peut tout de même démontrer que les rotations, définies comme dans B.2(iv), « font tourner » avec un angle (non orienté) constant :

Proposition B.4 *Soit* $r = s_{\mathcal{D}_2} \circ s_{\mathcal{D}_1}$ *une rotation de centre* O *et soit* ψ *une mesure de l'angle aigu délimité par* $\mathcal{D}_1$ *et* $\mathcal{D}_2$*. Alors pour toute demi-droite* δ *d'origine* O*, notant* $\delta' = r(\delta)$*, on a* $\widehat{\delta, \delta'} = 2\psi$*.*

Démonstration : Fixons deux demi-droites $\delta_1 \subset \Delta_1$ et $\delta_2 \subset \Delta_2$, d'origine O, telles que le secteur $[\delta_1, \delta_2]$ est aigu. Posons $\delta^* \overset{\text{déf}}{=} s_{\mathcal{D}_1}(\delta)$, $\alpha \overset{\text{déf}}{=} \widehat{\delta_1, \delta}$ et $\beta \overset{\text{déf}}{=} \widehat{-\delta_1, \delta}$. Distinguons trois cas. Faire un dessin pour chaque cas est obligatoire pour comprendre ce qui suit !

- $\delta \subset [\delta_1, \delta_2]^{\wedge}$. Alors $\widehat{\delta_1, \delta^*} = \widehat{\delta_1, \delta} = \alpha$ et $\widehat{\delta_2, \delta'} = \widehat{\delta_2, \delta^*} = \psi + \alpha$.
  Donc $\widehat{\delta, \delta'} = (\psi + \alpha) + (\psi - \alpha) = 2\psi$.

- $\delta \subset [\delta_1, \delta_2]^{\vee}$ et $\beta \leq \psi$. Alors $\widehat{-\delta_1, \delta^*} = \widehat{-\delta_1, \delta} = \beta$ et $\widehat{-\delta_2, \delta'} = \widehat{-\delta_2, \delta^*} = \psi - \beta$.
  Donc $\widehat{\delta, \delta'} = (\psi + \beta) + (\psi - \beta) = 2\psi$.

- $\delta \subset [\delta_1, \delta_2]^{\vee}$ et $\beta > \psi$. Alors $\widehat{-\delta_1, \delta^*} = \widehat{-\delta_1, \delta} = \beta$ et $\widehat{-\delta_2, \delta'} = \widehat{-\delta_2, \delta^*} = \beta - \psi$.
  Donc $\widehat{\delta, \delta'} = (\beta + \psi) - (\beta - \psi) = 2\psi$. □

La proposition suivante sera essentielle pour la démonstration du théorème B.3 :

Proposition B.5 *L'ensemble des points fixes d'une isométrie est soit vide, soit un point, soit une droite, soit E tout entier (dans ce dernier cas l'isométrie est* id_E*). En particulier, une isométrie qui fixe trois points non alignés est l'identité.*

Démonstration : Soit u une isométrie qui a deux points fixes distincts A et B. Montrons qu'alors toute la droite (AB) est fixe. Soit $M \in (AB)$ un point et $M' \overset{\text{déf}}{=} u(M)$ son image. On a $AM' = AM$ de sorte que si $M' \neq M$, le point A appartient à la médiatrice $\mathcal{D}$ de $[MM']$. De même B appartient à $\mathcal{D}$, donc $\mathcal{D} = (AB)$, ce qui est impossible car $M \in (AB)$. C'est donc que $M' = M$, donc la droite (AB) est fixe.

Montrons maintenant que si u a trois points fixes non alignés A, B, C, le plan entier est fixe. Soit $M \in E$ et $M' \overset{\text{déf}}{=} u(M)$. Comme ci-dessus on montre que si $M' \neq M$ alors A, B et C appartiennent à la médiatrice de $[MM']$, ce qui contredit l'hypothèse de non alignement. □

Proposition B.6 *Soient δ et δ' deux demi-droites (distinctes ou non) d'origine O. Alors il existe une unique rotation r de centre O et telle que $r(\delta) = \delta'$.*

Démonstration : Soient $\mathcal{D}$ la droite qui supporte δ et $\mathcal{B}$ la droite bissectrice du secteur $[\delta, \delta']$. Il est facile de vérifier que la rotation $r \overset{\text{déf}}{=} s_{\mathcal{B}} \circ s_{\mathcal{D}}$ envoie δ sur δ'.

Prenons maintenant deux rotations r_1 et r_2 qui envoient δ sur δ', on va montrer qu'elles sont égales. Supposons qu'il existe un point M du plan, dont les images $N_1 \overset{\text{déf}}{=} r_1(M)$ et $N_2 \overset{\text{déf}}{=} r_2(M)$ soient distinctes (donc, $M \notin \delta$). Soit A un point de δ distinct de O et soit $A' = r_1(A) = r_2(A)$. Comme les triangles $OA'N_1$ et $OA'N_2$ sont isométriques (tous les deux au triangle OAM), alors N_2 est le symétrique de N_1 par la réflexion d'axe (OA'). Donc les isométries $s_{(OA')} \circ r_1$ et r_2 coïncident en trois points non alignés O, A, M. Ainsi $s_{(OA')} \circ r_1 \circ r_2^{-1}$ fixe ces trois points, donc c'est l'identité (proposition B.5), donc $s_{(OA')} \circ r_1 = r_2$. Nous allons montrer que ceci est impossible.

Exhibons une demi-droite β d'image $\beta' = (s_{(OA')} \circ r_1)(\beta)$, telle que $\widehat{\beta, \beta'} \neq \widehat{\delta, \delta'}$. Si $\delta \neq \delta'$ on peut prendre pour β la demi-droite bissectrice de $[\delta, \delta']$ (définition 4.4.1(i)). Si $\delta = \delta'$ on peut prendre pour β n'importe quelle demi-droite distincte de δ. La vérification que $\widehat{\beta, \beta'} \neq \widehat{\delta, \delta'}$ est facile (il faut utiliser B.4 de nouveau). Donc $s_{(OA')} \circ r_1$ ne peut pas être une rotation, car ceci contredirait la proposition B.4. Donc $s_{(OA')} \circ r_1 = r_2$ est impossible. De la contradiction on déduit que pour tout point M on a $r_1(M) = r_2(M)$, donc $r_1 = r_2$. □

Les résultats précédents nous permettent de décomposer les rotations et les translations à l'aide de réflexions :

Corollaire B.7 *Soit r une rotation de centre O et $\mathcal{D}$ une droite passant par O. Alors*

(i) *il existe une unique droite $\mathcal{E}$ passant par O telle que $r = s_{\mathcal{E}} \circ s_{\mathcal{D}}$,*

(ii) *il existe une unique droite $\mathcal{F}$ passant par O telle que $r = s_{\mathcal{D}} \circ s_{\mathcal{F}}$.*

Démonstration : Soit $\delta \subset \mathcal{D}$ une demi-droite d'origine O.

Soient $\delta' \overset{\text{déf}}{=} r(\delta)$ et $\mathcal{E}$ la droite bissectrice de $[\delta, \delta']$ (définition 4.4.1). Ainsi r envoie δ sur δ' et on vérifie facilement que la rotation $s_{\mathcal{E}} \circ s_{\mathcal{D}}$ aussi, donc $r = s_{\mathcal{E}} \circ s_{\mathcal{D}}$ d'après B.6.

Soient $\delta'' \overset{\text{déf}}{=} r^{-1}(\delta)$ et $\mathcal{F}$ la droite bissectrice de $[\delta, \delta'']$. Ainsi r envoie δ'' sur δ et on vérifie facilement que la rotation $s_{\mathcal{D}} \circ s_{\mathcal{F}}$ aussi, donc $r = s_{\mathcal{D}} \circ s_{\mathcal{F}}$ d'après B.6.

On peut dire aussi que $\mathcal{E}$ est l'ensemble des points fixes de $r \circ s_{\mathcal{D}}$ et $\mathcal{F}$ est l'ensemble des points fixes de $s_{\mathcal{D}} \circ r$. Ceci montre que ces droites sont uniques. □

Proposition B.8 *Soit t, translation de vecteur $\vec{u}$ et $\mathcal{D}$, droite orthogonale à $\vec{u}$. Alors*

(i) *il existe une unique droite $\mathcal{E}$ parallèle à $\mathcal{D}$ telle que $t = s_{\mathcal{E}} \circ s_{\mathcal{D}}$,*

(ii) *il existe une unique droite $\mathcal{F}$ parallèle à $\mathcal{D}$ telle que $t = s_{\mathcal{D}} \circ s_{\mathcal{F}}$.*

Démonstration : La droite $\mathcal{E}$ est la translatée de $\mathcal{D}$ d'un vecteur $\frac{1}{2}\vec{u}$ et la droite $\mathcal{F}$ est la translatée de $\mathcal{D}$ d'un vecteur $-\frac{1}{2}\vec{u}$. Les vérifications, faciles, sont laissées en exercice. □

Corollaire B.9 *La composée de deux déplacements est un déplacement.*

Démonstration : Soient d et d' deux déplacements. Si ce sont deux translations, la composée est une translation de vecteur égal à la somme des vecteurs des deux translations.

Si ce sont des rotations de centres O et O', choisissons une droite $\mathcal{D}$ passant par O et O' : si $O \neq O'$ seul le choix de $\mathcal{D} = (OO')$ est possible. Par le corollaire B.7 il existe des droites (uniques) $\mathcal{E}$ et $\mathcal{F}$ passant par O, telles que $d = s_{\mathcal{E}} \circ s_{\mathcal{D}}$ et $d' = s_{\mathcal{D}} \circ s_{\mathcal{F}}$. Alors $d \circ d' = s_{\mathcal{E}} \circ s_{\mathcal{D}} \circ s_{\mathcal{D}} \circ s_{\mathcal{F}} = s_{\mathcal{E}} \circ s_{\mathcal{F}}$. C'est une rotation ou une translation, selon que $\mathcal{E}$ et $\mathcal{F}$ sont sécantes ou non.

Enfin si l'un est une translation et l'autre une rotation, par exemple si d est une translation de vecteur $\vec{v}$ et d' est une rotation de centre O, on appelle $\mathcal{D}$ la perpendiculaire à $\vec{v}$ passant par O. D'après B.8 il existe une unique droite $\mathcal{E}$ parallèle à $\mathcal{D}$ telle que $d = s_{\mathcal{E}} \circ s_{\mathcal{D}}$. De même d'après B.7 il existe une unique droite $\mathcal{F}$ passant par O telle que $d' = s_{\mathcal{D}} \circ s_{\mathcal{F}}$. On obtient $d \circ d' = s_{\mathcal{E}} \circ s_{\mathcal{F}}$ qui est une rotation. □

Corollaire B.10 *Soient δ et δ' deux demi-droites, distinctes ou non, d'origines O et O'. Alors il existe un unique déplacement d tel que $d(\delta) = \delta'$.*

Démonstration : En utilisant la translation de vecteur $\overrightarrow{OO'}$ puis une rotation (cf B.6) on peut envoyer δ sur δ'. Pour ce qui est de l'unicité, supposons qu'on ait deux déplacements d et d' qui envoient δ sur δ'. Alors $d^{-1} \circ d'$ fixe δ; d'après B.9 c'est un déplacement ; comme il a un point fixe (le point O) alors c'est une rotation. Par ailleurs l'identité est une autre rotation qui fixe δ. Par unicité (voir B.6) on a donc $d^{-1} \circ d' = \mathrm{id}_E$ i.e. $d' = d$. □

On est enfin en mesure de classifier les isométries du plan :

Démonstration du théorème de classification B.3.

Soit u une isométrie, et soit ABC un triangle avec A, B, C non alignés. Soit $A'B'C'$ le triangle image par u. D'après B.10 il existe un déplacement d qui envoie $[A'B']$ sur $[AB]$.

- Si d envoie $A'B'C'$ sur ABC alors $d \circ u$ fixe ABC, donc c'est l'identité d'après B.5. Cela signifie que $u = d^{-1}$, c'est une rotation ou une translation.

- Sinon, le point C' est envoyé sur le symétrique de C par la réflexion d'axe (AB), notée s. Comme précédemment on déduit que $s \circ d$ envoie $A'B'C'$ sur ABC, que $s \circ d \circ u$ fixe ABC, que c'est l'identité, et donc que $u = d^{-1} \circ s$. On utilise alors B.7 et B.8 pour se ramener à une réflexion ou une symétrie glissée.

On a fini ! □

On peut enfin définir les concepts d'orientation (voir 4.1.2), d'angle orienté de vecteurs (4.2.1) et décrire les rotations comme on en a l'habitude (5.1.3). Nous renvoyons au corps du cours pour tout cela.

Annexe C : Le plan euclidien assimilé à $\mathbb{R}^2$

Si on s'autorise à utiliser les nombres réels sans modération, un autre point de vue sur la Géométrie plane est de considérer que le plan euclidien est (par définition, si on veut) l'ensemble $E \stackrel{\text{déf}}{=} \mathbb{R}^2$ des couples de nombres réels.

Cette présentation se démarque de façon essentielle de celle développée par Euclide par le fait qu'on ne s'embarrasse plus pour justifier que la géométrie que l'on fait « colle » bien à la réalité. En contrepartie on peut *définir* tous les concepts qu'on étudie (points, droites, longueurs, angles...) et on n'a pas besoin de *postuler* qu'ils existent.

Dans cette annexe, nous rappelons comment sont définis, sous ce nouvel éclairage, les principaux concepts que nous avons passés en revue au long du cours.

C.1 Les points de $\mathbb{R}^2$ et le repère canonique

Un point $M \in E$ est donc donné par deux réels x, y qui sont ses *coordonnées*. On le note $M(x, y)$. Deux points sont égaux si et seulement si leurs coordonnées sont égales.

C.1.1 Vecteurs. Un vecteur $\vec{u}$ est donné par deux réels a, b qui sont ses coordonnées. On le note $\vec{u}(a, b)$. Cela peut sembler être la même chose qu'un point, mais il faut penser à un vecteur plutôt comme une « différence de points ». Ainsi deux points $A(x_A, y_A)$ et $B(x_B, y_B)$ déterminent un unique vecteur, noté $\overrightarrow{AB}$, dont les coordonnées sont

$$(x_B - x_A, y_B - y_A) \ .$$

D'autres points C et D peuvent déterminer le même vecteur, précisément, on a $\overrightarrow{CD} = \overrightarrow{AB}$ si et seulement si $x_D - x_C = x_B - x_A$ et $y_D - y_C = y_B - y_A$.

Le *vecteur nul* est le vecteur $\overrightarrow{0}$ de coordonnées $(0, 0)$. Le vecteur somme de $\vec{u}(a, b)$ et $\vec{u}\,'(a', b')$ est le vecteur $\vec{u} + \vec{u}\,'$ de coordonnées $(a + a', b + b')$. Par ailleurs, étant donné un nombre réel $\lambda \in \mathbb{R}$, on peut définir le vecteur $\lambda\vec{u}$ qui est le vecteur de coordonnées $(\lambda a, \lambda b)$.

Étant donnés deux vecteurs $\vec{u}(a, b)$ et $\vec{u}\,'(a', b')$ on peut définir leur *produit scalaire* noté $\vec{u}.\vec{u}'$ et leur *déterminant* noté $\det(\vec{u}, \vec{u}\,')$. Ce sont tous deux des nombres réels, ils sont définis par :

- $\vec{u}.\vec{u}\,' \stackrel{\text{déf}}{=} aa' + bb'$
- $\det(\vec{u}, \vec{u}\,') \stackrel{\text{déf}}{=} ab' - ba'$

On dit que $\vec{u}$ et $\vec{u}\,'$ sont *orthogonaux* ssi $\vec{u}.\vec{u}\,' = 0$, et *colinéaires* ssi $\det(\vec{u}, \vec{u}\,') = 0$.

(Choisissons deux droites quelconques $\mathcal{D}$ et $\mathcal{D}'$ de vecteurs directeurs $\vec{u}$ et $\vec{u}\,'$, voir § C.2 ci-dessous. Alors c'est la même chose de dire que $\vec{u}.\vec{u}\,' = 0$ ou que $\mathcal{D}$ et $\mathcal{D}'$ sont orthogonales, et c'est la même chose de dire que $\det(\vec{u}, \vec{u}\,') = 0$ ou que $\mathcal{D}$ et $\mathcal{D}'$ sont parallèles.)

C.1.2 Repère canonique. Dans $\mathbb{R}^2$ il y a trois points particulièrement importants : l'origine $O(0, 0)$ et les points $I(1, 0)$ et $J(0, 1)$. Ces points déterminent des vecteurs $\vec{\imath} \stackrel{\text{déf}}{=} \overrightarrow{OI}$ et $\vec{\jmath} \stackrel{\text{déf}}{=} \overrightarrow{OJ}$ qu'on appelle les *vecteurs canoniques*. Le *repère canonique* est le triplet $(O, \vec{\imath}, \vec{\jmath})$ composé de l'origine et des deux vecteurs canoniques.

Le repère canonique permet de représenter tous les vecteurs comme sommes de la forme $\vec{u} = a\vec{\imath} + b\vec{\jmath}$, et donc tous les points $M(x, y)$ par l'écriture : $\overrightarrow{OM} = x\vec{\imath} + y\vec{\jmath}$.

C.2 Droites, demi-droites, segments

C.2.1 Représentations paramétriques. Soient $A(x_A, y_A)$ et $B(x_B, y_B)$ deux points distincts du plan. La droite (AB) est l'ensemble des points $M(x, y)$ avec $x = x(t)$ et $y = y(t)$ tels que

$$\begin{cases} x = x_A + t(x_B - x_A) \\ y = y_A + t(y_B - y_A) \end{cases} \qquad (t \in \mathbb{R})$$

On dit que t est le *paramètre de M sur la droite*, dans le repère formé par A et B. Par exemple, A est le point de paramètre $t = 0$ et B est le point de paramètre $t = 1$. La demi-droite $[AB)$ est l'ensemble des points $M(x(t), y(t))$ comme ci-dessus, avec $t \geq 0$. Le segment $[AB]$ est l'ensemble des points $M(x(t), y(t))$ comme ci-dessus, avec $0 \leq t \leq 1$.

C.2.2 Équations. Une autre manière de décrire une droite (AB) est d'en donner une équation : c'est l'ensemble des points M dont les coordonnées (x, y) vérifient une équation $ax + by + c = 0$, avec a et b non tous les deux nuls.

On peut donner explicitement une équation de (AB) en fonction des coordonnées de A et B, à savoir l'équation $(x_B - x_A)(y - y_A) = (y_B - y_A)(x - x_A)$.

Étant donnée une droite $\mathcal{D}$ d'équation $ax + by + c = 0$, un vecteur directeur pour $\mathcal{D}$ est le vecteur $\vec{u}(-b, a)$. Bien sûr, n'importe quel vecteur $\lambda\vec{u}$ avec $\lambda \neq 0$ est aussi un vecteur directeur.

C.2.3 Coefficients directeurs. Soient $A(x_A, y_A)$ et $B(x_B, y_B)$ deux points distincts. Si $x_B \neq x_A$ on appelle *coefficient directeur* (ou *pente*) de la droite (AB) le nombre $m \overset{\text{déf}}{=} \frac{y_B - y_A}{x_B - x_A}$ et on met en général l'équation sous la forme $y = mx + p$.

Soient deux droites d'équations $y = mx + p$ et $y = m'x + p'$. Elles sont parallèles ssi $m = m'$, et orthogonales ssi $mm' = -1$.

Exercice C.2.4 Redémontrez la dernière affirmation sur le parallélisme et l'orthogonalité en trouvant des vecteurs directeurs $\vec{u}$ et $\vec{u}'$ pour les deux droites, et en traduisant ces conditions sur $\vec{u}$ et $\vec{u}'$.

C.3 Longueurs

Définition C.3.1 Soient $A(x_A, y_A)$ et $B(x_B, y_B)$ deux points du plan. On définit la *longueur* du segment $[AB]$ comme étant égale à $\sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}$.

Supposons que la longueur AB soit égale à 1. Alors, pour tout point $M \in (AB)$ repéré par son paramètre t (voir C.2.1), il est facile de vérifier que la longueur AM est égale à $|t|$.

Remarque C.3.2 Cette définition semble, bien sûr, justifiée par le théorème de Pythagore. Mais il faut bien comprendre que dans cette présentation de la géométrie plane, opposée à celle d'Euclide, on ne peut pas vraiment démontrer le théorème de Pythagore, car une égalité telle que $BC^2 = AB^2 + AC^2$ aura forcément lieu, par définition de la longueur !

Annexe D : Petite parenthèse de Sciences Physiques

Le fait de manipuler des grandeurs nous oblige à nous demander ce que c'est, et ce que veut dire mesurer une grandeur. Quelques rappels sont donc utiles.

D.1 Il y a dans la nature des *grandeurs* physiques. Cela n'a pas de sens de vouloir comparer entre elles des grandeurs différentes, comme la longueur d'une règle, le poids d'une pomme, le temps mis par la Terre pour tourner une fois sur elle-même, ou le volume d'un récipient. Ainsi cela n'a pas de sens d'écrire

« la longueur du terrain de foot est plus petite que son aire » .

Deux grandeurs différentes ne peuvent pas non plus être ajoutées ou retranchées, par exemple cela n'a pas de sens d'écrire

« l'aire du triangle rectangle + la longueur de l'hypothénuse » .

Par contre, on peut multiplier ou diviser des grandeurs physiques différentes, et on en obtient alors une nouvelle. Par exemple, si on divise une longueur par une durée on obtient une vitesse, et si on multiplie une longueur par une longueur on obtient une aire.

D.2 Chaque grandeur physique peut être mesurée si on choisit un *étalon* ou *unité*. Dans l'exemple de la longueur, on choisit donc une *longueur étalon* ou *longueur unité*. Mesurer une longueur veut dire la comparer à la longueur unité qu'on a choisie, et dès lors cette longueur unité devient *unité de longueur* pour la mesure. Une fois une unité choisie, la *mesure* d'une grandeur est le nombre de fois que l'unité intervient. Par exemple, la rotation de la Terre sur elle-même a une durée (c'est une grandeur) que l'on peut mesurer en heures ou en minutes (ce sont des unités). Le résultat est 24 heures, ou 1440 minutes : deux unités différentes donnent deux mesures différentes, pour la même grandeur. On voit donc qu'*il ne faut pas confondre « grandeur » et « mesure d'une grandeur »*.

Objet	Ex. de grandeur attachée	Unité de mesure de la grandeur	
segment	longueur	mètre	m
secteur angulaire	angle	radian	rad
domaine du plan	aire	mètre carré	m^2
cours de Maths	durée	seconde	s
casserole	température	degré celsius	^{o}C
saucisson	masse	kilogramme	kg
saucisson	poids	newton	N
saucisson	volume	mètre cube	m^3

(Une aire et une durée sont aussi attachées à la *surface* du saucisson et au *moment* où on le mange.)

D.3 Dans le cours, les grandeurs qui nous intéressent sont la longueur, l'angle, et l'aire. Pour ne pas alourdir le vocabulaire nous disons presque tout le temps « longueur » ou « aire » au lieu de « mesure de la longueur » ou « mesure de l'aire », mais en restant conscient du fait que ce n'est là qu'une commodité de langage.