Découverte des maths
Résumé de cours
L1, année 2017-2018

État d'avancement : chapitre 5 quasi-fini, chapitre 6 en cours

8 décembre 2017

Table des matières

Chapitre 1

Logique et raisonnements

1.0.1 Préambule : vocabulaire et ensembles classiques

Afin de pouvoir illustrer les notions de ce chapitre dans le contexte des mathématiques, on part du principe qu'un certain nombre de choses sont connues :

1. Les ensembles classiques : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, les mêmes privés de zéro : $\mathbb{N}^*$, ..., $\mathbb{C}^*$. Les lois de composition classiques sur ces ensembles : addition, multiplication, avec leurs règles de calcul.
2. L'égalité dans ces ensembles, la relation d'ordre dans $\mathbb{R}$: $x < y$ se lit « x est strictement inférieur à y », $x \leq y$ se lit « x est inférieur à y » (on précise parfois « inférieur ou égal » même si sans précision, une inégalité est toujours prise au sens large).
3. La relation de divisibilité dans $\mathbb{Z}$: la suite de symboles $a|b$ se lit « a divise b ».
4. Les notations d'appartenance d'un élément à un ensemble :on écrit $x \in E$ pour dire que x est un élément de l'ensemble E et $x \notin E$ sinon. Par exemple, $\dfrac{2}{3} \in \mathbb{Q}$, mais $\sqrt{2} \notin \mathbb{Q}$ (cela sera prouvé dans la suite du chapitre).
5. Les notations $\mathbb{R}_+$, $\mathbb{Q}_-$, etc pour des contraintes de signe (au sens large : 0 appartient à $\mathbb{Q}_+$ par exemple). On peut combiner : l'ensemble $\mathbb{R}_+^*$ est l'ensemble des réels strictement positifs.
6. Les fonctions classiques, comme la racine carrée et la valeur absolue.

Tout ceci sera revu en détail de toutes façons.

1.0.2 Propositions / assertions logiques

Définition 1.0.1. Une proposition est une phrase à laquelle on peut attribuer le statut « VRAI » ou « FAUX ». La phrase peut en outre comporter des symboles qui désignent des objets mathématiques (comme des chiffres) et d'autres symboles qui désignent des relations mathématiques entre objets (par exemple l'égalité, inégalité, divisibilité, appartenance à un ensemble...)

Par exemple « $2+2=3$ » et « $2+3=5$ » sont des propositions (la première est fausse, la seconde vraie). La phrase « le nombre complexe i est positif » (ou encore « quelle heure est-il ? ») ne sont pas des propositions, on ne peut pas leur affecter de statut : la première n'a pas de sens (un nombre complexe n'a pas de signe), la seconde a un sens mais on ne peut pas lui affecter de statut VRAI ou FAUX.

Variables, paramètres, assertions ouvertes et fermées Une proposition peut dépendre d'un ou plusieurs paramètres, ou variables. Un paramètre est un symbole qui désigne un élément (explicité ou pas) d'un ensemble.

Les symboles nouveau doivent **toujours** être définis (ou déclarés) avec leur type (l'ensemble auquel appartient l'objet), de sorte à pouvoir être sûr du fait que la phrase est bien une assertion, c'est-à-dire possède un statut VRAI ou FAUX.

Par exemple : Dans « $x \geq 0$ », le symbole x n'est pas défini, on ne peut pas être sûr que la phrase ait un sens. Si x était un nombre complexe par exemple, la phrase n'aurait aucun sens. Le symbole x pourrait désigner beaucoup d'autres objets mathématiques, par exemple ... un cercle, les coordonnées d'un point du plan, auquel cas la phrase n'a pas non plus de sens.

D'autre part si x est un nombre naturel, la phrase a un sens mais elle est trivialement vraie car tous les naturels sont positifs. Tout ceci montre qu'il est crucial de déclarer clairement les variables et leur type *avant* de commencer à les utiliser.

On déclare des objets à l'aide de la locution « Soit ». La phrase « Soit x un réel. » déclare un réel, que l'on note x. La phrase « Soit $k \in \mathbb{Z}$. » déclare un entier relatif (l'usage de $\in$ comme abréviation pour « appartenant à »est toléré dans ce cas-là, même si en général on interdit d'utiliser les symboles mathématiques comme des abréviations).

La phrase « Soit x. » n'est pas une déclaration correcte d'objet mathématique : on doit préciser le type.

Si on précise que x est un nombre réel, « $x \geq 0$ »devient une assertion mathématique bien formée. Le statut de cette proposition dépend de la valeur de x : elle est vraie si $x \in \mathbb{R}_+$, elle est fausse si $x \in \mathbb{R}_-^*$. Le fait ne pas pouvoir connaître explicitement le statut n'est pas un problème. De fait que lorsqu'on déclare un réel x, on ne sait pas a priori lequel c'est.

1.0.3 Construction de propositions

Considérons deux propositions A et B. Dans les exemples qui suivent, sauf précision, x est un nombre réel.

Conjonction : « A et B » La proposition « A et B » est vraie si A et B sont vraies. Elle est fausse dès que l'une au moins des deux est fausse.

Exemple : « $x > 2$ et $x < 5$ » est vraie si $x \in]2,5[$. Elle est fausse sinon.

Disjonction : « A ou B » La proposition « A ou B » est vraie dès que l'une des deux est vraie, elle est fausse si les deux sont fausses. Lorsqu'on affirme que « A ou B »est vraie, l'un n'exclut pas l'autre.

Exemple : « $x > 2$ ou $x < 5$ » est vraie pour tout nombre réel x.

Négation : « non A » La proposition « non A » est vraie si A est fausse et inversement.

Implication logique : « $A \Rightarrow B$ » La proposition « $A \Rightarrow B$ »signifie par définition « B ou non-A ». Elle est vraie si A est fausse ou si B est vraie.
Exemples : $2+2=4 \Rightarrow 2\times 2=4$ est vraie. $2+2=5 \Rightarrow 2\times 2=4$ est vraie. $2+2=5 \Rightarrow 2\times 2=5$ est vraie. $2+2=4 \Rightarrow 2\times 2=5$ est fausse. Autre exemple : si x est un nombre réel, la proposition $x>3 \Rightarrow x>4$ est vraie pour $x \leq 3$ ou pour $x>4$. Elle est fausse si $3 < x \leq 4$.

Attention : le symbole $\Rightarrow$ n'est en aucun cas une abréviation pour « donc ». La proposition $A \Rightarrow B$ ne veut pas dire « A est vraie donc B est vraie »!

Équivalence logique : « $A \Leftrightarrow B$ » La proposition « $A \Leftrightarrow B$ » signifie par définition « $A \Rightarrow B$ et $B \Rightarrow A$ ». Elle est vraie si A et B ont même statut, que ce soit vrai ou faux. Elle est fausse si A et B ont des statuts différents.
Exemples : $2+2=5 \Leftrightarrow 2\times 3=7$ est vraie. $1>0 \Leftrightarrow 2+2=4$ est vraie. Si x est un nombre réel, la proposition $x>3 \Leftrightarrow x<4$ est vraie pour $x \in]3,4[$. Elle est fausse sinon.

1.0.4 Quantificateurs

Soit $A(x)$ une proposition dépendant d'un paramètre x appartenant à un ensemble E (exemple : « $x>3$ », où $x \in \mathbb{Z}$).

Quantificateur universel : $\forall$ (quelque soit/pour tout)
La proposition « $\forall x \in E,\ A(x)$ » se lit « pour tout x dans E, $A(x)$ ». Elle est vraie si $A(x)$ est vraie pour toutes les valeurs que peut prendre x dans l'ensemble E. Elle est fausse dès qu'il existe une valeur spéciale de x pour laquelle $A(x)$ est fausse. Attention, contrairement à la proposition $A(x)$, la proposition $\forall x \in E,\ A(x)$ est une proposition qui ne dépend d'aucun paramètre : elle est soit vraie soit fausse : on dit que x est une variable muette, ou interne. Exemples : $\forall x \in R,\ x^2 > 1$ est fausse. La proposition $\forall x \in \mathbb{Z}^*,\ x^2 \geq 1$ est vraie.

Quantificateur existentiel : $\exists$ (il existe)
La proposition « $\exists x \in E / A(x)$ » se lit « il existe x dans E tel que $A(x)$ ». Elle est vraie s'il y a une valeur de x dans l'ensemble E telle que $A(x)$ soit vraie. Elle est fausse si $A(x)$ est fausse pour toutes les valeurs de x.

Théorème 1.0.2. On a les équivalences suivantes :
non (non A) $\Leftrightarrow$ A.
non (A ou B) $\Leftrightarrow$ (non A) et (non B).
non (A et B) $\Leftrightarrow$ (non A) ou (non B).
$(\forall x \in E,\ A(x)) \Leftrightarrow (\forall y \in E,\ A(y))$.
$\text{non}(\forall x \in E,\ A(x)) \Leftrightarrow \exists x \in E, \text{non}(A(x)))$.
$\text{non}(\exists x \in E,\ A(x)) \Leftrightarrow \forall x \in E, \text{non}(A(x)))$.

Démonstration : voir TD.

1.0.5 Méthodes de démonstration

Démonstration directe

Exemple : soit $n \in Z$; montrer que « n pair $\Rightarrow n^2$ pair ».
Exemple de rédaction:
Si n est pair, il existe $k \in Z$ tel que $n = 2k$. Alors, $n^2 = 4k^2 = 2(2k^2)$ est pair. (et si n est impair, l'implication est vraie par définition, il n'y a rien à prouver).□

Démonstration par contraposée

Principe : $(A \Rightarrow B)$ est équivalente à (non-$B \Rightarrow$ non-A).
Preuve du principe : (non-$B \Rightarrow$ non-A) $\Leftrightarrow$ (non-A ou $non - non - B$) $\Leftrightarrow$ (B ou $non - A$)□.
Exemple d'application : soit $n \in Z$; montrer que n^2 pair $\Rightarrow n$ pair.
Exemple de rédaction:
On va montrer la contraposée, autrement dit on va montrer « n impair $\Rightarrow n^2$ impair », qui est équivalente, mais plus facile à montrer. Supposons donc n impair. Alors il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$. Mais alors $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ est impair.
En combinant avec le résultat précédent, on a donc prouvé : « n^2 pair $\Leftrightarrow n$ pair »□

Démonstration par l'absurde

Principe : Si F désigne n'importe quelle proposition fausse, on a $A \Leftrightarrow$ (non-$A \Rightarrow F$).
Preuve du principe : (non-$A \Rightarrow F$) $\Leftrightarrow$ (F ou non-non-A) $\Leftrightarrow A$.
Donc pour montrer A, il suffit de supposer A faux et d'en déduire une contradiction (c'est-à-dire n'importe quelle proposition fausse).
Exemple d'application : Montrer que $\sqrt{2}$ n'est pas rationnel.
Exemple de rédaction:
Par l'absurde, supposons $\sqrt{2} \in \mathbb{Q}$. Alors il existe deux entiers p et q premiers entre eux tels que $\sqrt{2} = p/q$. Donc $p = q\sqrt{2}$ et donc $p^2 = 2q^2$, donc p^2 est pair, donc par l'exemple précédent p est pair. Donc il existe $k \in Z$ tel que $p = 2k$, d'où en remplacant $4k^2 = 2q^2$, donc en simplifiant q^2 est pair donc q est pair. Donc p et q sont tous les deux pairs, contradiction car ils sont premiers entre eux. Finalement cette contradiction prouve que $\sqrt{2} \notin \mathbb{Q}$.□

Démonstrations de propositions avec quantificateur universel

Pour démontrer $\forall x \in E,\ A(x)$, on écrit :
« Soit $x \in E$ un élément quelconque ».
Puis, on démontre $A(x)$.
Puis, pour conclure, on écrit : « x étant pris quelconque dans E, la propriété est bien démontrée ».

Exemple 1.0.3. Montrer que $\forall x \in \mathbb{R}, x^2+x+1>0$ ».

Exemple de rédaction :
Soit $x \in \mathbb{R}$. (déclaration de x)
On a $x^2+x+1=(x+\frac{1}{2})^2+\frac{3}{4}$. (Début preuve de $A(x)$)
Comme un carré est toujours positif, on a $(x+\frac{1}{2})^2 \geq 0$
et donc $x^2+x+1>0$. (fin preuve de $A(x)$)
Ceci montre donc bien $\forall x \in \mathbb{R}, x^2+x+1>0$ (Conclusion)

Exemple : Démontrer que $\forall x \in \mathbb{R},\ x^2+\cos(x)>0$.
Exemple de rédaction:
Soit $x \in \mathbb{R}$.
On distingue deux cas possibles suivant la valeur de x.
Si $0 \leq |x| < \pi/2$, alors $x^2 \geq 0$ et $\cos(x)>0$ donc $x^2+\cos(x)>0$.
Si $\pi/2 \leq |x|$, alors $x^2+\cos(x) \geq \pi^2/4-1>0$.
Comme x est quelconque, on a bien montré la propriété pour tout $x \in \mathbb{R}$.$\square$

Cas particulier : démonstrations par récurrence Dans le cas particulier où le quantificateur universel porte sur l'ensemble $\mathbb{N}$, on peut utiliser une méthode de preuve spécifique, la récurrence. Cette méthode de démonstration s'appuie sur le fait que toute partie non vide de $\mathbb{N}$ admet un plus petit élément (ce qui est faux pour la plupart des autres ensembles classiques). Il suffit alors de montrer d'une part que $A(0)$ est vraie, ce qui est généralement facile, puis de montrer que pour tout $n \in \mathbb{N}$, on a $A(n) \Rightarrow A(n+1)$. La première étape est cruciale et le raisonnement est faux si on l'omet.

Démonstrations de propositions avec quantificateur existentiel

Pour démontrer « $\exists x \in E / A(x)$, il faut soit construire un élément x tel que $A(x)$ soit vrai, soit utiliser un théorème qui affirme l'existence d'un tel objet, ou qui affirme l'existence d'un objet à partir duquel on peut obtenir l'existence de x.

Exemple 1 : soit f une fonction croissante de $[0,1]$ dans $\mathbb{R}$. Montrer que f est majorée, autrement dit montrer que $(\exists M \in \mathbb{R} / (\forall x \in [0,1],\ f(x) \leq M))$.
Exemple de rédaction:
Posons $M=f(1)$. On a bien $\forall x \in [0,1],\ f(x) \leq f(1)=M$, car f est croissante.$\square$

Exemple 2 : Montrer qu'il existe deux irrationnels a et b tels que a^b soit rationnel.
Exemple de rédaction:
Considérons le nombre réel $\sqrt{2}^{\sqrt{2}}$. Il est soit rationnel, soit irrationnel. Dans le premier cas, il suffit de poser $a=b=\sqrt{2}$ (irrationnels, voir exemple plus haut) et la preuve est terminée. Dans le second cas, il suffit de poser $a=\sqrt{2}^{\sqrt{2}}$ (qui est supposé irrationnel) et $b=\sqrt{2}$ On a

alors $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.□

Ce deuxième exemple montre que parfois, on n'a pas besoin de construire explicitement l'objet, seulement de montrer que ça existe, soit par l'analyse de cas de figure complémentaires, soit en utiisant un théorème qui affirme l'existence d'un certain objet sans forcément l'expliciter. Cela dit, la plupart du temps, il faut construire l'objet.

1.0.6 Résolution des équations

Soit $A(x)$ une proposition portant sur $x \in E$. Résoudre $A(x)$, c'est déterminer exactement l'ensemble des x tels que $A(x)$ soit vrai. Cet ensemble est un sous-ensemble de E, on l'appelle l'ensemble des solutions. Il peut parfois être vide (aucune solution) ou égal à E (équation triviale).

Méthode par équivalence
$A(x) \Leftrightarrow B(x) \Leftrightarrow \ldots \Leftrightarrow C(x)$ et on sait facilement résoudre $C(x)$. Cette méthode ne s'applique que rarement, essentiellement qu'aux (systèmes d') équations linéaires.

Exemple 1.0.4. Résoudre $2x+3=5$, d'inconnue $x \in \mathbb{R}$.
Exemple de rédaction :
Soit $x \in \mathbb{R}$. On a

$$\begin{aligned} 2x+3=8 &\iff 2x=5 \\ &\iff x=5/2. \end{aligned}$$

Méthode par conditions nécessaires et suffisantes
Lorsque $A(x) \Rightarrow B(x)$, on dit que $B(x)$ est une condition nécessaire à $A(x)$, et $A(x)$ est une condition suffisante pour $B(x)$.
Dans la pratique, on écrit $A(x) \Rightarrow B(x) \Rightarrow \ldots x \in \Omega$. Ensuite, parmi les éléments de Ω, on détermine ceux qui sont solution.

Exemple : résoudre $|x-1| = 2x+3$, d'inconnue $x \in \mathbb{R}$.
Exemple de rédaction:
Soit $x \in \mathbb{R}$. On a la chaîne d'implications $|x-1| = 2x+3 \Rightarrow |x-1|^2 = (2x+3)^2 \Leftrightarrow x^2-2x+1 = 4x^2+12x+9 \Leftrightarrow 3x^2+14x+8=0 \Leftrightarrow (x \in \{-4; -2/3\})$. Réciproquement, on vérifie que -4 n'est pas solution mais que $-2/3$ est solution. Finalement, l'équation a une unique solution, $-2/3$.□

Chapitre 2

Ensembles (VIDE)

Définition 2.0.1 (Restriction d'un ensemble)**.**

Définition 2.0.2 (Union, intersection et complémentaire de parties)**.**

Chapitre 3

Applications (VIDE)

Définition 3.0.1 (Applications entre ensembles)**.**

Définition 3.0.2. Soient A et B deux ensembles, et $f : A \to B$ une application. On dit que f est injective si

$$\forall (x, y) \in A^2, \quad f(x) = f(y) \Rightarrow x = y,$$

autrement dit si (contraposée)

$$\forall (x, y) \in A^2, \quad x \neq y \Rightarrow f(x) \neq f(y),$$

autrement dit si deux éléments distincts ont toujours des images distinctes. On dit aussi que f « sépare les points ».

Définition 3.0.3. On dit que f est surjective si

$$\forall b \in B, \quad \exists a \in A / f(a) = b,$$

autrement dit tout élément $b \in B$ a (au moins) un antécédent par f.

Définition 3.0.4. On dit que f est bijective si elle est injective et surjective.

Exemple 3.0.5. La fonction $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est ni injective, ni surjective. Elle n'est pas injective car bien que 1 soit différent de -1, ils ont la même image. Elle n'est pas surjective car -2 n'a pas d'antécédent dans $\mathbb{R}$: on ne peut pas trouver de réel x tel que $x^2 = -2$.

Exemple 3.0.6. La fonction $g : \mathbb{R} \to \mathbb{R}_+, x \mapsto x^2$ n'est pas injective pour les mêmes raisons que f, mais elle est surjective : l'ensemble d'arrivée est cette fois $\mathbb{R}_+$, et tout nombre réel positif $y \geq 0$ a au moins un antécédent, par exemple $-\sqrt{y}$.

Exemple 3.0.7. La fonction $h : \mathbb{R}_+ \to \mathbb{R}_+, x \mapsto x^2$ est injective et surjective, donc bijective. Elle est surjective pour la même raison que g, elle est injective, car si x et y sont des réels positifs ayant même carré, ils sont forcément égaux (ils sont positifs donc il n'y a pas l'ambiguité de signe).

En général, la surjectivité est plus dure à montrer que l'injectivité, car il faut résoudre une équation à paramètre : l'équation $f(x) = y$, de paramètre y, et d'inconnue x, et ce pour tous les paramètres y. La non surjectivité est en revanche souvent plus facile à montrer, il suffit de trouver un élément qui n'a pas d'antécédent, en général ça se voit (éventuellement après un petit calcul / majoration / développement d'expression).

Remarque 3.0.8. Si $f : A \to B$ est injective, alors on peut « identifier » A à un sous-ensemble de B grâce à f : un élément $a \in A$ est identifié à $f(a) \in B$. Cette identification n'est pas abusive grace à la propriété d'injectivité. La formulation correcte de cette identification est que f induit une bijection de A sur $f(A)$. Ceci n'est qu'une remarque.

Définition 3.0.9 (Restriction et prolongement d'une application)**.**

Chapitre 4

Entiers et ensembles finis, combinatoire (VIDE)

Chapitre vide.

4.1 L'ensemble $\mathbb{N}$ et la récurrence

4.2 Ensembles finis et cardinal

4.3 Coefficients binomiaux et combinatoire

Chapitre 5

Arithmétique

Attention, la présentation qui suit diffère sans doute beaucoup de celle vue en terminale : il faut faire l'effort de l'étudier en détail même si l'ordre dans lequel les notions sont introduites semble « mauvais » : en fait, c'est le « bon » ordre.

Le cours d'arithmétique des polynômes suivra le même canevas (définitions semblables, mêmes lemmes aux mêmes endroits, mêmes preuves), de même que le cours d'algèbre générale sur les anneaux par la suite.

5.1 Préliminaires

5.1.1 Division euclidienne

Proposition 5.1.1 (Division euclidienne)**.** Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}*$. Il existe un unique couple $(b, r) \in \mathbb{N}^2$ vérifiant les deux propriétés suivantes :

1. $a = bq + r$;
2. $r < b$.

L'entier b est le *quotient* de la division euclidienne de a par b, et r est le *reste*. Effectuer la division euclidienne de a par b, c'est écrire $a = bq + r$ avec b et q comme plus haut.

Exemple : $17 = 5 \times 3 + 2$ est la division euclidienne de 17 par 5. Le quotient est 3 et il reste 2. Par contre, l'écriture $17 = 5 \times 2 + 7$ bien que correcte n'est pas une division euclidienne, car le reste *doit* être strictement inférieur à 5, dans une division euclidienne.

5.1.2 Idéaux de $\mathbb{Z}$

Définition 5.1.2 (Ensembles $\alpha\mathbb{Z}$ et générateur principal)**.** Soit α un entier relatif. On note $\alpha\mathbb{Z}$ l'ensemble $\{\alpha k \mid k \in \mathbb{Z}\} = \{\dots, -2\alpha, -\alpha, 0, \alpha, 2\alpha, 3\alpha, \dots\}$. C'est l'ensemble des multiples de α. Les ensembles $\alpha\mathbb{Z}$ et $(-\alpha)\mathbb{Z}$ sont identiques.

Le *générateur principal* de $\alpha\mathbb{Z}$ est $|\alpha|$.

Exemples : $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, 9, 12, \dots\}$. Si $\alpha = 0$, alors $\alpha\mathbb{Z} = \{0\}$. On a $\alpha\mathbb{Z} = \mathbb{Z}$ ssi α est égal à 1 ou -1. Plus généralement, on a $a\mathbb{Z} = b\mathbb{Z}$ ssi $a = b$ ou $a = -b$.

Définition 5.1.3. Un sous-groupe de $\mathbb{Z}$ est une partie $G \subseteq \mathbb{Z}$ vérifiant les trois propriétés suivantes :

1. G contient 0.
2. G et est stable par somme :$\forall x, y \in G$, $x + y \in G$.
3. G et est stable par opposé :$\forall x \in G$, $-x \in G$.

Un ensemble de la forme $\alpha\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ (exercice). La proposition qui suit affirme que la réciproque est vraie.

Proposition 5.1.4. Soit $G \subseteq \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Alors, il existe $\alpha \in \mathbb{Z}$ tel que $G = \alpha\mathbb{Z}$.

Démonstration. Soit $G \subseteq \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Soit $G_+^* = G \cap \mathbb{N}^*$. Il y a deux cas :

1. Si G_+^* est vide, cela signifie que G ne possède aucun élément strictement positif. Comme G est stable par opposé, il ne peut pas non plus contenir d'éléments strictement négatifs. Cela signifie que $G = \{0\} = 0\mathbb{Z}$.
2. Sinon, c'est une partie non vide de $\mathbb{N}$, qui possède donc un plus petit élément, notons-le α. Par définition, G est stable par somme et opposé, donc $2\alpha \in G$ et $-\alpha \in G$ et plus généralement, pour tout $k \in \mathbb{Z}$, on a $k\alpha \in G$. Donc $\alpha \subseteq G$. Montrons l'inclusion inverse. Soit $x \in G$, positif. Écrivons la division euclidienne de x par α. On a $x = \alpha q + r$, avec $r < \alpha$. Comme G est stable par somme et différence et que $\alpha q \in G$, on en déduit que $r = x - \alpha q$ est également dans G. Or, $r < \alpha$, donc par minimalité de α, $r = 0$, ce qui montre que $x = \alpha q$, donc que $x \in \alpha\mathbb{Z}$. Si x est négatif, ce qui précède montre que $-x \in \alpha\mathbb{Z}$, donc que $x \in \alpha\mathbb{Z}$.

□

Proposition 5.1.5. Un sous-groupe G de $\mathbb{Z}$ est automatiquement *absorbant pour la multiplication*, c'est-à-dire :

$$\forall g \in G, \forall n \in \mathbb{Z}, ng \in G.$$

Pour cette raison et d'autres qui deviendront claires dans un futur cours d'algèbre, on utilise la dénomination « idéal de $\mathbb{Z}$ » au lieu de « sous-groupe de $\mathbb{Z}$ ». Les deux terminologies sont parfaitement équivalentes, dire *idéal* sert à rappeler la propriété supplémentaire d'être absorbant par multiplication.

5.2 Pgcd

Proposition 5.2.1. Soient a et b deux entiers. L'ensemble $\{ak+bl \mid k, l \in \mathbb{Z}\}$ noté par définition $a\mathbb{Z} + b\mathbb{Z}$, est un idéal de $\mathbb{Z}$. C'est le plus petit idéal de $\mathbb{Z}$ contenant a et b.

Démonstration. Il suffit de vérifier que c'est un sous-groupe de $\mathbb{Z}$. □

Définition 5.2.2. Soient a et b des entiers. Le générateur principal de $a\mathbb{Z} + b\mathbb{Z}$ est appelé le pgcd de a et b, il est noté $\mathrm{pgcd}(a, b)$ ou bien $a \wedge b$.

Proposition 5.2.3. Soient a et b des entiers, et $d = \mathrm{pgcd}(a, b)$. On a les propriétés suivantes

1. L'entier a est dans $a\mathbb{Z}+b\mathbb{Z}$, donc d divise a. De même, d divise b.
2. L'entier df est dans $d\mathbb{Z}$, donc il existe k et l dans $\mathbb{Z}$, tels que $d = ak + bl$. On dit que (k,l) est un couple (ou paire, par abus de langage) de Bézout pour a et b. L'égalité $d = ak + bl$ est appelée *relation de Bézout*.
3. Au sens de la divisibilité, d est le plus grand diviseur commun de a et b. Ceci explique le nom (*plus grand commun diviseur* de d. Cette propriété est précisée dans la proposition suivante.
4. Si $d = 0$, alors $a = b = 0$.
5. On a $\text{pgcd}(a,b) = \text{pgcd}(a,b) = \text{pgcd}(a,-b)$, car $a\mathbb{Z}+b\mathbb{Z} = b\mathbb{Z}+a\mathbb{Z} = a\mathbb{Z}+(-b)\mathbb{Z}$.
6. $\text{pgcd}(a,0) = |a|$.
7. $\text{pgcd}(a,1) = 1$.

Proposition 5.2.4. Si $x > 0$, $x|a$ et $x|b$, et $\forall m, m|a$ et $m|b \implies m|x$, alors $x = d$.

Démonstration. Si $x|a$ et $x|b$, alors $x|d$. D'autre part, $d|a$ et $d|a$, donc $d|x$. Donc finalement, $d = x$. Attention, la condition $x > 0$ est indispensable pour ce raisonnement. Deux entiers relatifs peuvent se diviser l'un l'autre, comme 1 et -1, sans être égaux. □

Proposition 5.2.5. Soit $k > 0$. On a $\text{pgcd}(ka,kb) = k\,\text{pgcd}(a,b)$.

Démonstration. Notons provisoirement $d_1 = \text{pgcd}(a,b)$ et $d_2 = \text{pgcd}(ka,kb)$.

Comme $d_1|a$ et $d_1|b$, on a $kd_1|ka$ et $kd_1|kb$ donc finalement $kd_1|d_2$. En particulier, $k|d_2$ donc $\dfrac{d_2}{k}$ est un entier.

D'autre part, $d_2|ka$ et $d_2|kb$, donc en divisant par k et en utilisant la remarque précédente, on a $\dfrac{d_2}{k}|a$ et $\dfrac{d_2}{k}|b$ donc $\dfrac{d_2}{k}|d_1$, d'où $d_2|kd_1$.

Comme kd_1 et d_2 sont positifs, on en déduit $d_2 = kd_1$. □

5.2.1 Algorithme d'Euclide

Lemme 5.2.6 (d'Euclide)**.** Soient a, b et k des entiers relatifs. Alors :

$$\text{pgcd}(a,b) = \text{pgcd}(a+kb,b).$$

Démonstration. Ils y a au moins deux façons de prouver le résultat : on peut montrer que les idéaux $a\mathbb{Z}+b\mathbb{Z}$ et $(a+kb)\mathbb{Z}+b\mathbb{Z}$ sont les mêmes, ce qui implique qu'ils ont le même générateur principal, ou alors on peut montrer que (a,b) et $(a+kb,b)$ ont les mêmes diviseurs communs, donc le même plus grand diviseur commun.
Première preuve (mêmes idéaux). D'une part, $(a+kb)\mathbb{Z}+b\mathbb{Z} \subseteq a\mathbb{Z}+b\mathbb{Z}$ car si i et j sont des entiers, alors $i(a+kb)+jb = ia+(iK+j)b \in a\mathbb{Z}+b\mathbb{Z}$. D'autre part, $a\mathbb{Z}+b\mathbb{Z} \subseteq (a+kb)\mathbb{Z}+b\mathbb{Z}$ car si i et j sont des entiers, alors $ia+jb = i(a+kb)+(j-ik)b \in (a+kb)\mathbb{Z}+b\mathbb{Z}$. Finalement, les idéaux $a\mathbb{Z}+b\mathbb{Z}$ et $(a+kb)\mathbb{Z}+b\mathbb{Z}$ sont identiques donc ont le même générateur principal.
Deuxième preuve (mêmes diviseurs). Si $m|a$ et $m|b$, alors $m|a+kb$ et $m|b$.
Si $m|a+kb$ et $m|b$, alors $m|a+kb-kb$ et $m|b$, donc m divise a et b.
On en déduit que les couples (a,b) et $(a+kb,b)$ ont les mêmes diviseurs communs. Ils ont donc le même pgcd. □

Corollaire 5.2.7. En particulier, si $a = bq + r$ est la division de a par $b \neq 0$, alors

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r).$$

Théorème 5.2.8 (Algorithme d'Euclide)**.** Appliquer l'algorithme d'Euclide aux entiers naturels a et b, c'est effectuer une suite de divisions euclidiennes :

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n \end{aligned}$$

en continuant tant que r_n n'est pas nul. Alors, on a les résultats suivants :

1. (terminaison de l'algorithme) Au bout d'un certain nombre d'étapes, on a $r_n = 0$, donc l'algorithme termine en un nombre fini d'étapes.
2. Le dernier reste non nul r_{n-1} est le pgcd de a et b.

Démonstration.

1. (Preuve de terminaison) Il s'agit de montrer que l'on ne peut pas continuer indéfiniment à faire des divisions euclidiennes. Par définition de ce qu'est une division euclidienne, on a : $b > r_1$, $r_1 > r_2$ et plus généralement $r_i > r_{i+1}$. La suite des restes est une suite strictement décroissante d'entiers positifs, elle ne peut pas être infinie.
2. (Preuve de correction du calcul de pgcd) Par le lemme d'Euclide et son corollaire appliqués à chaque étape, on a

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2) = \dots = \mathrm{pgcd}(r_{n-1}, r_n) = \mathrm{pgcd}(r_{n-1}, 0) = r_{n-1}.$$

□

On remarque qu'il n'est pas nécessaire que $a > b$ dans l'algorithme : si ce n'est pas le cas, l'algorithme les replace dans le bon ordre au cours de la première étape.

L'algorithme d'Euclide permet également d'obtenir une relation de Bézout en « remontant » les étapes de l'algorithme :

$$d = r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} = r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2} r_{n-3}) \dots = au + bv.$$

5.2.2 Nombres premiers entre eux, théorème de Gauß

Définition 5.2.9. Deux nombres relatifs a et b sont premiers entre eux si $\mathrm{pgcd}(a, b) = 1$. On note : $a \wedge b = 1$.

Proposition 5.2.10. Soient a et b des entiers. On a

$$a \wedge b = 1 \iff (\exists u, v \in \mathbb{Z} \mid au + bv = 1)$$

Démonstration. Sens $\Longrightarrow$: il existe une relation de Bézout.
Sens $\Longleftarrow$: si $au+bv=1$, alors $\text{pgcd}(a,b)$ divise 1, donc vaut 1. □

Proposition 5.2.11. Soient a et b des entiers. Si $a\wedge b=1$ et $a\wedge c=1$, alors $a\wedge bc=1$.

Démonstration. Si $au+bv=1$ et $au'+cv'=1$ sont des relations de Bézout, on a en multipliant les deux :

$$1=(au+bv)(au'+cv')=a(auu'+bvu'+ucv')+bcvv'.$$

□

Corollaire 5.2.12. Soient a, b et $n>0$, $m>0$ des entiers. Si $a\wedge b=1$, alors $a^n\wedge b^m=1$.

Démonstration. On a $a\wedge b=1 \implies a\wedge b^2=\ldots=a\wedge b^m=1$, puis $b^m\wedge a1 \implies b^m\wedge a^2=\ldots=b^m\wedge a^n=1$. □

Attention, ceci n'est **pas** un résultat de passage au produit avec le symbole $\wedge$! Si on a $a\wedge b=1$ et $c\wedge d=1$, on n'a **pas** $ac\wedge bd=1$. Exemple : $2\wedge 3=1$ et $3\wedge 2=1$ et pourtant $6\wedge 6\neq 1$.

Théorème 5.2.13 (« théorème/lemme de Gauß »)**.** Soient a, b et c des entiers. Si $a\wedge b=1$ et $a|bc$, alors $a|c$.

Démonstration. Soit $ak+bl=1$ une relation de Bézout pour a et b. Si a divise bc, alors il divise également blc. D'autre part, a divise akc. Donc $a|(bl+ak)c$ c'est-à-dire $a|c$. □

5.2.3 Résolution des équations diophantiennes du type $ax+by=c$

Définition 5.2.14. Une équation diophantienne est une équation du type $F(x_1,x_2,\ldots x_k)=0$, les inconnues x_1, … x_k appartiennent à $\mathbb{Z}$, ou une partie de $\mathbb{Z}$.

Exemples :
$12x+3y=8$, d'inconnues x et y dans $\mathbb{Z}$.
$2^n-3^m=7$ d'inconnues n et m dans $\mathbb{N}$.
$x^n+y^n=z^n$ d'inconnues x, y, z, n dans $\mathbb{N}$. (C'est l'équation de Fermat; il a été démontré en 1994 après trois siècles d'efforts que l'équation n'admet des solutions que si $n=2$.)

Dans ce cours, on s'intéresse aux équations du type $ax+by=c$ d'inconnues x et y dans $\mathbb{Z}$, et avec a, b et c des paramètres entiers.

Géométriquement, cela revient à trouver les points à coordonnées entières de la droite du plan d'équation cartésienne $ax+by=c$.

La méthode de résolution consiste, comme pour les équations différentielles linéaires, à trouver une solution particulière de l'équation, puis à y ajouter les solutions de l'équation homogène associée, qui est par définition l'équation obtenue en remplaçant le second membre par zéro : $ax+by=0$. C'est le contenu de la proposition suivante :

Proposition 5.2.15. Soient a, b des entiers non tous deux nuls, c un entier. On considère l'équation $(E)\,:\,ax+by=c$ d'inconnue $(x,y)\in\mathbb{Z}^2$, ainsi que l'équation homogène associée $(E_h)\,:\,ax+by=0$.

Si (x_p,y_p) est une solution particulière de (E), alors son ensemble de solutions est

$$\big\{(x_p,y_p)+(s,t)\mid (s,t)\text{ solution de }E_h\big\}$$

Démonstration. Soit (x, y) un couple d'entiers.

$$\begin{aligned} ax+by=c &\iff ax+by=ax_p+by_p \\ &\iff a(x-x_p)+b(y-y_p)=c-c=0, \end{aligned}$$

donc (x, y) est solution de (E) si et seulement si $(x-x_p, y-y_p)$ est solution de l'équation homogène (E_h) associée à (E). On en déduit le résultat. □

Il reste donc à établir un critère pour l'existence de solutions, et à donner une méthode pour trouver des solutions particulières, et pour résoudre les équations homogènes.

Proposition 5.2.16 (Existence de solutions et solution particulière)**.** Soient a, b et c des entiers.

1. L'équation (E) : $ax+by=c$ d'inconnue $(x, y) \in \mathbb{Z}^2$ admet des solutions si et seulement si $\operatorname{pgcd}(a, b)|c$.
2. Dans ce cas, en notant $k = c/\operatorname{pgcd}(a, b)$ et $au+bv = \operatorname{pgcd}(a, b)$ une relation de Bézout, une solution particulière est (ku, kv).

Preuve. Montrons d'abord que la condition est nécessaire. S'il existe une solution (x, y), alors $ax + by = c$ et donc tout diviseur commun de a et b divise aussi $ax + by$ et donc c. En particulier $\operatorname{pgcd}(a, b)|c$.

Réciproquement, montrons que la condition est suffisante en prouvant que le couple fourni est bien solution. En multipliant par k la relation de Bézout on obtient $auk + bvk = \operatorname{pgcd}(a, b)k = c$ donc (uk, vk) est bien une solution de (E). □

Proposition 5.2.17 (Résolution des équations homogènes)**.** Soient a, b des entiers non tous deux nuls, et notons $d = \operatorname{pgcd}(a, b)$. L'équation $ax + by = 0$ d'inconnue $(x, y) \in \mathbb{Z}^2$ a pour ensemble de solutions :

$$\left\{k\left(\frac{-b}{d}, \frac{a}{d}\right), k \in \mathbb{Z}\right\}$$

(Remarque : si a et b sont nuls, alors l'ensemble des solutions est $\mathbb{Z}^2$ tout entier...)

Démonstration. (de la proposition) Écrivons $a = da'$ et $b = db'$. L'équation s'écrit donc $da'x + db'y = 0$ et en simplifiant par d qui est non nul, on obtient l'équation équivalente $a'x + b'y = 0$, avec $a' \wedge b' = 1$.

Si un des deux entiers a ou b est nul, le résultat est facile.

Sinon, le théorème de Gauß donne alors $a'|y$, donc il existe $k \in \mathbb{Z}$ tel que $y = ka'$. On trouve alors $x = -kb'$ en simplifiant par a'. □

Exemple 5.2.18. L'ensemble des solutions entières de l'équation $2x+6y = 0$ est $\{k(3, -1) \mid k \in \mathbb{Z}\}$.

5.3 Ppcm

Proposition 5.3.1. Soient a, $b \in \mathbb{Z}$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ (qui est par définition l'ensemble des entiers qui sont à la fois multiples de a et multiples de b, c'est-à-dire l'ensemble des multiples communs de a et b) est un idéal de $\mathbb{Z}$.

Démonstration. On a déjà vu qu'il suffit de montrer que c'est un sous-groupe de $\mathbb{Z}$, donc que $a\mathbb{Z} \cap b\mathbb{Z}$ contient 0, est stable par somme et par opposé.

1. $0 \in a\mathbb{Z}$ et $0 \in b\mathbb{Z}$, donc $0 \in a\mathbb{Z} \cap b\mathbb{Z}$.
2. Soient x, y dans $a\mathbb{Z} \cap b\mathbb{Z}$. Comme x et y sont dans $a\mathbb{Z}$, $x + y \in a\mathbb{Z}$ car $a\mathbb{Z}$ est stable par somme. On montre de même que $x + y \in b\mathbb{Z}$. Donc $x + y \in a\mathbb{Z} \cap b\mathbb{Z}$.
3. Soit $x \in a\mathbb{Z} \cap b\mathbb{Z}$. Comme $x \in a\mathbb{Z}$, on a $-x \in a\mathbb{Z}$ car $a\mathbb{Z}$ est stable par opposé. On montre de même que $-x \in b\mathbb{Z}$. Donc $-x \in a\mathbb{Z} \cap b\mathbb{Z}$.

De façon générale et en anticipant sur un futur cours d'algèbre, l'intersection de deux sous-groupes est un sous-groupe. □

Définition 5.3.2. Soient $a, b \in \mathbb{Z}$. Le générateur principal de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$ est appelé *plus petit commun multiple* (sous-entendu, le plus petit parmi ceux strictement positifs) et noté $\mathrm{ppcm}(a, b)$.

Proposition 5.3.3. Soient a, $b \in \mathbb{Z}$. On a :

1. $\mathrm{ppcm}(a, 1) = |a|$.
2. $\mathrm{ppcm}(a, 0) = 0$.
3. Si M est un multiple de a et de b, alors c'est un multiple de $\mathrm{ppcm}(a, b)$.

Proposition 5.3.4. Soient a et b des naturels non nuls. On a :

$$\mathrm{pgcd}(a, b) \times \mathrm{ppcm}(a, b) = ab.$$

Démonstration.
— Premier cas : $a \wedge b = 1$. Soit $m = \mathrm{ppcm}(a, b)$. Alors a divise m donc on peut écrire $m = ka$. D'autre part b divise m, donc b divise ka, par le théorème de Gauss, comme b est premier avec a, on en déduit que b divise k. Donc $ab|m$. D'autre part, ab est un multiple commun de a et de b, donc $m|ab$. Finalement, $m = ab$.
— Deuxième cas : $d = \mathrm{pgcd}(a, b) \geq 1$. Écrivons $a = da'$ et $b = db'$. On a donc $a' \wedge b' = 1$. Donc $\mathrm{ppcm}(a', b') = a'b'$, puis $\mathrm{ppcm}(da', db') = da'b' = ab/d$.

□

5.4 Nombres premiers

5.4.1 Définition

Définition 5.4.1. Un entier naturel p est dit *premier* s'il possède exactement deux diviseurs positifs distincts : 1 et p. En particulier, un nombre premier est toujours ≥ 2.

Le nombre 1 n'est pas premier. Les nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23 etc.

Proposition 5.4.2. Soit p un nombre premier et $a \in \mathbb{Z}$. Alors $p|a$ ou $a \wedge p = 1$.

Démonstration. On a $\text{pgcd}(a, p)|p$ donc $\text{pgcd}(a, p)$ vaut 1 ou p. □

Définition 5.4.3. Un entier naturel $n \geq 2$ qui n'est pas premier est dit *composé*. Cela revient à :

$$\exists a, b \in [\![2, n-1]\!] \mid n = ab.$$

Proposition 5.4.4 (Test de primalité)**.** Un entier n est premier si $\forall a \leq \sqrt{n}$ entier, a ne divise pas n.

Démonstration. Si n est composé, alors $n = ab$ avec $a, b \in [\![2, n-1]\!]$, donc au moins un des deux entiers a ou b est $\sqrt{n}$ (sinon on aurait $n = ab > \sqrt{n}^2 = n$, absurde). L'autre sens de l'équivalence est évident. □

5.4.2 Décomposition en produit de nombres premiers

Soit $\mathscr{P}$ l'ensemble des nombres premiers.

Proposition 5.4.5.

$$\forall n \geq 1, \exists!(\alpha_p)_{p\in\mathscr{P}}, n : \prod_{p\in\mathscr{P}} p^{\alpha_p}.$$

En fait, seul un nombre fini des α_p sont non nuls.

Démonstration. On montre l'existence par récurrence forte sur n. Pour $n \geq 1$, notons $A(n)$ l'assertion $\exists(\alpha_p)_{p\in\mathscr{P}}, n = \prod_{p\in\mathscr{P}} p^{\alpha_p}$.

Initialisation. Pour $n = 1$, la suite nulle $\alpha_p = 0$ (pour tout p) convient.

Hérédité sous hypothèse de récurrence forte. Soit $n \geq 1$, et supposons $A(k)$ vraie pour tout $k \leq n$. Montrons $A(k+1)$. Si $n+1$ est premier, alors la suite $\alpha_{n+1} = 1$ et $\alpha_i = 0$ pour $i \neq n+1$ convient. Si $n+1$ est composé, écrivons $n = bc$ avec $b, c \leq n$. Par hypothèse de récurrence appliquée à b et c, on peut écrire $b = \prod_{p\in\mathscr{P}} p^{\beta_p}$ et $c = \prod_{p\in\mathscr{P}} p^{\gamma_p}$. On a donc

$$bc = \prod_{p\in\mathscr{P}} p^{\beta_p} \cdot \prod_{p\in\mathscr{P}} p^{\gamma_p} = \prod_{p\in\mathscr{P}} p^{\beta_p+\gamma_p}$$

et la suite $\alpha_p = \beta_p + \gamma_p$ convient.

L'unicité de la décomposition est laissée en exercice. □

Définition 5.4.6 (Valuation p-adique)**.** Soit n un entier et p un nombre premier. On appelle *valuation p-adique de n* et on note $v_p(n)$l'exposant de p dans la décomposition de n en facteurs premiers. On peut donc écrire

$$n = \prod_{p\in\mathscr{P}} p^{v_p(n)}.$$

Exemples : $v_2(16) = 4$, $v_3(17) = 0$, $v_2(18) = 1$.

Proposition 5.4.7 (Propriétés fondamentales de la valuation p-adique)**.**

$$v_p(n) \geq 1 \iff p|n.$$

$$v_p(nm) = v_p(n) + v_p(m).$$

Proposition 5.4.8 (Critère de divisibilité en termes de valuations p-adiques)**.**

$$n|m \iff \big(\forall p \in \mathscr{P},\ v_p(n) \leq v_p(m)\big)$$

Démonstration. Si $m = kn$, alors pour tout $p \in \mathscr{P}$, $v_p(m) = v_p(k) + v_p(n) \geq v_p(n)$.

Réciproquement, on a

$$m = \prod_{p \in \mathscr{P}} p^{v_p(m)} = \prod_{p \in \mathscr{P}} p^{v_p(n)} \cdot \prod_{p \in \mathscr{P}} p^{v_p(m) - v_p(n)}$$

donc $n|m$. □

Corollaire 5.4.9 (pgcd et ppcm en termes de valuations p-adiques)**.**

$$\mathrm{pgcd}(n,m) = \prod_{p \in \mathscr{P}} p^{\min(v_p(n), v_p(m))},$$

$$\mathrm{ppcm}(n,m) = \prod_{p \in \mathscr{P}} p^{\max(v_p(n), v_p(m))}.$$

Démonstration. Notons $d = \mathrm{pgcd}(n,m)$ et $a = \prod_{p \in \mathscr{P}} p^{\min(v_p(n), v_p(m))}$.

Pour tout $p \in \mathscr{P}$, on a $v_p(a) \leq v_p(n)$ donc $a|n$. De même, $a|m$. Donc a est un diviseur commun de m et n, et il divise donc leur pgcd : $a|d$.

D'autre part, soit $\in \mathscr{P}$. On a $d|m$ donc $v_p(d) \leq v_p(m)$, et de même, $d|n$ donc $v_p(d) \leq v_p(n)$. On en déduit que $v_p(d) \leq \min(v_p(n), v_p(m)) = v_p(a)$. Comme ceci vaut pour tout $p \in \mathscr{P}$, on a $d|a$.

Finalement on a $a|d$ et $d|a$, donc $\boxed{d = a}$.

Le résultat sur le ppcm se démontre de la même manière. □

Exemple 5.4.10. $\mathrm{pgcd}(120, 252) = \mathrm{pgcd}(2^3 \cdot 3 \cdot 5, 2^2 \cdot 3^2 \cdot 7) = 2^2 \cdot 3 = 12$. Pour les nombres faciles à factoriser, c'est toujours comme cela que l'on procède, l'algorithme d'Euclide est à réserver aux cas difficiles, ou aux calculs de relations de Bézout.

5.4.3 Infinitude des nombres premiers

Proposition 5.4.11. L'ensemble $\mathscr{P}$ des nombres premiers est infini.

Démonstration. Supposons par l'absurde qu'il soit fini, et soir M son plus grand élément. Pour tout $k \leq M$, k divise $M!$, donc le reste par la division euclidienne de $M! + 1$ par k est 1. On en déduit que k ne divise pas $M! + 1$. En particulier, aucun nombre premier ne divise $M! + 1$, qui ne possède donc pas de décomposition en facteurs premiers, absurde. □

Chapitre 6

Relations d'ordre et d'équivalence

6.1 Relations binaires

Définition 6.1.1. Soit E un ensemble. Une *relation binaire* R sur E est une application de $E \times E$ dans {vrai, faux}.

Une relation R est caractérisée par la partie de $E \times E$ constituée des couples (x, y) tels que $R(x, y) =$ vrai. On notera « xRy » au lieu de « $R(x, y) =$ vrai » et « $x \not R y$ » au lieu de « $R(x, y) =$ faux »

Exemples 6.1.2. Les symboles $\leq$, $<$, $\geq$, $>$, $|$ (divise), $//$ (parallèle à), $\perp$ (perpendiculaire à), $\subseteq$ (inclus dans) désignent des relations binaires entre ensembles.

6.2 Relations d'ordre

Définition 6.2.1. Soit E un ensemble. Une relation binaire R sur E est

1. réflexive ssi $\forall x \in E, xRx$;
2. transitive ssi $\forall x, y, z \in E, xRy$ et $yRz \implies xRz$;
3. antisymétrique ssi $\forall x, y \in E, xRy$ et $yRx \implies x = y$.

Une relation est une *relation d'ordre* ssi elle est réflexive, transitive et antisymétrique.

Exemples 6.2.2. $\leq$ est une relation d'ordre sur $\mathbb{N}$, ou sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. (Mais pas sur $\mathbb{C}$: la relation $\leq$ n'est même pas *définie* sur $\mathbb{C}$.) $\subset$ est une relation d'ordre sur $\mathscr{P}(E)$. $|$ (« divise ») est une relation d'ordre sur $\mathbb{N}^*$

Attention : $<$ n'est pas une relation d'ordre sur $\mathbb{R}$ (ni sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{Q}$), car elle n'est pas réflexive, et $|$ n'est pas une relation d'ordre sur $\mathbb{Z}^*$, car elle n'est pas antisymétrique : $1|-1$ et $-1|1$ et pourtant $1 \neq -1$.

Définition 6.2.3. Si R est une relation d'ordre sur E, on peut lui associer une relation *d'ordre strict*, définie par « xRy et $x \neq y$ ». (Remarque : une relation d'ordre strict n'est pas une relation d'ordre puisqu'elle n'est pas réflexive.)

Un ensemble E muni d'une relation d'ordre R est appelé ensemble ordonné. Par exemple, $(\mathbb{R}, \leq)$ est un ensemble ordonné. S'il n'y a pas de confusion possible sur la relation d'ordre, on peut simplement dire que E est ordonné. (Cependant, il y a en général plusieurs relations d'ordre sur un ensemble.)

Dans ce cours, on notera en général $\leq_E$ au lieu de R une relation d'ordre sur E (même si la relation n'a rien à voir avec l'inégalité $\leq$ sur $\mathbb{R}$).

6.2.1 Vocabulaire sur les ensembles ordonnés

Définition 6.2.4. Une relation d'ordre $\leq_E$ sur un ensemble E est *totale* si :

$$\forall x, y \in E, x \leq_E y \text{ ou } y \leq x.$$

Un ensemble muni d'un ordre total est appelé *ensemble totalement ordonné*.

Exemples 6.2.5. La relation d'ordre $\leq$ sur $\mathbb{R}$ (ou $\mathbb{N}$, $\$Q$, $\mathbb{Z}$) est totale. Par contre, $\subset$ et $|$ ne sont pas totales. Par exemple, dans $\mathscr{P}(\mathbb{R})$, les parties $\mathbb{R}_+$ et $]-3,6]$ ne sont pas comparables pour l'inclusion. Dans $\mathbb{N}^*$, les éléments 2 et 3 ne sont pas comparables pour la divisibilité.

Définition 6.2.6. Soient $(E, \leq_E)$ et $(F, \leq_F)$ des ensembles ordonnés, et $f : E \to F$. On dit que f est *croissante* si :

$$\forall x, y \in E, x \leq_E y \implies f(x) \leq_F f(y),$$

et *décroissante* si :

$$\forall x, y \in E, x \leq_E y \implies f(y) \leq_F f(x).$$

(Remarque : dans cette situation, il est crucial de distinguer les relations d'ordre sur E et sur F.)

Exemple 6.2.7.

1. L'application $f : \mathbb{R} \to \mathbb{R}, x \mapsto x + e^x$ est croissante pour l'ordre usuel $\leq$ sur $\mathbb{R}$.
2. Si E est fini, l'application $f : \mathscr{P}(E) \to \mathbb{N}$, $A \mapsto \mathrm{Card}(A)$ est croissante entre les ensembles ordonnés $(\mathscr{P}(E), \subset)$ et $(\mathbb{N}, \leq)$.
3. L'application $f : \mathscr{P}(E) \to \mathscr{P}(E)$, $A \mapsto A^c$ est décroissante pour l'inclusion, car $A \subset B \implies B^c \subset A^c$.

Comme d'habitude, après les définitions viennent les propositions et théorèmes.

Proposition 6.2.8.

1. La composée de deux applications croissantes est croissante.
2. La composée de deux applications décroissantes est décroissante.
3. La composée d'une application décroissante et d'une décroissante est décroissante.

Démonstration. Application directe de la définition. □

6.2.2 Éléments remarquables dans un ensemble ordonné

Soit $(E, \leq_E)$ un ensemble ordonné et $A \subset E$ une partie non vide. Un élément $m \in E$ est un *majorant* de A si $\forall a \in A, a \leq_E m$.

La partie A est majorée si elle possède des majorants.

La partie A possède un plus grand élément s'il existe un élément $m \in A$ qui majore A.

Exemple 6.2.9. La partie $[0,1]$ est majorée dans $\mathbb{R}$ car 1, 2, π sont des majorants. Elle possède un plus grand élément : 1.

La partie $[0,1[$ est majorée dans $\mathbb{R}$ (pour les mêmes raisons). Par contre, elle n'a pas de plus grand élément. Elle possède par contre un plus petit majorant réel, à savoir 1, mais il n'appartient pas à A.

Proposition 6.2.10. Si $A \subset E$ possède un plus grand élément, il est unique.

Démonstration. Soient m et m' deux plus grands éléments de A. Comme m est un plus grand élément, on a par définition $\forall x \in A, x \leq_E m$ et donc en particulier $m' \leq_E m$. De même, comme m' est un plus grand élément, on a $m \leq_E m'$. Par antisymétrie de la relation d'ordre, on a $m = m'$. □

Si A possède un plus grand élément (unique par ce qui précède), on le note $\max(A)$. Toutes les parties n'ont pas de plus grand élément, par exemple $]3, +\infty[$, ou $\mathbb{N}$ n'ont pas de plus grand élément.

On définit de même la notion de minorant, de plus petit élément, et on montre que s'il existe un plus petit élément d'une partie A, il est unique. On le note alors $\min(A)$.

Définition 6.2.11. La partie $A \subset E$ admet une borne supérieure $s \in E$ ssi :

1. s est un majorant de A ;
2. tout majorant de A majore s.

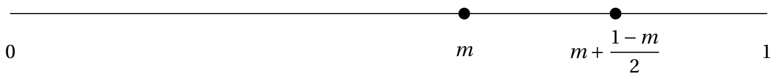
(En d'autres termes, s est le plus petit des majorants de A, ou encore : l'ensemble de tous les majorants de A possède un plus petit élément s.)

Attention, contrairement à un plus grand élément, une borne supérieure de A, s'il en existe, n'appartient pas forcément à A.

Exemple 6.2.12. La partie $\mathbb{R}_+ \subseteq \mathbb{R}$ n'a pas de borne supérieure. La partie $A = [0,1[\subseteq \mathbb{R}$ n'a pas de plus grand élément, mais possède une borne supérieure : 1.

Démonstration. Pour le premier point, la partie n'a même pas de majorant donc c'est clair. D'une part, il est clair que 1 est un majorant de $[0,1[$, c'est-à-dire que $\forall x \in [0,1[$, $x \leq 1$.

Vérifions la seconde partie de la définition. Soit m un majorant de $[0,1[$ et supposons par l'absurde que $m < 1$. On doit forcément avoir $0 \leq m$ puisque $0 \in [0,1[$. Donc $m + \frac{1-m}{2} = 1 + \frac{m}{2} \in [0,1[$.



Comme m est un majorant, on doit avoir $1 + \dfrac{m}{2} \le m$, donc $1 + m \le 2m$ donc $m \ge 1$, absurde. $\square$

Proposition 6.2.13. Soit $(E, \le_E)$ un ensemble ordonné $A \subseteq E$. Si A admet une borne supérieure et que $\sup(A) \in A$, alors c'est son plus grand élément. Si A admet un plus grand élément, c'est aussi sa borne supérieure.

Démonstration. Exercice, appliquer les définitions. $\square$

6.2.3 Ordre produit et ordre lexicographique

Proposition–Définition 6.2.14. Soient $(E \le_E)$ et $F, \le_F)$ des ensembles ordonnés. L'ordre produit sur $E \times F$ est défini par :

$$(x, y) \le_{E\times F} (x', y') \iff \big(x \le_E x' \text{ et } y \le_F y'\big).$$

Démonstration. Il s'agit de prouver que la relation binaire définie est bien une relation d'ordre donc réflexive, antisymétrique et transitive. Exercice. $\square$

Attention, même si $\le_E$ et $\le_F$ sont totales, l'ordre produit n'est pas forcément un ordre total. Par exemple, pour $E = F = \mathbb{R}$ et l'ordre usuel sur $\mathbb{R}$ qui est bien total, on remarque que l'ordre produit $\le_{\mathbb{R}\times\mathbb{R}}$ sur $\mathbb{R} \times \mathbb{R}$ n'est pas total car $(1,2)$ et $(2,1)$ ne sont pas comparables.

Proposition–Définition 6.2.15. Soient $(E \le_E)$ et $F, \le_F)$ des ensembles **totalement** ordonnés. L'ordre lexicographique sur $E \times F$ est défini par :

$$(x, y) \le_{E\times F} (x', y') \iff \big(x < x' \text{ ou } (x = x' \text{ et } y \le_F y')\big).$$

C'est un ordre total.

Démonstration. La propriété de relation d'ordre est laissée en exercice. Prouvons que l'ordre est total.

Soient en effet (x, y) et (x', y') distincts. Si $x \neq x'$, alors comme $\le_E$ est un ordre total, on a forcément $x <_E x'$ ou bien $x' <_E x$. Si $x = x'$, alors on a forcément $y \neq y'$ et comme $\le_F$ est un ordre total, on a forcément $y <_F y'$ ou bien $y' <_F y$.

En conclusion, on a bien soit $(x, y) \le_{E\times F} (x', y')$, soit $(x', y') \le_{E\times F} (x, y)$. $\square$

Exemple 6.2.16. Avec l'ordre usuel sur l'alphabet, l'ordre lexicographique sur les mots est l'ordre dans lequel les mots sont classés dans un dictionnaire.

6.3 Relations d'équivalence

6.3.1 Définitions

6.3.2 Partition en classes d'équivalence