Chapitre 1 : Éléments de logique - Ensembles - Arithmétique

Dans ce premier chapitre, nous présentons certaines notions mathématiques fondamentales sur lesquelles nous nous appuierons tout au long de l'année. Il s'agit en particulier d'introduire les éléments de logique qui permettront de structurer de façon rigoureuse le raisonnement, au cœur de l'activité mathématique. *Il sera ultérieurement complété par un bilan méthodologique sur la pratique de la démonstration.*

PARTIE A : ÉLÉMENTS DE LOGIQUE ET ENSEMBLES

I Proposition et opérateurs logiques

I.1 Proposition

Définition

Une **proposition logique** ou plus simplement **proposition** est une affirmation à laquelle on peut donner un sens et qui possède *deux valeurs de vérité* : soit « vrai » soit « faux ». [1]
*Une proposition est parfois également qualifiée d'**assertion**.*

Illustrations

- « Quelle heure est-il ? » : .....
- « Saint-Louis est le roi Louis IX » : .....
- « Saint-Louis vécut au XII^{e} siècle » : .....
- « $\sqrt{3+2\sqrt{2}} = 1+\sqrt{2}$ » : .....
  .....
  .....
  .....
  .....
- P : « $\sqrt{2} \in \mathbb{Q}$ » : .....
  .....

  Remarque : pour nommer une proposition, on recourt en général aux lettres majuscules.
- Q : « $\sqrt{(3-\pi)^2} = 3-\pi$ » : .....
  .....

Proposition dépendant d'un paramètre

Une proposition peut dépendre d'un ou plusieurs paramètres (ou variables) : on parle alors de **prédicat**.

Par exemple : . la proposition « $(x-1)^2 < 1$ » dépend (à priori) du réel x ;
. la proposition « n divise 45 » dépend (à priori) de l'entier n.

On veillera dans cas à correctement nommer de telles propositions, en faisant apparaître dans le nom le (ou les) paramètre(s) : par exemple ici, $P(x)$ pour la première, $Q(n)$ pour la seconde (et pas seulement P et Q).
On écrira ainsi : « pour $x \in \mathbb{R}$, notons $P(x) : (x-1)^2 < 1$ » ou « soit $x \in \mathbb{R}$; notons $P(x) : (x-1)^2 < 1$ » ...

La valeur de vérité d'un prédicat dépend de la valeur prise par le (ou les) paramètre(s) en jeu.

Par exemple ici : . $P(\dots)$ est vraie mais $P(\dots)$ est fausse ;
. $Q(\dots)$ est vraie mais $Q(\dots)$ est fausse.

Convention

La plupart du temps, on écrira « on a P » ou « ... donc P » au lieu de « P est vraie » ou « ... donc P est vraie ». On écrira de même « supposons P » au lieu de « supposons que P est vraie ». Dans le même ordre d'idée, lorsqu'on écrira « démontrer P », on sous-entendra toujours « démontrer que P est vraie ».

1. Dans le langage courant, on dit qu'une proposition est *soit vraie*, *soit fausse* (elle ne peut être simultanément *vraie* et *fausse*).

I.2 Opérateurs logiques

Dans ce paragraphe, on considère deux propositions P et Q (sans préjuger de leur valeur de vérité). Il va alors s'agir d'envisager de nouvelles propositions, construites à partir de P et Q.

I.2.1 Négation, conjonction, disjonction

Définitions

- La **négation de P**, notée « **non P** », est la proposition qui est vraie si P est fausse, fausse si P est vraie. On parle parfois de *proposition contraire* à la proposition P et on trouve également $\overline{P}$ comme notation.
- La **conjonction de P avec Q**, notée « **P et Q** », est la proposition qui est vraie si P et Q sont *simultanément* vraies, fausse dans tous les autres cas (donc fausse si au moins l'une des deux propositions P ou Q est fausse).
- La **disjonction de P avec Q**, notée « **P ou Q** », est la proposition qui est vraie si *au moins* l'une des deux propositions P ou Q est vraie (et donc fausse uniquement lorsque P et Q sont toutes les deux fausses).

Remarques et illustrations

- « non », « et » et « ou » sont des *opérateurs (logiques). On parle également de connecteurs logiques.*
- La définition des opérateurs « et » et « ou » pourrait être formulée en faisant appel à une phrase utilisant les mots « *et* » et « *ou* ». Mais la conjonction de coordination « *ou* » est ambiguë en français, car elle le plus souvent exclusive (penser à l'expression « fromage *ou* dessert »), alors que l'opérateur « ou » n'est jamais exclusif.
- Si P est la proposition « cette carte est un as » et Q la proposition « cette carte est un cœur » alors :
  - la proposition « non P » est la proposition : .....
  - la proposition « P et Q » est la proposition : .....
  - la proposition « P ou Q » est la proposition : .....
  .....
- Soit x un réel.
  - la proposition « non $(x > 1)$ » est : .....
  - la proposition « non $(x \leqslant -2)$ » est : .....
  - la proposition « $-1 \leqslant x < 1$ » s'écrit aussi : .....

Table de vérité

- Lorsqu'une proposition est définie à partir d'autres propositions, il peut se révéler pratique et précieux de récapituler dans un tableau les valeurs de vérité de cette nouvelle proposition, en fonction des valeurs de vérité des propositions initiales (vrai (V), faux (F)) : un tel tableau est appelé **table de vérité**.
- Dressons à titre d'exemple les tables de vérité de « P et Q » et « P ou Q » :

P	Q	P et Q

Table de vérité de « P et Q »

P	Q	P ou Q

Table de vérité de « P ou Q »

I.2.2 Implication et équivalence

Définition : Implication

La proposition « (non P) ou Q » est notée « $\boldsymbol{P \Longrightarrow Q}$ » et se lit « **P implique Q** ».

Remarques

- Dressons la table de vérité de « $P \Longrightarrow Q$ » :

P	Q	non P	$P \Longrightarrow Q$

Table de vérité de « $P \Longrightarrow Q$ »

- La proposition $P \Longrightarrow Q$ n'est donc fausse que si .....
- Comme le suggère la table de vérité précédente, lorsque l'implication $P \Longrightarrow Q$ est vraie, on dit parfois : « **si** P est vraie **alors** Q l'est aussi » ou plus simplement « **si** P **alors** Q ».

Point Méthode : Démontrer l'implication $P \Longrightarrow Q$ (ie. démontrer que $P \Longrightarrow Q$ est vraie)

Pour démontrer l'implication $P \Longrightarrow Q$:

- si P est fausse, il n'y a rien à faire ;
- si P est vraie, on est alors dans l'obligation de prouver que Q est vraie.

Remarque

On est rassuré de retrouver au bout du compte la méthode employée dans le secondaire et qui se révèle donc parfaitement correcte !

Exemple 1

x désignant un réel, examiner, selon les valeurs de x, la valeur de vérité des implications suivantes :

- $(1 \leqslant x < 2) \implies x \in [0\,;2]$ ($(1 \leqslant x < 2)$ s'écrit aussi .....
  .....
  .....
  .....
  .....
  .....
- $(2 = 3) \implies x^2 < 0$
  .....
  .....

Condition nécessaire, condition suffisante

Considérons les deux propositions P : « il pleut » et Q : « il y a des nuages ».
L'implication $P \Longrightarrow Q$ est notoirement vraie [2], en ce sens que si effectivement il pleut alors le temps est nuageux, et un jour donné, on est dans l'une des trois situations suivantes ;

- il pleut et il y a des nuages ;
- il ne pleut pas et il y a des nuages (malgré tout) ;
- il ne pleut pas et il n'y a pas de nuages.

À l'examen de ces trois situations, il ressort que :

- pour qu'il pleuve, il est *nécessaire* qu'il y ait des nuages : on dira que la **condition** « Q » est **nécessaire** à la condition « P ».
- pour qu'il y ait des nuages (pour être certain qu'il y en ait !), il est *suffisant* de savoir qu'il pleut : on dira que la **condition** « P » est **suffisante** à la condition « Q ».

Définitions

Lorsque l'implication $P \Longrightarrow Q$ est vraie :

- on dit que « $\boldsymbol{Q}$ **est une condition nécessaire de** $\boldsymbol{P}$ » : « pour que P soit vraie, il faut (il est nécessaire) que Q soit vraie » (en ce sens que si Q est fausse, P ne peut être vraie) ;
- on dit aussi que « $\boldsymbol{P}$ **est une condition suffisante de** $\boldsymbol{Q}$ » : « pour que Q soit vraie, il suffit que P soit vraie ».

Définition : Implication réciproque

Considérant l'implication « $P \Longrightarrow Q$ », l'implication « $Q \Longrightarrow P$ » est qualifiée d'**implication réciproque**.

Remarque

Comme l'illustre l'exemple qui précède (« il pleut » $\Longrightarrow$ « il y a des nuages »), lorsque l'implication $P \Longrightarrow Q$ est vraie, rien n'indique que l'implication réciproque $Q \Longrightarrow P$ est vraie (on l'a dit, l'implication $P \Longrightarrow Q$ est vraie, tandis que l'implication réciproque $Q \Longrightarrow P$ ne l'est pas puisqu'il peut y avoir des nuages sans qu'il pleuve).

2. **Attention !** Lorsqu'une implication $P \Longrightarrow Q$ est vraie, cela ne signifie en rien, au sens courant, que P est la *cause* de Q (ce sont par exemple ici les nuages qui sont la cause de la pluie !).

Définition : Équivalence

La proposition « $(P \Longrightarrow Q)$ et $(Q \Longrightarrow P)$ » est notée « $\boldsymbol{P \Longleftrightarrow Q}$ » et se lit « **P équivalente à Q** » ou « **P équivaut à Q** » ou « **P et Q équivalentes** ».

Remarque

Dressons la table de vérité de « $P \Longleftrightarrow Q$ » :

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$P \Longleftrightarrow Q$

Proposition 1

Au vu de la table de vérité précédente, dire que la proposition $P \Longleftrightarrow Q$ est vraie signifie donc que les propositions P et Q .....

Point Méthode : Démontrer que l'équivalence $\boldsymbol{P \Longleftrightarrow Q}$ est vraie

Pour démontrer que l'équivalence $P \Longleftrightarrow Q$ est vraie, on peut démontrer que l'implication $P \Longrightarrow Q$ et que l'implication $Q \Longrightarrow P$ sont vraies, autrement dit démontrer que :

- si P est vraie alors Q est vraie ;
- réciproquement, si Q est vraie alors P est vraie.

*On parle alors de **raisonnement par double implication**. On verra que d'autres méthodes sont possibles : recours aux tables de vérité par exemple, raisonnement direct par équivalences...*

Définition

- Lorsque l'équivalence $P \Longleftrightarrow Q$ est vraie, on dira que « **P est une condition nécessaire et suffisante de Q** » : en effet, comme $P \Longrightarrow Q$ est vraie, P est une condition suffisante de Q, par ailleurs $Q \Longrightarrow P$ est vraie et P est également une condition nécessaire de Q.
- Notons que lorsque l'équivalence $P \Longleftrightarrow Q$ est vraie, une autre formulation possible est « P est vraie **si et seulement si** Q est vraie » (ou « P **si et seulement si** Q » ou en abrégé « P **ssi** Q »).

Illustration et remarque

- a et b désignant deux réels, la célébrissime équivalence : $ab = 0 \iff a = 0$ ou $b = 0$ s'énonce en disant : « un produit de facteurs est nul si et seulement si au moins un des facteurs est nul ».
- Dans la pratique, on ne s'intéressera qu'aux propositions vraies. Aussi, en dehors de ce chapitre théorique sur les éléments de logique (et en particulier de cette partie), on écrira à l'avenir « $P \Longrightarrow Q$ » ou « $P \Longleftrightarrow Q$ » uniquement lorsque ces propositions sont vraies.

Proposition 2

P et Q désignant deux propositions, on a les équivalences (vraies) suivantes :

1. $P \Longleftrightarrow$ non (non P)
2. (P et Q) $\Longleftrightarrow$ (Q et P)
3. (P ou Q) $\Longleftrightarrow$ (Q ou P)
4. **non (P et Q) $\Longleftrightarrow$ (non P) ou (non Q)**
5. **non (P ou Q) $\Longleftrightarrow$ (non P) et (non Q)**
6. **($P \Longrightarrow Q$) $\Longleftrightarrow$ (non $Q \Longrightarrow$ non P)**
7. **non ($P \Longrightarrow Q$) $\Longleftrightarrow$ P et (non Q)**

Démonstration (des points 4., 6. et 7.)

Les 3 premiers points sont assez clairs, les 4 suivants sont essentiels. À titre d'exemple, nous nous proposons de démontrer les points **4.**, **6.** et **7.** en recourant à deux méthodes différentes.

4. non $(P$ et $Q) \iff$ (non P) ou (non Q)

*L'équivalence précédente se lira également : « la négation de (P et Q) **est** (non P ou non Q) ».*

Pour ce point, on propose de comparer les tables de vérité des propositions de part et d'autre de l'équivalence.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. $(P \implies Q) \iff (\text{non}\, Q \implies \text{non}\, P)$

On se propose ici (et pour le point suivant) de raisonner directement par équivalences.

.....

.....

7. non $(P \implies Q) \iff P$ et (non Q)

.....

.....

Définition : Contraposée d'une implication

L'implication « non $Q \implies$ non P » est qualifiée de **contraposée** de l'implication « $P \implies Q$ ».

Remarques

- Le point **6.** s'exprime donc en disant qu'« une implication est vraie, si et seulement si sa contraposée est vraie ». Et on conçoit en effet que la proposition « si P est vraie alors Q est vraie » équivaut bien à « si Q est fausse alors P ne peut être que fausse ».
  *Cette proposition sera à la base du **raisonnement par contraposition**.*
- Le dernier point fournit une méthode pour démontrer que l'implication $P \implies Q$ est fausse : on démontre que

  .....
- Il est important d'être rapidement à l'aise avec ces différentes équivalences. En cas d'hésitation, il peut se révéler intéressant de se ramener à des situations concrètes et parlantes.
  À titre d'exemple, si l'on s'intéresse aux propositions P : « Marcel pratique le foot » et Q : « Marcel pratique le ski », la proposition (P et Q) est « Marcel pratique le foot et le ski ». La proposition non (P et Q) est alors « Marcel ne pratique pas les deux sports », autrement dit « soit Marcel ne pratique pas le foot, soit Marcel ne pratique pas le ski » qui correspond bien à la proposition (non P ou non Q).

Illustration

Pour $x \in \mathbb{R}$, la proposition « $(-1 \leqslant x < 1)$ » est : .....

On a donc : « non $(-1 \leqslant x < 1)$ » $\iff$ .....

.....

.....

II Quantificateurs

II.1 Quantificateur universel et quantificateur existentiel

On l'a déjà signalé, une affirmation peut dépendre d'une ou plusieurs variables (on parle également de paramètres) : elle est alors qualifiée de **prédicat**.

Définitions

Soit $P(x)$ un prédicat à une variable x prenant ses valeurs dans un ensemble E.

- La proposition « $\forall \boldsymbol{x \in E}$, $\boldsymbol{P(x)}$ » se lit « pour tout x (ou quel que soit x) appartenant à E, on a $P(x)$ » ;
  - elle est vraie lorsque les propositions $P(x)$ sont vraies pour tous les éléments x de l'ensemble E ;
  - le symbole « $\forall$ » est appelé **quantificateur universel** (on parle parfois de *proposition universelle*).
- La proposition « $\exists \boldsymbol{x \in E \,/\, P(x)}$ » se lit « il existe x appartenant à E tel que $P(x)$ » ;
  - elle est vraie lorsqu'il existe (au moins) un élément x_0 de E pour lequel $P(x_0)$ est vraie ;
  - le symbole « $\exists$ » est appelé **quantificateur existentiel** (on parle parfois de *proposition existentielle*).

Remarques

- Le symbole « / » du « tel que » n'est pas officiel : on trouve aussi « | ». Il peut par ailleurs être remplacé par une virgule « , » ou même omis : « $\exists x \in E$, $P(x)$ » ou « $\exists x \in E \;\; P(x)$ ».
- **Le symbole $\exists!$: existence et unicité**

  Considérant f une fonction définie sur $\mathbb{R}$, la proposition « $\exists x \in \mathbb{R} \,/\, f(x) = 0$ » signifie qu'il existe *au moins un* réel en lequel f s'annule, mais elle ne précise en rien si ce réel est ou non *unique*. S'il se trouve en fait qu'il y a unicité, on pourra écrire : « $\exists! \, x \in \mathbb{R} \,/\, f(x) = 0$ ».
- Les deux propositions « $\forall x \in E$, $P(x)$ » et « $\exists x \in E \,/\, P(x)$ » ne dépendent pas de x : les x apparaissant dans ces propositions sont qualifiées de *variables muettes* et peuvent être remplacées par n'importe quelle lettre.

Exemple 2

Examiner la valeur de vérité de chacune des propositions suivantes :

- « $\forall x \in]-\infty\,;-1]$, $x^2 \geqslant 1$ » : .....
  .....
  .....
  .....

  Remarquons que la proposition proposée s'écrit aussi : $\big(\forall x \in \mathbb{R}, (x \in]-\infty\,;-1] \implies x^2 \geqslant 1)\big)$.
- « $\forall x \in \mathbb{R}$, $x^2 \geqslant 1$ » : .....
  .....
  .....
- « $\exists n \in \mathbb{N} \,/\, n^2 - 10n > 0$ » : .....
  .....
- « $\exists! \, n \in \mathbb{N} \,/\, n^2 + n \leqslant 0$ » : .....
  .....
  .....
  .....

Point Méthode : Autour des quantificateurs

- **Démontrer une proposition du type « $\forall \boldsymbol{x \in E}$, $\boldsymbol{P(x)}$ »**

  On commence par se donner un élément quelconque x dans E, pour lequel il va s'agir d'établir $P(x)$.

  D'un point de vue rédactionnel on commencera alors obligatoirement par « ***Soit x un élément de E*** » ou « ***Soit $x \in E$*** » ; le « soit » permet de fixer un élément x quelconque dans E et ainsi d'envisager $P(x)$: ***en mathématiques, chaque objet introduit doit impérativement avoir été préalablement défini***.

  En particulier, pour montrer la proposition « $\forall \boldsymbol{x \in E}$, $\boldsymbol{P(x) \implies Q(x)}$ », il faudra commencer par se donner un x dans E puis montrer l'implication $P(x) \implies Q(x)$, ce qui amène à supposer que $P(x)$ est vraie. Le début de rédaction d'une telle démonstration sera ainsi : « ***Soit $x \in E$ tel que $P(x)$*** » (ou encore : « **Soit $x \in E$. Supposons que $P(x)$ est vraie**… »).
- **Démontrer une proposition du type « $\exists \boldsymbol{x \in E \,/\, P(x)}$ »**

  Pour démontrer ce type de proposition, la méthode consiste à exhiber (ou construire) un élément x_0 de E pour lequel on a $P(x_0)$.
- **Exploiter une proposition du type « $\forall \boldsymbol{x \in E}$, $\boldsymbol{P(x)}$ »**

  Quand on sait que « $\forall x \in E$, $P(x)$ » est vraie, on peut se permettre de choisir un *bon* élément x_0 de E pour lequel on exploitera que $P(x_0)$ est vraie (ce choix dépendra de l'objectif visé).

Exemple 3

Soit f la fonction définie sur $\mathbb{R}$ par $f(x) = x^2 + 3x + 3$.

1. Démontrer la proposition : $\forall x \in \mathbb{R},\ f(x) > 0$.

2. Démontrer la proposition : $\exists x \in \mathbb{R} \,/\, f(x) < 1$.

On rappelle qu'il s'agit de prouver que ces propositions sont vraies.

.....

.....

.....

.....

.....

.....

.....

Exemple 4

a, b, c désignant trois réels, on considère la fonction f définie sur $\mathbb{R}$ par $f(x) = ax^2 + bx + c$.
On suppose que f est la fonction nulle. Justifier que $a = b = c = 0$.

.....

.....

.....

.....

.....

.....

.....

.....

.....

Mise en garde : Ordre des quantificateurs

On peut écrire des propositions en combinant plusieurs quantificateurs. Il faudra alors être très vigilant à l'ordre d'écriture de ces quantificateurs, en particulier dans le cas d'une combinaison $\forall$ et $\exists$.
Considérons par exemple les propositions : « $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R} \,/\, y > x$ » et « $\exists x \in \mathbb{R} \,/\, \forall y \in \mathbb{R},\ y > x$ ».

.....

.....

.....

.....

.....

.....

.....

II.2 Négation de propositions avec quantificateurs

Proposition 3

- La négation de « $\forall x \in E,\ P(x)$ » est « $\exists x \in E \,/\, \text{non}\big(P(x)\big)$ ».
- La négation de « $\exists\, x \in E \,/\, P(x)$ » est « $\forall x \in E,\ \text{non}\big(P(x)\big)$ ».

Remarques et illustrations

- Ces propositions sont assez claires, il est là encore important de se les approprier
  On peut si besoin se ramener à des exemples concrets. Ainsi naturellement, le contraire de la proposition « tous les Parisiens sont franciliens » (qui est vraie) est « il existe au moins un Parisien qui n'est pas francilien » (qui est fausse).

- Ce qui précède se généralise aux propositions comportant une suite de deux quantificateurs.
  Ainsi, pour nier une proposition du type :
  - « $\forall x \in E$, $\exists \ldots$ », on commence par écrire « $\exists x \in E \,/\, \forall$ » et on nie tout ce qui suit ;
  - « $\exists x \in E \,/\, \forall \ldots$ », on commence par écrire « $\forall x \in E$, $\exists$ » et on nie tout ce qui suit.
- La négation de P : « $\exists n \in \mathbb{N} \,/\, n+1 \leqslant 0$ » est $\text{non}\, P$: .....
  .....
  .....
- La négation de Q : « $\forall x \in \mathbb{R}$, $x^2 - x - 10 < 0$ » est $\text{non}\, Q$: .....
  .....
  .....

  *Dans ce dernier exemple, dans l'examen de la valeur de vérité de la proposition Q : « $\forall x \in \mathbb{R}$, $x^2-x-10<0$ », on pourra dire que le réel $x_0 = \ldots$ fournit un **contre-exemple** permettant d'affirmer que Q est fausse, ce qui revient à dire que x_0 est un exemple de réel assurant la démonstration de non$Q$ est vraie : un exemple permet de démontrer qu'une proposition existentielle (avec quantificateur $\exists$) est vraie, un contre-exemple permet de démontrer qu'une proposition universelle (avec quantificateur $\forall$) est fausse.*

Exemple 5
On considère la proposition : $\forall n \in \mathbb{N}$, $\exists p \in \mathbb{N} \,/\, n = p^2$.
La formuler dans le langage courant, en donner la négation. La proposition de départ est-elle vraie ou fausse ?
.....
.....
.....
.....
.....
.....

III Ensembles

III.1 Introduction

- La notion d'*ensemble* est omniprésente en mathématiques et vous en avez déjà rencontré de très nombreux exemples : l'ensemble des réels $\mathbb{R}$, l'ensemble des entiers naturels $\mathbb{N}$, l'ensemble des fonctions affines, l'ensemble des vecteurs du plan, l'ensemble $\mathscr{M}_2(\mathbb{R})$ des matrices carrées d'ordre 2 à coefficients réels, l'ensemble des solutions d'une équation ou d'une inéquation...
- Un **ensemble** est une collection d'*objets*. Les objets qui composent un ensemble sont appelés **éléments**.
- Étant donné un ensemble E, la proposition « x est un élément de E » (ie. « x appartient à E ») est notée « $\boldsymbol{x \in E}$ » et sa négation « $\boldsymbol{x \notin E}$ ».
- On admet qu'il existe un ensemble particulier, celui ne contenant aucun élément. Cet ensemble est unique, c'est l'**ensemble vide** noté $\boldsymbol{\varnothing}$.

III.2 Différentes façons de définir un ensemble

Il existe principalement deux façons de définir un ensemble.

- On peut d'abord citer *entre accolades* les éléments qui composent l'ensemble : on parle dans ce cas là de **définition en extension**. Par exemple : $\{0\,;3\,;5\,;7\,;11\}$, $\{1+\mathrm{i}\,;1-\mathrm{i}\}$, $\left\{\binom{1}{0};\binom{0}{1}\right\}$ ou même $\mathbb{N} = \{0\,;1\,;2\,;3\,;4\ldots\}$.
  Dans le cadre d'ensembles infinis, il est possible d'indiquer la forme des éléments de l'ensemble. Par exemple, $\{2n, n \in \mathbb{Z}\} = \{2n\}_{n\in\mathbb{Z}}$ .....
  Signalons que dans une définition en extension, l'ordre des éléments n'importe pas et les éventuelles répétitions ne comptent pas. Ainsi par exemple : $\{1\,;0\,;1\,;1\} = \{1\,;0\} = \{0\,;1\}$.
- On peut également définir un ensemble par une propriété que ses éléments vérifient et sont les seuls à vérifier : on parle alors de **définition en compréhension**. Citons quelques exemples :
  - $\{x \in \mathbb{R} \,/\, \exists n \in \mathbb{N} \,/\, x = n^2\}$: .....
    On peut également noter cet ensemble : .....
  - $\{x \in \mathbb{R} \,/\, 0 \leqslant x \leqslant 1\}$: .....

- $\mathbb{U} = \{z \in \mathbb{C} \,/\, |z| = 1\}$: .....
  On peut également noter : $\mathbb{U} =$ .....
- $S = \{x \in \mathbb{R} \,/\, 2x^2 + x - 3 = 0\}$: .....
  .....

Remarque : Intervalles d'entiers

Si p et q sont deux entiers relatifs tels que $p < q$, $[\![p, q]\!]$ désigne tous les entiers relatifs compris entre p et q (bornes incluses) ; il contient .....
Par exemple, $[\![5\,;10]\!] =$ .....

III.3 Inclusion

Dans cette partie, E et F désignent deux ensembles.

Définitions

- Dire que $\boldsymbol{E}$ **est inclus dans** $\boldsymbol{F}$ (ou que F contient E) signifie que tout élément de E est également un élément de F, autrement dit : $\forall x \in E,\ x \in F$. On écrit alors $\boldsymbol{E \subset F}$ (ou $F \supset E$).
  Lorsque $E \subset F$, E est qualifiée de **partie** ou **sous-ensemble** de F.
- Les deux **ensembles** E et F sont dit **égaux** s'ils sont composés exactement des mêmes éléments : tout élément de l'un est également élément de l'autre et réciproquement : on écrit alors $\boldsymbol{E = F}$.

Proposition 4

Très clairement, deux ensembles sont égaux si et seulement si le premier est inclus dans le second et réciproquement. On a donc : $E = F \iff (E \subset F \text{ et } F \subset E)$.

Remarque

Il faudra veiller à bien faire la différence entre les notions d'appartenance (d'un élément à un ensemble) et d'inclusion (d'une partie dans un ensemble).
Ainsi, si l'on se donne un certain élément x d'un ensemble E, lui même inclus dans F, on aura : $x \in E$, $E \subset F$ et $x \in F$. En revanche, ***il serait faux d'écrire*** : $\cancel{E \in F}$, $\cancel{x \subset E}$ ou $\cancel{x \subset F}$.

Point Méthode : Démontrer une inclusion, une égalité entre deux ensembles

- **Démontrer l'inclusion « $\boldsymbol{E \subset F}$ »**
  Par définition, $E \subset F$ signifie : $\forall x \in E,\ x \in F$ (ou encore : $\forall x,\ (x \in E \Longrightarrow x \in F)$).
  Pour démontrer ce type de proposition, on commence ainsi généralement par se donner un élément quelconque x de l'ensemble E, (en écrivant « $\boldsymbol{Soit\ x \in E}$ ») et il va alors s'agir d'établir que $x \in F$.
- **Démontrer l'égalité des deux ensembles « $\boldsymbol{E = F}$ »**
  On dispose pour prouver une telle égalité de deux méthodes principales :
  - conformément à ce qui a été vu, on peut procéder par **double inclusion** en montrant que d'une part $E \subset F$ et que d'autre part $F \subset E$;
  - par ailleurs, revenant à la définition de $E = F$ en peut montrer directement l'équivalence caractérisant cette égalité : $\forall x, (x \in E \iff x \in F)$.

Définition et notation

Étant donné un ensemble E, on peut envisager l'**ensemble des parties de** $\boldsymbol{E}$ généralement noté $\boldsymbol{\mathscr{P}(E)}$.

Remarques

- $A \subset E \iff$ .....
- $\forall x \in E,$ .....
- On a toujours :
  - $E \in \mathscr{P}(E)$ .....
    .....
  - $\varnothing \in \mathscr{P}(E)$ .....
    .....
    .....

Illustrations

▶ Considérant $E = \{a\,;b\,;c\}$ ensemble à 3 éléments, on peut déterminer $\mathscr{P}(E)$.

.....

.....

▶ On a $\mathscr{P}(\{1\}) =$ ..... et $\mathscr{P}\big(\mathscr{P}(\{1\})\big) =$ .....

.....

.....

.....

.....

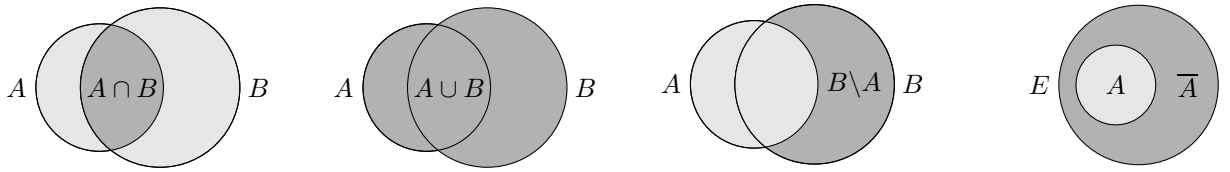
III.4 Opérations sur les ensembles

Dans cette partie, A, B, C et E désignent quatre ensembles.

Définitions

- L'**intersection de A et B**, notée $\boldsymbol{A \cap B}$, est l'ensemble des éléments appartenant simultanément à A et B.
  On a donc $A \cap B =$ .....
- L'**union de A et B**, notée $\boldsymbol{A \cup B}$, est l'ensemble des éléments appartenant à au moins l'une des deux parties A ou B.
  On a donc $A \cup B =$ .....
- La **différence de A dans B**, notée $\boldsymbol{B \backslash A}$ l'ensemble des éléments de B n'appartenant pas à A.
  On a donc $B \backslash A =$ .....
- On suppose à présent que A est une partie de E : $A \subset E$.
  Le **complémentaire de A dans E** est l'ensemble des éléments de E qui ne sont pas dans A.
  Il s'agit donc de $\boldsymbol{E \backslash A}$ que l'on note plus simplement, lorsqu'il n'y a pas d'ambiguïté sur l'ensemble de référence E : $\overline{\boldsymbol{A}}$ ou encore $\boldsymbol{A^c}$. [3]

Illustration



Intersection $A \cap B$ — Union $A \cup B$ — Différence $B \backslash A$ — Complémentaire $\overline{A}$

Remarques et propriétés immédiates

- $A \cup B$ est l'ensemble des éléments appartenant à A ou à B ou aux deux (le « ou » mathématiques n'est pas exclusif).
- $A \cap B = B \cap A$ et $A \cup B = B \cup A$. *On dit que l'intersection et l'union sont des opérations commutatives.*
- $A \cap (B \cap C) = (A \cap B) \cap C$ ce qui autorise à simplement écrire : $A \cap B \cap C$.
  De même $A \cup (B \cup C) = (A \cup B) \cup C$, ce qui autorise à simplement écrire : $A \cup B \cup C$.
  On dit que l'intersection et l'union sont des opérations associatives.
- $A \cap A = \ldots$, $A \cap \varnothing = \ldots$, $A \cup A = \ldots$, $A \cup \varnothing = \ldots$, $\overline{E} = \ldots$, $\overline{\varnothing} = \ldots$ et $\overline{\overline{A}} = \ldots$
- Dans le cas où A et B sont des parties de E, $B \backslash A = \{x \in E \,/\, x \in B \text{ et } x \in \overline{A}\}$ d'où $\boldsymbol{B \backslash A = B \cap \overline{A}}$.
- Comme nous allons le voir dans le cadre de l'exemple qui suit, pour toutes parties A et B on a les relations fondamentales suivantes : $\boldsymbol{A \cap B} \ldots \boldsymbol{A}$ et $\boldsymbol{A} \ldots \boldsymbol{A \cup B}$ (résultats qu'on pourra directement utiliser !).

Exemple 6

E désignant un certain ensemble, on considère A une partie de E et B une partie de A ($B \ldots A$).
Démontrer que $A \cap B = \ldots$ puis que $A \cup B = \ldots$.

Le but de cet exemple est avant tout de s'entraîner à mettre en œuvre les méthodes classiques de comparaison d'ensembles. Il faut se convaincre que les deux résultats ici obtenus sont clairs (à ce titre, on pourra dans la suite directement les utiliser).

3. Signalons également la notation $\complement_{\boldsymbol{E}}^{\boldsymbol{A}}$ ou plus simplement $\complement\boldsymbol{A}$ (s'il n'y pas pas d'ambiguïté sur l'ensemble de référence E).

Remarque : Généralisation des opérations d'intersection et de réunion

Les définitions d'intersection et de réunion se généralisent et peuvent être envisagées pour un nombre quelconque (éventuellement infini) d'ensembles.

I désignant un ensemble (généralement ce sera une partie de $\mathbb{N}$ ou même $\mathbb{N}$ tout entier), on peut envisager des ensembles que nous notons A_i où $i \in I$. L'ensemble $\{A_i\,, i \in I\}$ est alors un ensemble d'ensembles. [4]

- On appelle *intersection des ensembles* A_i, i décrivant I, l'ensemble $\bigcap_{i\in I} A_i = \{x \,/\, \forall i \in I,\, x \in A_i\}$.
  Il s'agit de l'ensemble des éléments appartenant à tous les A_i.
- On appelle de même *réunion des ensembles* A_i, i décrivant I, l'ensemble $\bigcup_{i\in I} A_i = \{x \,/\, \exists i \in I,\, x \in A_i\}$.
  C'est l'ensemble des éléments appartenant à au moins l'un des A_i.

Exemple 7

Pour $n \in \mathbb{N}^*$, on pose $I_n = \left[-\frac{1}{n}\,;\frac{1}{n}\right]$. Déterminer $\bigcup_{n\in\mathbb{N}^*} I_n$ et $\bigcap_{n\in\mathbb{N}^*} I_n$.

Définitions

- Deux ensembles A et B sont dits **disjoints** lorsque $A \cap B = \varnothing$ (A et B n'ont aucun élément commun) et dans ce cas, leur réunion peut être notée $\boldsymbol{A \sqcup B}$.
  Pour un ensemble $\{A_i\,, i \in I\}$ d'ensembles deux à deux disjoints, la réunion $\bigcup_{i\in I} A_i$ peut être notée $\bigsqcup_{\boldsymbol{i\in I}} \boldsymbol{A_i}$.
- Soit E un ensemble et $\{A_i\,, i \in I\}$ un ensemble de parties de E deux à deux disjointes.
  Lorsque $E = \bigsqcup_{i\in I} A_i$, on dit que l'ensemble $\{A_i\,, i \in I\}$ est un **recouvrement disjoint** de E. [5]
  Si de plus aucun des A_i n'est vide, on dira que l'ensemble $\{A_i\,, i \in I\}$ est une **partition** de E.

4. On dit également que les ensembles A_i forment la **famille** $\boldsymbol{(A_i)_{i\in I}}$.
5. Un ensemble de parties de E forme donc un recouvrement disjoint de E lorsque ces parties sont deux à deux disjointes, leur réunion valant E.

Illustration

On considère un ensemble E, A et B deux parties de E.

- **Exemples de recouvrements disjoints de E à partir de deux parties A et B de E.**
  - à 2 parties : .....
  - à 3 parties : .....
  - à 4 parties : .....
- **Exemple de partition de E** non vide : .....

Proposition 5 : Propriétés autour de l'intersection et de la réunion

- **Distributivité de $\cap$ par rapport à $\cup$ et réciproquement**
  A, B et C désignant trois ensembles, on a :
  $$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ et } A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
- **Complémentaire d'une intersection et d'une réunion (lois de Morgan)**
  A et B désignant deux parties d'un ensemble E, on a : $\overline{A \cap B} = \overline{A} \cup \overline{B}$ et $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Démonstration

Nous démontrons le premier point de chacune des deux propriétés, en choisissant de travailler par équivalences.

- On a : $x \in A \cap (B \cup C) \iff x \in A$ et $x \in B \cup C$
  $\iff x \in A$ et $(x \in B$ ou $x \in C)$
  $\iff (x \in A$ et $x \in B)$ ou $(x \in A$ et $x \in C)$ *
  $\iff x \in A \cap B$ ou $x \in A \cap C$
  $\iff x \in \big((A \cap B) \cup (A \cap C)\big)$ d'où $\boldsymbol{A \cap (B \cup C) = (A \cap B) \cup (A \cap C)}$.

  * *On a utilisé la distributivité assez claire du « et » par rapport au « ou ».*
- Soit $x \in E$.
  On a : $x \in \overline{A \cap B} \iff x \notin A \cap B$
  $\iff$ non $(x \in A \cap B)$
  $\iff$ non $(x \in A$ et $x \in B)$
  $\iff$ non $(x \in A)$ ou non $(x \in B)$
  $\iff x \in \overline{A}$ ou $x \in \overline{B}$
  $\iff x \in \overline{A} \cup \overline{B}$ d'où $\boldsymbol{\overline{A \cap B} = \overline{A} \cup \overline{B}}$. **

  ** *Les éléments n'appartenant pas à $A \cap B$ sont ceux n'appartenant pas à A ou n'appartenant pas à B.*

Remarque

Les propositions précédentes s'étendent à la réunion et à l'intersection d'un nombre quelconques d'ensembles.
Avec des notations naturelles on a par exemple : $A \cap \Big(\bigcup\limits_{i \in I} B_i\Big) = \bigcup\limits_{i \in I} (A \cap B_i)$ et $\overline{\bigcap\limits_{i \in I} A_i} = \bigcup\limits_{i \in I} \overline{A_i}$.

III.5 Ensembles usuels de nombres réels : parties de $\mathbb{R}$

- Pour rappel, on donne ci-dessous les parties les plus usuelles de $\mathbb{R}$.
  - L'ensemble $\mathbb{N}$ des **entiers naturels** : $\mathbb{N} = \{0, 1, 2, \dots\}$.
  - L'ensemble $\mathbb{Z}$ des **entiers relatifs**, constitué des entiers naturels et de leurs opposés : $\mathbb{Z} = \mathbb{N} \cup \{-n, n \in \mathbb{N}\}$.
  - L'ensemble $\mathbb{D}$ des **décimaux**, ensemble des réels pouvant s'écrire sous la forme $\frac{p}{10^n}$ avec $p \in \mathbb{Z}$ et $n \in \mathbb{N}$.[6]
  - L'ensemble $\mathbb{Q}$ des **rationnels**, ensemble des réels pouvant s'écrire sous la forme $\frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.[7]
    On écrira : .....
- On a les inclusions : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R}$.
  Ces inclusions sont strictes. On pourrait par exemple préciser $\mathbb{Q} \subsetneq \mathbb{R}$: il existe des réels qui ne sont pas des rationnels (ie. qui ne peuvent pas s'écrire sous la forme d'un quotient d'entiers) ; on les qualifie d'**irrationnels**.
  Par exemple : .....

6. C'est l'ensemble des réels qui *peuvent* s'écrire avec un nombre de chiffres fini après la virgule.
7. On choisit de faire porter le signe d'un rationnel par le numérateur.
Nous verrons que dans l'écriture d'un rationnel, il est possible d'imposer que p et q n'aient aucun diviseur commun supérieur à 1.

- On peut envisager des sous-parties des parties précédentes :
  - $\mathbb{R}^*$ désigne l'ensemble des réels non nuls : $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$; on définit de même $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$;
  - $\mathbb{R}_+$ (resp. $\mathbb{R}_-$) désigne l'ensemble des réels positifs ou nuls (resp. négatifs ou nuls) ;
  - $\mathbb{R}_+^*$ (resp. $\mathbb{R}_-^*$) désigne l'ensemble des réels strictement positifs (resp. strictement négatifs) ...

III.6 Produit cartésien

Définition

E et F désignant deux ensembles non vides, le **produit cartésien de E et F** noté $\boldsymbol{E \times F}$ est l'ensemble des *couples* (x, y) avec $x \in E$ et $y \in F$.
On a donc $E \times F = \{z \,/\, \exists x \in E,\, \exists y \in F \,/\, z = (x, y)\}$ ou plus simplement $E \times F = \{(x, y),\, x \in E,\, y \in F\}$.

Remarques et exemples

- Lorsque $E = F$, le produit cartésien $E \times E$ est plutôt noté E^2.
- Dans l'écriture d'un couple, l'ordre est essentiel : en général, $E \times F \neq F \times E$ et $(x, y) \neq (y, x)$.
- Il est important de bien noter la différence entre :
  - le *couple* $(1\,;2)$ (avec $(1\,;2) \neq (2\,;1)$) ;
  - l'ensemble à deux éléments $\{1\,;2\}$ pour lequel l'ordre des éléments n'a pas d'importance $\{1\,;2\} = \{2\,;1\}$: on parle alors de *paire*.
- L'**égalité de deux couples** est définie par : $(x_1, y_1) = (x_2, y_2) \iff x_1 = x_2$ et $y_1 = y_2$.
- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y),\, x \in \mathbb{R},\, y \in \mathbb{R}\}$.
  On notera indifféremment : $(x, y) \in \mathbb{R} \times \mathbb{R}$; $(x, y) \in \mathbb{R}^2$; $x \in \mathbb{R}$, $y \in \mathbb{R}$ ou même x, $y \in \mathbb{R}$.
- Le produit cartésien $\mathbb{R} \times \mathbb{R}$ est couramment utilisé quand on travaille dans le plan rapporté à un certain repère et que chaque point du plan est identifié avec le couple de ses coordonnées.
- La notion de produit cartésien de deux ensembles s'étend sans difficulté à un nombre fini d'ensembles non vides : pour une *famille* $(E_1, \ldots, E_n)$ d'ensembles non vides ($n \in \mathbb{N}^*$), l'ensemble des *familles*[8] $(x_1, \ldots, x_n)$ avec $x_1 \in E_1, \ldots, x_n \in E_n$ représente le produit cartésien de $E_1, \ldots, E_n$ et se note $E_1 \times \cdots \times E_n$ (lorsque $E_1 = \cdots = E_n = E$, ce produit cartésien est plutôt noté E^n).

PARTIE B : ARITHMÉTIQUE

Dans cette Partie, nous manipulons des entiers (relatifs ou naturels).
Il s'agit de reprendre la plupart des éléments du programme d'arithmétique vus dans le cadre de l'option mathématiques expertes de Terminale. Mais pas toutes, certaines deviennent hors programme : la relation de congruence, les théorèmes de Bézout et de Gauss ....[9]

Dans la suite, nous admettrons les deux résultats intuitivement clairs[10] suivants :

- « toute partie non vide de $\mathbb{N}$ admet un minimum (ou plus petit élément) » ;
- « toute partie non vide et majorée de $\mathbb{N}$ (ou $\mathbb{Z}$) admet un maximum (ou plus grand élément) ».

IV Divisibilité dans $\mathbb{Z}$ et division euclidienne

IV.1 Relation de divisibilité dans $\mathbb{Z}$

Définitions

Soient $a, b \in \mathbb{Z}$.

- On dit que $\boldsymbol{b}$ **divise** $\boldsymbol{a}$ ou que b est un **diviseur** de a lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = kb$.
  On note alors $\boldsymbol{b|a}$ et ainsi : $\boldsymbol{b|a \iff \exists k \in \mathbb{Z} \,/\, a = kb}$.
- Lorsque b divise a, on dit que a est un **multiple** de b.

8. Dans une famille, l'ordre des éléments compte. La famille $(x_1, \ldots, x_n)$ peut également être qualifiée de n-uplet : un couple est une famille à deux éléments, un triplet (ou 3-uplet) une famille à trois éléments ...

9. Dans ce cours, nous nous limitons strictement au programme officiel de PCSI. La notion de congruence étant cependant particulièrement pratique, nous rappelons en toute fin de chapitre les principales notions vues à son sujet en classe de Terminale.

10. Ces résultats sont en réalité liés à la construction de $\mathbb{N}$ qui est hors programme.

Remarques

- $\forall b \in \mathbb{Z}$, $b|0$: tout entier divise 0 ($\forall b \in \mathbb{Z}$, $0 = 0 \times b$), autrement dit, 0 est multiple de tout entier.
- $\forall a \in \mathbb{Z}$, $0|a \iff a = 0$: le seul entier que 0 divise est lui-même.
- Pour $a \in \mathbb{Z}$, l'ensemble des multiples de a est noté $\boldsymbol{a\mathbb{Z}}$: $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\} = \{ak\}_{k\in\mathbb{Z}}$.
- Pour $a \in \mathbb{Z}$, on notera dans la suite de ce cours $\boldsymbol{\mathcal{D}(a)}$ l'ensemble des diviseurs de a (notation non officielle).
  - on a par exemple : $\mathcal{D}(18) = \{\pm1\,, \pm2\,, \pm3\,, \pm6\,, \pm9\,, \pm18\}$;
  - on a toujours : ▪ $\forall b \in \mathbb{Z}$, $b \in \mathcal{D}(a) \iff -b \in \mathcal{D}(a)$ ▪ $\pm1 \in \mathcal{D}(a)$ ▪ $\pm a \in \mathcal{D}(a)$ ▪ $\mathcal{D}(a) = \mathcal{D}(-a) = \mathcal{D}(|a|)$;
- Pour $a, b \in \mathbb{Z}^*$, $b|a \Longrightarrow |b| \leqslant |a|$ (car pour $a, b \in \mathbb{Z}^*$, $b|a \Rightarrow \exists k \in \mathbb{Z}^* \,/\, a{=}kb$ soit $|a|{=}|k||b|$ avec $|k| \geqslant 1\ldots$). Ainsi en particulier, pour $a, b \in \mathbb{N}^*$, $b|a \Longrightarrow b \leqslant a$.

Proposition 6 : Propriétés autour de la relation de divisibilité

Soient $a, b, c, d \in \mathbb{Z}$

1. $(b|a \text{ et } a|c) \Longrightarrow b|c$
2. $b|a \Longrightarrow (\forall u \in \mathbb{Z},\ b|au)$
3. $bc|a \Longrightarrow (b|a \text{ et } c|a)$
4. $(b|c \text{ et } b|d) \Longrightarrow (\forall u, v \in \mathbb{Z},\ b|uc + vd)$
5. $(b|a \text{ et } d|c) \Longrightarrow bd|ac$
6. $b|a \Longrightarrow (\forall k \in \mathbb{N},\ b^k|a^k)$
7. $(b|a \text{ et } a|b) \Longrightarrow |a| = |b|$

Démonstration

1. En supposant que $b|a$ et $a|c$, il existe $k, \ell \in \mathbb{Z}$ tels que $a = kb$ et $c = \ell a$.
   D'où $c = \ell(kb) = (\ell k)b$ avec $(\ell k) \in \mathbb{Z}$ soit $b|c$. *La relation « | » est dite transitive.*
2. Soit $u \in \mathbb{Z}$.
   En supposant que $b|a$, il existe $k \in \mathbb{Z}$ tel que $a = kb$ d'où $au = (ku)b$ avec $(ku) \in \mathbb{Z}$: on a donc $b|au$.
   En d'autres termes, ***si b divise a, b divise tout multiple de a****.*
3. En supposant que $bc|a$, il existe $k \in \mathbb{Z}$ tels que $a = kbc$ d'où $a = (kc)b = (kb)c$ avec $(kc) \in \mathbb{Z}$ et $(kb) \in \mathbb{Z}$: on a donc $b|a$ et $c|a$. *En d'autres termes,* ***si un entier divise a, tout diviseur de cet entier divise a.***
4. Soient $u, v \in \mathbb{Z}$.
   En supposant que $b|c$ et $b|d$, il existe $k, \ell \in \mathbb{Z}$ tels que $c = kb$ et $d = \ell b$.
   D'où $uc + vd = (uk + \ell v)b$ avec $(uk + \ell v) \in \mathbb{Z}$ soit $b|uc + vd$.
   On dira que ***si un entier en divise deux autres, cet entier divise toute combinaison linéaire (à coefficients entiers) de ces deux autres****.*[11]
5. En supposant que $b|a$ et $d|c$, il existe $k, \ell \in \mathbb{Z}$ tels que $a = kb$ et $c = \ell d$.
   D'où par produit, $ac = (k\ell)bd$ avec $(k\ell) \in \mathbb{Z}$ soit $bd|ac$. *La relation « | » est dite compatible par produit.*
6. On suppose que $b|a$ et on démontre par récurrence que : $\forall k \in \mathbb{N}$, $b^k|a^k$.
   - Comme $1|1$, la proposition est vraie au rang 0.
   - Soit $k \in \mathbb{N}$. On suppose que la propositions est vraie au rang k.
     On a donc $b^k|a^k$ avec en outre par hypothèse, $b|a$: d'où par produit (point **5.**), $b^{k+1}|a^{k+1}$ et la proposition est vraie au rang $k + 1$.
   - On a donc bien : $\forall k \in \mathbb{N}$, $b^k|a^k$.

   Notons qu'en écrivant l'égalité caractérisant $b|a$ et en élevant chacun des membres de cette égalité à une certaine puissance $k \in \mathbb{N}$, le résultat visé en découlerait immédiatement.
7. On suppose que $b|a$ et $a|b$: il existe $k, \ell \in \mathbb{Z}$ tels que $a = kb$ et $b = \ell a$ et par conséquent, $a = k\ell a$.
   Si $a = 0$, alors $b = 0$ et on a bien $|a| = |b|$.
   Sinon ($a \neq 0$), $k\ell = 1$ et par conséquent $k = \ell = \pm1$ (k et ℓ sont des entiers de produit 1). Ainsi, a et b sont égaux ou opposés soit $|a| = |b|$.
   Par disjonction des cas, on a donc bien démontré le résultat souhaité.
   On en déduit que dans le cas où a et b sont des entiers naturels, $\boldsymbol{(b|a \text{ et } a|b) \Longrightarrow a = b}$.

11. En particulier, si $(b|c \text{ et } b|d)$ alors $b|c + d$ et $b|c - d$.

Remarques

- Les points **4.** et **7.** sont les plus importants, les autres sont assez naturels.
- Certaines de ces implications sont en fait des équivalences, celle du point **2.** par exemple (si $\forall u \in \mathbb{Z},\ b|au$, on a en particulier, en choisissant $u = 1 : b|a$). Si on ne les écrit pas, c'est qu'elles sont évidentes et ne présentent guère d'intérêt.
- Attention, d'autres ne sont que des implications (leur réciproque est fausse).
  C'est par exemple le cas de celle du point **3.** : on a $4|12$ et $6|12$ mais $4 \times 6 = 24$ ne divise pas 12 ![12]

Exemple 8

Montrer que pour tout $n \in \mathbb{N}$, 7 divise $2^{3n} - 1$.

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exemple 9

Pour $a, b \in \mathbb{Z}$, démontrer l'équivalence : $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.
Autrement dit, a divise b revient à dire que tout multiple de b est multiple de a (ce résultat est à connaître). [13]

.....

.....

.....

.....

.....

.....

.....

.....

.....

IV.2 Division euclidienne

Proposition 7 : Théorème de la division euclidienne dans $\mathbb{Z}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec $0 \leqslant r < b$. [14]
Dans cette **division euclidienne de a par b**, a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

Démonstration

Le théorème de la division euclidienne est un théorème d'*existence* et d'*unicité* : en tant que tel, il sera démontré en deux temps.

- **Existence**
  Notons $\mathcal{E} = \{a - bk, k \in \mathbb{Z}\} \cap \mathbb{N} : \mathcal{E}$ est une partie de $\mathbb{N}$ *non vide.*
  En effet : . si $a \geqslant 0,\ a \in \mathcal{E}$ (valeur $k = 0$) ;
  . si $a < 0,\ a - ba = (1 - b)a$ avec $(1 - b) \leqslant 0$ soit $(1 - b)a \geqslant 0$ et donc $a - ba \in \mathcal{E}$ (valeur $k = a$).
  Ainsi, $\mathcal{E}$ admet un plus petit élément que nous notons $\boldsymbol{r} : r \geqslant 0$ et r peut donc s'écrire $r = a - bq \iff a = bq + r$ avec $\boldsymbol{q} \in \mathbb{Z}$.

12. Sous l'hypothèse complémentaire que b et c sont *premiers entre eux* (ie. n'admettent pas d'autres diviseurs positifs communs que 1), on aurait bien la réciproque : $(b|a \text{ et } c|a) \Longrightarrow bc|a$.
13. Par exemple, comme $4|8$, tout multiple de 8 est également un multiple de 4.
14. Dans la division euclidienne d'un entier par $b \in \mathbb{N}^*$, le reste r appartient à $[\![0\,;b-1]\!]$.

Il est assez clair que $r < b$. En effet, si on avait $r \geqslant b$, on aurait alors $r - b \geqslant 0$ soit $r' = a - b(q+1) \in \mathcal{E}$ avec par ailleurs $r' < r$: d'où contradiction puisque r est censé être le plus petit élément de $\mathcal{E}$.
On a ainsi réussi à mettre en évidence l'**existence** d'un couple $(q\,,r) \in \mathbb{Z}\times\mathbb{N}$ tel que $a = bq+r$ avec $0 \leqslant r < b$.

- **Unicité**
  On suppose qu'il existe 2 couples de division euclidienne de a par b : $(q\,,r)$ et (q',r').
  On a donc : $a = bq + r = bq' + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b \iff -b < -r' \leqslant 0$ soit $-b < r - r' < b$.
  Il en découle que $r - r' = b(q' - q)$ et l'entier $r - r'$ est ainsi un multiple de b tel que $-b < r - r' < b$: cela entraîne que $r - r' = 0$ soit $r = r'$.
  Dès lors, $bq = bq' \iff q = q'$ $(b \neq 0)$ et ainsi $(q\,,r) = (q',r')$, ce qui achève la preuve de l'**unicité**.

Remarques et illustrations

- Dire que $b|a$ équivaut à dire que le reste de la division euclidienne de a par b vaut 0.
- Avec les notations précédentes, si $a \in \mathbb{N}$ alors $q \in \mathbb{N}$ (en effet, comme $r = a - bq$, $q < 0$ entraînerait $r > b$).
- Avec les notations et hypothèses précédentes :
  $0 \leqslant a - bq < b \iff -a \leqslant -bq < b - a \iff \frac{a}{b} \geqslant q > -1 + \frac{a}{b} \iff \frac{a}{b} - 1 < q \leqslant \frac{a}{b}$.
  Il en découle que q est la *partie entière* de $\frac{a}{b}$ soit $q = \left\lfloor \frac{a}{b} \right\rfloor$.[15]
- Par exemple, dans les cas suivants, la division euclidienne de a par 5 s'écrit :
  - $a = 38$: .....
  - $a = -47$: .....
- Considérant $b \in \mathbb{N}^*$, il est possible de partitionner $\mathbb{N}$ (ou $\mathbb{Z}$) en les sous-ensembles constitués des entiers dont les restes dans la division euclidienne par b valent respectivement 0, 1, ... , $b-1$.
  - Dans le cas où $b = 2$, on distingue ainsi les entiers s'écrivant $2k$ (entiers pairs) et ceux s'écrivant $2k+1$ (entiers impairs).
  - Dans le cas où $b = 3$, on distingue de même les entiers s'écrivant $3k$ (les multiples de 3), $3k+1$ et $3k+2$.

Exemple 10

Montrer que pour tout $n \in \mathbb{Z}$, $A_n = n(5n^2+1)$ est divisible par 3.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

V PGCD et PPCM de deux entiers

V.1 PGCD de deux entiers

V.1.1 Définition

Définition

Soient a et b deux entiers relatifs non simultanément nuls.
On appelle **plus grand commun diviseur** ou **PGCD** de a et b le plus grand élément de l'ensemble des diviseurs communs de a et b.
Le PGCD de a et b se note $\boldsymbol{\mathrm{PGCD}(a,b)}$ ou $\boldsymbol{a \wedge b}$.

15. Pour $x \in \mathbb{R}$, nous verrons que la **partie entière de x** est l'unique entier noté $\lfloor x \rfloor$ vérifiant $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1 \Leftrightarrow x - 1 < \lfloor x \rfloor \leqslant x$.

Remarques

- Cette définition suppose que l'ensemble des diviseurs communs de a et b possède un plus grand élément, ce qui est bien le cas. En effet, si $a \neq 0$ (par exemple), cet ensemble de diviseurs communs est une partie d'entiers non vide (1 y appartient) et majorée (par $|a|$) : elle admet donc bien un plus grand élément.
  On pourrait bien sûr remplacer dans la définition « diviseurs communs » par « diviseurs communs positifs ».
  On a donc : $\mathbf{PGCD(a,b) = \max\big(\mathcal{D}(a) \cap \mathcal{D}(b)\big)}$ (le maximum étant défini au sens de la relation « $\leqslant$ »).
- La définition précédente ne permettant pas de définir $\mathrm{PGCD}(0,0)$ (en effet, $\big(\mathcal{D}(0) \cap \mathcal{D}(0)\big) = \mathbb{Z}$), on convient de poser $\mathbf{PGCD(0,0) = 0}$.
- On a par exemple : $\mathrm{PGCD}(12,30) =$ .... puisque .....
- Pour tous entiers $a, b \in \mathbb{Z}^*$ on a assez clairement :
  . $a \wedge b = b \wedge a$. $a \wedge b = |a| \wedge |b|$. $a \wedge 1 =$ .... . $a \wedge b \leqslant$ .....
  . $\mathbf{PGCD(a,0) = |a|}$ (car .....
- Pour tous entiers relatifs a et b tels que $a|b$, on a : $\mathrm{PGCD}(a,b) =$ .....

Définition

Lorsque deux entiers a et b sont tels que $\mathrm{PGCD}(a,b) = 1$, ils sont dits **premiers entre eux** (leurs seuls diviseurs communs sont ± 1 et 1 est leur seul diviseur commun positif).

V.1.2 Algorithme d'Euclide

Lemme d'Euclide

- Pour tous $a, b, k \in \mathbb{Z}$, $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a+bk, b)$.
- En particulier, pour tous $a, b \in \mathbb{Z} \times \mathbb{N}^*$, $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r)$ où r est le reste de la division euclidienne de a par b.

Démonstration

- Le premier point étant clair si $b = 0$, on peut supposer que $b \neq 0$.
  Pour obtenir le résultat visé, il suffit d'établir que les couples (a,b) et $(a+bk,b)$ ont mêmes diviseurs communs, soit $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a+bk) \cap \mathcal{D}(b)$. On le montre par double inclusion en considérant $d \in \mathbb{Z}$:
  . si $d|a$ et $d|b$ alors $d|(a+bk)$ (et $d|b$) ;
  . si $d|a+bk$ et $d|b$ alors $d|(a+bk-bk)$ soit $d|a$ (et $d|b$).
- Pour tous $a, b \in \mathbb{Z} \times \mathbb{N}^*$, la division euclidienne de a par b s'écrit $a = bq + r$ avec $q \in \mathbb{Z}$ et $0 \leqslant r \leqslant b-1$.
  On a alors d'après ce qui précède, $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a-bq,b) = \mathrm{PGCD}(r,b) = \mathrm{PGCD}(b,r)$.

Exemple 11

Pour $n \in \mathbb{Z}$, déterminer $\mathrm{PGCD}(5n+2, 2n+3)$.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Du lemme d'Euclide découle l'*algorithme d'Euclide* permettant de déterminer le PGCD de deux *entiers naturels*.

Algorithme d'Euclide (pour des entiers naturels)

Soient $a, b \in \mathbb{N}$ tels que $0 \leqslant b \leqslant a$.

À partir de la donnée de a et b, on définit la suite $r_0, r_1 \dots$ de la manière suivante :

- On pose au départ $r_0 = a$ et $r_1 = b$.
- Pour $k \in \mathbb{N}$, **tant que** $r_{k+1} \neq 0$, on effectue la division euclidienne de r_k par r_{k+1} et on note r_{k+2} le reste de cette division ($0 \leqslant r_{k+2} < r_{k+1}$).
- On construit ainsi une suite d'entiers $r_0, r_1, r_2 \dots$ telle que $r_0 \geqslant r_1 > r_2 \dots \geqslant 0$ d'où, puisque le nombre d'entiers inférieurs à r_0 est fini, il existe un entier $n \in \mathbb{N}^*$ tel que $r_n = 0$, ce qui assure que **l'algorithme se termine**.
- En vertu du lemme d'Euclide on a : $\boldsymbol{a \wedge b} = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n-1} \wedge r_n = r_{n-1} \wedge 0 = \boldsymbol{r_{n-1}}$.

On a donc construit un algorithme nous permettant d'obtenir le PGCD de deux entiers naturels : **en effectuant les divisions euclidiennes successives selon le procédé précédemment exposé, il suffit de retourner la valeur $\boldsymbol{r_n}$ dès que $\boldsymbol{r_{n+1} = 0}$.**

Remarque : Examen des cas particuliers

- Si $a = b = 0$ (cas non exclu), $r_0 = r_1 = 0$: le premier test ($k = 0$) conduit à constater que $r_1 = 0$ et l'algorithme renvoie $r_0 = 0$, résultat conforme avec $\text{PGCD}(0, 0) = 0$.
- Si $b = 0$ et $a \neq 0$, l'algorithme renvoie $r_0 = a$, résultat conforme avec $\text{PGCD}(a, 0) = a$.
- Si $a = b$ ($\neq 0$), $r_0 = r_1 = a$ ($\neq 0$) et le reste de la division euclidienne de a par a étant $r_2 = 0$, l'algorithme renvoie $r_1 = a$, résultat conforme avec $\text{PGCD}(a, a) = a$.

Généralisation : Algorithme d'Euclide généralisé

Dans le cas de deux entiers a et b quelconques, compte tenu de $a \wedge b = |a| \wedge |b|$ et $a \wedge b = b \wedge a$, on peut se ramener au cas précédent en appliquant l'algorithme à : $b' = \min\big(|a|, |b|\big)$ et $a' = \max\big(|a|, |b|\big)$.

Proposition 8

Le PGCD de deux entiers est le dernier reste non nul de la suite des restes obtenue dans l'algorithme d'Euclide (éventuellement généralisé).

Illustration et remarque

- On peut à titre d'illustration déterminer $\text{PGCD}(600, 124)$ par l'algorithme d'Euclide :

  .....
  .....
  .....
  .....

- L'algorithme d'Euclide constitue un moyen systématique d'obtention du PGCD de deux entiers, mais il serait maladroit de systématiquement y recourir !
  Si l'on cherche par exemple $\text{PGCD}(765432, 15)$:

  .....
  .....
  .....

V.1.3 Propriétés du PGCD

Proposition 9 : Propriétés du PGCD de deux entiers

Soient $a, b, c, k \in \mathbb{Z}$.

- **Diviseurs communs et diviseurs du PGCD**
  L'ensemble des diviseurs communs de a et b coïncide avec l'ensemble des diviseurs de $\text{PGCD}(a, b)$.
  Autrement dit : $\forall c \in \mathbb{Z},\ (c|a \text{ et } c|b) \iff c|\text{PGCD}(a, b)$.
- **Factorisation par un diviseur commun** : $\text{PGCD}(ka, kb) = |k|\,\text{PGCD}(a, b)$.

Démonstration

- Avec les notations de la démonstration de l'algorithme d'Euclide, on a grâce au lemme d'Euclide :
  $\mathcal{D}(a)\cap\mathcal{D}(b)=\mathcal{D}(r_0)\cap\mathcal{D}(r_1)=\mathcal{D}(r_1)\cap\mathcal{D}(r_2)=\ldots=\mathcal{D}(r_{n-1})\cap\mathcal{D}(r_n)=\mathcal{D}(r_{n-1})\cap\mathcal{D}(0)=\mathcal{D}(r_{n-1})\cap\mathbb{Z}$.
  Or $\mathcal{D}(r_{n-1})\cap\mathbb{Z}=\mathcal{D}(r_{n-1})=\mathcal{D}\big(\text{PGCD}(a,b)\big)$ d'où $\boldsymbol{\mathcal{D}(a)\cap\mathcal{D}(b)=\mathcal{D}\big(\text{PGCD}(a,b)\big)}$.
  On a vu que $\text{PGCD}(12,30)=6$ *et on a bien* .....
- Pour le second point, notons que le résultat est immédiat si $k=0$ ($0\wedge 0=0$).
  Compte tenu par ailleurs de $(ka)\wedge(kb)=(|k|a)\wedge(|k|b)$, on peut désormais supposer que $k>0$.
  Pour la suite, on se contente de traiter le cas où a et b sont positifs ($a\wedge b=|a|\wedge|b|$) et sans perte de généralité on suppose que $0\leqslant b\leqslant a$.
  Le cas $b=0$ ne pose pas de difficulté : en effet, $(ka)\wedge 0=ka=|k|(a\wedge 0)$.
  Pour $b>0$, la division euclidienne de a par b s'écrit $a=bq+r$ où $0\leqslant r<b$.
  Il en découle que $ka=(kb)q+kr$ avec $0\leqslant kr<kb$: c'est donc la division euclidienne de ka par kb.
  L'algorithme d'Euclide appliqué à ka et kb fournit donc une suite de restes proportionnelle de rapport k à celle obtenue en l'appliquant à a et b, ce qui permet de prouver que $(ka)\wedge(kb)=k(a\wedge b)=|k|(a\wedge b)$ (en examinant les derniers restes non nuls). Le résultat dans le cas général en découle.

Corollaire : Forme irréductible d'un rationnel

L'ensemble des rationnels peut s'écrire : $\mathbb{Q}=\left\{\frac{p}{q},\ p\in\mathbb{Z},\ q\in\mathbb{N}^*,\ \text{PGCD}(p,q)=1\right\}$.
L'écriture d'un rationnel sous la forme $\frac{p}{q}$ avec $\text{PGCD}(p,q)=1$ est qualifiée de **forme irréductible** de ce rationnel.

Démonstration

Notons $Q'=\left\{\frac{p}{q},\ p\in\mathbb{Z},\ q\in\mathbb{N}^*,\ \text{PGCD}(p,q)=1\right\}$: il s'agit de montrer que $Q'=\mathbb{Q}$ soit $\mathbb{Q}\subset Q'$, l'autre inclusion étant évidente.
Soit $r\in\mathbb{Q}$: il existe $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$ tels que $r=\frac{p}{q}$.
En notant $d=\text{PGCD}(p,q)$, il existe $p'\in\mathbb{Z}$ et $q'\in\mathbb{N}^*$ tels que $p=dp'$ et $q=dq'$: on a alors $r=\frac{dp'}{dq'}=\frac{p'}{q'}$.
Comme $d=\text{PGCD}(dp',dq')=d\text{PGCD}(p',q')$ avec $d>0$ (p et q non simultanément nuls), $\text{PGCD}(p',q')=1$.
Ainsi, $r=\frac{p'}{q'}$ avec $\text{PGCD}(p',q')=1$ et par conséquent $\mathbb{Q}\subset Q'$. Finalement $\boldsymbol{Q'=\mathbb{Q}}$.

On retiendra que **pour $p,q\in\mathbb{Z}\times\mathbb{N}^*$, en notant $d=\text{PGCD}(p,q)$, il existe $p',q'\in\mathbb{Z}\times\mathbb{N}^*$ tels que $p=dp'$, $q=dq'$ et $\text{PGCD}(p',q')=1$**.

Exemple 12

Soient $a,b,c\in\mathbb{Z}$ tels que $\text{PGCD}(a,b)=\text{PGCD}(a,c)=1$ (a,b et a,c premiers entre eux).
Montrer que $\text{PGCD}(a,bc)=1$.

.....
.....
.....
.....
.....
.....
.....

V.2 PPCM de deux entiers

V.2.1 Définition

Définition

Soient deux entiers $a,b\in\mathbb{Z}^*$ (aucun n'est nul).
On appelle **plus petit commun multiple** ou **PPCM** de a et b, le plus petit élément de l'ensemble des multiples communs *strictement positifs* de a et b.
Le PPCM de a et b se note $\boldsymbol{\text{PPCM}(a,b)}$ ou $\boldsymbol{a\vee b}$.

Remarques

- On a donc par définition : pour $a,b\in\mathbb{Z}^*$, $\text{PPCM}(a,b)=\min\big(a\mathbb{Z}\cap b\mathbb{Z}\cap\mathbb{N}^*\big)$ (le minimum étant défini au sens de la relation « $\leqslant$ »).

- Cette définition suppose que l'ensemble des multiples communs strictement positifs de a et b possède un plus petit élément, ce qui est bien le cas. En effet, cet ensemble est une partie d'entiers non vide de $\mathbb{N}$ ($|ab|$ y appartient) minorée (par 0) : elle admet donc un plus petit élément.
- La définition précédente ne permettant pas de définir le PPCM de deux entiers dont l'un est nul (l'ensemble des multiples communs strictement positifs serait alors vide), on convient de poser : pour tout $a \in \mathbb{Z}$, $\mathbf{PPCM(a,0) = 0}$ (et en particulier $\mathbf{PPCM(0,0) = 0}$).
- On a par exemple : $\text{PPCM}(12,30) = \ldots.$ puisque .....
  .....
- Pour tous entiers $a, b \in \mathbb{Z}^*$ on a assez clairement :
  ▪ $a \vee b = b \vee a$ ▪ $a \vee b = |a| \vee |b|$ ▪ $a \vee 1 = \ldots.$ ▪ si $a|b$, $a \vee b = \ldots.$ ▪ $a \vee b \leqslant \ldots\ldots$

V.2.2 Propriétés du PPCM

Proposition 10 : Multiples communs et multiples du PPCM

Soient $a, b \in \mathbb{Z}$.

L'ensemble des multiples communs de a et b coïncide avec l'ensemble des multiples de $\text{PPCM}(a,b)$, ce qui peut s'écrire : $\boldsymbol{a\mathbb{Z} \cap b\mathbb{Z} = \text{PPCM}(a,b)\mathbb{Z}}$.

Autrement dit : $\forall c \in \mathbb{Z},\ (a|c \text{ et } b|c) \iff \text{PPCM}(a,b)|c$.

Démonstration

On peut noter que le résultat est acquis si $a = 0$ ou $b = 0$ puisque alors $\text{PPCM}(a,b) = 0$.

On considère désormais a et b non nuls, et sans perte de généralité, compte tenu de $\text{PPCM}(a,b) = \text{PPCM}(|a|,|b|)$, on peut supposer $a > 0$ et $b > 0$. Notons qu'on a alors $\text{PPCM}(a,b) \neq 0$.

Pour alléger les écritures on pose $m = \text{PPCM}(a,b)$ *et on se propose de démontrer par double implication l'équivalence traduisant l'égalité* $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ (et écrite ci-dessus).

▪ $\Longleftarrow$

Soit $c \in \mathbb{Z}$ multiple de m. Comme m est un multiple commun à a et b, c est à fortiori un multiple de a et b (ce qui établit la première implication).

▪ $\Longrightarrow$

Soit $c \in \mathbb{Z}$ multiple commun de a et b.

La division euclidienne de c par $m \neq 0$ s'écrit : $c = mq + r$ avec $q \in \mathbb{Z}$ et r entier vérifiant $0 \leqslant r < m$.

Puisque c et m sont des multiples communs de a et b, $r = c - mq$ est également un multiple commun de a et b, vérifiant $0 \leqslant r < m$: il en découle que $r = 0$ (par définition, m est le plus petit multiple commun strictement positif) et ainsi, c est un multiple de m (ce qui établit la seconde implication).

On a par exemple vu que $\text{PPCM}(12,30) = 60$ *: l'ensemble des multiples communs de* 12 *et* 30 *est* .....

Proposition 11 : Lien entre PGCD et PPCM

Pour $a, b \in \mathbb{Z}$, $\mathbf{PGCD(a,b) \times PPCM(a,b) = |ab|}$.

Démonstration

On peut noter que le résultat est acquis si $a = 0$ ou $b = 0$ puisque alors $a \vee b = 0$.

On considère désormais que a et b sont non nuls, et sans perte de généralité, on peut supposer $a > 0$ et $b > 0$.

Posons $d = \text{PGCD}(a,b)$ et $m = \text{PPCM}(a,b)$ (a et b non simultanément nuls donc $d \neq 0$).

Il s'agit de montrer que $dm = ab$.

▪ Montrons d'abord que $dm|ab$.
Comme $d|a$ et $d|b$, il existe $a', b' \in \mathbb{N}$ tels que $a = da'$ et $b = db'$. En posant $\mu = da'b' = ab' = a'b$, $a|\mu$ et $b|\mu$ d'où $m|\mu$ (propriété du PPCM). Ainsi $dm|d\mu$ (par produit puisque $d|d$) soit $\underline{dm|ab}$ (car $d\mu = da'db' = ab$).

▪ Montrons à présent que $ab|dm$.
Puisque ab est un multiple de a et b, c'est un multiple de $\text{PPCM}(a,b) = m$: il existe $n \in \mathbb{N}$ tel que $ab = mn$. Or m est un multiple de a, donc il existe $c \in \mathbb{N}$ tel que $m = ac$. Ainsi, $ab = mn = acn$ d'où $b = cn$ ($a \neq 0$) et $n|b$. Comme par ailleurs m est un multiple de b, on montrerait de même que $n|a$. Par conséquent, comme $n|a$ et $n|b$, $n|d$ (propriété du PGCD). On en déduit que $mn|md$ (par produit puisque $m|m$) soit $\underline{ab|dm}$.

Finalement, $dm|ab$ et $ab|dm$ d'où $dm = ab$ soit $\mathbf{PGCD(a,b) \times PPCM(a,b) = ab}$.

On a par exemple vu que $\text{PGCD}(12,30) = 6$ *et* $\text{PPCM}(12,30) = 60$ *: on bien* .....

VI Nombres premiers

Dans cette partie, les entiers considérés sont des entiers naturels.

VI.1 Définition et premières propriétés

Définition

Soit $p \in \mathbb{N}$.

L'entier p est dit **premier** si $p \neq 1$ et si p n'admet comme seuls diviseurs que 1 et lui-même.

Remarques

- En vertu de la définition, 1 n'est pas premier.
- 2 est le premier entier premier et c'est le seul qui soit pair.
- Il faut au moins connaître la liste des nombres premiers inférieurs à 50 : .....
  .....
- Un entier naturel non premier différent de 1 est qualifié de **composé**. Un tel entier admet des *diviseurs stricts* (c'est-à-dire des diviseurs autres que 1 et lui-même).
- Nous noterons dans la suite $\mathbb{P}$ l'ensemble des nombres premiers.
- Considérant p entier premier, on a pour tout entier naturel n : $\text{PGCD}(n,p) = \begin{cases} \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$

Proposition 12

Tout entier naturel strictement supérieur à 1 admet un diviseur premier.

Démonstration

Se donnant un entier $n > 1$, l'idée de la démonstration va consister à considérer le plus petit diviseur de n strictement supérieur à 1 et à montrer que ce dernier est premier.

Soit $n \in \mathbb{N}$ avec $n > 1$.

On considère l'ensemble $\mathcal{E}$ des diviseurs de n strictement supérieurs à 1 : $\mathcal{E}$ est une partie de $\mathbb{N}$ non vide (puisqu'elle contient n) et minorée (par 2) : elle admet ainsi un plus petit élément que nous noterons p.

Comme tout diviseur de p est un diviseur de n (n est un multiple de p), par minimalité, p ne peut admettre de diviseur compris strictement entre 1 et p. Compte tenu de $p \geqslant 2$, il en découle que p est premier.

Proposition 13 : Infinité de l'ensemble des nombres premiers

Il existe une infinité de nombres premiers.

Démonstration

On raisonne par l'absurde en supposant que $\mathbb{P}$ est fini et en notant $p_1, \ldots, p_r$ la liste finie des entiers premiers.

On considère alors l'entier $N = p_1 \times \cdots \times p_r + 1$. Comme $N \geqslant 2$, N admet d'après la proposition précédente un diviseur premier, donc nécessairement de la forme p_k avec $k \in [\![1, r]\!]$.

Mais alors, p_k divise $N - p_1 \times \cdots \times p_r$ soit p_k divise 1 et donc $p_k = 1$: d'où contradiction avec p_k premier.

Dans la fin de ce paragraphe, on affine l'énoncé de la Proposition 12 afin de décrire un algorithme permettant de déterminer tous les entiers premiers inférieurs à un seuil donné : le crible d'Ératosthène.

Proposition 14

Tout entier $n \geqslant 2$ non premier admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

Démonstration

Soit $n \geqslant 2$ non premier.

On considère son plus petit diviseur $p > 1$: d'après la démonstration de la Proposition 12, p est premier.

On peut écrire $n = pq$, et comme n n'est pas premier, $q > 1$. Puisque q est un diviseur de n, on a donc $q \geqslant p$ par minimalité de p soit $n \geqslant p^2 \iff p \leqslant \sqrt{n}$.

Crible d'Eratosthène

Il s'agit donc de présenter un algorithme permettant de déterminer les entiers premiers inférieurs à un seuil donné (nous allons l'illustrer avec le seuil 100).

- On écrit tous les entiers de 2 à 100.
- L'entier 2 est le plus petit entier premier : on le conserve (il est repassé ci-contre en **gras**) et on élimine tous ses multiples stricts puisqu'ils ne sont pas premiers (on les grise).
- Le premier nombre non éliminé suivant (ie. 3) est nécessairement premier puisqu'il n'admet pas de diviseur premier qui lui soit strictement inférieur : on le garde puis on élimine tous ses multiples stricts.
- On procède de même avec les entiers non éliminés suivants (nécessairement premiers), à savoir 5 puis 7.
- L'entier non éliminé suivant est 11 qui est premier. Mais puisqu'un entier non premier inférieur à 100 admet un diviseur premier inférieur ou égal à $\sqrt{100} = 10$ avec $11 > 10$, les entiers non éliminés restants sont nécessairement des entiers premiers.

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Les entiers non éliminés restants (en gras) sont donc les entiers premiers inférieurs à 100.

VI.2 Décomposition d'un entier en produit de facteurs premiers

Proposition 15 : Théorème de la décomposition d'un entier en produit de facteurs premiers

Soit $n \in \mathbb{N}$ avec $n \geqslant 2$.

Il existe un entier $r \geqslant 1$, des nombres premiers $p_1 < \cdots < p_r$ ainsi que des entiers naturels *non nuls* $\alpha_1, \ldots, \alpha_r$ tels que :

$$\boldsymbol{n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}}$$

Les nombres premiers $p_1, \ldots, p_r$ sont appelés **facteurs premiers** de n, et la **décomposition en produit de facteurs premiers** est unique, à l'ordre de ces facteurs près.

Illustrations

- On a par exemple :
  - $10 =$ .....
  - $49 =$ .....
  - $75 =$ .....
- D'une manière générale, on peut obtenir la décomposition d'un entier en produits de facteurs premiers en effectuant des divisions euclidiennes successives, par les diviseurs premiers rangés par ordre croissant, à partir de l'entier à décomposer. Illustrons cette méthode sur l'entier $n = 792$.

.....

.....

.....

.....

.....

.....

.....

Remarques

- La démonstration de ce théorème de décomposition (théorème fondamental de l'arithmétique) est hors programme. La preuve de l'existence est en fait parfaitement accessible (par récurrence, s'y essayer !), la preuve de l'unicité est plus délicate.
- Dans la suite, considérant un entier $n \geqslant 2$ nous opterons pour une écriture générique de sa décomposition, qualifiée de *décomposition primaire générique* :

  $\boldsymbol{n = \prod_{p \in \mathbb{P}} p^{\alpha_p}}$, les α_p désignant des entiers naturels *éventuellement nuls**.

  * *En réalité, tous les α_p sont nuls, sauf un nombre fini d'entre eux, et le produit est faussement infini.*

  Dans cette écriture, pour p nombre premier : si α_p est non nul, p est facteur premier de n ; si $\alpha_p = 0$, p n'est pas facteur premier de n.

Proposition 16

Soient a, b deux entiers naturels supérieurs ou égaux à 2, de décomposition générique primaire :

$$a = \prod_{p\in\mathbb{P}} p^{\alpha_p} \quad \text{et} \quad b = \prod_{p\in\mathbb{P}} p^{\beta_p}.$$

1. **Critère de divisibilité** : $b|a \iff \forall p \in \mathbb{P},\ \beta_p \leqslant \alpha_p$.
2. **Calcul de PGCD et de PPCM**

   On a : . $\text{PGCD}(a,\, b) = \prod_{p\in\mathbb{P}} p^{\min\{\alpha_p,\beta_p\}}$ et . $\text{PPCM}(a,\, b) = \prod_{p\in\mathbb{P}} p^{\max\{\alpha_p,\beta_p\}}$

Démonstration

1. $\Longrightarrow$

   Supposons que $b|a$: il existe $c \in \mathbb{N}^*$ tel que $a = bc$.

   En notant $c = \prod_{p\in\mathbb{P}} p^{\gamma_p}$ la décomposition primaire de c on a : $a = bc \iff \prod_{p\in\mathbb{P}} p^{\alpha_p} = \prod_{p\in\mathbb{P}} p^{\beta_p+\gamma_p}$.

   Par unicité de décompositions en produit de facteurs premiers : $\forall p \in \mathbb{P},\ \alpha_p = \beta_p + \gamma_p$ soit $\forall p \in \mathbb{P},\ \beta_p \leqslant \alpha_p$.

   $\Longleftarrow$

   On suppose réciproquement que $\forall p \in \mathbb{P},\ \beta_p \leqslant \alpha_p \iff \alpha_p - \beta_p \geqslant 0$.

   En posant $c = \prod_{p\in\mathbb{P}} p^{\alpha_p-\beta_p}$, on a donc $c \in \mathbb{N}$ et $a = bc$ d'où $b|a$.

2. . Posons $d = \prod_{p\in\mathbb{P}} p^{\min\{\alpha_p,\beta_p\}}$. Comme $\forall p \in \mathbb{P}$, $\min\{\alpha_p, \beta_p\} \leqslant \alpha_p$ et $\min\{\alpha_p, \beta_p\} \leqslant \beta_p$, $d|a$ et $d|b$ (cf. 1.).

   En posant alors $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$, on a $a' = \prod_{p\in\mathbb{P}} p^{\alpha_p-\min\{\alpha_p,\beta_p\}}$ et $b' = \prod_{p\in\mathbb{P}} p^{\beta_p-\min\{\alpha_p,\beta_p\}}$.

   Or pour tout $p \in \mathbb{P}$, $\alpha_p - \min\{\alpha_p, \beta_p\} = 0$ ou $\beta_p - \min\{\alpha_p, \beta_p\} = 0$, ce qui signifie que soit p ne divise pas a, soit p ne divise pas b. Ainsi, a' et b' n'ont pas de facteur premier commun donc pas de diviseur commun autre que 1. D'où $\text{PGCD}(a', b') = 1$ et donc, $\text{PGCD}(a,\, b) = \text{PGCD}(da',\, db') = d\text{PGCD}(a',\, b') = d$.

   . Compte tenu de $\text{PGCD}(a,\, b) \times \text{PPCM}(a,\, b) = ab$ et de ce qui précède :

   $$\text{PPCM}(a,\, b)\prod_{p\in\mathbb{P}} p^{\min\{\alpha_p,\beta_p\}} = \prod_{p\in\mathbb{P}} p^{\alpha_p}\prod_{p\in\mathbb{P}} p^{\beta_p} \text{ soit } \text{PPCM}(a,\, b) = \prod_{p\in\mathbb{P}} p^{\alpha_p+\beta_p-\min\{\alpha_p,\beta_p\}}.$$

   Montrons pour conclure que $\forall p \in \mathbb{P},\ \alpha_p + \beta_p - \min\{\alpha_p, \beta_p\} = \max\{\alpha_p, \beta_p\}$.

   Considérons donc $p \in \mathbb{P}$:

   - si $\alpha_p \geqslant \beta_p$, $\min\{\alpha_p, \beta_p\} = \beta_p$ et $\max\{\alpha_p, \beta_p\} = \alpha_p$ d'où $\alpha_p + \beta_p - \min\{\alpha_p, \beta_p\} = \alpha_p + \beta_p - \beta_p = \alpha_p$ soit $\alpha_p + \beta_p - \min\{\alpha_p, \beta_p\} = \max\{\alpha_p, \beta_p\}$.
   - si $\alpha_p < \beta_p$, $\min\{\alpha_p, \beta_p\} = \alpha_p$ et $\max\{\alpha_p, \beta_p\} = \beta_p$ d'où $\alpha_p + \beta_p - \min\{\alpha_p, \beta_p\} = \alpha_p + \beta_p - \alpha_p = \beta_p$ soit $\alpha_p + \beta_p - \min\{\alpha_p, \beta_p\} = \max\{\alpha_p, \beta_p\}$.

   Par disjonction des cas, on a bien le résultat visé.

Illustration

Soient $a = 840$ et $b = 450$. Déterminons le PGCD de a et b, le PPCM a et b, et la forme irréductible de $\frac{a}{b}$.

Exemple 13

Soient a et b deux entiers naturels supérieurs ou égaux à 2. On suppose qu'il existe $k \in \mathbb{N}^*$ tel que $b^k | a^k$.
Montrer que $b|a$.

.....

.....

.....

.....

.....

.....

.....

Complément : Relation de congruence modulo un entier naturel

Nous l'avons déjà dit, la notion de congruence n'est pas officiellement au programme de PCSI. À titre culturel, nous rappelons cependant les principaux résultats concernant la congruence vus en classe de Terminale et proposons quelques exemples pour les illustrer.

Définition

Soient $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.
Lorsque $n|(a-b)$, on dit que $\boldsymbol{a}$ **est congru à** $\boldsymbol{b}$ **modulo** $\boldsymbol{n}$ et on note alors $\boldsymbol{a \equiv b\ [n]}$.
On a donc : $a \equiv b\ [n] \iff \exists k \in \mathbb{Z} \,/\, a = b + kn$ ($a \equiv b\ [n]$ signifie que a et b diffèrent d'un multiple de n).

Remarque

On a l'équivalence immédiate et fondamentale : $\boldsymbol{n|a \iff a \equiv 0\ [n]}$.

Propriétés de la relation de congruence modulo un entier

Soient $a, b, c, d \in \mathbb{Z}$ et $n, m \in \mathbb{N}$.

1. **Somme** : Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$.
2. **Produit** : Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $ac \equiv bd\ [n]$.
3. **Passage à une puissance entière positive** : Si $a \equiv b\ [n]$ alors pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\ [n]$.
4. **Multiplication / Division par un entier non nul** : Si $m \neq 0$, $a \equiv b\ [n] \iff ma \equiv mb\ [mn]$.

Démonstration

1. Par hypothèse, $n|(a-b)$ et $n|(c-d)$ d'où par somme, $n|\big((a+c)-(b+d)\big)$ soit $a + c \equiv b + d\ [n]$.
2. Par hypothèse, $n|(a-b)$ et $n|(c-d)$ d'où $n|\big((a-b)c + b(c-d)\big) \iff n|(ac - bd)$ soit $ac \equiv bd\ [n]$.
3. Ce résultat se démontre très simplement par récurrence sur k, à partir du résultat précédent.
4. On a successivement : $a \equiv b\ [n] \iff n|(a-b) \underset{m \neq 0}{\iff} mn|m(a-b) \iff ma \equiv mb\ [mn]$.

Remarques et illustration

- Si $a \equiv b\ [n]$ on a en particulier : pour tout $k \in \mathbb{Z}$, $a + k \equiv b + k\ [n]$ et $ka \equiv kb\ [n]$ (car $k \equiv k\ [n]$).
- Si $a \equiv b\ [n]$, on a ainsi par exemple $2a \equiv 2b\ [n]$ (car $2 \equiv 2\ [n]$) et par ailleurs d'après **4.**, $2a \equiv 2b\ [2n]$.
  Notons que cette seconde relation est plus forte que la première puisque si $A \equiv B\ [2n]$, on a $2n|(A-B)$ et donc à fortiori, $n|(A-B)$.
- **Mise en garde** : Pour $a \in \mathbb{Z}$, $p, q, n \in \mathbb{N}$: $p \equiv q\ [n] \not\Longrightarrow a^p \equiv a^q\ [n]$ (par exemple, $4 \equiv 1\ [3]$ mais $2^4 \not\equiv 2^1\ [3]$).
- Reprenons l'Exemple 8 p.15 et redémontrons via la congruence (de manière beaucoup plus rapide !) que pour tout $n \in \mathbb{N}$, $2^{3n} - 1$ est un multiple de 7.
  On a : $2^3 = 8 \equiv 1\ [7]$ d'où $\forall n \in \mathbb{N}$, $2^{3n} = (2^3)^n \equiv 1\ [7] \iff 2^{3n} - 1 \equiv 0\ [7]$ soit $\boldsymbol{\forall n \in \mathbb{N},\ 3|2^{3n} - 1}$.

Application : Trois critères de divisibilité

Pour $n \in \mathbb{N}$, rappelons et démontrons les trois critères de divisibilité suivants :

- n est un multiple de 4 si et seulement si, le nombre formé par ses deux derniers chiffres est un multiple de 4.
- n est un multiple de 9 si et seulement si, la somme de ses chiffres est un multiple de 9.
- n est un multiple de 11 si et seulement si, la somme de ses chiffres de rang pair diminuée de la somme de ses chiffres de rang impair est un multiple de 11 (on parle de *somme alternée* des chiffres de n).

Démonstration

Soit $n \in \mathbb{N}$. On peut écrire : $n = \sum_{k=0}^{r} a_k 10^k$ avec $\forall k \in [\![0, r]\!]$, $a_k \in [\![0\,;9]\!]$ (on a alors : $n = \overline{a_r \dots a_1 a_0}$).

- $10^2 \equiv 0\ [4]$ d'où $\forall k \geqslant 2\,(k \in \mathbb{N}), 10^k \equiv 0\ [4]$ et $\sum_{k=2}^{r} a_k 10^k \equiv 0\ [4]$.
  Ainsi, $n \equiv 10a_1 + a_0\ [4]$ soit $n \equiv \overline{a_1 a_0}\ [4]$ et on a bien : $\boldsymbol{4 | n \iff 4 | \overline{a_1 a_0}}$.
- $10 \equiv 1\ [9]$ d'où $\forall k \in \mathbb{N}, 10^k \equiv 1\ [9]$ soit $n = \sum_{k=0}^{r} a_k 10^k \equiv \big(\sum_{k=0}^{r} a_k\big)\ [9]$. Ainsi on a bien : $\boldsymbol{9 | n \iff 9 | \sum_{k=0}^{r} a_k}$.
- $11 \equiv -1\ [11]$ d'où $\forall k \in \mathbb{N}, 10^k \equiv (-1)^k\ [11]$ soit $n = \sum_{k=0}^{r} a_k 10^k \equiv \big(\sum_{k=0}^{r} (-1)^k a_k\big)\ [11]$.
  Ainsi : $11 | n \iff 11 | \sum_{k=0}^{r} (-1)^k a_k$ soit $\boldsymbol{11 | n \iff 11 | \big(\sum_{k\ \text{pair}} a_k - \sum_{k\ \text{impair}} a_k\big)}$.
  Par exemple, $n = 95601$ *est un multiple de* 11 *puisque* $9 - 5 + 6 - 0 + 1 = 11$ *et* $11 | 11$.

Lien entre division euclidienne et congruence

- Pour $a, b \in \mathbb{Z} \times \mathbb{N}^*$, le théorème de la division euclidienne s'écrit : $\exists !\, r \in [\![0\,; b-1]\!] \,/\, a \equiv r\ [b]$.
  Autrement dit, tout entier relatif a est congru modulo b à un unique entier r compris entre 0 et $b-1$.
- Il découle du point précédent que pour tous $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$: **$a \equiv b\ [n]$ si et seulement si, a et b ont même reste dans la division euclidienne par n.**

Exemple : Tableau de congruences

On reprend l'Exemple 10 p.16. On se propose de redémontrer, en recourant cette fois aux congruences, que pour tout $n \in \mathbb{Z}$, $A_n = n(5n^2 + 1)$ est divisible par 3.

Une méthode peut consister, par disjonction des cas, à examiner les différentes possibilités de congruence modulo 3 *de l'entier* n *: d'après ce qui précède, il suffit d'envisager* 3 *cas, correspondant aux* 3 *restes possibles de la division euclidienne de* n *par* 3*. On dresse alors un* ***tableau de congruences modulo 3*** *que l'on renseigne en utilisant les propriétés relatives aux opérations sur les congruences.*

$n \equiv$	0	1	2
$n^2 \equiv$	0	1	$4 \equiv 1$
$5n^2 + 1 \equiv$	1	$6 \equiv 0$	$6 \equiv 0$
$n(5n^2 + 1) \equiv$	0	0	0

Au vu du tableau on constate que pour tout $n \in \mathbb{Z}$, $n(5n^2+1) \equiv\ [3]$.
Autrement dit comme souhaité : $\boldsymbol{\forall n \in \mathbb{Z},\ 3 | A_n}$.

Notes et compléments