

# Résumé de cours :

## Semaine 6, du 9 au 13 octobre.

### 1 Relations d'équivalence

**Définition.** Une relation binaire sur un ensemble  $E$  est une relation d'équivalence si et seulement si  $R$  est réflexive, symétrique et transitive.

**Exemple fondamental :** Soit  $E$  et  $F$  deux ensembles et  $f : E \longrightarrow F$  une application. Convenons que, pour tout  $x, y \in E$ ,  $x R y \iff f(x) = f(y)$ . Alors  $R$  est une relation d'équivalence sur  $E$ .

**Définition.** Soit  $R$  une relation d'équivalence sur  $E$ .

Si  $x \in E$ , on note  $\bar{x}$  l'ensemble des  $y \in E$  tels que  $xRy$ .

$\bar{x}$  s'appelle la classe d'équivalence de  $x$ .

On désigne par  $E/R$  l'ensemble des classes d'équivalence :  $E/R = \{\bar{x}/x \in E\}$ .

$E/R$  s'appelle l'ensemble quotient de  $E$  par  $R$ .

**Propriété.** pour tout  $x, y \in E$ ,  $xRy \iff \bar{x} = \bar{y}$ .

**Il faut savoir le démontrer.**

**Définition.** Une partition  $\mathcal{P}$  de  $E$  est une partie de  $\mathcal{P}(E)$  telle que :

- pour tout  $A, B \in \mathcal{P}$ ,  $A \neq B \implies A \cap B = \emptyset$ ,
- pour tout  $A \in \mathcal{P}$ ,  $A \neq \emptyset$ ,
- et  $\bigcup_{A \in \mathcal{P}} A = E$ .

**Théorème.** Si  $R$  est une relation d'équivalence sur  $E$ , son ensemble quotient  $E/R$  est une partition de  $E$ . Réciproquement, si  $\mathcal{P}$  est une partition de  $E$ , il existe une unique relation d'équivalence  $R$  sur  $E$  telle que  $\mathcal{P} = E/R$  : Elle est définie par  $\forall x, y \in E$ ,  $[xRy \iff (\exists C \in \mathcal{P}, x, y \in C)]$ . En résumé, la donnée d'une relation d'équivalence sur  $E$  est équivalente à la donnée d'une partition de  $E$ .

**Il faut savoir démontrer la première phrase.**

### 2 Axiome du choix

En voici deux énoncés équivalents.

- Pour tout ensemble  $I$ , pour toute famille  $(E_i)_{i \in I}$  d'ensembles tous non vides, il existe une famille  $(x_i)_{i \in I}$  telle que, pour tout  $i \in I$ ,  $x_i \in E_i$ .
- Pour tout ensemble  $E$ , pour toute relation d'équivalence sur  $E$ , il existe un ensemble  $R$  tel que l'intersection de  $R$  avec chaque classe d'équivalence est un singleton.

### 3 L'art de la démonstration

La structure d'une démonstration se construit avant tout en fonction de la structure de la propriété à démontrer. En conséquence, on regarde d'abord la cible à atteindre et seulement lorsque c'est

nécessaire les hypothèses dont on dispose pour y parvenir. On ne sait pas a priori sous quelles formes ces hypothèses seront utilisées.

### 3.1 Démontrer une disjonction

Pour montrer  $P \vee Q$ , on peut supposer que  $P$  est fausse et démontrer  $Q$ , ou bien supposer que  $Q$  est fausse et montrer  $P$ .

### 3.2 Démonstration par disjonction de cas

Pour démontrer une propriété dépendant de certains paramètres, on peut être amené à étudier plusieurs cas selon les valeurs de ces paramètres. Il importe que la réunion des différents cas étudiés recouvre toutes les valeurs possibles des paramètres.

### 3.3 Résoudre une équation

**Définition.** Si  $P$  est un prédicat sur un ensemble  $E$ , “résoudre l'équation  $P(x)$ , en l'inconnue  $x \in E$ ”, c'est calculer  $\{x \in E/P(x)\}$  qu'on appelle alors l'ensemble des solutions de l'équation. “calculer” signifie “donner l'ensemble des solutions sous la forme la plus simple possible”.

**Remarque.** La plupart des équations sont de la forme “ $f(x) = g(x)$ ”, où  $f$  et  $g$  sont deux applications de  $E$  dans un autre ensemble  $F$ .

Lorsque  $F = \mathbb{R}$ , on rencontre parfois des équations de la forme “ $f(x) \leq g(x)$ ”, ou “ $f(x) < g(x)$ ”. Dans ce cas, on parle plutôt d'*inéquations*.

**Méthode :**

- Précisez d'abord pour quelles valeurs  $x \in E$  l'équation a bien un sens. Par exemple, pour une équation de la forme “ $f(x) = g(x)$ ”, il faudra d'abord rechercher les domaines de définition de  $f$  et de  $g$ .
- Autant que possible, raisonnez par équivalence comme dans l'exemple précédent. Cependant le fait de raisonner par équivalence impose parfois trop de lourdeur à la rédaction. Lorsqu'on choisit de raisonner par implication, après avoir montré que  $P(x) \implies x \in S$ , pour une certaine partie  $S$  de  $E$ , il restera à rechercher quels sont les éléments de  $S$  qui sont effectivement solutions.

### 3.4 Implication

Pour montrer  $[P \implies Q]$ , on suppose que  $P$  est vraie (hypothèse supplémentaire) et on démontre  $Q$ .

**Raisonnement par contraposition :** l'implication  $P \implies Q$  est logiquement équivalente à  $(\neg Q) \implies (\neg P)$ , qui est appelée sa contraposée. Ainsi, pour démontrer  $P \implies Q$ , on peut raisonner par contraposition, c'est-à-dire démontrer  $(\neg Q) \implies (\neg P)$  : on suppose que  $Q$  est fausse et on démontre que  $P$  est fausse.

**Le raisonnement par l'absurde :** cela consiste à supposer que  $R$  est fausse et à aboutir à une contradiction, souvent de la forme  $S \wedge (\neg S)$ .

Pour montrer que  $[P \iff Q]$ , on montre souvent  $[P \implies Q]$  puis la réciproque  $[Q \implies P]$ . Dans des cas simples, on peut raisonner par une succession d'équivalences.

Pour montrer que les propriétés  $P_1, \dots, P_k$  sont équivalentes, on peut se contenter de montrer le cycle d'implications  $P_1 \implies P_2 \implies \dots \implies P_k \implies P_1$ . Mais la liste  $P_1, \dots, P_k$  n'est pas toujours donnée dans l'ordre idéal. Il convient donc parfois de la réordonner.

### 3.5 Quantificateurs

Pour montrer que  $[\forall x \in E, P(x)]$ , le plus souvent, on prend  $x$  quelconque dans  $E$ , en écrivant “soit  $x \in E$ ”, puis on démontre  $P(x)$ .

Pour montrer que  $[\exists x \in E, P(x)]$ , la méthode directe consiste à construire un élément  $x$  de  $E$  satisfaisant  $P(x)$ .

On peut aussi raisonner par l'absurde, en supposant que  $[\forall x \in E, \neg(P(x))]$  et en recherchant une contradiction. Il faut cependant que cette nouvelle hypothèse se marie bien avec les autres hypothèses.

Pour montrer que  $\neg(\forall x \in E, P(x))$ , on peut rechercher un  $x$  dans  $E$  tel que  $P(x)$  est fausse. Dans ce contexte,  $x$  est appelé un contre-exemple du prédicat  $P(x)$ .

### 3.6 Existence et unicité

Comment montrer une propriété de la forme  $[\exists! x \in E, P(x)]$  ?

Dans de nombreux exercices et problèmes, l'énoncé d'une telle propriété se présente sous la forme : “montrer qu'il existe  $x \in E$  tel que  $P(x)$ , puis montrer que  $x$  est unique”.

Sur le plan ontologique, tout objet mathématique est unique, mais ce n'est pas du tout ce qui est demandé par l'énoncé. La propriété “ $x$  est unique” dépend de  $P$ .

En mathématiques, l'unicité est toujours prononcée relativement à un prédicat. Par exemple, 2 est l'unique entier premier et pair, mais 2 n'est pas l'unique entier pair inférieur à 10.

Pour montrer qu'il existe un unique  $x \in E$  tel que  $P(x)$ , il est souvent préférable de séparer l'existence et l'unicité. Pour l'unicité, il faut montrer que  $\{x \in E/P(x)\}$  ne possède pas deux éléments distincts, par exemple en supposant qu'il existe  $x, y \in E$  vérifiant  $P(x)$  et  $P(y)$  et en prouvant que  $x = y$ .

Mais il y a d'autres méthodes :

- On peut montrer que  $\{x \in E/P(x)\}$  est un singleton.
- On peut résoudre l'équation “ $P(x)$ ” en l'inconnue  $x$  pour montrer qu'elle admet une seule solution.
- On peut raisonner par analyse-synthèse :

### 3.7 Démonstration par analyse-synthèse

Ce mode de raisonnement est envisageable lorsque la propriété à démontrer est de la forme  $[\exists x \in E, P(x)]$ . Il se décompose en deux parties :

◇ **L'analyse** : on suppose qu'il existe  $x \in E$  tel que  $P(x)$ .

C'est a priori très étrange, car on suppose justement ce qu'il faut démontrer !

A partir du fait que  $x$  vérifie  $x \in E$  et  $P(x)$ , on cherche à préciser quelles sont les valeurs possibles pour  $x$ .

Il est fréquent que l'analyse conduise à une seule valeur possible pour  $x$ .

◇ **La synthèse** : Parmi ces différentes valeurs possibles, on en recherche une qui vérifie  $P(x)$ .

### 3.8 Démonstrations par récurrence

**Principe de récurrence** :

Soit  $n_0 \in \mathbb{N}^*$ . Soit  $R(n)$  un prédicat défini pour tout entier  $n \geq n_0$ .

Si  $R(n_0)$  est vraie et si pour tout  $n \geq n_0$ ,  $R(n)$  implique  $R(n+1)$ ,

alors pour tout  $n \in \mathbb{N}$  tel que  $n \geq n_0$ ,  $R(n)$  est vraie.

**Principe de récurrence ascendante finie** : Soit  $n, m \in \mathbb{N}$  avec  $n \leq m$ .

Soit  $R(k)$  un prédicat défini pour  $k \in \llbracket n, m \rrbracket$ .

Si  $R(n)$  est vraie et si pour tout  $k \in \llbracket n, m-1 \rrbracket$ ,  $R(k)$  implique  $R(k+1)$ ,

alors  $R(k)$  est vraie pour tout  $k \in \llbracket n, m \rrbracket$ .

**Principe de récurrence descendante finie :** Soit  $n, m \in \mathbb{N}$  avec  $n \leq m$ .

Soit  $R(k)$  un prédicat défini pour  $k \in \llbracket n, m \rrbracket$ .

Si  $R(m)$  est vraie et si pour tout  $k \in \llbracket n + 1, m \rrbracket$ ,  $R(k)$  implique  $R(k - 1)$ ,

alors  $R(k)$  est vraie pour tout  $k \in \llbracket n, m \rrbracket$ .

**Principe de récurrence forte :**

Soit  $n_0 \in \mathbb{N}$ . Soit  $R(n)$  un prédicat défini pour tout entier  $n \geq n_0$ .

Si  $R(n_0)$  est vraie et si pour tout  $n \geq n_0$ ,  $[\forall k \in \{n_0, \dots, n\}, R(k)]$  implique  $R(n + 1)$ ,

alors pour tout  $n \in \mathbb{N}$  tel que  $n \geq n_0$ ,  $R(n)$  est vraie.

**Principe de récurrence double :**

Soit  $n_0 \in \mathbb{N}$ . Soit  $R(n)$  un prédicat défini pour tout entier  $n \geq n_0$ .

Si  $R(n_0)$  et  $R(n_0 + 1)$  sont vraies et si

pour tout  $n \geq n_0$ ,  $[R(n) \wedge R(n + 1)]$  implique  $R(n + 2)$ ,

alors pour tout  $n \in \mathbb{N}$  tel que  $n \geq n_0$ ,  $R(n)$  est vraie.

## 4 $\mathbb{Z}$

### 4.1 Construction de $\mathbb{Z}$

**Définition.**  $\mathbb{Z} = \mathbb{N}^2 / R$ , où  $R$  est la relation d'équivalence suivante sur  $\mathbb{N}^2$  :

$\forall a, b, c, d \in \mathbb{N}$ ,  $(a, b)R(c, d) \iff a + d = b + c$ .

Si  $(a, b), (c, d) \in \mathbb{Z}$ , on pose  $(a, b) + (c, d) \stackrel{\Delta}{=} (a + c, b + d)$

et  $(a, b) \times (c, d) \stackrel{\Delta}{=} (ac + bd, ad + bc)$ .

### 4.2 L'anneau $\mathbb{Z}$

**Propriété.** L'addition sur  $\mathbb{Z}$  vérifie les propriétés suivantes :

- $0 \stackrel{\Delta}{=} (0, 0)$  est neutre :  $\forall m \in \mathbb{Z}$ ,  $m + 0 = 0 + m = m$ .
- Associativité :  $\forall n, m, k \in \mathbb{Z}$ ,  $(n + m) + k = n + (m + k)$ .
- Commutativité :  $\forall n, m \in \mathbb{Z}$ ,  $n + m = m + n$ .
- Tout élément possède un symétrique :  $\forall n \in \mathbb{Z}$ ,  $\exists m \in \mathbb{Z}$ ,  $n + m = 0$ .

On résume ces propriétés en disant que  $(\mathbb{Z}, +)$  est un groupe commutatif.

**Propriété.** La multiplication sur  $\mathbb{Z}$  vérifie les propriétés suivantes :

- $1 \stackrel{\Delta}{=} (1, 0)$  est neutre :  $\forall m \in \mathbb{Z}$ ,  $m \times 1 = 1 \times m = m$ .
- Distributivité de la multiplication par rapport à l'addition :  
 $\forall n, m, p \in \mathbb{Z}$ ,  $n(m + p) = nm + np$ .
- Associativité :  $\forall n, m, k \in \mathbb{Z}$ ,  $(n \times m) \times k = n \times (m \times k)$ .
- Commutativité :  $\forall n, m \in \mathbb{Z}$ ,  $n \times m = m \times n$ .

On résume ces propriétés et le fait que  $(\mathbb{Z}, +)$  est un groupe commutatif en disant que  $(\mathbb{Z}, +, \times)$  est un anneau commutatif.

### 4.3 L'ordre de $\mathbb{Z}$

**Compatibilité de la relation d'ordre avec l'addition :**

$\forall x, y, x', y' \in \mathbb{Z}$ ,  $[x \leq y] \wedge [x' \leq y'] \implies x + x' \leq y + y'$ .

**Identification de  $\mathbb{N}$  avec une partie de  $\mathbb{Z}$  :** on identifie  $n \in \mathbb{N}$  avec  $(n, 0)$ .

**Règle des signes :**

- $\forall n \in \mathbb{Z}, n \geq 0 \iff n \in \mathbb{N}$ .
- $\forall n, m \in \mathbb{Z}, ([n \geq 0] \wedge [m \geq 0]) \implies nm \geq 0$ .
- $\forall n \in \mathbb{Z}, n \geq 0 \iff -n \leq 0$ .
- $\forall x, y, a \in \mathbb{Z}, \begin{cases} \text{si } a \geq 0, & x \leq y \implies ax \leq ay, \\ \text{si } a \leq 0, & x \leq y \implies ax \geq ay. \end{cases}$

**Propriété.** Toute partie non vide majorée de  $\mathbb{Z}$  possède un maximum.  
Toute partie non vide minorée de  $\mathbb{Z}$  possède un minimum.

**Définition.** Soit  $n \in \mathbb{Z}$ .

Le signe de  $n$  au sens large est

- 1 ou bien “positif” lorsque  $n \geq 0$ ,
- -1 ou bien “négatif” lorsque  $n \leq 0$ .

Le signe de  $n$  au sens strict est

- 1 ou bien “strictement positif” lorsque  $n > 0$ ,
- 0 ou bien “nul” lorsque  $n = 0$ ,
- -1 ou bien “strictement négatif” lorsque  $n < 0$ .

**Définition.** Pour tout  $n \in \mathbb{Z}$ , on note  $|n| = \max\{-n, n\}$ .

**Propriété.** Pour tout  $n \in \mathbb{Z}, n \leq |n|$ , avec égalité si et seulement si  $n \geq 0$ . De plus  $|n|^2 = n^2$ .

**Propriété.**  $\forall n, m \in \mathbb{Z}, |nm| = |n||m|$ .

**Propriété.**  $\mathbb{Z}$  est un anneau intègre, c'est-à-dire que, pour tout  $n, m \in \mathbb{Z}, nm = 0 \implies [(n = 0) \vee (m = 0)]$ .

**Propriété.** Soit  $n, m \in \mathbb{Z}^2. nm \geq 0$  si et seulement si  $n$  et  $m$  sont de même signe au sens large.

**Propriété.** Soit  $a, b, n \in \mathbb{Z}$  tels que  $an \leq bn$ . Si  $n > 0$  alors  $a \leq b$  et si  $n < 0$ , alors  $a \geq b$ .

**Inégalité triangulaire :**  $\forall n, m \in \mathbb{Z}, |n + m| \leq |n| + |m|$ , avec égalité si et seulement si  $n$  et  $m$  sont de même signe.

**Il faut savoir le démontrer.**

#### 4.4 Les sous-groupes de $\mathbb{Z}$

**Division euclidienne dans  $\mathbb{Z}$  :** Pour tout  $a, b \in \mathbb{Z}$  avec  $b \neq 0$ , il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que  $a = bq + r$  et  $0 \leq r < |b|$ .  $q$  et  $r$  sont appelés les quotient et reste.

**Définition.** Une partie  $G$  de  $\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$  si et seulement si

- $G \neq \emptyset$ ,
- $\forall (x, y) \in G^2, x + y \in G$ ,
- $\forall x \in G, -x \in G$ .

**Propriété.** Soit  $G$  un sous-groupe de  $\mathbb{Z}$ .

Pour tout  $n \in \mathbb{Z}$  et  $g \in G, ng \in G$ .

Pour tout  $n \in G, n\mathbb{Z} \subset G$ .

**Il faut savoir le démontrer.**

**Corollaire.** Soit  $G$  un sous-groupe de  $\mathbb{Z}$ . Alors  $\boxed{1 \in G \iff G = \mathbb{Z}}$ .

**Théorème.** Les sous-groupes de  $(\mathbb{Z}, +)$  sont exactement les  $n\mathbb{Z}$ , où  $n \in \mathbb{N}$ .

**Il faut savoir le démontrer.**

**Propriété.** Une intersection de sous-groupes de  $\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ .

**Il faut savoir le démontrer.**

**Définition.** Soit  $B$  une partie de  $\mathbb{Z}$ . Le groupe engendré par  $B$  est l'intersection des sous-groupes de  $\mathbb{Z}$  contenant  $B$ . C'est le plus petit sous-groupe contenant  $B$ . On le note  $Gr(B)$ .

**Propriété.** Soient  $B$  et  $C$  deux parties de  $\mathbb{Z}$  telles que  $C \subset B$ . Alors  $Gr(C) \subset Gr(B)$ .

**Propriété.**  $Gr(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in \mathbb{Z}^n, (b_1, \dots, b_n) \in B^n \right\}$ .

Il faut savoir le démontrer.

## 4.5 Divisibilité

**Définition.** Soit  $n, m \in \mathbb{Z}$ .  $n|m$  si et seulement si il existe  $k \in \mathbb{Z}$  tel que  $m = kn$ .

**Propriété.** Soit  $a, b \in \mathbb{Z}$  avec  $b \neq 0$ . Alors  $b$  divise  $a$  si et seulement si le reste de la division euclidienne de  $a$  par  $b$  vaut 0.

**Remarque.** Tout entier relatif divise 0 mais 0 ne divise que lui-même.

**Remarque.** Si  $n, m \in \mathbb{Z}$ ,  $n$  divise  $m$  si et seulement si  $|n|$  divise  $|m|$  dans  $\mathbb{N}$ .

**Propriété.** Soit  $a, b, c \in \mathbb{Z}$ .

- si  $b|a$ , alors pour tout  $\alpha \in \mathbb{Z}$ ,  $b|\alpha a$ .
- Si  $b|a$  et  $b|c$ , alors  $b|(a+c)$ .
- Si  $b|a$  et  $d|c$ , alors  $bd|ac$ .
- si  $b|a$ , pour tout  $p \in \mathbb{N}$ ,  $b^p|a^p$ .

**Propriété.** Soit  $p \in \mathbb{N}$  et  $b, a_1, \dots, a_p, c_1, \dots, c_p \in \mathbb{Z}$ .

Si pour tout  $i \in \{1, \dots, p\}$ ,  $b|a_i$ , alors  $b|\sum_{i=1}^p c_i a_i$ .

**Propriété.** Pour tout  $(a, b) \in \mathbb{Z}^2$ ,  $a|b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$ .

**Propriété.** La relation de divisibilité est réflexive et transitive.

**Remarque.** La relation de divisibilité n'est pas un ordre sur  $\mathbb{Z}$  car  $-1|1$  et  $1|-1$ .

**Définition.** Soit  $a, b \in \mathbb{Z}$ . On dit que  $a$  et  $b$  sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de  $a$  et  $b$  sont 1 et  $-1$ .

**Définition.** Soit  $n \in \mathbb{N}$  avec  $n \geq 2$  et  $a_1, \dots, a_n \in \mathbb{Z}$ .

- $a_1, \dots, a_n$  sont deux à deux premiers entre eux si et seulement si, pour tout  $i, j \in \{1, \dots, n\}$  avec  $i \neq j$ ,  $a_i$  et  $a_j$  sont premiers entre eux.
- $a_1, \dots, a_n$  sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de  $a_1, \dots, a_n$  sont 1 et  $-1$ .

**Propriété.** Si  $p \in \mathbb{P}$  et  $a \in \mathbb{Z}$ , alors ou bien  $p|a$ , ou bien  $p$  et  $a$  sont premiers entre eux.

**Propriété.** Soit  $p \in \mathbb{N} \setminus \{0, 1\}$ . Les propriétés suivantes sont équivalentes :

1.  $p$  est premier.
2.  $p$  est premier avec tout entier qu'il ne divise pas.
3.  $p$  est premier avec tout nombre premier contenu dans  $\llbracket 2, \sqrt{p} \rrbracket$ .

Il faut savoir le démontrer.

**le crible d'Ératosthène :** pour dresser la liste ordonnée des nombres premiers inférieurs à  $n$ , initialement, on pose  $L = \llbracket 2, n \rrbracket$  et on positionne un curseur sur 2. On supprime de  $L$  les multiples de 2, sauf 2, puis on déplace le curseur sur l'entier suivant de  $L$  : il s'agit de 3, car il n'a pas été supprimé. On supprime de  $L$  tous les multiples de 3, sauf 3, etc. Ainsi, à chaque itération, on déplace le curseur

sur le premier entier suivant qui est encore dans  $L$  et l'on supprime de  $L$  tous les multiples du curseur, sauf le curseur. On arrête l'algorithme dès que le curseur est strictement supérieur à  $\sqrt{n}$ .

**Théorème.**  $\mathbb{P}$  est de cardinal infini.

Il faut savoir le démontrer.

## 4.6 Congruence

**Définition. Relation de congruence :** Soit  $k \in \mathbb{Z}$ .  $\forall n, m \in \mathbb{Z}$ ,  $n \equiv m [k] \iff k|(n - m)$ .  
C'est la relation de congruence modulo  $k$ , qui est une relation d'équivalence.

**Propriété.** Soit  $a, b \in \mathbb{Z}$  avec  $b \neq 0$  : il existe  $r \in \{0, \dots, |b| - 1\}$  tel que  $a \equiv r [b]$ .  
 $r$  est le reste de la division euclidienne de  $a$  par  $b$ .

**Notation.** La classe d'équivalence de  $n$  modulo  $k$  est  $\bar{n} = \{n + kh/h \in \mathbb{Z}\} \stackrel{\Delta}{=} n + k\mathbb{Z}$ .

**Compatibilités de la congruence avec l'addition et la multiplication :**

Pour tout  $n, m, h, k \in \mathbb{Z}$ ,

- $n \equiv m [k] \implies h + n \equiv h + m [k]$  et
- $n \equiv m [k] \implies hn \equiv hm [k]$ .

**Corollaire :**  $\forall a, b, k \in \mathbb{Z}$ ,  $\forall n \in \mathbb{N}$ ,  $(a \equiv b [k] \implies a^n \equiv b^n [k])$ .

**Petit théorème de Fermat :** (Admis pour le moment) Si  $p \in \mathbb{P}$  et  $a \in \mathbb{Z}$ ,  
 $(a \not\equiv 0 [p]) \implies a^{p-1} \equiv 1 [p]$ , donc dans tous les cas,  $a^p \equiv a [p]$ .

**Définition.** Soit  $x_0 \in \mathbb{R}$ . Pour tout  $x, y \in \mathbb{R}$ , on dit que  $x$  est congru à  $y$  modulo  $x_0$  et on note  $x \equiv y [x_0]$  si et seulement si il existe  $k \in \mathbb{Z}$  tel que  $x - y = kx_0$ . La relation de congruence modulo  $x_0$  est une relation d'équivalence sur  $\mathbb{R}$ . Elle est compatible avec l'addition entre réels mais pas avec la multiplication entre réels.

## 4.7 PGCD

**Définition.** Soit  $(a, b) \in \mathbb{Z}^2$ .  $a\mathbb{Z} + b\mathbb{Z}$  est le sous-groupe de  $\mathbb{Z}$  engendré par  $\{a, b\}$ , donc il existe un unique  $d \in \mathbb{N}$  tel que  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ . On dit que  $d$  est le PGCD de  $a$  et  $b$ . On note  $d = \text{PGCD}(a, b) = a \wedge b$ .

**Propriété.** Pour la relation d'ordre de divisibilité dans  $\mathbb{N}$ ,  $a \wedge b = \inf_{|} \{|a|, |b|\}$ .

Il faut savoir le démontrer.

**Remarque.** Lorsque  $a$  ou  $b$  est un entier relatif non nul, au sens de l'ordre naturel sur  $\mathbb{N}$ ,  $a \wedge b$  est aussi le plus grand diviseur commun de  $a$  et  $b$ .

**Propriété.**  $a$  et  $b$  sont premiers entre eux si et seulement si  $a \wedge b = 1$ .

**Définition.** Plus généralement, si  $k \in \mathbb{N}^*$  et si  $a_1, \dots, a_k \in \mathbb{Z}$ , on dit que  $d$  est le PGCD de  $a_1, \dots, a_k$  si et seulement si  $d \in \mathbb{N}$  et  $d\mathbb{Z} = a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = \text{Gr}\{a_1, \dots, a_k\}$ . Alors  $d = \inf_{|} \{a_1, \dots, a_k\}$ .

Si  $B$  est une partie quelconque de  $\mathbb{Z}$ , on dit que  $d$  est le PGCD de  $B$  si et seulement si  $d \in \mathbb{N}$  et  $d\mathbb{Z} = \text{Gr}(B)$ . Alors  $d = \inf_{|}(B)$ .

**Propriété.** Soit  $k \in \mathbb{N}$ ,  $a_1, \dots, a_k \in \mathbb{Z}$  et  $h \in \{1, \dots, k\}$ .

- Commutativité du PGCD :  
 $\text{PGCD}(a_1, \dots, a_k)$  ne dépend pas de l'ordre de  $a_1, \dots, a_k$ .
- Associativité du PGCD :  
 $\text{PGCD}(a_1, \dots, a_k) = \text{PGCD}(a_1, \dots, a_h) \wedge \text{PGCD}(a_{h+1}, \dots, a_k)$ .
- Distributivité de la multiplication par rapport au PGCD : pour tout  $\alpha \in \mathbb{Z}$ ,  
 $\text{PGCD}(\alpha a_1, \dots, \alpha a_k) = |\alpha| \text{PGCD}(a_1, \dots, a_k)$ .

Il faut savoir le démontrer.