Chap. C1 : Structures des ensembles de nombres et arithmétique dans $\mathbb{Z}$

> Si on prend clairement conscience des causes et des origines [des règles de l'arithmétique], alors on sera plus ou moins en mesure d'inventer soi-même de nouvelles règles et l'on sera capable, au moyen de celles-ci, de résoudre des problèmes pour lesquelles les règles habituelles n'auraient pas été suffisantes. L'on ne doit pas craindre que l'apprentissage de l'arithmétique s'avère ainsi plus difficile et demande plus de temps que lorsque l'on présente les règles sans explications. Car chaque homme comprend et garde en mémoire beaucoup plus facilement ce dont il appréhende clairement les causes et les origines.
>
> L. Euler, Préface de sa "vollständige Anleitung zur Algebra".

I Structures algébriques :

1) Loi de composition interne (l.c.i.) propriétés et exemples :

a) **Déf.** *Soit E un ensemble, on appelle l.c.i. sur E ou dans E toute application de $E \times E$ dans E.*

Exemple (fondamental) de $+, \times$ dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$...

Contre-exemple de la "loi" $-$ dans $\mathbb{N}$ (pas interne), mais bien une l.c.i. dans $\mathbb{Z}$.

Exemple de $(a, b) \mapsto a^b$.

Ailleurs que dans les ensembles de nombres : loi $\circ$ dans $\mathcal{F}(A, A)$, lois $\cap$ et $\cup$ dans $\mathcal{P}(A)$, où A est un ensemble qcq.

Lois $+, \times$ dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Sur un ensemble fini, on peut décrire une l.c.i. en se donnant son "tableau".

Exple du tableau de $(\{-1, 1\}, \times)$.

Ci-dessous, on donne des prop. possibles des l.c.i. Ce sont les propriétés qui permettent de *calculer* :

b) associativité

(i) **Déf.** *Une l.c.i. $*$ sur un ensemble E est dite* associative *si, et seulement si :*

$$\forall\, (a, b, c) \in E^3,\ (a * b) * c = a * (b * c)$$

(ii) Exemples de $+$, $\times$ dans $\mathbb{N}$ (et les ens. de nbres), $\circ$ dans $\mathcal{F}(A, A)$ (*savoir dém.*)

(iii) Contre exemples de $-$ ou de $(x, y) \mapsto x^y$.

c) commutativité

(i) **Déf.** *Une l.c.i. $*$ sur un ensemble E est dite* commutative *si, et seulement si :*

$$\forall\, (a, b) \in E^2,\ a * b = b * a$$

(ii) Exemple $+$, $\times$ dans les ensemble de nombres, $\cap, \cup$ dans $E = \mathcal{P}(A)$.

(iii) Une loi importante non-commutative : loi $\circ$.

Précisément : dès que A est un ensemble avec au moins deux éléments, il existe deux éléments $(f, g) \in \mathcal{F}(A, A)^2$ tels que $f \circ g \neq g \circ f$ *dém.*

d) Existence d'un élément neutre

(i) Déf. (attention aux deux côtés si loi non commutative).

(ii) Exemples dans la liste du a).

(iii) Le neutre est unique s'il existe (*dém.*), peut ne pas exister (exemples : $-$ dans $\mathbb{Z}$, $+$ dans $\mathbb{N}^*$).

e) Existence d'un *symétrique* pour un élément

Terminologies : *opposé* si loi $+$, *inverse* si loi $\times$, *appl. inverse ou récip.* pour $\circ$.

Attention si non commutatif : rappel sur les inverses à gauche et à droite dans $(\mathcal{A}(E), \circ)$.

Prop. (*dém.*) Si E avec l.c.i. *assoc.* avec un élément neutre, *unicité* du symétrique d'un élément.

Exercice abstrait (!) : Ctre-exple si loi non-associative (sur un ensemble fini).

Scholie. L'intérêt de ces définitions générales est de s'appliquer à des objets variés, venant de l'algèbre, l'analyse ou la géométrie. Dans ce chapitre cependant, on ne considère que des "nombres". En particulier les lois seront *commutatives*.

2) Structure de groupe :

a) Déf. centrale en mathématiques et en physique !

(i) **SAVOIR POUR TOUJOURS :** (Quatre propriétés)

$(G, *)$ est un groupe ssi $*$ est une lc.i. de G, $*$ est assoc., a un neutre, et tout élément de G admet un symétrique dans G.

(ii) On ne demande pas la commutativité parce qu'on aime bien la loi $\circ$!

Si en plus la loi est commutative : groupe commutatif ou abélien.

b) Exemples et Ctre Exples :

(i) $(\mathbb{N}, +)$ n'est pas un groupe. On invente $\mathbb{Z}$ pour palier à ce défaut.

(ii) Même pb. avec $(\mathbb{Z}^*, \times)$. On invente $\mathbb{Q}$: $(\mathbb{Q}^*, \times)$ est un groupe.

De même pour $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ (*ne pas oublier d'enlever* 0).

(iii) Exemple de groupe fini dans les ensembles de nombres : $(\mathbb{U}_2 = \{-1, 1\}, \times)$

c) Exemple de groupe non commutatif : $(\mathcal{B}(E), \circ)$. Non commutatif dès que $\text{Card}(E) \geq 3$.

Exemple de $\mathcal{B}(E)$ quand $E = \{a, b\}$ et $E = \{a, b, c\}$.

On retrouvera ces groupes de bijections en géométrie notamment.

d) Un intérêt de la structure de groupe : dans $\mathbb{Z}$ on peut toujours résoudre l'équation $a + x = b$.

Généralisation : Si $(G, *)$ est un groupe, l'équation $a * x = b$ admet un unique solution dans G.

Notation plus commode : noter $(G, .)$, le neutre e, et a^{-1} pour le symétrique de a. Mais attention à la traduction si la loi s'appelle $+$.

3) Sous-groupe :

a) Déf. **SAVOIR POUR TOUJOURS :** (Trois propriétés) Soit $H \subset G$, où $(G, *)$ groupe.

H sous-groupe de $(G, *)$ ssi $*$ est une l.c.i. de H, H contient e_G, H contient les sym. de tous ses élmts.

(ii) Remarque : une autre façon de dire : "$*$ est une l.c.i. de H" est de dire que "H est stable par $*$".

(iii) Remarque (variante de la déf. du (i)) : H contient e et $\forall\, (a, b) \in H^2$, $ab^{-1} \in H$.

(iv) Prop. : Soit $(G, *)$ un groupe et $H \subset G$: si H sous-groupe de $(G, *)$ alors $(H, *)$ est un groupe.

(v) Ctre exple $\mathbb{N}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

Exple : $2\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, plus généralement tous les $n\mathbb{Z}$.

(vi) Exple : $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, mais $\mathbb{D}^*$ n'est pas un sous-groupe de $(\mathbb{Q}^*, \times)$.

b) Sous-groupe engendré par un élément.

(i) Notation : si $(G, .)$ est un groupe quelconque (avec la notation du 2) d)), et si $a \in G$, on notera $a^0 = e$, pour tout $k \in \mathbb{N}$, $a^k = a.\ldots.a$ (avec a figurant k fois), et $a^{-k} = a^{-1}.\ldots.a^{-1}$ (avec a^{-1} figurant k fois), (déf. correcte par rec.).

On a donc défini la notation a^k pour tout $k \in \mathbb{Z}$.

Rem. on vérifie immédiatement, que pour tout $k \in \mathbb{Z}$, a^{-k} est alors le symétrique de a^k.

(ii) Déf. : $< a >= \{a^k,\, k \in \mathbb{Z}\}$. Prop. $< a >$ est un sous-groupe de $(G, .)$

(iii) Attention à la différence d'écriture suivant les lois.

Exemple dans $(\mathbb{Z}, +)$: $a\mathbb{Z}$, et dans $(\mathbb{R}^*, \times)$: $a^{\mathbb{Z}}$.

(iv) Prop. $< a >$ est le plus petit sous-groupe de $(G, .)$ contenant a, ce qui signifie que tout sous-groupe de $(G, .)$ contenant a contient $< a >$.

c) Intersection de sous-groupes

(i) Prop. c'est un sous-groupe. (ii) Exemple de $2\mathbb{Z} \cap 3\mathbb{Z}$.

(iii) Contre-exemple pour la réunion $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un groupe.

II L'anneau $(\mathbb{Z}, +, \times)$: divisibilité et division euclidienne

0) Rappels sur l'ordre dans $\mathbb{N}$:

On utilisera dans ce qui suit les deux prop. importantes de l'ordre dans $\mathbb{N}$ (cf. chap. A2) :

(P1) *Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.*

(P2) *Toute partie non vide de $\mathbb{N}$ majorée admet un plus grand élément.*

1) La structure d'anneau sur $\mathbb{Z}$:

a) Propriété des $(\mathbb{Z}, +, \times)$:

(i) $(\mathbb{Z}, +)$ est un groupe abélien

(ii) $(\mathbb{Z}, \times)$ est un ensemble avec l.c.i. associative avec neutre
(iii) La multiplication est distributive par rapport à l'addition.
b) La notion d'anneau en général :

$(A, +, \times)$ est un anneau ssi $(A, +)$ groupe commutatif, $\times$ est assoc. avec neutre, et distributivité.

Dans le cas non commutatif, la distributivité demande *deux* égalités.
Si en plus $\times$ est commutative, on dit que l'anneau est commutatif.
Dans ce chapitre on ne considérera que des *anneaux commutatifs* et pour commencer $\mathbb{Z}$.

c) Sur les éléments inversibles de l'anneau $(\mathbb{Z}, +, \times)$

Prop. Les seuls éléments de $\mathbb{Z}$ inversibles pour la multiplication sont 1 et -1.

Preuve – Il est clair que 1 et -1 sont inversibles pour $\times$ d'inverse eux-mêmes. On sait que 0 n'est pas inversible. Soit $a \in \mathbb{Z} \setminus \{0, -1, 1\}$.
Alors $|a| \geq 2$, alors pour tout $b \in \mathbb{Z}^*$, $|ab| = |a||b| \geq 2$, et donc il est exclu que $ab = 1$. □

d) Des anneaux meilleurs que les autres les corps
Exemple de $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +\times)$, $(\mathbb{C}, +, \times)$.

2) La divisibilité dans $\mathbb{Z}$:

a) La relation *divise* dans $\mathbb{Z}$:

(i) Déf. Soit $(a, b) \in \mathbb{Z}^2$. On dit que b *divise* a et on note $b|a$, si, et seulement si, il existe un $k \in \mathbb{Z}$ tel que $a = k.b$.
On dit encore que a est *divisible* par b ou que a est un *multiple* de b.

(ii) Cas spécial de 0 : la déf. du (i), dit que :
• pour tout $a \in \mathbb{Z}$, $a|0$, car $0 = 0.a$.
• en revanche, le seul nombre "divisible par 0" est 0 : car $0|a$ signifie que $a = k.0$ donc $a = 0$.

(iii) **Scholie :** La relation de divisibilité dans $\mathbb{Z}$ est non triviale car $\mathbb{Z}$ est un anneau qui n'est pas un corps. Dans un corps (par exemple dans $\mathbb{R}$ ou $\mathbb{Q}$) tout le monde divise tout le monde (en mettant 0 à part).

b) Remarque : $\forall\, (a, b) \in \mathbb{Z}^2,\ [a|b \text{ et } b|a] \Leftrightarrow |a| = |b|$.

Preuve – Sens $\Leftarrow$ immédiat. En effet, si $|a| = |b|$ alors $b = \varepsilon a$ et $a = \varepsilon b$ avec $\varepsilon \in \{-1, 1\}$.
Sens $\Rightarrow$: on suppose que $a|b$ et $b|a$.
1er cas : $a = 0$. Alors $a|b$ entraîne que $b = 0$ et donc $|a| = |b| = 0$.
2ème cas : $a \neq 0$.
On a $a|b$ donc il existe un $k \in \mathbb{Z}$ tel que $b = k.a$.
De même $b|a$ donc il existe un $k' \in \mathbb{Z}$ tel que $a = k'b$.
Donc $a = kk'a$ et comme $a \neq 0$, on en déduit que $kk' = 1$ donc que k et k' sont inversibles pour $\times$, ce qui par 1), montre que $k = k' \in \{-1, 1\}$. □

c) Premier lien avec les sous-groupes :

(i) Remarque 1 : soit $a \in \mathbb{Z}$, par déf. le sous-groupe $< a >= a\mathbb{Z}$ est l'ensemble des multiples de a. Ainsi par déf. :

a divise b si, et seulement si, $b \in a\mathbb{Z}$.

(ii) Remarque 2 :

$$b \in a\mathbb{Z} \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}.$$

Preuve de la remarque 2 : Sens $\Leftarrow$ (évident) : comme $b \in b\mathbb{Z}$, $b\mathbb{Z} \subset a\mathbb{Z} \Rightarrow b \in a\mathbb{Z}$.
Sens $\Rightarrow$ (un peu moins) : si on a $b \in a\mathbb{Z}$, comme $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ contenant b, il contient le plus petit sous-groupe de $(\mathbb{Z}, +)$ contenant b i.e. $b\mathbb{Z}$. □

(iii) Attention au sens des inclusions : on a $4\mathbb{Z} \subset 2\mathbb{Z}$ et non l'inverse !

(iv) Traduction de la remarque du b) :

$$\forall\, (a, b) \in \mathbb{Z}^2,\ a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow |a| = |b|.$$

3) Division euclidienne dans $\mathbb{Z}$

a) Thm. – $\forall\, (a, b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \exists\ !\, (q, r) \in \mathbb{Z} \times \mathbb{N},\ \begin{cases} a = bq + r, \\ \text{et } 0 \leq r < |b| \end{cases}$.

b) Exemple : attention à la convention de signe : r est toujours positif.

P.ex. si $(a,b) = (25,6)$ l'égalité de div. euclidienne s'écrit $25 = 6\times 4+1$. On chante : dans 25 combien de fois 6 ? Réponse : 4 fois et il reste 1.

Mais si par exemple $(a,b) = (-25,6)$, on doit changer de stratégie car on veut toujours un reste positif, donc on doit "aller un cran plus loin". L'égalité de division euclidienne est ici : $-25 = 6\times(-5)+5$.

Enfin, si $(a,b) = (-25,-6)$, ce sera $-25 = -6\times 5+5$.

c) Dém. du théorème. (*à bien connaître, sur notes perso.*).

Pour l'existence : on traite seulement le cas $(a,b)\in\mathbb{N}\times\mathbb{N}^*$, l'exple du b) expliquant comment s'y ramener. On utilise une propriété fondamentale (P_2) ci-dessus.

d) En Python (3) : connaître les opérateurs `//` et `%` qui renvoient respectivement le quotient et le reste de la division euclidienne de deux entiers.

Savoir écrire l'algorithme de division euclidienne simplement par différences successives : cf. cours d'info.

III Congruence dans $(\mathbb{Z},+,\times)$, anneaux de congruences

1) Définition :

Gauss (1777-1855) avait remarqué qu'il utilisait beaucoup la formule "le nombre a donne le même reste que b quand on fait la division euclidienne par m" et que cette relation se comportait beaucoup comme une égalité. Il en tira le *concept* de *congruence*.

Définition Soit m un entier naturel non nul. Soient a et b dans $\mathbb{Z}$. On dira que a et b sont *congrus modulo* m si, et seulement si, a et b ont le *même reste* quand on les divise par m suivant la division euclidienne. On notera dans ce cas (suivant Gauss !) : $a\equiv b\,[m]$.

Exemple 7 et 13 sont *congrus modulo 3* car tous les deux ont reste 1 dans la division euclidienne par 3.

Caractérisation − Une autre façon de formuler la déf. précédente est : $a\equiv b\,[m]$ si, et seulement si, m divise la différence $a-b$.

(Exercice : prouver l'équivalence entre ces deux formulations).

Ceci sera pour nous la *working-def.* des congruences, qu'on retiendra sous la forme suivante, en étendant la définition à tous les $m\in\mathbb{Z}$:

$$\boxed{a\equiv b\,[m]\Leftrightarrow\exists\,k\in\mathbb{Z},\ a=b+km.}$$

En reprenant l'exemple précédent : Cette fois on dit que $13\equiv 7\,[3]$ parce que $13 = 7+2\times 3$.

Lien important entre congruence et divisibilité :

$$\boxed{\forall\,(a,m)\in\mathbb{Z}^2,\ m|a\Leftrightarrow a\equiv 0\,[m].}$$

2) Propriétés fondamentales : R.S.T.

Soit $m\in\mathbb{Z}$, la notation introduite par Gauss suggère que la relation de congruence modulo m, ressemble à une égalité. En fait, elle partage avec l'égalité les trois propriétés suivantes :

$$\begin{aligned}\text{Réflexivité :}\quad &\forall\,a\in\mathbb{Z},\ a\equiv a\,[m].\\ \text{Symétrie :}\quad &\forall\,(a,b)\in\mathbb{Z}^2,\ a\equiv b\,[m]\Leftrightarrow b\equiv a\,[m].\\ \text{Transitivité :}\quad &\forall\,(a,b,c)\in\mathbb{Z}^3,\ a\equiv b\,[m]\text{ et }b\equiv c\,[m]\Rightarrow a\equiv c\,[m].\end{aligned}$$

Ce sont les propriétés *intuitives pour tout le monde* du "même" : ici il s'agit d'avoir le "même reste modulo m".

Définition Toute relation sur un ensemble E (i.e. toute *correspondance de E dans E*) vérifiant ces trois propriétés R.S.T. s'appelle une *relation d'équivalence*.

(En analyse, on a vu la relation $\underset{x_0}{\sim}$ par exemple).

3) Compatibilité de la congruence avec les opérations + et ×

a) **Prop.** Soit $m\in\mathbb{Z}$. La relation *congru mod. m* est *compatible* avec la loi + de $\mathbb{Z}$ i.e. :

$$\forall\,(a,b,c,d)\in\mathbb{Z}^4,\quad \left.\begin{array}{l}a\equiv b\,[m]\\ c\equiv d\,[m]\end{array}\right\}\Rightarrow a+c\ \equiv b+d\,[m]$$

b) **Prop.** Soit $m \in \mathbb{Z}$. La relation *congru mod. m* est *compatible* avec la loi $\times$ de $\mathbb{Z}$ i.e. :

$$\forall\,(a,b,c,d) \in \mathbb{Z}^4,\quad \left.\begin{array}{l} a \equiv b\,[m] \\ c \equiv d\,[m] \end{array}\right\} \Rightarrow a.c \;\equiv b.d\,[m]$$

c) **Exercice-à-faire :** *prouvez les deux prop. précédentes. Utilisez plutôt la w-def.*

4) Exemples d'applications des congruences à des problèmes de divisibilité :

a) L'exemple de la preuve par 9 :

(i) Un "truc d'école élémentaire" : un nombre est divisible par 9 (resp. par 3) si, et seulement si, la somme de ses chiffres est divisible par 9 (resp. par 3).

(ii) Enoncé plus général avec preuve : tout nombre entier est congru modulo 9 (et donc en part. modulo 3) à la somme de ses chiffres dans l'écriture en base dix.

b) Divisibilité pour des grandes puissances

(i) Exple : recherche des $n \in \mathbb{N}$ tels que 7 divise $2^{5n+3} + 3^{3n+1}$.

(ii) Méthode : • compatibilité des congruences avec $\times$ et $+$.

• A chaque étape, on remplace les nombres par leur *représentant canonique* modulo 7 i.e.leur reste par la division euclidienne par 7.

• A cause de la finitude de l'ensemble $[0,6]$ des rep. canoniques, les suites de puissances sont toujours *périodiques* (au moins A.P.C.R a priori).

• Un autre représentant utile : un nombre congu à 6 mod. 7 est aussi congru à -1.

L'exemple précédent nous a fait ramener tous les calculs sur les congruences mod. 7 dans l'ensemble fini $[[0,6]]$ *: nous allons développer et formaliser cette idée.*

5) Les anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, pour $n \geq 2$

a) Définition : classe modulo n, notation $\bar{k}$ pour la classe $k + n\mathbb{Z}$, ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes.
Réprésentant d'une classe d'équivalence, le représentant canonique est dans $[[0, n-1]]$.
Deux écritures équivalentes : $a \equiv b\,[n]$ et $\bar{a} = \bar{b}$ dans $\mathbb{Z}/n\mathbb{Z}$.

b) Opérations sur les classes, le point clef : la relation *congru modulo n* est *compatible avec* $+$ *et* $\times$ dans $\mathbb{Z}$.
Exemples de tables pour $+$ et $\times$ dans $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$

c) Prop. Pour tout $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.
Parmi les exemples précédents, $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont même des corps.

IV P.P.C.M. et P.G.C.D.

0) Une reformulation (abstraite mais essentielle !) du théorème de division euclidienne :

Thme : (*dém.*) : *tous les sous-groupes de* $(\mathbb{Z}, +)$ *sont de la forme* $a\mathbb{Z}$.
Remarque : pour $H \neq \{0\}$, on a $a = \min H \cap \mathbb{N}^*$.

1) P.P.C.M.

a) P.P.C.M. est l'acronyme de Plus Petit Commun Multiple. En anglais Least Common Multiple (L.C.M.). Mais qu'est-ce que cela veut dire : plus petit ? Intuitivement clair mais précisons !

b) Première approche : en mettant zéro à part, soit $(a,b) \in (\mathbb{Z}^*)^2$:

On sait que l'ensemble des multiples de a est $a\mathbb{Z}$*, donc l'ensemble des multiples communs à a et b est* $M(a,b) = a\mathbb{Z} \cap b\mathbb{Z}$ *et donc le P.P.C.M. est par déf.* $\min(M(a,b) \cap \mathbb{N}^*))$ *qui existe bien par la prop.* (P_1) *de l'ordre dans* $\mathbb{N}$*, et parce que a et b sont non nuls.*

N.B. – Le ppcm est toujours pris *positif.*

c) **Prop. fondamentale (w.-def. du ppcm)** Soit $(a,b) \in \mathbb{Z}^2$ quelconques. Il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

On a l'équivalence essentielle : $\boxed{m = ppcm(a,b) \Leftrightarrow \begin{cases} a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \\ \text{et } m \geq 0. \end{cases}}$

d) Corollaire : *tous les multiples communs sont des multiples du ppcm.*

On a donc l'équivalence : $\forall\,(a,b) \in (\mathbb{Z}^*)^2, \forall\,\mu \in \mathbb{Z}^*, \begin{cases} a|\mu, \\ b|\mu \end{cases} \Leftrightarrow \text{ppcm}(a,b)|\mu.$

Scholie : Cette propriété est l'analogue pour la divisibilité de propriété suivante pour l'ordre dans $\mathbb{Z}$: $\forall\,(a,b)\in\mathbb{Z}^2, \forall\,\mu\in\mathbb{Z}\ \begin{cases} a\leq\mu, \\ b\leq\mu \end{cases} \Leftrightarrow \max(a,b)\leq\mu$.

Cette analogie fait comprendre qu'en fait le ppcm de deux entiers joue le même rôle que le max en considérant comme *relation d'ordre* non pas l'ordre usuel $\leq$ mais la *divisibilité* (on reviendra au chapitre E sur la notion générale de *relation d'ordre*).

e) Généralisation :
(i) Déf. (la bonne, une fois qu'on a compris le c)
$\forall\,(a_1,\dots,a_n)\in(\mathbb{Z})^n,\ \exists\,!m\in\mathbb{N},\ a_1\mathbb{Z}\cap\dots\cap a_n\mathbb{Z}=m\mathbb{Z}$.
Par déf. $m=ppcm(a_1,\dots,a_n)$.
(ii) Associativité du ppcm : obtenue par associativité de $\cap$.

2) P.G.C.D. de deux entiers (première partie)
a) Plus Grand Commun Diviseur. En anglais Greatest Common Divisor (G.C.D.).

b) Première approche pour la déf., en excluant 0 : *soient* $(a,b)\in(\mathbb{Z}^*)^2$, *on note* $\Delta(a)$ *l'ensemble des diviseurs de a dans* $\mathbb{N}$ *et* $\Delta(a,b)=\Delta(a)\cap\Delta(b)$. *On définit le pgcd(a,b) comme* $\max(\Delta(a,b))$ *qui existe par* P_2 *: en effet* $\Delta(a,b)$ *est non vide, car il contient* 1 *et il est majoré par* $\min(|a|,|b|)$ *car a et b sont non nuls !*
N.B. – Le pgcd toujours pris *positif*.

c) Prop analogue au 1) d) : tous les diviseurs communs divisent le pgcd
On a donc l'équivalence : $\forall\,(a,b)\in(\mathbb{Z}^*)^2, \forall\,d\in\mathbb{Z}^*, \begin{cases} d|a, \\ d|b \end{cases} \Leftrightarrow d|$ pgcd(a,b).
Notation : $\text{pgcd}(a,b)=a\wedge b$.

e) Première étape de la preuve de la prop. du c) :
c est un diviseur commun à a et b ssi $c\mathbb{Z}\supset a\mathbb{Z}\cup b\mathbb{Z}$.

3) Excursion : retour sur la théorie des groupes (abéliens) :
a) Déf. somme de sous-groupes (d'un groupe abelien).

b) Caract. : Plus petit sous-groupe contenant la réunion.

c) Retenir : si $(G,+)$ groupe abélien, et H_1 et H_2 sont deux sous-groupes de $(G,+)$ alors pour tout sous-groupe H de $(G,+)$, on a l'équivalence :
$\begin{cases} H_1\subset H, \\ H_2\subset H \end{cases} \Leftrightarrow (H_1+H_2)\subset H$.

4) Retour sur le P.G.C.D. : caractérisation en terme de sous-groupes
a) Par 5) e) et 6), c diviseur commun à a et b ssi $c\mathbb{Z}\supset a\mathbb{Z}+b\mathbb{Z}$.
Or par 3), $\exists d>0$, $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$, d vérifie bien la prop. du pgcd, et la prop. du 5) d).

b) Retenir par coeur : (working def. du p.g.c.d.) :
Caract . $\forall\,(a,b)\in(\mathbb{Z}^*)^2\ d=a\wedge b\ \Leftrightarrow d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$ et $d>0$.
c) Extension à $(a,b)\in\mathbb{Z}^2$ (et le cas particulier de $(a,b)=(0,0)$).
Déf. $\forall\,(a,b)\in\mathbb{Z}^2,\ \exists\,!d\in\mathbb{N},\ d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$, par déf. $d=pgcd(a,b)$.
N.B. Dans le cas où $a=b=0$, cette définition donne que $pgcd(0,0)=0$. Cela peut paraître choquant car l'ensemble des diviseurs de 0 est $\mathbb{Z}$ entier et l'on pourrait penser qu'ils n'ont pas de « plus grand » diviseur commun. En fait si : 0 est le plus grand des entiers pour la relation *divise* : donc dans PGCD, le mot « plus grand » fait référence à la divisibilité.

5) Cas particuliers des nombres premiers entre eux : Bézout
a) Déf. a et b sont *premiers entre eux* si, et seulement si, $a\wedge b=1$.
Par la caract. du p.g.c.d $a\wedge b=1\Leftrightarrow a\mathbb{Z}+b\mathbb{Z}=Z$.
b) (i) Prop. (Bézout) $a\wedge b=1\Leftrightarrow\exists\,(u,v)\in\ \mathbb{Z}^2,\ au+bv=1$.
(ii) Preuve.
(iii) Rem. sur la preuve : *Un sous-groupe* G *de* $\mathbb{Z}$ *est égal à* $\mathbb{Z}$ *entier, ssi, il contient* 1.
(iv) Attention : pour $d\neq1$, une identité $au+bv=d$ prouve seulement que $a\wedge b$ divise d.

d) Caractérisation utile du pgcd en se ramenant au cas premiers entre eux :
$d = a \wedge b \Leftrightarrow a = a_1 d$, $b = b_1 d$, et $a_1 \wedge b_1 = 1$.
Preuve : ex. planche.

6) P.G.C.D. de n entiers :

a) Prop.-déf : d =pgcd$(a_1, \dots, a_n)$ et seulement si, $d \geq 0$ et $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\,\mathbb{Z}$.

b) Déf. Pour $n > 2$: déf. de "premiers entre eux dans leur ensemble" et "deux à deux premiers entre eux".

c) Soit $(a_1, \dots, a_n) \in (\mathbb{Z}^*)^n$. Si on considère les trois propriétés : (i) $(a_1, \dots, a_n)$ sont deux à deux premiers entre eux,
(ii) il existe (au moins) un couple $(i, j) \in [\![1, n]\!]^2$ tel que $a_i \wedge a_j = 1$.
(iii) $(a_1, \dots, a_n)$ sont premiers entre eux dans leur ensemble.
Alors $(i) \Rightarrow (ii) \Rightarrow (iii)$, mais (ii) n'est pas nécessaire pour avoir (iii) (ctre-exple).

d) L'identité de Bézout vaut dès que $(a_1, \dots, a_n)$ premiers entre eux dans leur ensemble.

7) Conséquences (de Bézout)

a) Thm. de Gauss : $a|bc$ et $a \wedge b = 1 \Rightarrow a|c$. (*dém.*).

b) Si $a \wedge b_i = 1$ pour tout $i = 1, \dots, n$ alors $a \wedge (b_1 \dots b_n) = 1$. (*dém.*).

c) Conséquence du lemme de Gauss :
(i) Prop. si a et b sont premiers entre eux alors $ppcm(a, b) = ab$.
(ii) Reformulation de la prop. Si $a \wedge b = 1$ et $n \in \mathbb{Z}$, si $a|n$ et $b|b$ alors $a.b|n$.
(iii) Dém. du (ii) avec le lemme de Gauss.
(iv) Le résultat du (ii) est crucial pour les exercices : pour montrer qu'un nombre est divisible par 6 il suffit de montrer. qu'il est divisible par 2 et par 3.

8) Algorithme d'Euclide pour l'obtention du PGCD

a) Lemme-clef : si $a = bq + r$ alors $a \wedge b = b \wedge r$.

b) Application : **algorithme d'Euclide** : divisions euclidiennes itérées donnent le pgcd.
(i) Un exemple concret.
(ii) Description mathématique : construction de la suite (r_k) des restes successifs, qui décroît strictement tant qu'elle ne s'annule pas.

c) Algorithme à implémenter : cf. cours d'info.

d) Inversement : obtention de coeff. (u, v) d'une identité de Bézout $au + bv = d$.

e) Résol. des éq. diophantiennes : $ax + by = c$ (pts à coord. entières sur une droite à coeff. entiers).
(i) C.N. évidente : $(a \wedge b)|c$.
(ii) Obtention d'une sol. part. via l'algo. d'Euclide avec remontée.
(iiii) Forme générale de l'ensemble des solutions (méthode SSM).
(iv) Interprétation géométrique.