QUELQUES RAPPELS ET COMPLÉMENTS

1. Relation d'équivalence, relation d'ordre

1.1. Définitions.

Définition 1.1. Soit E un ensemble et $E \times E$ le produit cartésien. Une relation binaire (ou correspondance binaire) $\mathscr{R}$ sur E est la donnée d'une partie (non vide) $\mathscr{G} \subset E \times E$. On dit que x est en relation avec y (x et y étant des éléments de E), ce qui s'écrit $x\mathscr{R}y$, si et seulement si $(x,y) \in \mathscr{G}$. L'ensemble $\mathscr{G}$ s'appelle le graphe de la relation $\mathscr{R}$.

Dans la pratique, les relations binaires sont définies par une propriété caractérisant les éléments en relation. Si $P(x,y)$ est une proposition relativement à (x,y) on définit par exemple la relation $\mathscr{R}$ par

$$x\mathscr{R}y \Leftrightarrow P(x,y) \text{ est vraie.}$$

Dans ce cas le graphe de $\mathscr{R}$ est défini par $\mathscr{G} = \{(x,y) \in E \times E ; P(x,y) \text{ est vraie}\}$.

Remarque 1.2. L'écriture « $P(x,y)$ est vraie » n'est pas la plus appropriée. En général $P(x,y)$ (ou P) est une proposition mathématique qui est vraie ou fausse, le mot « vraie » est donc redondant. On notera donc plutôt

$$x\mathscr{R}y \Leftrightarrow P(x,y).$$

Exemple 1.3.

(1) Si $E = \mathbb{N}$, on vérifie que $b - a$ est multiple de 5 définit une relation sur E.

(2) Si $E = \mathbb{R}$, soit $\mathscr{R}$ la relation définie par $x\mathscr{R}y$ si et seulement si $x^2 > y^2$.

(3) Dans l'ensemble des droites du plan, une droite Δ est en relation avec une droite Δ' si on a $\Delta \perp \Delta'$.

1.2. Relation d'équivalence.

Définition 1.4. Une relation binaire sur un ensemble E est une relation d'équivalence si
– $\forall x \in E$, on a $x\mathscr{R}x$ (réflexivité) ;
– $\forall x, y \in E$ si $x\mathscr{R}y$ alors $y\mathscr{R}x$ (symétrie) ;
– $\forall x, y, z \in E$, si $x\mathscr{R}y$ et $y\mathscr{R}z$ alors on a $x\mathscr{R}z$ (transitivité).

On trouve souvent les notations suivantes, $x\mathscr{R}y$, $x \sim y$, $x \equiv y (\mathrm{mod}\mathscr{R}_1)$ et on dit que x est équivalent à y.

Définition 1.5. Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. Pour tout élément a de E, on appelle classe d'équivalence de a, l'ensemble des éléments équivalents à a. On note $cl(a)$ ou $\dot{a}$ ou encore $\bar{a}$.

$$cl(a) = \{x \in E ; a\mathscr{R}x\}.$$

Remarque 1.6. Par définition, une classe d'équivalence n'est pas vide ($a \in cl(a)$). De plus si a et b sont deux éléments de E alors

$$b \in cl(a) \Leftrightarrow b\mathscr{R}a.$$

Proposition 1.7. *Pour tout a, b dans E on a :*
– $a\mathscr{R}b \Leftrightarrow cl(a) = cl(b)$
– $cl(a) = cl(b)$ *ou bien* $cl(a) \cap cl(b) = \emptyset$ *(deux classes sont égales ou bien disjointes).*

Démonstration. Montrons la première assertion. Supposons que $a\mathscr{R}b$. Soit $x \in cl(a)$. Par définition nous avons $a\mathscr{R}x$, ce qui entraîne par symétrie et transitivité que $b\mathscr{R}x$, d'où $x \in cl(b)$. Ainsi nous avons $cl(a) \subset cl(b)$ et en inversant les rôles de a et b on obtient $cl(a) = cl(b)$. Réciproquement, si $cl(a) = cl(b)$, il est clair que $b \in cl(a)$ ce qui donne $a\mathscr{R}b$.

Pour la deuxième assertion, si $cl(a) \cap cl(b) \neq \emptyset$, montrons que $cl(a) = cl(b)$. Dans ce cas, soit x un élément de E tel que $x \in cl(a)$ et $x \in cl(b)$. L'élément x est tel que $a\mathscr{R}x$ et $b\mathscr{R}x$, d'où (par symétrie et transitivité) $a\mathscr{R}b$, soit $cl(a) = cl(b)$. En conclusion, soit $cl(a) \cap cl(b) = \emptyset$ soit $cl(a) \cap cl(b) \neq \emptyset$ ce qui entraîne $cl(a) = cl(b)$. □

Rappelons la définition d'une partition et d'un recouvrement.

Définition 1.8. Soient $(A_i)_{i\in I}$ une famille indexée par l'ensemble I (non vide) de sous-ensembles de E et F un sous-ensemble non vide de E.

— la famille $(A_i)_{i\in I}$ est appelée recouvrement de F si

$$F \subset \bigcup_{i\in I} A_i$$

— la famille $(A_i)_{i\in I}$ est appelée partition de F si

$$\forall i \in I, \quad A_i \neq \emptyset$$
$$\forall i, j \in I, \quad (i \neq j) \Rightarrow A_i \cap A_j = \emptyset$$
$$F = \bigcup_{i\in I} A_i$$

Le lien entre classes d'équivalence et partition est l'objet de la proposition suivante.

Proposition 1.9. *Les classes d'équivalence distinctes constituent une partition de E, c'est à dire,*
– $\forall a \in E$, $\exists cl(x)$ tel que $a \in cl(x)$;
– deux classes distinctes sont disjointes.

Démonstration. Comme pour tout $a \in E$ on sait que $a \in cl(a)$ alors pour tout a dans E on peut trouver au moins une classe contenant a. De plus si deux classes sont distinctes, alors elles ne sont pas égales et d'après la proposition précédente on en conclut qu'elles sont disjointes. □

Définition 1.10. On note $E/\mathscr{R}$ l'ensemble des classes d'équivalence des éléments de E, c'est l'ensemble quotient.

Exercice 1.11. Des trois exemples de relation, quelles sont les relations d'équivalence ?

Exemple 1.12. Dans $\mathbb{Z}$, on définit la relation $\mathscr{R}$ par $a\mathscr{R}b$ si et seulement si $a - b$ est pair. On vérifie que c'est une relation d'équivalence et que $cl(0)$ est l'ensemble des entiers pairs et $cl(1)$ l'ensemble des entiers impairs. Ainsi $\mathbb{Z}/\mathscr{R}$ possède deux éléments.

Exercice 1.13. On définit sur $\mathbb{R}^2$ la relation suivante :

$$(x_0, y_0)\mathscr{R}(x_1, y_1) \text{ si et seulement si } y_0 - x_0^2 = y_1 - x_1^2.$$

Montrer que c'est une relation d'équivalence. Décrire les classes d'équivalence.

1.3. **Relation d'ordre.**

Définition 1.14. Soit E un ensemble et $\mathscr{R}$ une relation binaire sur E. On dit que $\mathscr{R}$ est une relation d'ordre sur E si
– $\forall x \in E$, on a $x\mathscr{R}x$ (réflexivité) ;
– $\forall x, y \in E$ si $x\mathscr{R}y$ et $y\mathscr{R}x$ alors $x = y$ (antisymétrie) ;
– $\forall x, y, z \in E$, si $x\mathscr{R}y$ et $y\mathscr{R}z$ alors on a $x\mathscr{R}z$ (transitivité).

On trouve souvent les notations suivantes, $x \leq y$, $x \prec y$. Si E est muni d'une relation d'ordre $\prec$ on dit que E est un ensemble ordonné par $\prec$.

Exemple 1.15.

(1) $\mathscr{P}(E)$ muni de l'inclusion.

(2) $\mathbb{N}$ muni de l'inégalité $\leq$ (inégalité usuelle).

(3) $\mathbb{N}^*$ muni de la relation $a \mathscr{D} b$ si et seulement si a divise b.

Définition 1.16. Soit E un ensemble muni d'une relation d'ordre notée $\leq$.

– $(E, \leq)$ est dit totalement ordonné (ou que l'ordre est total) si deux éléments quelconques de E sont comparables, c'est à dire si

$$\forall (x, y) \in E^2, \quad x \leq y \quad \text{ou} \quad y \leq x \quad \text{est vérifiée.}$$

– $(E, \leq)$ est partiellement ordonné (ou que l'ordre est partiel) si il existe x et y éléments de E tel que $x \leq y$ et $y \leq x$ ne soient ni l'une ni l'autre vérifiées.

Exemple 1.17. Reprenons les trois exemples précédents. On démontre que $(\mathscr{P}(E), \subset)$ et $(\mathbb{N}^*, \mathscr{D})$ sont partiellement ordonnés. Clairement $(\mathbb{N}, \leq)$ (l'inégalité usuelle) est totalement ordonné.

Exercice 1.18. On définit sur $\mathbb{R}^2$ la relation suivante :

$$(a_1, b_1) \leq_P (a_2, b_2)$$

si et seulement si

$$b_1 - a_1^2 < b_2 - a_2^2, \text{ ou } b_1 - a_1^2 = b_2 - a_2^2 \text{ et } a_1 \leq a_2.$$

Montrer que c'est une relation d'ordre. Essayer de donner une interprétation géométrique de cette relation. Est-ce une relation d'ordre total ?

1.4. **Éléments remarquables dans un ensemble ordonné.** Dans la suite E est ensemble, $\leq$ est une relation d'ordre sur E et A est une partie non vide de E.

1.4.1. *Majorant, minorant.* S'il existe $a \in E$ tel que $\forall x \in A$ on a $x \leq a$, a est appelé majorant de A.

S'il existe $a \in E$ tel que $\forall x \in A$ on a $a \leq x$, a est appelé minorant de A.

Un ensemble A qui admet au moins un majorant (resp. minorant) est dit majoré (resp. minoré). Si A est majoré et minoré, A est dit borné.

1.4.2. *Plus grand élément, plus petit élément.* S'il existe a_0 tel que $a_0 \in A$ et a_0 majorant de A, alors a_0 est unique et est appelé plus grand élément de A (ou élément maximum de A).

$$a_0 \text{ plus grand élément de } A \Leftrightarrow (a_0 \in A) \text{ et } (\forall x \in A, x \leq a_0).$$

S'il existe a_0' tel que $a_0' \in A$ et a_0' minorant de A, alors a_0' est unique et est appelé plus petit élément de A (ou élément minimum de A).

$$a_0' \text{ plus petit élément de } A \Leftrightarrow (a_0' \in A) \text{ et } (\forall x \in A, a_0' \leq x).$$

Montrons que le plus grand élément de A (s'il existe) est unique. Soient a et b «deux» plus grands éléments de A. Comme $b \in A$ on a $b \leq a$, et comme $a \in A$ on a $a \leq b$. Comme $\leq$ est une relation d'ordre, l'antisymétrie nous donne $a = b$, d'où l'unicité du plus grand élément quand celui-ci existe.

Exemple 1.19. Dans $(\mathbb{R}, \leq)$ (l'inégalité usuelle), l'ensemble $[0, 1[$ possède un plus petit élément (0) mais pas de plus grand élément.

1.4.3. *Borne supérieure, borne inférieure.* Supposons que la partie A admette au moins un majorant, soit M l'ensemble des majorants de A ($M \neq \emptyset$ et $M \subset E$). Si M admet un plus petit élément, il est unique et est appelé borne supérieure de A. La borne supérieure de A est le plus petit des majorants de A ou encore

$$m_0 \text{ borne supérieure de } A \Leftrightarrow \begin{cases} m_0 \text{ majorant de } A, \text{ (i.e. } \forall x \in A,\ x \leq m_0) \\ \text{et } \forall m \in M,\ m_0 \leq m. \end{cases}$$

Remarque 1.20 (exercice)**.** Si A possède un plus grand élément alors ce plus grand élément est la borne supérieure de A. D'où

— si a est le plus grand élément de A alors a est la borne supérieure de A

— si a est la borne supérieure de A alors a est un majorant de A.

De la même façon, on définit la borne inférieure de A.

Supposons que la partie A admette au moins un minorant, soit N l'ensemble des minorants de A ($N \neq \emptyset$ et $N \subset E$). Si N admet un plus grand élément, il est unique et est appelé borne inférieure de A. La borne inférieure de A est le plus grand des minorants de A ou encore

$$n_0 \text{ borne inférieure de } A \Leftrightarrow \begin{cases} n_0 \text{ minorant de } A, \text{ (i.e. } \forall x \in A,\ n_0 \leq x) \\ \text{et } \forall n \in N,\ n \leq n_0. \end{cases}$$

On note $m_0 = \sup A$ et $n_0 = \inf A$.

Exercice 1.21. Montrer que $\sup[0,1[= 1$ et $\inf[0,1[= 0$. Que vaut $\inf\{\frac{1}{x+1/x}\,;\, x \in]1;+\infty[\}$?

1.4.4. *Élément maximal, élément minimal.*

On dit que m est un élément maximal de E si $m \in E$ et si $\forall x \in E$, $(m \leq x) \Rightarrow (m = x)$. La partie $\{m\}$ n'admet pas de majorant strict.

On dit que m' est un élément minimal de E si $m' \in E$ et si $\forall x \in E$, $(x \leq m') \Rightarrow (m' = x)$. La partie $\{m'\}$ n'admet pas de minorant strict.

Exemple 1.22. Dans $(\mathbb{N} \setminus \{1\}, \mathscr{D})$, on démontre que tout nombre premier est élément minimal.

1.5. **Un exercice (pour informaticien). Monoïde libre, monoïde plaxique.** Soit $\mathscr{A}$ un alphabet. On appelle monoïde libre sur $\mathscr{A}$ le monoïde formé de l'ensemble des mots sur $\mathscr{A}$ muni du produit de la concaténation [un monoïde est un magma unifère associatif]. Cet ensemble est noté $\mathscr{A}^*$. Plus précisément :

— un mot sur un alphabet $\mathscr{A}$ est une suite $a_1 a_2 \dots a_n$ (éventuellement vide) de lettres de $\mathscr{A}$; lorsque cette suite est vide, le mot correspondant est noté 1 et est appelé mot vide ;

— la loi interne sur l'ensemble des mots est la concaténation, définie par : si $u = a_1 \dots a_n$ et $v = b_1 \dots b_m$ sont deux mots de $\mathscr{A}^*$ la concaténation de u et v est le mot uv défini par

$$uv = a_1 \dots a_n b_1 \dots b_m.$$

— clairement le mot vide est l'élément neutre de l'ensemble $\mathscr{A}^*$ muni de la concaténation qui est aussi clairement une loi associative.

Considérons l'alphabet $\mathscr{A}$ composé des deux lettres a et b et le monoïde libre $\mathscr{A}^*$ engendré par l'alphabet $\mathscr{A}$. Ajoutons deux règles qui sont

$$\begin{cases} aba = baa, \\ bba = bab, \end{cases}$$

ce qui revient à dire que le mot ba commute avec les lettres a et b. Définissons la relation R_1 sur $\mathscr{A}^*$ par la liste des ses seuls éléments en relation :

$$abaR_1baa \text{ et } bbaR_1bab,$$

ce qui donne que la graphe de R_1 est égal à $\{(aba, baa), (bba, bab)\}$. Définissons alors la relation R_2 sur $\mathscr{A}^*$ par $u_1 R_2 u_2$ si et seulement si u_1 et u_2 peuvent s'écrire sous la forme $u_1 = x v_1 y$ et $u_2 = x v_2 y$ avec des mots x, y, v_1, v_2 de $\mathscr{A}^*$ tels que $v_1 R_1 v_2$ ou $v_2 R_1 v_1$. Définissons (enfin) la relation $\mathscr{R}$ sur $\mathscr{A}^*$ par $u \mathscr{R} v$ si et seulement si il existe $n \in \mathbb{N}$ et une suite de mots $(u_0, u_1, \ldots, u_n)$ tels que

$$u = u_0 R_2 u_1 R_2 u_2 \cdots u_{n-1} R_2 u_n = v,$$

ce qui veut dire *in extenso* que $u = u_0$, $u_n = v$ et que pour tout $i \in \{0, n-1\}$ on a $u_i R_2 u_{i+1}$.

(a) Constater que

-i- $abab \mathscr{R} baab$

-ii- $bbaaba \mathscr{R} bababa = (ba)^3$

-iii- $baaaba \mathscr{R} (ba)^2 a^2$

-iv- $abababab \mathscr{R} (ba)^3 ab$.

(b) Montrer que $\mathscr{R}$ est une relation d'équivalence sur $\mathscr{A}^*$.

(c) Montrer pour tout mot u dans $\mathscr{A}^*$ il existe un unique triplet (i, j, k) tel que $u \mathscr{R} (ba)^i a^j b^k$. Ceci définit donc une application φ de $\mathscr{A}^*$ dans $\mathbb{N}^3$ avec la convention $\varphi(1) = (0, 0, 0)$.

(d) L'application φ permet de définir sur $\mathbb{N}^3$ une loi de composition interne : si $(i_1, j_1, k_1) \in \mathbb{N}^3$ et $(i_2, j_2, k_2) \in \mathbb{N}^3$ on a

$$(i, j, k) = (i_1, j_1, k_1) * (i_2, j_2, k_2)$$

si et seulement si

$$(ba)^i a^j b^k \mathscr{R} (ab)^{i_1} a^{j_1} b^{k_1} (ab)^{i_2} a^{j_2} b^{k_2}$$

ou encore $(i, j, k) = \varphi((ab)^{i_1} a^{j_1} b^{k_1} (ab)^{i_2} a^{j_2} b^{k_2})$.

Montrer que $(i, j, k) = (i_1, j_1, k_1) * (i_2, j_2, k_2)$ est tel que

$$(i, j, k) = \begin{cases} (i_1 + i_2 + j_2, j_1, k_1 - j_2 + k_2) \text{ si } j_2 < k_1, \\ (i_1 + i_2 + k_1, j_1 + j_2 - k_1, k_2) \text{ sinon.} \end{cases}$$

2. L'ENSEMBLE $\mathbb{N}$

Tout le monde manipule l'ensemble des entiers naturels depuis son enfance ! Comme le métier de mathématicien est de construire de façon rigoureuse les objets qu'il manipule, comment construire $\mathbb{N}$, l'addition, la relation d'ordre ? Dans une première lecture il est possible de survoler le début et de lire très sérieusement à partir du théoréme 2.5 qui est fondamental.

2.1. **Définition axiomatique de l'ensemble $\mathbb{N}$ des entiers naturels.** On peut définir $\mathbb{N}$ au moyen des cinq axiomes suivants, appelés axiomes de Peano (mathématicien italien, 1858–1932),

Axiome 1. Il existe un ensemble noté $\mathbb{N}$ dont les éléments sont appelés entiers naturels et auquel 0 appartient.

Axiome 2. Tout entier naturel n possède un successeur, qui est un entier naturel, provisoirement noté n^+. Le successeur de 0 est noté 1, celui de 1 est noté 2, etc.

Axiome 3. 0 n'est le successeur d'aucun entier naturel.

Axiome 4. Deux entiers naturels distincts ont nécessairement des successeurs distincts.

Axiome 5. Si un ensemble d'entiers naturels contient 0 ainsi que le successeur de tout entier lui appartenant, alors il est confondu avec $\mathbb{N}$.

Exercice 2.1.

(a) Démontrer que tout entier naturel non nul est le successeur d'un entier naturel. [indication : considérer l'ensemble A égal à la réunion de $\{0\}$ et de l'ensemble des successeurs d'entiers naturels]

(b) Démontrer le principe du raisonnement par récurrence.

2.2. **Lois de composition interne sur $\mathbb{N}$.** On définit l'addition et la multiplication par les formules suivantes

$$\forall n, p \in \mathbb{N}, \quad n+0=n, \quad n+p^+=(n+p)^+, \quad n\times 0=0, \quad n\times p^+=n\times p+n.$$

Exercice 2.2 (propriétés usuelles)**.** Vérifier que ces formules ont bien un sens et définissent l'addition et la soustraction sur tout l'ensemble des entiers naturels, puis établir les propriétés suivantes ($\forall n, p, q \in \mathbb{N}$) :

(1) $0+n=n+0=n$ ou encore 0 est élément neutre pour l'addition

(2) $n^+=n+1$

(3) $(n+p)+q=n+(p+q)$ ou encore l'associativité de l'addition

(4) $n+p=p+n$ ou encore la commutativité de l'addition

(5) $n+p=0 \Leftrightarrow n=p=0$

(6) $n+p=n+q \Rightarrow p=q$

(7) $n\times 0=0\times n=0$ ou encore 0 est élément absorbant pour la multiplication

(8) $n\times 1=1\times n=n$ ou encore 1 est élément neutre pour la multiplication

(9) $(n\times p)\times q=n\times(p\times q)$ ou encore l'associativité de la multiplication

(10) $n\times p=p\times n$ ou encore la commutativité de la multiplication

(11) $n\times(p+q)=(n\times p)+(n\times q)$ ou encore la distributivité de la multiplication par rapport à l'addition

(12) $n\times p=1 \Leftrightarrow n=p=1$

(13) $n\times p=0 \Leftrightarrow (n=0 \text{ ou } p=0)$

(14) Si $n\neq 0$ alors $(n\times p=n\times q \Leftarrow p=q)$

2.3. **Relation d'ordre sur $\mathbb{N}$.** On définit sur $\mathbb{N}$ la relation binaire : $\forall n, p \in \mathbb{N}$, on dit que $n \leq p$, ou encore $p \geq n$, s'il existe un entier naturel u tel que $n+u=p$. On pose $n<p$ si et seulement si ($n \leq p$ et $n \neq p$) si et seulement si $p>n$.

Exercice 2.3. Montrer que, $\forall n, p \in N$,

(a) $n<n+1$

(b) $n \leq p \Leftrightarrow n<p+1$

(c) si $n \leq p$, alors l'entier naturel u tel que $n+u=p$ est unique. On le note $p-n$ (la différence entre p et n).

(d) si $p\neq 0$, alors il existe un entier naturel q tel que $q+1=p$. On le note $q=p-1$ et on l'appelle le prédécesseur de p.

Exercice 2.4. Montrer que

(a) $\leq$ est une relation d'ordre

(b) $(\mathbb{N}, \leq)$ est ensemble totalement ordonné.

(c) 0 est le plus petit élément de $\mathbb{N}$

(d) $\mathbb{N}$ n'a pas de plus grand élément (raisonner par l'absurde)

(e) $\forall n,p,q \in \mathbb{N}: \quad n \leq p \Leftrightarrow n+p \leq q+p$

(f) $\forall n \in \mathbb{N}\setminus\{0\}, \quad \forall p,q \in \mathbb{N} : \ q \leq p \Leftrightarrow n \times q \leq n \times p$

Le théorème suivant est fondamental et est équivalent au principe de récurrence.

Théorème 2.5. *Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.*

Démonstration. La preuve se fait par l'absurde. Soit A une partie non vide de $\mathbb{N}$ et supposons que A ne possède pas de plus petit élément. L'élément 0 n'appartient pas à A, car d'après l'exercice précédent 0 est le plus petit élément de $\mathbb{N}$. Considérons donc la partie non vide B définie par $\{n \in \mathbb{N};\ n < a,\ \forall a \in A\}$ (B non vide car $0 \in B$).

Montrons que B contient le successeur de chacun de ses éléments, ce qui entraînera d'après le 5ème axiome de Peano que $B = \mathbb{N}$. Soit n un élément de B et soit a élément de A ($a-1$ désigne le prédécesseur de a). Nous avons $n < a$ et comme $a = (a-1)+1$ il vient (voir exercice 2.3) que $n < (a-1)+1$ d'où $n \leq a-1$ soit (d'après l'exercice 2.4) $n+1 \leq (a-1)+1 = a$. Donc pour tout $a \in A$ nous avons $n+1 \leq a$. Si $n+1$ est élément de A alors $n+1$ est le plus petit élément de A, ce qui est contradictoire. Donc $n+1$ n'est pas élément de A et pour tout $a \in A$ nous avons $n+1 < a$. Finalement si $n \in B$ alors $n+1$ est élément de B. Le cinquième axiome de Peano implique que $B = \mathbb{N}$. A est donc une partie vide. En effet si ce n'est pas la cas il existerait un élément $a \in A$ tel que pour tout $n \in B = \mathbb{N}$ on ait $n < a$ ou encore il existerait un majorant de $\mathbb{N}$. A ne peut être que la partie vide, ce qui contredit l'hypothèse de départ. □

Corollaire 2.6. *Toute partie non vide de $\mathbb{N}$, majorée, possède un plus grand élément.*

2.4. **Division euclidienne dans $\mathbb{N}$.**

Théorème 2.7. *Pour tout couple d'entiers naturels (a,b) avec $b \neq 0$ il existe un unique couple d'entiers naturels (q,r) tel que $a = bq + r$ et $0 \leq r < b$. L'entier q est appelé le quotient, l'entier r le reste de la division euclidienne de a par b.*

Démonstration. Considérons l'ensemble $A = \{q \in \mathbb{N};\ a < b(q+1)\}$. On montre successivement que A est une partie non vide de $\mathbb{N}$, possède un plus petit élément noté q et que le couple $(q, r = a - bq)$ convient. L'unicité se démontre aisément. □

3. Un peu de $\mathbb{Z}$

Naïvement définir les entiers relatifs consiste à ajouter les entiers négatifs... Plus précisément on définit sur $\mathbb{N}^2$ la relation binaire suivante

$$(a,b)\mathscr{R}(c,d) \Leftrightarrow a+d = b+c.$$

La relation $\mathscr{R}$ est une relation d'équivalence (le vérifier). Notons $\overline{(a,b)}$ la classe du couple (a,b) pour la relation $\mathscr{R}$ et appelons la $a-b$ (lire "a moins b"). On définit alors l'ensemble $\mathbb{Z}$ par l'ensemble quotient $\mathbb{N}^2/\mathscr{R}$. Un entier relatif est donc une classe d'équivalence $a-b$, a et b étant des entiers naturels. Un entier relatif est aussi appelé un entier.

On définit sur $\mathbb{Z}$ les deux opérations suivantes

$$\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}, \qquad \overline{(a,b)} \otimes \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$$

ce qui s'écrit avec la notation $(a-b)$

$$(a-b) \oplus (c-d) = (a+c) - (b+d), \qquad (a-b) \otimes (c-d) = (ac+bd) - (ad+bc)$$

Pour que les deux expressions précédentes aient un sens il est nécessaire de démontrer que le résultat ne dépend pas du choix des représentants de chaque classe d'équivalence. Ensuite on montre que l'addition et la multiplication dans $\mathbb{Z}$ possèdent les mêmes propriétés générales que celles de $\mathbb{N}$. Montrer que l'application qui à chaque entier naturel n associe l'entier relatif $(n-0)$ est injective. On identifie ainsi n et $(n-0)$, ce qui nous donne, pour simplifier, $\mathbb{N}\subset\mathbb{Z}$. On retrouve ainsi les conventions et les règles usuelles (et connues) de calcul dans $\mathbb{Z}$ et bien sûr $\oplus$ et $\otimes$ deviennent nos addition et multiplication préférées usuelles...

3.1. **Division euclidienne dans $\mathbb{Z}$.** Si $a\in\mathbb{R}$ on note $|a|$ le plus grand des entiers a et $-a$.

Théorème 3.1. *Pour tout couple d'entiers (a,b) avec $b\neq 0$ il existe un unique couple $(q,r)\in\mathbb{Z}\times\mathbb{Z}$ tel que*

$$a=bq+r \quad et \quad 0\leq r<|b|$$

L'entier q est appelé le quotient, l'entier r le reste de la division euclidienne de a par b.

Démonstration. Considérons l'ensemble $A=\{a-bk\,;\,k\in\mathbb{Z}\}\cap\mathbb{N}$. Il faut tout d'abord montrer que A est non vide. Si $a\geq 0$, c'est immédiat en considérant $a-b\times 0=a\in A$. Si $a<0$ et $b>1$ alors l'entier $a(1-b)$ est positif et ainsi $a-b\times a\in A$. Si $a<0$ et $b<-1$ alors l'entier $a(1+b)$ est positif et ainsi $a-b\times(-a)\in A$.

L'ensemble A est donc une partie non vide de $\mathbb{N}$. D'après la propriété fondamentale de $\mathbb{N}$, A possède un plus petit élément, que nous noterons r. Par définition de A, $r\in\mathbb{N}$ et, soit $q\in\mathbb{Z}$ tel que $a=bq+r$. Pour montrer que $r<|b|$ raisonnons par contradiction. Si $r\geq|b|$ alors

$$0\leq r-|b|\leq a-bq+|b|=a-b(q+\varepsilon)\in A \quad \text{avec} \quad \varepsilon=\pm 1.$$

Comme $r-|b|<r$, le caractère minimal de r est contredit, ce qui permet de conclure quant à l'existence du couple (q,r).

Pour l'unicité, il suffit de supposer qu'il y a un deuxième couple (q',r') vérifiant les hypothèses. Nous avons $a=bq+r=bq'+r'$ soit

$$|b|\times|q-q'|=|r'-r|.$$

Comme $0\leq r<|b|$ et $0\leq r'<|b|$, on a $-|b|<r'-r<|b|$, soit $|r'-r|<|b|$. Il résulte donc des deux inégalités précédentes que $|q-q'|<1$. Or $|q-q'|$ est un entier naturel, d'où $q=q'$. Par suite on a $r=r'$. □

3.2. **Arithmétique dans $\mathbb{Z}$.** Voici quelques définitions :

(1) un entier non nul a divise un entier b s'il existe $q\in\mathbb{Z}$ tel que $b=aq$

(2) un nombre premier est un entier naturel supérieur à 2 tel que l'ensemble des entiers naturels qui le divisent soit réduit à 1 et lui-même

(3) tout entier $n\geq 2$ est produit de nombres premiers

(4) l'ensemble des nombres premiers est infini

(5) deux entiers a et b sont premiers entre eux si les seuls diviseurs communs sont 1 et -1.

Pour démontrer que l'ensemble des nombres premiers est infini, on procède par contradiction. Soit $p_1,\ldots,p_n$ l'ensemble des nombres premiers. Considérons $n=1+p_1\times p_2\times\cdots p_n$, qui n'est pas premier (car non égal à p_1, p_2, ...ou p_n). Comme n est nécessairement un produit d'entiers premiers, soit p un nombre premier divisant n. Or p divise $p_1\times p_2\times\cdots p_n$, donc p divise $n-p_1\times p_2\times\cdots p_n=1$, ce qui entraîne une contradiction.

Exercice 3.2. Soit n un entier naturel non nul. Montrer que l'intervalle des entiers compris entre $n!+2$ et $n!+n$ ne contient aucun nombre premier.

Théorème 3.3 (Lemme d'Euclide)**.** *Soient a et b deux entiers relatifs et p un nombre premier divisant ab. Alors p divise l'un des entiers a ou b.*

Démonstration. Supposons que p ne divise pas a et montrons que p divise b. Pour cela considérons l'ensemble

$$A = \{n \geq 1\,;\, p \text{ divise } an\}.$$

A est une partie non vide de $\mathbb{N}$ ($p \in A$ par exemple). D'après la propriété fondamentale de $\mathbb{N}$, soit m le plus petit élément de A. Comme nous avons supposé que p ne divise pas a, alors $m \geq 2$.

Soit $n \in A$ et montrons que m divise n. La division euclidienne de n par m nous donne $n = mq + r$ avec $0 \leq r < m$. Comme p divise an et am alors p divise an et amq donc p divise $ra = na - amq$. Si r est non nul, on a alors $r \in A$ et $r < m$ ce qui contredit le caractère minimal de m. Donc r est nul et $n = mq$ soit m divise n.

L'entier p étant dans A, on a m divise p. Comme $m \geq 2$ et p premier on obtient $m = p$. Pour conclure il suffit de constater que $|b|$ est dans A. □

Remarque 3.4. En TD une autre preuve sera présentée.

Le Lemme d'Euclide se généralise pour un produit d'entiers.

Corollaire 3.5. *Si un nombre premier divise un produits d'entiers relatifs alors il divise au moins un de ses entiers relatifs. En particulier si un nombre premier divise un produit de nombre premier il est égal à l'un d'eux.*

La conséquence est la décomposition (unique à l'ordre près) d'un entier en puissance entière de nombres premiers.

Théorème 3.6. *Tout entier $n \geq 2$ s'écrit de façon unique*

$$n = p_1^{r_1} \times p_2^{r_2} \times \cdots p_q^{r_q},$$

où $r_i \geq 1$ pour tout $1 \leq i \leq q$ et où p_1, p_2, …, p_q sont des nombres premiers vérifiant $p_i < p_{i+1}$ pour tout $1 \leq i \leq q-1$.

3.2.1. *PGCD.*

Définition 3.7. Soient a et b deux entiers non nuls. Considérons l'ensemble des diviseurs non nuls positifs communs. Cet ensemble admet un plus grand élément, appelé plus grand commun diviseur de a et b, noté encore $\text{pgcd}(a,b)$.

Remarque 3.8. L'ensemble des diviseurs communs est nécessairement borné, d'où l'existence d'un plus grand élément.

Théorème 3.9 (Identité de Bezout)**.** *Soient a et b deux entiers non nuls. Alors il existe u et v tels que $au + bv = \text{pgcd}(a,b)$. De plus tout diviseur commun à a et b divise* $\text{pgcd}(a,b)$.

Démonstration. Soit H l'ensemble défini par

$$H = \{an + bm\,;\, n, m \in \mathbb{Z}\}.$$

Alors il existe un unique entier naturel d tel que $H = d\mathbb{Z} = \{dn\,;\, n \in \mathbb{Z}\}$ et on montre que $d = \text{pgcd}(a,b)$.

Soit $H^+ \setminus \{0\}$ la partie strictement positive de H. Comme $a^2 + b^2 > 0$ l'ensemble $H^+ \setminus \{0\}$ est une partie non vide de $\mathbb{N}$. D'apès un théorème fondamental concernant $\mathbb{N}$, soit d le plus petit élément de $H^+ \setminus \{0\}$. Montrons que $H = d\mathbb{Z}$. Il est clair que $d\mathbb{Z} \subset H$ car H est stable par multiplication et addition. Pour l'autre inclusion soit p un élément de H et montrons que d divise p. La division euclidienne de p par d nous donne un couple (q,r) tel que $p = qd + r$ et $0 \leq r < d$. Or comme p

et d sont éléments de H il est facile de voir que $r = p - qd$ est aussi élément de H. Par définition d est le plus petit élément de $H^+ \setminus \{0\}$, r ne peut être que nul (en particulier comme a et b sont éléments de H nous avons démontré que d divise a et b). Finalement nous avons démontré que $H = d\mathbb{Z}$.

Le fait qu'il existe u et v dans $\mathbb{Z}$ tels que $d = au + bv$ vient de la définition de H.

Soit p un diviseur commun à a et b. Clairement p divise $au + bv$ donc divise d. Si p est positif alors $p \leq d$, donc $d = \text{pgcd}(a, b)$. □

Nous en déduisons le théorème de Bezout et le théorème de Gauss

Théorème 3.10. *Deux entiers a et b sont premiers entre eux si et seulement si il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration. Soient a et b deux entiers. D'après ce qui précède nous savons que si a et b sont premiers entre eux alors $d = \text{pgcd}(a, b) = 1$, d'où l'existence du couple (u, v).

Réciproquement, supposons qu'il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$. Soit p un diviseur commun à a et b. Clairement p divise au et p divise bv donc p divise $au + bv = 1$. Ainsi p divise 1 nous donne $p = \pm 1$. □

Théorème 3.11 (Théorème de Gauss)**.** *Soient a, b et c trois entiers. Si a divise bc et si a est premier avec b alors a divise c.*

Démonstration. exercice □

3.2.2. *PPCM.*

Définition 3.12. Soient a et b deux entiers non nuls. L'ensemble des multiples communs positifs à a et b admet un plus petit élément, appelé plus petit commun multiple et noté $\text{ppcm}(a, b)$.

Théorème 3.13. *Soient a et b deux entiers non nuls. Alors tout multiple commun à a et b est divisible par* $\text{ppcm}(a, b)$*. De plus* $|ab| = \text{pgcd}(a, b) \times \text{ppcm}(a, b)$*.*

Démonstration. Considérons l'ensemble A des multiples positifs et communs à a et b. A étant non vide ($|ab| \in A$), par définition soit $\text{ppcm}(a, b)$ le plus petit élément. Soit $p \in A$ et montrons que $\text{ppcm}(a, b)$ divise p. La division euclidienne de p par $\text{ppcm}(a, b)$ nous donne $p = q\,\text{ppcm}(a, b) + r$ avec $0 \leq r < \text{ppcm}(a, b)$. En écrivant $r = p - q\,\text{ppcm}(a, b)$ on voit que si $r \neq 0$ alors r est un multiple commun positif à a et b, ce qui contredit le caractère minimal de $\text{ppcm}(a, b)$. Donc $r = 0$ et $\text{ppcm}(a, b)$ divise p.

Notons $d = \text{pgcd}(a, b)$ et soient k et k' tels que $a = dk$ et $b = dk'$. Les entiers k et k' sont premiers entre eux car si p divise k et k' alors dp divise $dk = a$ et $dk' = b$ ce qui entraîne dp diviseur commun à a et b. Constatons que $d|kk'|$ est un multiple de a et b. Soient q et q' tels que $\text{ppcm}(a, b) = aq$ et $\text{ppcm}(a, b) = bq'$. Comme $aq = bq'$ on obtient $dkq = dk'q'$ d'où $kq = k'q'$. Les entiers k et k' étant premiers entre eux et k divisant $k'q'$ on en déduit que k divise q'. Donc $|q'| \geq |k|$ soit $\text{ppcm}(a, b) = |bq'| \geq |dkk'|$. Par définition du ppcm on obtient $\text{ppcm}(a, b) = d|kk'|$ d'où le résultat. □

3.2.3. *Algorithme d'Euclide.* Comment calculer le pgcd de deux entiers (et aussi les entiers u et v intervenant dans l'identité de Bezout) ? C'est l'objet de l'algorithme ou comment les divisions euclidiennes successives mènent au pgcd.

En effet soient a et b deux entiers naturels non nuls avec $a > b$. Posons $r_0 = a$, $r_1 = b$ et supposons construits les entiers r_0, r_1,..., r_i. Si $r_i \neq 0$ on définit r_{i+1} comme le reste de la division euclidienne de r_{i-1} par r_i. Si $r_i = 0$ alors le procédé s'arrête. On construit ainsi la suite r_i.

Le procédé s'arrête nécessairement. En effet par définition de la division euclidienne on a $r_{i+1} < r_i$, la suite d'entiers naturels r_i étant strictement décroissante il existe un entier n tel que

$$0 < r_n < r_{n-1} < r_{n-2} < \cdots < r_1 \leq r_0 \quad \text{et} \quad r_{n+1} = 0.$$

Dans la suite nous aurons aussi besoin des quotients, notés q_1, q_2, etc définis par

$$r_{i-1} = q_i r_i + r_{i+1}, \quad \forall 1 \leq i \leq n.$$

Proposition 3.14. *On a* $\text{pgcd}(a,b) = r_n$ *ou encore le pgcd de* a *et* b *est égal au dernier reste non nul du procédé des divisions successives.*

Démonstration. Pour tout $1 \leq i \leq n$, l'égalité $r_{i-1} = q_i r_i + r_{i+1}$ entraîne que les diviseurs communs à r_{i-1} et r_i sont les diviseurs communs à r_i et r_{i+1}. Les diviseurs communs étant identiques on a $\text{pgcd}(r_{i-1}, r_i) = \text{pgcd}(r_i, r_{i+1})$. Ainsi

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

et comme $r_{n+1} = 0$ (ou encore r_n divise r_{n-1}) on déduit que $\text{pgcd}(r_{n-1}, r_n) = r_n$, d'où le résultat. □

Par l'identité de Bezout soient u et v tel que

$$au + bv = r_n$$

Pour calculer explicitement les entiers u et v, on peut « remonter » le procédé des divisions successives ou encore ajouter un calcul de suite à l'algorithme (c'est alors l'algorithme étendu d'Euclide).

On définit les suites $u_0, \ldots, u_n$ et $v_0, \ldots, v_n$ par

$$u_0 = 1, \quad u_1 = 0, \quad v_0 = 0, \quad v_1 = 1$$

et par la relation de récurrence, pour tout $1 \leq i \leq n-1$

$$u_{i+1} = u_{i-1} - u_i q_i$$
$$v_{i+1} = v_{i-1} - v_i q_i.$$

On démontre alors

Proposition 3.15. *On a* $r_n = au_n + bv_n$

Démonstration. Montrons que pour $0 \leq i \leq n$ l'égalité $r_i = au_i + bv_i$ est vérifiée. Pour $i = 0$ on a bien $r_0 = a = a \times 1 + b \times 0$ et pour $i = 1$ on a bien $r_1 = b = a \times 0 + b \times 1$! Supposons que pour $k \in \{1, \ldots, n-1\}$ on ait la propriété $r_i = au_i + bv_i$ vérifiée pour $0 \leq i \leq k$. Par définition de r_{i+1}, a

$$r_{i+1} = r_{i-1} - q_i r_i = au_{i-1} + bv_{i-1} - q_i(au_i + bv_i) = a(u_{i-1} - q_i u_i) + b(v_{i-1} - q_i v_i) = au_{i+1} + bv_{i+1}.$$

Par récurrence on a donc démontré le résultat désiré. □

On choisit l'algorithme d'Euclide ou l'algorithme d'Euclide étendu selon la question posée. Dans la pratique on peut présenter l'algorithme d'Euclide étendu sous forme de tableau ou du moins en présentant à chaque étape le calcul de la division euclidienne et les résultats (q_i, r_i, u_i, v_i).

3.2.4. *Congruences.*

Définition 3.16. Soit n un entier naturel supérieur ou égal à 2. On dit que a et b sont congrus modulo n, noté $a \equiv b[n]$ ou encore $a \equiv b(\mathrm{mod} n)$ si n divise $a-b$ (ce qui s'écrit encore $a = b+kn$, $k \in \mathbb{Z}$).

On démontre les propriétés suivantes

- $a \equiv a[n]$ (réflexivité)
- $a \equiv b[n]$ équivalent à $b \equiv a[n]$ (symétrie)
- si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (transitivité)

Proposition 3.17. *Soient n un entier supérieur ou égal à 2 et a_1, a_2, b_1 et b_2 tels que*

$$a_1 \equiv b_1[n] \qquad a_2 \equiv b_2[n].$$

Alors

- $a_1 + a_2 \equiv b_1 + b_2[n]$
- $a_1 a_2 \equiv b_1 b_2[n]$
- $a_1^q \equiv b_1^q[n]$ *pour tout* $q \geq 1$.

4. Un peu de rationnels

Pour définir l'ensemble $\mathbb{Q}$ des rationnels on considère sur $\mathbb{Z} \times \mathbb{Z}^*$ ($\mathbb{Z}^*$ désigne $\mathbb{Z} \setminus \{0\}$) la relation d'équivalence

$$(a,b)\mathscr{R}(c,d) \Leftrightarrow (ad = bc),$$

l'ensemble quotient $\mathbb{Z} \times \mathbb{Z}^*/\mathscr{R}$ que l'on munit de deux opérations

$$(a,b) \oplus (c,d) = (ad + cb, bd) \qquad (a,b) \otimes (c,d) = (ac, bd)$$

et l'on démontre que tout se passe bien...

5. Notion de cardinal

Un ensemble E est dit fini s'il est soit vide soit en bijection avec l'ensemble des entiers naturels compris entre 1 et n, pour un certain entier naturel non nul n. Dans ce dernier cas, l'entier n est unique et il est appelé le cardinal de E. Si E est vide on dit que son cardinal est nul. On a utilisé ici le fait apparemment évident mais long à démontrer *in extenso* que si n et p sont deux entiers naturels distincts alors il n'existe pas de bijection entre $\{1,\ldots,n\}$ et $\{1,\ldots,p\}$ – l'écrire. Un ensemble E est dit infini s'il n'est pas fini. Deux ensembles infinis ne sont pas en général en bijection ($\mathbb{N}$ et $\mathbb{R}$ ne sont pas en bijection).

Quand deux ensembles sont finis et ont même cardinal il découle immédiatement que ces deux ensembles sont en bijection. Plus généralement (même si les ensembles sont de cardinal infini) deux ensembles sont même cardinal s'ils sont en bijection. Un ensemble qui a le même cardinal que $\mathbb{N}$ est dit dénombrable. L'ensemble $\mathbb{Z}$ et l'ensemble des rationnels sont dénombrables mais l'ensemble des réels n'est pas dénombrable.

Soient E et F deux ensembles quelconques. On dit que le cardinal de E est inférieur (au sens large) à celui de F s'il existe une application injective de E dans F et on écrit $|E| \leq |F|$. On a le théorème de Cantor–Bernstein que nous admettrons

Théorème 5.1. *Soient E et F deux ensembles tels que $|E| \leq |F|$ et $|F| \leq |E|$. Alors on a $|E| = |F|$ et il existe une bijection de E dans F.*