Ensembles et Arithmétique

Commentaires : *Cessez d'employer des tournures infantiles de la forme « D'après Gauss... », « Bézout donne... » ! Derrière la faible qualité littéraire de la tournure, vous oubliez que Gauss, Bézout et les autres ne sont pas vos amis et sont morts depuis bien longtemps donc ne donnent ou ne disent plus rien. Leur théorème, par contre, ainsi que leur mémoire sont immortels.*

Exercice I (Sans les fonctions indicatrices) : Dans tout cet exercice, pour faciliter la lecture, on notera $\overline{A} = E\backslash A$.

1. Il suffit d'appliquer les définitions et les lois de Morgan :

$$\begin{aligned}
A\triangle B &= (A\cup B)\backslash(A\cap B) = (A\cup B)\bigcap\overline{(A\cap B)} \\
&= (A\cup B)\cap(\bar{A}\cup\bar{B}) \qquad \text{(lois de De Morgan)} \\
&= \underbrace{(A\cap\bar{A})}_{=\varnothing}\cup(A\cap\bar{B})\cup(B\cap\bar{A})\cup\underbrace{(B\cap\bar{B})}_{=\varnothing} \qquad \text{(distributivité)} \\
&= (A\cap\bar{B})\cup(B\cap\bar{A}) \\
&= (A\backslash B)\cup(B\backslash A).
\end{aligned}$$

Commentaires : *On pouvait également le démontrer par double inclusion mais à condition de bien démontrer les deux.*

Remarque : Par définition de $\triangle$ et commutativité de $\cup$ et $\cap$, il est assez clair que $\triangle$ est une opération commutative sur les parties de E.

2. Ici encore, on applique les formules et on simplifie $A\cap\overline{A} = B\cap\overline{B} = C\cap\overline{C} = \varnothing$ dans les réunions :

$$\begin{aligned}
(A\Delta B)\Delta C &= (((A\cap\bar{B})\cup(\bar{A}\cap B))\cap\bar{C})\cup((\bar{A}\cup B)\cap(A\cup\bar{B})\cap C) \\
&= (A\cap\bar{B}\cap\bar{C})\cup(\bar{A}\cap B\cap\bar{C})\cup(\bar{A}\cap\bar{B}\cap C)\cup(A\cap B\cap C).
\end{aligned}$$

Cette expression est symétrique en A, B et C donne donc le résultat. Comme on est en début d'année, je poursuis les calculs en utilisant l'associativité et la commutativité de $\cup$ et $\cap$:

$$\begin{aligned}
&= (B\cap\bar{C}\cap\bar{A})\cup(\bar{B}\cap C\cap\bar{A})\cup(\bar{B}\cap\bar{C}\cap A)\cup(B\cap C\cap A) \\
&= (B\Delta C)\Delta A \\
&= A\triangle(B\triangle C). \qquad \text{(par commutativité de } \triangle\text{)}
\end{aligned}$$

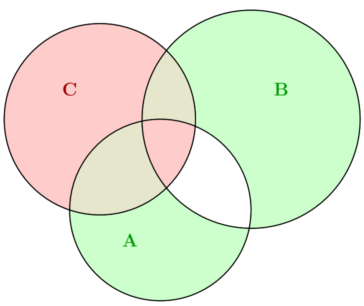

Figure II.1 – $(A\Delta B)\Delta C$

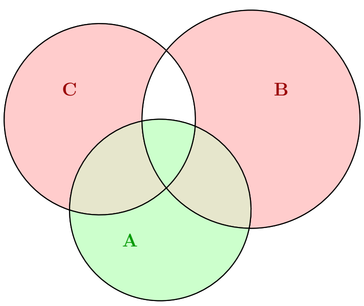

Figure II.2 – $A\Delta(B\Delta C)$

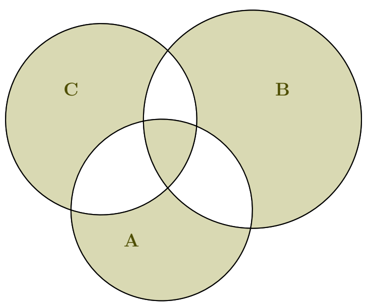

Figure II.3 – $A\Delta B\Delta C$

3 Montrons que l'unique partie B de E vérifiant $A \triangle B = B \triangle A = A$ est $\varnothing$.

Si $B = \varnothing$, alors, pour toute partie A de E, on a :

$$A \triangle \varnothing = (A \backslash \varnothing) \cup (\varnothing \backslash A) = A \cup \varnothing = A.$$

Par commutativité de $\triangle$, on a également $\varnothing \triangle A = A$.

L'ensemble vide répond donc à la question et l'existence est prouvée.

Supposons qu'il existe deux parties B_1, B_2 répondant à la question. Il suffit de traduire et d'utiliser la commutativité de $\triangle$:

- Par définition de B_1, pour toute partie A de E, on a $B_1 \triangle A = A$.

  En particulier, pour $A = B_2$, on obtient $B_1 \triangle B_2 = B_2$.
- De même, par définition de B_2, pour toute partie A de E, on a $A \triangle B_2 = A$.

  En particulier, pour $A = B_1$, on obtient $B_1 \triangle B_2 = B_1$.

Par transitivité de l'égalité, $B_1 = B_2$, une telle partie est donc unique, c'est $\varnothing$.

Commentaires : *Ce type de raisonnement est le même que pour montrer que le neutre d'une loi commutative, s'il existe, est unique.*

$\varnothing$ est donc le seul élément neutre pour la loi $\triangle$.

4 $A \triangle A' = \varnothing \iff A \cup A' = A \cap A' \iff A = A'$. De même pour $A' \triangle A$ par commutativité.

En conclusion, $A \triangle A' = A' \triangle A = \varnothing$ si, et seulement si $A = A'$.

Commentaires : *On pouvait également des tables d'appartenance mais à condition d'expliquer ce que cela voulait dire.*

Exercice I (Avec les fonctions indicatrices) :

1 On rappelle que deux ensembles X etY sont égaux si et seulement si ils ont même fonction indicatrice :

$$X = Y \iff \mathbb{1}_X = \mathbb{1}_Y$$

On raisonne donc sur les fonctions indicatrices. D'une part :

$$\begin{aligned}
\mathbb{1}_{A \triangle B} &= \mathbb{1}_{(A \cup B) \backslash (A \cap B)} && \text{par définition de } A \triangle B \\
&= \mathbb{1}_{A \cup B} - \mathbb{1}_{A \cap B} && \text{fonction indicatrice de la différence} \\
&= \mathbb{1}_A + \mathbb{1}_B - 2 \times \mathbb{1}_{A \cap B} && \text{fonction indicatrice de l'union et de l'intersection}
\end{aligned}$$

D'autre part :

$$\begin{aligned}
\mathbb{1}_{(A \backslash B) \cup (B \backslash A)} &= \mathbb{1}_{A \backslash B} + \mathbb{1}_{B \backslash A} - \mathbb{1}_{(A \backslash B) \cap (B \backslash A)} && \text{fonction indicatrice de l'union} \\
&= \mathbb{1}_A - \mathbb{1}_B + \mathbb{1}_B - \mathbb{1}_A - (\mathbb{1}_A - \mathbb{1}_B)(\mathbb{1}_B - \mathbb{1}_A) \\
&= (\mathbb{1}_A)^2 + (\mathbb{1}_B)^2 - 2 \times \mathbb{1}_{A \cap B} \\
&= \mathbb{1}_A + \mathbb{1}_B - 2 \times \mathbb{1}_{A \cap B}
\end{aligned}$$

On en déduit que :

$$\mathbb{1}_{A \triangle B} = \mathbb{1}_A + \mathbb{1}_B - 2 \times \mathbb{1}_{A \cap B} = \mathbb{1}_{(A \backslash B) \cup (B \backslash A)} \tag{II.1}$$

D'après le rappel, on conclus que $\boxed{A \triangle B = (A \backslash B) \cup (B \backslash A)}$.

2 Soient A, B et C trois parties de E. On calcule à l'aide de l'équation (II.1) :

$$\begin{aligned}\mathbb{1}_{(A\triangle B)\triangle C} &= \mathbb{1}_{A\triangle B} + \mathbb{1}_C - 2\times \mathbb{1}_{A\triangle B}\cdot \mathbb{1}_C\\ &= \mathbb{1}_A + \mathbb{1}_B - 2\times \mathbb{1}_A\mathbb{1}_B + \mathbb{1}_C - 2\left(\mathbb{1}_A + \mathbb{1}_B - 2\times \mathbb{1}_A\mathbb{1}_B\right)\mathbb{1}_C\\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\left(\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C + \mathbb{1}_B\mathbb{1}_C\right) + 4\times \mathbb{1}_A\mathbb{1}_B\mathbb{1}_C.\end{aligned}$$

Le même calcul donne également :

$$\mathbb{1}_{A\triangle(B\triangle C)} = \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\left(\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C + \mathbb{1}_B\mathbb{1}_C\right) + 4\times \mathbb{1}_A\mathbb{1}_B\mathbb{1}_C$$

De l'égalité des fonctions indicatrices, on conclut : $\boxed{(A\triangle B)\triangle C = A\triangle(B\triangle C)}$

3 Par analyse-synthèse :

Analyse : Soit X une partie de E telle que : $\forall A \in \mathcal{P}(E),\ A\triangle X = A$.

Soit $A \in \mathcal{P}(E)$:

$$\begin{aligned}A\triangle X = A &\iff \mathbb{1}_{A\triangle X} = \mathbb{1}_A.\\ &\iff \mathbb{1}_A + \mathbb{1}_X - 2\times \mathbb{1}_A\cdot\mathbb{1}_X = \mathbb{1}_A\\ &\iff \mathbb{1}_X - 2\times \mathbb{1}_A\cdot\mathbb{1}_X = 0\end{aligned}$$

Or cette égalité doit être vraie pour toute partie A de E ; en particulier, pour $A = E$, on a $\mathbb{1}_E = 1$ et on obtient :

$$\mathbb{1}_X - 2\times\mathbb{1}_E\cdot\mathbb{1}_X = 0 \iff \mathbb{1}_X = 0$$

On en déduit que si une telle partie X existe, alors nécessairement $X = \varnothing$.

Synthèse : Posons $X = \varnothing$:

$$\forall A \in \mathcal{P}(E),\quad \mathbb{1}_{A\triangle X} = \mathbb{1}_A + \mathbb{1}_X - 2\mathbb{1}_A\mathbb{1}_X = \mathbb{1}_A$$

Conclusion : $\boxed{\text{l'unique partie X de E vérifiant } \forall A\in\mathcal{P}(E),\ A\triangle X = A \text{ est l'ensemble vide.}}$

4 Encore une fois, par analyse synthèse, montrons que :

$$\forall A \in \mathcal{P}(E), \exists! A' \in \mathcal{P}(E),\quad A\triangle A' = X = \varnothing$$

Soit A une partie de E.

Analyse : soit A' une partie de E vérifiant $A\triangle A' = \varnothing$. Cela se traduit en terme de fonction indicatrice :

$$\begin{aligned}\mathbb{1}_{A\triangle A'} = \mathbb{1}_X = 0 &\iff \mathbb{1}_A + \mathbb{1}_{A'} - 2\times\mathbb{1}_A\mathbb{1}_{A'} = 0\\ &\iff \forall x\in E,\quad \mathbb{1}_A(x) + \mathbb{1}_{A'}(x) - 2\times\mathbb{1}_A(x)\mathbb{1}_{A'}(x) = 0\\ &\iff \forall x\in E,\quad \mathbb{1}_A(x) + \mathbb{1}_{A'}(x) = 2\times\mathbb{1}_A(x)\mathbb{1}_{A'}(x)\end{aligned}$$

On a alors :

- Si $x \in A$, alors $\mathbb{1}_A(x) = 1$ et donc $\mathbb{1}_{A'}(x) = 1$
- Si $x \notin A$, alors $\mathbb{1}_A(x) = 0$ et donc $\mathbb{1}_{A'}(x) = 0$

On en déduit que nécessairement $A' = A$.

Synthèse. On vérifie que $A\triangle A = \varnothing$ directement par la définition :

$$A \triangle A = (A \cup A) \setminus (A \cap A) = A \setminus A = \varnothing$$

Conclusion : $\boxed{\text{A}' = \text{A est l'unique partie de E telle que } A \triangle A' = A' \triangle A = X.}$

Exercice 2 :

Partie I : Théorème de Bézout

1 Pour $m = \pm 1$ suivant le signe de a et $n = 0$, $\mathcal{G}$ contient $|a| > 0$. C'est donc une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément $d = au + bv$.

Commentaires : *À cause de leur signe, il n'était nullement garanti que a ou b appartiennent à $\mathcal{G}$.*

2 (a) Par définition de d, $\exists\ (u\,;v) \in \mathbb{Z}^2$ tel que $d = au + bv$.

Par compatibilité de la division avec les combinaisons linéaires entières tout diviseur de a et b divise d. En particulier le plus grand :

$$\text{pgcd}\,(a\,;b) \mid d.$$

(b) Montrons que d divise a.

La division euclidienne de a par d s'écrit $a = dq + r$ avec $0 \leqslant r < d$.

$$\begin{aligned} \text{D'où, } r &= a - dq \\ r &= a - (au + bv)q \\ r &= a(1 - uq) + b(-vq). \end{aligned}$$

Donc $r \in \mathcal{G}$ et $r < d$. Cette condition ne peut être remplie sans contredire la définition de d que si $r = 0$ *i.e.* $d|a$.

Par le même raisonnement, on montre que $d|b$.

Le nombre d est donc un diviseur de a et b. C'est un diviseur de $\text{pgcd}\,(a\,;b)$.

3 D'après les deux questions précédentes, $d = \text{pgcd}\,(a\,;b)$ ce qui est exactement le résultat demandé :

$$\exists\ (u\,;v) \in \mathbb{Z}^2,\ au + bv = \text{pgcd}\,(a\,;b)\,.$$

4 Le sens direct est exactement le résultat précédent dans le cas où $\text{pgcd}\,(a\,;b) = 1$.

Réciproquement, s'il existe deux entiers (relatifs) u et v tels que $au + bv = 1$ alors tout diviseur de a et b divise nécessairement 1. C'est donc 1 et $\text{pgcd}\,(a\,;b) = 1$: les entiers a et b sont premiers entre eux.

En conclusion, deux entiers relatifs a et b sont premiers entre eux si, et seulement si il existe deux entiers (relatifs) u et v tels que $au + bv = 1$.

Commentaires : *Le théorème de Bézout ne porte pas sur la combinaison linéaire mais sur l'existence du couple $(u\,;v)$.*

5 Appliquons l'algorithme d'Euclide :

$$\begin{aligned} 59 &= 27 \times 2 + \boxed{5} \\ 27 &= 5 \times 5 + \boxed{2} \\ 5 &= 2 \times 2 + \boxed{1} \end{aligned} \quad \Longrightarrow \quad \begin{aligned} \boxed{1} &= 5 - 2 \times \boxed{2} \\ &= 5 - 2 \times (27 - 5 \times 5) \\ &= 11 \times \boxed{5} - 2 \times 27 \\ &= 11 \times (59 - 27 \times 2) - 2 \times 27 \\ 1 &= 11 \times 59 - 24 \times 27. \end{aligned}$$

D'après la question précédente, 27 et 59 sont premiers entre eux et le couple $(u\,;v) = (-24\,;11)$ convient.

Partie II : Applications

1 **Le théorème de Gauss :** Avec le théorème de Bézout, la démonstration est simple. On traduit l'énoncé et on observe :

- Comme $a|bc$, il existe $k \in \mathbb{Z}$ tel que $bc = ka$.
- Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = 1$.
- En multipliant par c, on a :

$$acu + (bc)v = c \iff a(cu + kv) = c.$$

Donc a divise c.

2

$$59x + 27y = 3. \tag{E}$$

a) On sait déjà que $11 \times 59 - 24 \times 27 = 1$. Il suffit de multiplier les deux membres de l'équation par ... 3.

Donc, $(x_0\,; y_0) = (33\,; -72)$ est solution de (E).

b) Tout couple $(x\,; y)$ solution de (E) vérifie $59x + 27y = 3$.

En retranchant l'équation $59x_0 + 27y_0 = 3$ membre à membre à la précédente, on obtient :

$$59(x - 33) + 27(y + 72) = 0.$$

c) D'après la question précédente, tout couple $(x\,; y)$ solution de (E), vérifie :

$$59(x - 33) = -27(y + 72).$$

Comme 59 divise $27(y + 72)$ tout en étant premier avec 27, le thorème de Gauss affirme que 59 divise $y + 72$:

$$\exists\, k \in \mathbb{Z},\ y = -72 + 59k.$$

En substituant dans l'équation précédente, on obtient alors :

$$x = 33 - 27k.$$

Les couples cherchés sont donc de la forme :

$$(33-27k\,;-72+59k)\,,\ k\in\mathbb{Z}.$$

On vérifiera que de tels points sont effectivement solution de l'équation. Ce sont les points à coordonnées entières de la droite passant par le point $(33\,;-72)$ et de vecteur directeur $\begin{pmatrix}-27\\59\end{pmatrix}$.

Commentaires : *Remarquez bien que le paramètre k est le même dans les deux coordonnées.*