L'identité de Bezout pour les nombres entiers

La preuve du théorème des noyaux et donc du théorème de décomposition primaire repose sur l'*identité de Bezout*[1] *pour les polynômes* qui est démontrée dans l'annexe A du polycopié du premier semestre (page 129).

Dans ce document nous expliquons l'identité de Bezout pour les nombres entiers (qui est plus simple). Elle s'énonce de la façon suivante : *Soient a et b sont deux éléments non nuls de $\mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que $ax + by = 1$.*

Par exemple 8 et 15 sont premiers entre eux et on peut écrire 1 sous la forme $2 \cdot 8 - 1 \cdot 15 = 1$.

Rappelons que, par définition, $a, b \in \mathbb{Z}$ sont *premiers entre eux* si les seuls diviseurs communs de a et b sont ± 1 : si $d \in \mathbb{N}$ divise a et b (i.e. $\frac{a}{d}$ et $\frac{b}{d}$ sont des entiers), alors $d = \pm 1$. est un entier) et d divise b, alors $d = \pm 1$.

Pour démontrer l'identité de Bezout, on suppose d'abord que $a, b \in \mathbb{Z}$ sont premiers entre eux et on considère le sous-ensemble $\mathcal{I} \subset \mathbb{Z}$ défini de la façon suivante :

$$\mathcal{I} = \{z \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} \text{ tels que } z = ax + by\} \subset \mathbb{Z},$$

et on note

$$m = \min(\mathcal{I} \cap \mathbb{N})$$

le plus élément positif de $\mathcal{I}$. Nous affirmons que m divise a. Pour le voir, on écrit la division euclidienne de a par m :

$$a = qm + r, \quad \text{avec } q, r \in \mathbb{Z} \text{ et } 0 \leq r < m.$$

Puisque m est un élément de $\mathcal{I}$, on peut trouver $x, y \in \mathbb{Z}$ tels que $m = ax + by$, on a donc

$$r = a - qm = a - q(ax + by) = (1 - qx)a - (qy)b,$$

ce qui prouve que $r \in \mathcal{I}$. Mais puisque $0 \leq r < m$ et m est l'élément minimal de $\mathcal{I} \cap \mathbb{N}$, on doit avoir $r = 0$. Cela montre que $a = qm$, i.e. m est un diviseur de a. De la même manière, on prouve que m est un diviseur de b. Or nous avons supposé que a et b sont premiers entre eux, par conséquent $m = 1$. On a prouvé que $1 \in \mathcal{I}$, par conséquent il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$ et on a démontré une direction de l'identité de Bezout.

L'implication inverse se prouve par l'absurde. Supposons que $ax + by = 1$ mais que a et b ne sont pas premiers entre eux. Alors il existe un entier $d \geq 2$ et $u, v \in \mathbb{Z}$ tels que $a = du$ et $b = dv$. On a donc

$$1 = ax + by = dux + dvy = d(ux + vy),$$

ce qui est absurde car 1 ne peut pas être un multiple de $d \geq 2$.

L'identité de Bezout se généralise sans difficulté à une famille de n entiers : *Des entiers non nuls $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ sont premiers entre eux si et seulement si il existe $x_1, x, \ldots, x_n \in \mathbb{Z}$ tels que $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1$.*

1. Etienne Bezout, 1730–1783.