Remarque sur $\mathrm{pgcd}(X^n - 1, X^m - 1) = X^{\mathrm{pgcd}(n,m)} - 1$

Jean-François Burnol, 22 octobre 2017

Voici une approche complète, rapide (ne nécessitant pas de récurrence), et explicite, qui fonctionne sur $\mathbf{Z}[X]$.

Théorème 1. *Soit* $n, m \in \mathbf{N}$. *L'idéal* $(X^n - 1, X^m - 1)$ *de* $\mathbf{Z}[X]$ *est principal et engendré par* $X^{\mathrm{pgcd}(n,m)} - 1$.

Preuve. Notons $d = \mathrm{pgcd}(n, m)$. En particulier si $n = m = 0$ et seulement dans ce cas on a $d = 0$.

Rappelons en préliminaire l'identité remarquable

$$X^{ki} - 1 = (X^i - 1) \sum_{j=0}^{k-1} X^{(k-1-j)i} \tag{1}$$

qui joue évidemment un rôle important.

Si $d = n$ alors n divise m, donc $X^n - 1$ divise $X^m - 1$ et l'idéal $(X^n - 1, X^m - 1)$ est engendré par $X^n - 1 = X^d - 1$. De même si $d = m$.

On peut donc supposer $1 \leqslant d < n \neq m$. Partons d'une identité de Bézout, par exemple celle fournie par l'algorithme d'Euclide étendu, on a $d = um + vn$ avec u et v des entiers relatifs non nuls, de signes opposés. Supposons par exemple $v > 0$, alors on pose $N = vn > 0$, $M = -um > 0$ et donc $N - M = d$. La preuve qui suit serait similaire si c'était u qui était négatif (on pourrait d'ailleurs aussi rendre u positif en lui ajoutant n et v négatif en lui retirant m, par exemple $-1 \times 5 + 2 \times 3 = 2 \times 5 + (2 - 5) \times 3 = 2 \times 5 - 3 \times 3$).

Ainsi $N = M + d$ et on sort de son chapeau :

$$X^d - 1 = (X^N - 1) - X^d \cdot (X^M - 1) \tag{2}$$

Comme $X^m - 1$ divise $X^M - 1$ dans $\mathbf{Z}[X]$ et $X^n - 1$ divise $X^N - 1$, ceci prouve (de manière complètement explicite si l'on veut avec (1)) que $X^d - 1$ est dans l'idéal engendré dans $\mathbf{Z}[X]$ par $X^m - 1$ et $X^n - 1$.

Comme réciproquement $X^m - 1$ et $X^n - 1$ sont dans l'idéal engendré par $X^d - 1$, c'est donc que ce dernier est bien un générateur de $(X^n - 1, X^m - 1)$. □

L'équation (2) est si triviale que je me dis que j'ai dû délirer en imaginant qu'on me démontre Théorème 1 différemment d'habitude.