Pas de titre

Emmanuel Vieillard-Baron[1], Alain Soyeur[2], and François Capaces[3]

[1]Enseignant en CPGE, Lycée Kléber, Strasbourg
[2]Enseignant en CPGE, Lycée Pierre de Fermat, Toulouse
[3], ,

21 janvier 2022

Exercice 0.1 ★★★ ***Pas de titre***

Soit n et m deux entiers naturels.

1. *Démontrer que si $d \mid n$ alors $X^d - 1 \mid X^n - 1$.*
2. *On pose $n = mq + r$ à la faveur d'une division euclidienne. Démontrer que $X^n - 1 \wedge X^m - 1 = X^m - 1 \wedge X^r - 1$.*
3. *Démontrer que $X^n - 1 \wedge X^m - 1 = X^{n \wedge m} - 1$.*
4. *Soit a un entier naturel. Démontrer que $a^n - 1 \wedge a^m - 1 = a^{n \wedge m} - 1$.*
5. *Montrer que si a et b sont deux entiers premiers entre eux alors $\forall\, P \in \mathbb{K}[X], (P^a - 1).(P^b - 1)$ divise $(P - 1).(P^{ab} - 1)$.*

Solution :

1. *On écrit $n = dk$ et on a immédiatement $X^n - 1 = \left(X^d\right)^k - 1 = \left(X^d - 1\right)\left(1 + X^d + X^{2d} + \ldots + X^{d(k-1)}\right)$ ce qui permet de conclure.*
   Sinon on écrit $X^d - 1 = \prod_{m=0}^{d-1} \left(X - \exp\left(\frac{2i\pi km}{n}\right)\right)$. Cela veut dire que toutes les racines de $X^d - 1$ sont aussi racines de $X^n - 1$. Cela veut dire que $X^n - 1$ est divisible par chacun des $X - \exp\left(\frac{2i\pi km}{n}\right)$ donc par leur produit puisque toutes ces racines sont notoirement distinctes.
2. *On écrit $X^n - 1 = X^{mq+r} - X^r + X^r - 1 = X^r\left(X^{mq} - 1\right) + X^r - 1 = X^r\left(X^m - 1\right)\left(1 + X^m + X^{2m} + \ldots + X^{m(q-1)}\right) + X^r - 1$. Comme $\deg X^r - 1 = r < m = \deg X^m - 1$ on en déduit que $X^r - 1$ est le reste et $X^r\left(1 + X^m + X^{2m} + \ldots + X^{m(q-1)}\right)$ est le quotient. Par application de l'algorithme d'Euclide, on en déduit $X^n - 1 \wedge X^m - 1 = X^m - 1 \wedge X^r - 1$.*
3. *On effectue en parallèle l'algorithme d'Euclide pour n et m d'une part, et pour $X^n - 1$ et $X^m - 1$ d'autre part. Dans le premier cas on appelle $r_0, r_1, \ldots, r_p, 0$ la suite des restes. D'après le résultat précédent, la suite des restes pour $X^n - 1$ et $X^m - 1$ est $X^{r_0} - 1, X^{r_1} - 1, \ldots, X^{r_p} - 1, 0$. Dans les deux cas le PGCD est le dernier reste non nul. On en déduit bien que $X^n - 1 \wedge X^m - 1 = X^{r_p} - 1$ avec $r_p = n \wedge m$. Ce qu'il fallait démontrer.*

4. *On peut parfaitement appliquer la méthode précédente.*
5. *On va commencer par démontrer le résultat pour $P = X$. On sait que $X^a - 1$ divise $X^{ab} - 1$ soit $X^{ab} - 1 = Q_1 (X^a - 1)$. De même $X^{ab} - 1 = Q_2 \left(X^b - 1\right)$. Or on sait aussi que le PGCD de $X^a - 1$ et $X^b - 1$ égale $X - 1$. Donc on peut écrire $X^a - 1 = (X - 1)Q_3$ et $X^b - 1 = (X - 1)Q_4$ avec $Q_3 \wedge Q_4 = 1$. Donc on a $Q_1 Q_3 = Q_2 Q_4$. Q_3 divise $Q_2 Q_4$ et $Q_3 \wedge Q_4 = 1$, donc d'apès le lemme de Gauss, Q_3 divise Q_2. Autrement dit $Q_2 = Q_3 D$. Résumons-nous : $\left(X^{ab} - 1\right)(X - 1) = Q_3(X - 1)DQ_4(X - 1) = D(X)\left(X^a - 1\right)\left(X^b - 1\right)$. En toute généralité, on a $\left(P^{ab} - 1\right)(P - 1) = D(P(X))\left(P^a - 1\right)\left(P^b - 1\right)$. Ce qu'il fallait démontrer.*

Références