Le groupe des unités de $A[X]$.

Bruno Winckler

Je m'intéresse aux polynômes inversibles d'un anneau $A[X]$, où A est un anneau commutatif quelconque. Dans le cas où A est intègre, il est relativement connu que les inversibles de $A[X]$ sont exactement les polynômes constants, de coefficient inversible. En d'autres termes, $A[X]^* = A^*$. Si A n'est plus intègre, il y a bien plus d'éléments inversibles ; par exemple, pour $A = \mathbb{Z}/4\mathbb{Z}$, le polynôme $2X+1$ est inversible, d'inverse $2X+1$, comme un calcul direct le prouve. Je propose de décrire $A[X]^*$ dans le cas général :

Proposition 1 *Soit $P = \sum_{i=0}^n a_i X^i \in A[X]$. Alors P est inversible si, et seulement si a_0 est inversible, et $a_1, \ldots, a_n$ sont nilpotents.*

Je rappelle qu'un élément a d'un anneau R est nilpotent si, élevé à une certaine puissance, il égale 0. Par exemple, 2 est nilpotent dans $\mathbb{Z}/4\mathbb{Z}$: $2^2 = 0$.

Preuve. Je commence par prouver que si a_0 est inversible et $a_1, \ldots, a_n$ sont nilpotents, alors P est inversible. Ceci découle du lemme suivant, valable en toute généralité :

Lemme 2 *Dans un anneau commutatif R, la somme d'un élément inversible et d'un élément nilpotent est un élément inversible.*

Preuve du lemme 2. Soit u un élément inversible, et n un élément nilpotent ; on a donc $n^p = 0$ pour un certain $p \in \mathbb{N}^*$. Alors :

$$(u+n)\left(u^{-1}\sum_{k=0}^{p-1}(-u^{-1}n)^k\right) = u(1-(-u^{-1}n))\left(u^{-1}\sum_{k=0}^{p-1}(-u^{-1}n)^k\right) = 1-(-u^{-1}n)^p = 1,$$

car $(-u^{-1}n)^p = (-u^{-1})^p n^p = 0$ dans un anneau commutatif. Bref, $u+n$ est inversible, d'inverse $\left(u^{-1}\sum_{k=0}^{p-1}(-u^{-1}n)^k\right)$.

Alors, dans notre contexte, a_0 est inversible et a_1X nilpotent, donc $a_0 + a_1X$ est inversible, et de la même manière $a_0 + a_1X + a_2X^2$ est inversible, *etc.*, pour finalement en déduire que P est inversible.

Réciproquement, soit P un polynôme inversible ; il existe donc Q un polynôme à coefficients dans A tel que $PQ = 1$. Écrivons $Q = \sum_{i=0}^m b_i X^i$. Alors, en comparant les coefficients de X^i dans PQ et 1, on trouve :

$$a_0 b_0 = 1 \tag{1}$$

$$\forall i \geq 1, \sum_{k=0}^{i} a_k b_{i-k} = 0, \tag{2}$$

avec la convention traditionnelle que a_k est nul si k dépasse le degré de P, et de même pour les b_k. La première égalité me montre que a_0 est inversible (et b_0 également). Si je regarde l'équation (2) pour $i = n+m$, $a_n b_m = 0$. Et pour $i = n+m-1$, on obtient $a_n b_{m-1} + a_{n-1} b_m = 0$. Si je multiplie cette dernière égalité par a_n, j'obtiens, toujours en gardant à l'esprit que $a_n b_m = 0$:

$$a_n^2 b_{m-1} + a_{n-1}(a_n b_m) = 0 \Leftrightarrow a_n^2 b_{m-1} = 0.$$

De la même manière, je trouve $a_n^3 b_{m-2} = 0$, et ainsi de suite, je trouve $a_n^l b_{m-l+1} = 0$ pour tout l : sachant que $a_n^j b_{m-j+1} = 0$ pour tout $j \leq l$, j'ai juste à multiplier l'égalité (2) par a_n^l pour avoir le résultat au rang $j = l+1$. Une récurrence soignée serait la bienvenue...

Bref, je finis par avoir $a_n^{m+1} b_0 = 0$, d'où, en multipliant par a_0 (qui est l'inverse de b_0) : $a_n^{m+1} = 0$, donc a_n est nilpotent.

Pour montrer que a_{n-1} est nilpotent également, j'applique le raisonnement précédent à $P - a_n X^n$: c'est possible, car P étant inversible et $a_n X^n$ nilpotent, $P - a_n X^n$ est également inversible. Par récurrence sur le degré de P que je vous laisse rédiger, on obtient que a_{n-1} est nilpotent, et plus généralement que a_k l'est pour tout k supérieur à 1. $\square$