Exercice 3

On va montrer que $\bar{x} \in K[x,y,z,w]/(xy-zw)$ est irréductible. Ceci revient à ce que s'il existe des polynômes $f,g,h \in K[x,y,z,w]$ tels que

$$fg = x + (xy - zw)h \tag{0.1}$$

alors on a aussi $c \in K, c \neq 0$ tel que

$$f \equiv c \pmod{xy-zw} \text{ et } g \equiv c^{-1}x \pmod{xy-zw}$$

ou l'inverse.

Pour ceci on va utiliser une récurrence sur la somme des degrés $\deg(f)+\deg(g)$. On rappelle que le degré d'un monôme $cx^\alpha y^\beta z^\gamma w^\delta$, $c \neq 0$ est $\alpha+\beta+\gamma+\delta$ et le degré d'un polynôme est le plus haut degré d'un monôme non nul.

Tout d'abord, vu que $(xy-zw)h$ n'a que des termes de degré au moins 2 on déduit de (0.1) que l'on peut supposer que l'on a $f = 1 + f_1$ et $g = x + g_1$ où f_1, g_1 n'ont que des termes de degré au moins 2. On veut montrer que $(xy-zw)$ divise f_1 et g_1 : c'est clair si l'un des deux est nul.

On suppose maintenant que $\deg(f)+\deg(g) = d \geq 2$ et que le résultat est connu pour tous les p,q tels que $\deg(p)+\deg(q) < d$. Soient A_f, A_g les termes de plus haut degrés de f_1 et g_1 respectivement et $f_2 = f_1 - A_g$, $g_2 = g_1 - A_g$. On a :

$$fg = x + g_2 + xf_2 + A_f g_2 + A_g f_2 + A_f A_g$$

On voit que $A_f A_g$ est le terme de plus haut degré à droite (en effet, vu que l'on a supposé $\deg(f), \deg(g) \geq 2$ les autermes sont de degrés au plus $\deg(f)+\deg(g)-1$). Comme $(xy-zw)$ divise $fg-x$ et est homogène il divise aussi son terme de plus haut degré (si $fg - x = (xy-zw)h$ et A_h est le terme de plus haut degré de h alors $A_g A_f = (xy-zw)A_h$). Comme $xy-zw$ est premier dans $K[x,y,z,w]$ il divise A_f ou A_g. Supposons qu'il divise A_f ; on pose alors $p = f - A_f$ et $q = g$ et il vient :

$$pq = fg - A_f g \equiv fg \pmod{xy-zw}$$

et vu que $\deg(p) < \deg(f)$ et donc $\deg(p)+\deg(q) < d$ il suit par l'hypothèse de récurrence il suit qu'il existe h_p, h_q tels que $p = 1 + (xy-zw)h_p$ et $q = x + (xy-zw)h_q$, puis que f, g sont aussi de cette forme. Si $(xy-zw) | A_g$ on procède de la même manière.

Exercice 7

1. On va démontrer ceci par récurrence. Pour $k = 0$ on a

$$(1+p)^{p^0} = 1 + p$$

et l'énoncé est donc vrai (avec $x = 1$).

Supposons maintenant que $k \geq 0$ et que l'on ait $(1+p)^{p^k} = 1 + p^{k+1}x$ avec $p \not| x$. On a $(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p$ et il suit que :

$$\begin{aligned}
(1+p)^{p^{k+1}} &= (1+p^{k+1}x)^p \\
&= \sum_{l=0}^{p} \binom{p}{l} p^{l(k+1)} x^l \\
&= 1 + p^{k+2} \sum_{l=1}^{p} \frac{1}{p}\binom{p}{l} p^{(l-1)(k+1)} x^l
\end{aligned}$$

Comme p divise $\binom{p}{l}$ pour $1 \leq l \leq p-1$ on voit que :

$$x' = \sum_{l=1}^{p} \frac{1}{p}\binom{p}{l} p^{(l-1)(k+1)} x^l$$

est bien un entier. Il reste à voir que $p \not| x'$ pour terminer la démonstration de l'étape de récurrence. Pour ceci on écrit :

$$\begin{aligned} x' &= \frac{1}{p}\binom{p}{1}x^l + \sum_{l=2}^{p}\frac{1}{p}\binom{p}{l}p^{(l-1)(k+1)}x^l \\ &= x^l + p^k\sum_{l=2}^{p}\binom{p}{l}p^{(l-2)(k+1)}x^l \end{aligned}$$

(si $k = 1$ la somme est nulle). Comme p ne divise pas x^l mais par contre divise la somme il suit que p ne divise pas x'.

2. Tout d'abord on a bien $1 + p \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ vu qu'il n'est pas divisible par p et donc premier à p^k (exercice : écrire une relation de Bézout explicite entre les deux).

Soit π le morphisme d'anneaux $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ défini par

$$\pi(x + p^m\mathbb{Z}) = x + p\mathbb{Z}$$

et ϕ le morphisme de groupes $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ obtenu en restreignant π. Ona $\ker(\phi) = \pi^{-1}(\{1\})$ et donc $\ker(\phi) = 1 + \ker(\pi)$ [1]. Le cardinal de $\ker(\pi)$ vaut

$$|\ker(pi)| = \frac{|\mathbb{Z}/p^m\mathbb{Z}|}{|\mathbb{Z}/p\mathbb{Z}|} = p^{m-1}$$

et il suit par le théorème de Lagrange que $1 + p$ est d'ordre divisant p^{m-1}, c'est-à-dire d'ordre p^k pour un $0 \leq k \leq m - 1$. D'autre part d'après la question 1. on a que p^m ne divise pas $(1 + p)^{p^k} - 1$ si $k \leq m - 2$. Il suit que $(1 + p)$ ne peut pas être d'ordre $1, p, \ldots, p^{m-2}$ et il est donc forcément d'ordre p^{m-1}.

1. Attention : le noyau à gauche est un noyau d'un morphisme de groupes $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, et à droite celui d'un morphisme d'anneaux $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ qui coïncident en tant qu'ensembles.