## Partie *I*

*Calculs en caractéristique p*

**I.1**) Si $0 < i < p$ alors $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$, $i\binom{p}{i} = p\binom{p-1}{i-1}$, donc $p$ divise $i\binom{p}{i}$, or il est premier avec $i$ car $0 < i < p$ et $p$ est premier, donc d'après le théorème de Gauss $p$ divise $\binom{p}{i}$.

**I.2**) Ecrivons la formule du binôme :

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i}.x^i y^{p-i} = \sum_{i=0}^{p} (\binom{p}{i}.1_{\mathbb{K}})x^i y^{p-i} = x^p + y^p,$$

car pour $1 \leq i < p$ : $\binom{p}{i}.1_{\mathbb{K}} = 0$.

En écrivant $(x+y)^{p^n} = \left((x+y)^{p^{n-1}}\right)^p$, on prouve par récurrence sur l'entier $n$ que

$$\forall (x,y) \in \mathbb{K}^2 (x+y)^{p^n} = x^{p^n} + y^{p^n}.$$

D'autre part le petit théorème de Fermat nous dit que pour tout entier $m$, $m^p \equiv m \bmod p$, et par itération $m^{p^n} \equiv m \bmod p$. Donc, pour tout élément $a$ de $\mathbb{F}_p$ et tout entier $n$ : $a^{p^n} = a$.

Si maintenant $R = \sum_{i=0}^{d} a_i X^i$ est un élément de $\mathbb{F}_p[X]$, alors pour tout entier $n$ et tout élément $x$ de $\mathbb{K}$ :

$$\begin{aligned}
(R(x))^{p^n} &= \left(\sum_{i=0}^{d} a_i x^i\right)^{p^n} \\
&= \sum_{i=0}^{d} \left(a_i x^i\right)^{p^n} \\
&= \sum_{i=0}^{d} (a_i)^{p^n} \left(x^i\right)^{p^n} \\
&= \sum_{i=0}^{d} a_i \left(x^{p^n}\right)^i \\
(R(x))^{p^n} &= R(x^{p^n})
\end{aligned}$$