DM n°1 (année 2023/2024) - corrigé

Exercice 1. (1) On a $\sigma(0)=0$ et $\sigma(1)=1$. Par ailleurs, on a $\sigma(n+1)=\sigma(n)+\sigma(1)=\sigma(n)+1$ pour tout $n\in\mathbf{N}$: par récurrence, on a $\sigma(n)=n$ pour tout $n\in\mathbf{N}$. Si $n\in\mathbf{Z}_{<0}$, on a $-n\in\mathbf{N}$, d'où $-\sigma(n)=\sigma(-n)=-n$ *i.e.* $\sigma(n)=n$. Enfin, si $r\in\mathbf{Q}$, il existe $d\in\mathbf{N}_{>0}$ tel que $dr\in\mathbf{Z}$. On a alors $dr=\sigma(dr)=\sigma(d)\sigma(r)=d\sigma(r)$ en vertu de ce qui précède, et donc $\sigma(r)=r$.
(2) Si $x\in\mathbf{R}_{>0}$, on a $x=(\sqrt{x})^2$, donc $\sigma(x)=\sigma(\sqrt{x})^2\in\mathbf{R}_{\geq 0}$ (un carré est positif dans $\mathbf{R}$). Comme $x\neq 0$, on a en outre $\sigma(x)\neq 0$ (parce que σ est un automorphisme), et donc $\sigma(x)>0$.
(3) Si $x_1<x_2$ sont des réels, on a $x_2-x_1>0$, d'où $\sigma(x_2)-\sigma(x_1)=\sigma(x_2-x_1)>0$ (*cf* question précédente), soit encore $\sigma(x_2)>\sigma(x_1)$: l'application σ est donc strictement croissante.
(4) Soit $x\in\mathbf{R}$. Si $N\in\mathbf{N}$, on a $\lfloor 2^N x\rfloor\leq 2^N x<\lfloor 2^N x\rfloor+1$, d'où $\lfloor 2^N x\rfloor\leq\sigma(2^N x)<\lfloor 2^N x\rfloor+1$ (*cf* questions (1) et (3)). Comme $\sigma(2^N x)=2^N\sigma(x)$, il en résulte que $\frac{\lfloor 2^N x\rfloor}{2^N}\leq\sigma(x)<\frac{\lfloor 2^N x\rfloor+1}{2^N}$, soit encore $\left|\sigma(x)-\frac{\lfloor 2^N x\rfloor}{2^N}\right|<\frac{1}{2^N}$. Comme $\lim\limits_{N\to\infty}\frac{\lfloor 2^N x\rfloor}{2^N}=x$, on a $\sigma(x)=x$. C'est vrai pour tout $x\in\mathbf{R}$, donc $\sigma=\mathsf{Id}_{\mathbf{R}}$.

Exercice 2. (1) Comme $P(X)=Q(X^p)$, on a $P'(X)=pX^{p-1}Q'(X^p)=0$. Par ailleurs, on a $P=FG$, donc $P'=F'G+FG'$: on en déduit que $FG'=-F'G$. Comme $\mathsf{pgcd}(F,G)=1$, le lemme de Gauss implique que F divise F' : pour des raisons de degré, on a nécessairement $F'=0$. Écrivons $F=\sum\limits_{i\geq 0}a_iX^i$ (avec $a_i=0$ pour $i\gg 0$) : on a $F'=\sum\limits_{i=1}^{d}ia_iX^{i-1}$, et donc $ia_i=0$ pour tout $i\in\mathbf{N}$. Si $p\nmid i$, l'image de i dans K est inversible (elle l'est dans $\mathbf{F}_p$) : cela implique $a_i=0$. Cela montre que $F=\sum\limits_{j\geq 0}a_{pj}X^{pj}=\widetilde{F}(X^p)$ avec $\widetilde{F}=\sum\limits_{j\geq 0}a_{pj}X^j\in K[X]$. De même, G est un polynôme en X^p.
(2) Si $c\in\mathbf{F}_p$, on a $Q(\alpha+c)=(\alpha+c)^p-(\alpha+c)+a$. Comme K est de caractéristique p, on a $(\alpha+c)^p=\alpha^p+c^p$. Par ailleurs, on a $c^p=c$ (Fermat), ce qui montre que $Q(\alpha+c)=\alpha^p+c-(\alpha+c)+a=Q(\alpha)=0$. Les éléments $\alpha+c$ avec $c\in\mathbf{F}_p$ fournissent donc p racines distinctes de Q. Comme $\deg(Q)=p$, ce sont précisément *les* racines de Q.
(3) La question qui précède implique que le polynôme Q est séparable (il a $p=\deg(Q)$ racines distinctes, on pouvait aussi le voir en disant que $Q'=-1$ est premier à Q) et que $K[\alpha]$ est le corps de décomposition de Q dans $\overline{K}$. Cela implique que l'extension $K[\alpha]/K$ est normale et séparable (*i.e.* galoisienne).
(4) Par hypothèse, $\alpha\notin K$: le polynôme minimal $P_{\alpha,K}$ de α sur K est de degré >1. On a $P_{\alpha,K}\mid Q$: il existe $c_0\in\mathbf{F}_p^\times$ tel que $P_{\alpha,K}(\alpha+c_0)=0$. D'après le théorème de prolongement des isomorphismes, il existe un unique K-morphisme $\sigma\colon K[\alpha]\to K[\alpha]$ tel que $\sigma(\alpha)=\alpha+c_0$: si $i\in\mathbf{N}$, on a $\sigma^i(\alpha)=\alpha+ic_0$ (récurrence immédiate), d'où $P_{\alpha,K}(\alpha+ic_0)=P_{\alpha,K}(\sigma^i(\alpha))=\sigma^i\big(P_{\alpha,K}(\alpha)\big)=0$. Comme $c_0\in\mathbf{F}_p^\times$, ic_0 parcourt $\mathbf{F}_p$ quand i parcourt $\mathbf{N}$. Cela implique que $P_{\alpha,K}(\alpha+c)=0$ pour tout $c\in\mathbf{F}_p$, et donc $Q\mid P_{\alpha,K}$, soit encore $P_{\alpha,K}=Q$ vu que $P_{\alpha,K}\mid Q$ et $P_{\alpha,K}$ et Q sont unitaires. Il en résulte que Q est irréductible sur K.
(5) • Supposons $P=FG$ avec $F,G\in K[X]$ premiers entre eux : d'après la question (1), il existe $\widetilde{F},\widetilde{G}\in K[X]$ tels que $F=\widetilde{F}(X^p)$ et $G=\widetilde{G}(X^p)$. On a donc $Q(X^p)=P=\widetilde{F}(X^p)\widetilde{G}(X^p)$, ce qui implique $Q=\widetilde{F}\widetilde{G}$ dans $K[X]$. Comme Q est irréductible sur K en vertu de la question précédente, on a $\widetilde{F}\in K^\times$ ou $\widetilde{G}\in K^\times$, et donc $F\in K^\times$ ou $G\in K^\times$. Si P est réductible sur K, il est donc nécessairement de la forme $P=P_1^m$ avec $m\in\mathbf{N}_{>0}$ et $P_1\in K[X]$ irréductible sur K. On a alors $p^2=\deg(P)=m\deg(P_1)$, et donc $p\mid m$, d'où $a=-P(0)=(-1)^pP_1(0)^m\in K^p$, contredisant l'hypothèse $a\notin K^p$.
• D'après le théorème de prolongement des isomorphismes, le nombre de K-morphismes $K[\beta]\to\overline{K}$ est égal au nombre de racines de P dans $\overline{K}$. Notons $\mathsf{Z}(P)$ (resp. $\mathsf{Z}(Q)$) l'ensemble des racines de P (resp. de Q) dans $\overline{K}$. Le morphisme de Frobenius $\varphi\colon\overline{K}\to\overline{K};x\mapsto x^p$ est un isomorphisme, et si $x\in\overline{K}$, on a $x\in\mathsf{Z}(P)\Leftrightarrow\varphi(x)\in\mathsf{Z}(Q)$. Cela montre que φ induit une bijection $\mathsf{Z}(P)\xrightarrow{\sim}\mathsf{Z}(Q)$. Comme $\#\,\mathsf{Z}(Q)=p$ (*cf* question (2)), on a $\#\,\mathsf{Z}(P)=p$, et le nombre de K-morphismes $K[\beta]\to\overline{K}$ est p.