Corrigé du DM02

Cyclicité de $\mathbb{K}^*$ lorsque $\mathbb{K}$ est un corps fini
Extrait de l'agrégation interne 2023, épreuve 1.

Première partie :

1. Si p est premier et $i \in \mathbb{N}^*$, alors pour tout $k \in [\![1, p^i]\!]$, on a

$$pgcd(k, p^i) = 1 \iff pgcd(k, p) = 1 \iff k \notin p\mathbb{Z},$$

donc

$$\varphi(p^i) = Card\left([\![1, p^i]\!] \setminus \{kp,\ 1 \leq k \leq p^{i-1}\}\right) = p^i - p^{i-1} = p^{i-1}(p-1).$$

On en déduit que pour tout $k \in \mathbb{N}^*$:

$$f(p^k) = \sum_{d \in \mathcal{D}_{p^k}} \varphi(d) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} (p^i - p^{i-1}) = p^k.$$

2. • L'application $P : \begin{cases} \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} & \longrightarrow & \mathcal{D}_{m_1 m_2} \\ (d_1, d_2) & \longmapsto & d_1 d_2 \end{cases}$ est bien définie car

$$(d_1, d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} \implies (d_1 | m_1 \text{ et } d_2 | m_2) \implies d_1 d_2 | m_1 m_2,$$

et ce même si m_1 et m_2 ne sont pas premiers entre eux.

- Etant donnés deux couples (d_1, d_2) et (d_1', d_2') de $\mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$ tels que $d_1 d_2 = d_1' d_2'$, on a $d_1' | d_1 d_2$ et $pgcd(d_1', d_2) = 1$ (puisque $pgcd(d_1', d_2)$ divise d_1' et d_2, donc divise m_1 et m_2 qui sont premiers entre eux), donc d'après le lemme de Gaüss, on a $d_1' | d_1$. Symétriquement $d_1 | d_1'$, donc $d_1' = d_1$ (puisque ce sont des entiers naturels). Et de même, on a $d_2' = d_2$ donc finalement $(d_1', d_2') = (d_1, d_2)$, ce qui montre que l'application P est injective.
- Enfin, étant donné un diviseur $d \in \mathcal{D}_{m_1 m_2}$, il peut s'écrire $d = d_1 d_2$, avec $d_1 | m_1$ et $d_2 | m_2$. En effet, par analyse :

$$d_1 d_2 = d \implies d_1 | m_1 \text{ et } d_1 | d \implies d_1 | pgcd(m_1, d).$$

Testons alors $d_1 = pgcd(m_1, d)$ et $d_2 = \frac{d}{d_1}$.
On a bien $d_1 d_2 = d$, puis $d_1 | m_1$ et enfin, $d_2 | \frac{m_1}{d_1} \times m_2$ (puisque $d | m_1 m_2$) avec
$pgcd(d_2, \frac{m_1}{d_1}) = pgcd(\frac{d}{d_1}, \frac{m_1}{d_1}) = 1$, donc par le lemme de Gaüss, $d_2 | m_2$.
Ainsi, le couple $(d_1, d_2) = (pgcd(m_1, d), \frac{d}{pgcd(m_1, d)})$ est bien un antécédent de d par P, ce qui montre la surjectivité de P.

En définitive, l'application P est bien une bijection de $\mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$ vers $\mathcal{D}_{m_1 m_2}$.

Variante : on peut aussi procéder en utilisant les décompositions primaires de m_1, m_2 et d pour montrer la bijectivité de P, en déterminant directement l'antécédent (d_1, d_2) d'un diviseur quelconque d de $m_1 m_2$, mais c'est plus lourd au niveau des notations : en notant $(p_i)_{i \in \mathbb{N}^*}$ la suite des nombres premiers, on peut écrire

$$m_1 = \prod_{i \in I} p_i^{\alpha_i}, \qquad m_2 = \prod_{j \in J} p_j^{\beta_j},$$

où I et J sont deux parties finies de $\mathbb{N}^*$, et les α_i, β_j des entiers de $\mathbb{N}^*$. Puisque m_1, m_2 sont premiers entre eux, on a $I \cap J = \emptyset$, donc la décomposition primaire de $m_1 m_2$ s'écrit :

$$m_1 m_2 = \prod_{i \in I \cup J} p_i^{\gamma_i},$$

avec $\gamma_i = \alpha_i$ si $i \in I$ et $\gamma_i = \beta_i$ si $i \in J$. Etant donné un diviseur $d \in \mathcal{D}_{m_1 m_2}$, on a

$$d = \prod_{i \in I \cup J} p_i^{\gamma_i'},$$

avec $0 \leq \gamma_i' \leq \gamma_i$ pour tout i.
Puisque tout couple de diviseur $(d_1, d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$ s'écrit

$$(d_1, d_2) = \left(\prod_{i \in I} p_i^{\alpha_i'}, \prod_{i \in J} p_i^{\beta_i'} \right), \qquad 0 \leq \alpha_i' \leq \alpha_i, \quad 0 \leq \beta_i' \leq \beta_i,$$

on en déduit par unicité de la décomposition primaire de d que

$$d = d_1 d_2 \iff \prod_{i \in I \cup J} p_i^{\gamma_i'} = \prod_{i \in I} p_i^{\alpha_i'} \prod_{i \in J} p_i^{\beta_i'} \iff \begin{cases} \forall i \in I, \ \alpha_i' = \gamma_i' \\ \forall i \in J, \ \beta_i' = \gamma_i' \end{cases},$$

ce qui montre que d possède un unique antécédent (d_1, d_2) par P (puisque d_1, d_2 sont uniquement déterminés par les exposants α_i', β_i'), qui est donc une application bijective.

3. Si m_1 et m_2 sont premiers entre eux, alors par définition de f :

$$f(m_1 m_2) = \sum_{d \in \mathcal{D}_{m_1 m_2}} \varphi(d).$$

En utilisant la bijection P, cela se réécrit :

$$f(m_1 m_2) = \sum_{d \in P(\mathcal{D}_{m_1} \times \mathcal{D}_{m_2})} \varphi(d) = \sum_{(d_1, d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}} \varphi(d_1 d_2).$$

Or, les couples (d_1, d_2) de la somme vérifient $pgcd(d_1, d_2) = 1$ (puisque m_1 et m_2 sont premiers entre eux), donc d'après les propriétés de l'indicatrice d'Euler :

$$f(m_1 m_2) = \sum_{(d_1, d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}} \varphi(d_1)\varphi(d_2) = \sum_{d_1 \in \mathcal{D}_{m_1}} \varphi(d_1) \times \sum_{d_2 \in \mathcal{D}_{m_2}} \varphi(d_2) = f(m_1) f(m_2).$$

4. Soit $n \in \mathbb{N}^*$, on considère sa décomposition primaire :

$$n = \prod_{i \in I} p_i^{\alpha_i},$$

avec I une partie finie de $\mathbb{N}^*$, les $(p_i)_{i \in I}$ des nombres premiers distincts et les α_i dans $\mathbb{N}^*$.
Vu que les $(p_i^{\alpha_i})_{i \in I}$ sont premiers entre eux deux à deux, on a directement d'après la question précédente et la question 1. :

$$f(n) = \prod_{i \in I} f(p_i^{\alpha_i}) = \prod_{i \in I} p_i^{\alpha_i} = n,$$

ce qui permet de conclure que $n = f(n) = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Deuxième partie :

5. L'application $\theta : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \tilde{P} \end{cases}$ est un morphisme d'anneaux car :

- $\theta(1) = \tilde{1} = 1_{\mathbb{K}^{\mathbb{K}}}$, puisque la fonction associée à $P = 1$ est la fonction constante égale à 1.
- Pour tout $(P, Q) \in \mathbb{K}[X]^2$:

$$\theta(P + Q) = (x \mapsto \tilde{P}(x) + \tilde{Q}(x)) = \tilde{P} + \tilde{Q} = \theta(P) + \theta(Q).$$

- Pour tout $(P, Q) \in \mathbb{K}[X]^2$:

$$\theta(PQ) = (x \mapsto \tilde{P}(x)\tilde{Q}(x)) = \tilde{P}\tilde{Q} = \theta(P)\theta(Q).$$

6. Soit $P \in Ker(\theta)$. Alors $\tilde{P}$ est la fonction nulle, c'est-à-dire que tous les éléments $x \in \mathbb{K}$ sont racines de P. Puisque $\mathbb{K}$ est infini, cela implique que P possède une infinité de racines, donc $P = 0$ (en effet, un polynôme non nul possède un degré $d \in \mathbb{N}$, et donc possède au plus d racines, comme on le redémontre par la suite, en question 8.(c)). Ainsi, $Ker(\theta) = \{0\}$ et donc le morphisme θ est injectif.
7. Si $\mathbb{K} = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, alors le polynôme $P = X^2 + \overline{1}$ est non nul (coefficients non nuls), mais sa fonction polynôme associée est nulle, puisque $\tilde{P}(\overline{0}) = \overline{0}^2 + \overline{0} = \overline{0}$ et $\tilde{P}(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{0}$.
Donc θ n'est pas injective (puisqu'on a trouvé un polynôme non nul dans $Ker(\theta)$).
8. (a) Soit $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ non nul. Montrons qu'il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$.
   - **Existence** : Evidente pour $A = 0$ (poser $Q = R = 0$).
     Si $A \neq 0$, on procède par récurrence forte sur $\deg(A)$:
     * le résultat est évident pour $\deg(A) = 0$: il suffit de poser $(Q, R) = (0, A)$ si $\deg(B) > 0$ et $(Q, R) = (A/B, 0)$ si $\deg(B) = 0$ (dans ce cas, B est constant non nul donc c'est un élément inversible du corps $\mathbb{K}$) ;
     * soit $n \in \mathbb{N}$. Supposons le résultat vrai pour tout $A \in \mathbb{K}_n[X]$, et montrons-le pour $A = a_{n+1}X^{n+1} + \cdots + a_0$ avec $a_{n+1} \neq 0$. Notons $p \in \mathbb{N}$ le degré de B et $b_p \neq 0$ son coefficient dominant. Si $p > n + 1$, alors $(Q, R) = (0, A)$ convient.
       Sinon, si $p \leq n + 1$, on pose $\tilde{A} = A - \frac{a_{n+1}}{b_p}X^{n+1-p}B$. Ce polynôme est de degré $\leq n$ (les termes dominants se simplifient), donc par hypothèse de récurrence, il existe $(\tilde{Q}, \tilde{R})$ dans $\mathbb{K}[X]^2$ tels que $\tilde{A} = B\tilde{Q} + \tilde{R}$ et $\deg(\tilde{R}) < p$. Donc finalement :

$$A = \tilde{A} + \frac{a_{n+1}}{b_p}X^{n+1-p}B = B\tilde{Q} + \tilde{R} + \frac{a_{n+1}}{b_p}X^{n+1-p}B = BQ + R,$$

       avec $Q = \tilde{Q} + \frac{a_{n+1}}{b_p}X^{n+1-p}$ et $R = \tilde{R}$ de degré $< p$.

     Remarque
     On comprend bien que cette preuve d'existence ne fonctionne pas dans $C[X]$ lorsque C est seulement un anneau et pas un corps. En effet, il est nécessaire que le coefficient dominant du diviseur B soit inversible pour pouvoir construire le polynôme $\tilde{A}$ et ainsi utiliser l'hypothèse de récurrence.
     Par exemple, dans $\mathbb{Z}[X]$, la division euclidienne de A par B fonctionne à condition que le coefficient dominant de B soit dans $\mathbb{Z}^\times = \{-1, 1\}$: dans ce cas, il existe $(Q, R) \in \mathbb{Z}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

   - **Unicité** : si $A = BQ + R = B\tilde{Q} + \tilde{R}$ avec $\deg(R) < \deg(B)$ et $\deg(\tilde{R}) < \deg(B)$, alors $B(Q - \tilde{Q}) = \tilde{R} - R$. Si $Q - \tilde{Q} \neq 0$, alors $\deg(\tilde{R} - R) = \deg(B) + \deg(Q - \tilde{Q}) \geq \deg(B)$, ce qui contredit $\deg(\tilde{R} - R) < \deg(B)$. Donc $Q = \tilde{Q}$, ce qui entraîne $R = \tilde{R}$.

     Remarque
     La formule $\deg(P_1P_2) = \deg(P_1) + \deg(P_2)$ est vraie dans $\mathbb{K}[X]$, et même dans $C[X]$ dès que C est un anneau intègre (dans ce cas, le coefficient dominant de P_1P_2 est le produit des coefficients dominants de P_1 et P_2, qui sont non nuls, donc ce produit est non nul par intégrité de l'anneau C).

   (b) Si $X - a$ divise P, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$, donc en évaluant en $X = a$, on obtient $P(a) = 0$.
   Réciproquement si $P(a) = 0$, alors par division euclidienne, il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = (X - a)Q + R$ et $\deg(R) < 1$ (c'est-à-dire R constant). En évaluant en $X = a$, on obtient $R = R(a) = P(a) = 0$, donc $X - a$ divise P.

   (c) Si P possède au moins $d + 1$ racines dans $\mathbb{K}$, notées $x_0, \cdots, x_d$, alors (par la question précédente) P est divisible par $X - x_0, \cdots, X - x_d$, donc puisque ces polynômes sont premiers entre eux, P est divisible par $\prod_{k=0}^{d}(X - x_k)$. Cela entraîne $\deg(P) \geq d + 1$.
   Par contraposée, on a donc : si $\deg(P) \leq d$, alors P possède au plus d racines.

Troisième partie :

9. On sait que pour tout $x \in \mathbb{K}^*$, l'ordre de x, noté $ord(x)$, est nécessairement un diviseur strictement positif de $Card(\mathbb{K}^*) = c$.
En notant donc $\Omega_d = \{y \in \mathbb{K}^*,\ ord(y) = d\}$ pour tout entier d, on a la réunion disjointe

$$\mathbb{K}^* = \bigcup_{d \in \mathcal{D}_c} \Omega_d,$$

(avec les Ω_d éventuellement vides *a priori*). En passant aux cardinaux, on obtient

$$\sum_{d \in \mathcal{D}_c} N(d) = c.$$

10. (a) On a $H = \langle x \rangle = \{1, x, \cdots, x^{d-1}\}$ cyclique de cardinal $d = ord(x)$. Puisque $x^d = 1$, tous les éléments de H sont des racines du polynôme $P = X^d - 1 \in \mathbb{K}[X]$ (vu que pour tout k, on a $(x^k)^d = (x^d)^k = 1^k = 1$). On a donc l'inclusion

$$H \subset \{\text{racines de } P \text{ dans } \mathbb{K}\}.$$

Mais $\mathbb{K}$ étant un corps, P possède au maximum d racines dans $\mathbb{K}$, et donc puisque $Card(H) = d$, on a nécessairement

$$H = \{\text{racines de } P \text{ dans } \mathbb{K}\}.$$

Cela entraîne que tout élément $y \in \mathbb{K}^*$ d'ordre d est dans H
(puisque $ord(y) = d \implies y^d = 1 \iff y$ est racine de P).

(b) Puisque x est d'ordre d, on a pour tout $\ell \in \mathbb{N}^*$:

$$(x^k)^\ell = 1 \iff x^{k\ell} = 1 \iff d | k\ell \iff \frac{d}{pgcd(k,d)} | \frac{k\ell}{pcgd(k,d)} \iff \frac{d}{pgcd(k,d)} | \ell,$$

la dernière équivalence résultant du lemme de Gaüss, puisque $\frac{d}{pgcd(k,d)}$ et $\frac{k}{pgcd(k,d)}$ sont premiers entre eux. Ainsi :

$$(x^k)^\ell = 1 \iff l \text{ multiple de } \frac{d}{pgcd(k,d)},$$

ce qui montre que $ord(x^k) = \frac{d}{pgcd(k,d)}$.

(c) Soit $d \in \mathcal{D}_c$.
Si $N(d) = 0$, alors on a évidemment $N(d) \leq \varphi(d)$ (puisque $\varphi(d) \in \mathbb{N}^*$).
Si $N(d) \geq 1$, alors en utilisant 10.(a) et le sous-groupe H :

$$N(d) = Card\{y \in H,\ ord(y) = d\} = Card\{k \in [\![0, d-1]\!],\ ord(x^k) = d\}.$$

Vu que pour tout entier k, on a $ord(x^k) = \frac{d}{pgcd(k,d)}$, on en déduit que

$$N(d) = Card\{k \in [\![0, d-1]\!],\ pgcd(k,d) = 1\} = \varphi(d).$$

Dans tous les cas, on a donc $N(d) \leq \varphi(d)$.

11. Reste à voir que tous les $N(d)$ sont non nuls (c'est-à-dire que tous les ordres possibles sont représentés dans le groupe fini $\mathbb{K}^*$). Cela résulte de l'égalité

$$\sum_{d \in \mathcal{D}_c} (\varphi(d) - N(d)) = c - c = 0$$

(qui provient des questions 4. et 9.) et de la positivité des termes $\varphi(d) - N(d)$, qui entraînent :

$$\forall d \in \mathcal{D}_c, \qquad N(d) = \varphi(d) \in \mathbb{N}^*.$$

12. En particulier $N(c) \neq 0$, donc $\mathbb{K}^*$ est cyclique, puisqu'il possède au moins un élément d'ordre c.