RÉVISIONS : CORRIGÉ DU DEVOIR

Problème 1 — 1. Quel que soit l'entier $n \geq 2$, les classes de 1 et -1 dans $\mathbb{Z}/n\mathbb{Z}$ sont manifestement des solutions de l'équation $x^2 = 1$. Ces deux classes coïncident si et seulement si $2 \equiv 0 \pmod{n}$, donc si et seulement si $n = 2$; par suite, $\lambda(2) = 1$ et $\lambda(n) \geq 2$ pour tout $n \geq 3$.

Si n est un nombre premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps commutatif et le polynôme $X^2 - 1$ a alors au plus 2 racines dans $\mathbb{Z}/n\mathbb{Z}$; on a par suite $\lambda(3) = \lambda(5) = \lambda(7) = 2$.

Il reste à étudier les cas $n = 4$, $n = 6$ et $n = 8$, que l'on peut traiter directement en calculant x^2 pour tout élément x de $\mathbb{Z}/n\mathbb{Z}$. On obtient $\lambda(4) = \lambda(6) = 2$ et $\lambda(8) = 4$ (les solutions sont les classes de 1, -1, 3 et -3).

2. Quels que soient les nombres entiers naturels n et n' premiers entre eux, l'application

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}, \quad m \mapsto (m \pmod{n}, m \pmod{n'})$$

induit un isomorphisme d'anneaux $\overline{f}$ entre $\mathbb{Z}/nn'\mathbb{Z}$ et l'anneau produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ (théorème chinois des restes). L'équation $x^2 - 1 = 0$ a par suite autant de solutions dans l'anneau $\mathbb{Z}/nn'\mathbb{Z}$ qu'elle en a dans l'anneau $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$. Écrivant les éléments de ce dernier anneau sous la forme $x = (y, y')$, $x^2 = (y^2, y'^2)$ et $1 = (1,1)$ donc les solutions de l'équation $x^2 - 1 = 0$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ sont les couples (y, y') constitués d'une solution de cette équation dans $\mathbb{Z}/n\mathbb{Z}$ et d'une solution dans $\mathbb{Z}/n'\mathbb{Z}$; comme il y a $\lambda(n)\lambda(n')$ couples de cette forme, nous en déduisons $\lambda(nn') = \lambda(n)\lambda(n')$.

3. Considérons un nombre premier $p \geq 3$ et un nombre entier $\alpha \geq 1$. Quel que soit le nombre entier x, $\operatorname{pgcd}(x-1, x+1) = 2$ et donc p^α divise $x^2 - 1 = (x-1)(x+1)$ si et seulement si p^α divise $x - 1$ ou $x + 1$, de sorte que les classes de 1 et -1 sont les seules solutions de l'équation $x^2 - 1 = 0$ dans l'anneau $\mathbb{Z}/p^\alpha\mathbb{Z}$.

4. (i) On a déjà calculé $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(8) = 4$. On peut déterminer $\lambda(16)$ de manière directe en calculant x^2 pour tout élément x de $\mathbb{Z}/16\mathbb{Z}$, ce qui conduit à $\lambda(16) = 4$ (les solutions sont les classes de 1, -1, 7 et -7).

(ii) Considérons un nombre entier $\alpha \geq 3$ et un nombre entier $x \in \mathbb{Z}$ tel que $2^\alpha | x^2 - 1$. Comme $2 | x^2 - 1$, $x \equiv 1 \pmod{2}$ et donc $x = 1 + 2y$ avec $y \in \mathbb{Z}$. On a alors $x^2 - 1 = (1+2y)^2 - 1 = 4y + 4y^2 = 4y(y+1)$ et donc $2^{\alpha-2} | y(y+1)$ puisque $2^\alpha | x^2 - 1$.

Réciproquement, tout nombre entier x de la forme $1 + 2y$ avec $y \in \mathbb{Z}$ et $y \equiv 0 \pmod{2^{\alpha-2}}$ vérifie

$$\begin{aligned} x^2 - 1 = 4y(y+1) &\equiv 0 \pmod{4.2^{\alpha-2}} \\ &\equiv 0 \pmod{2^\alpha}. \end{aligned}$$

(iii) Quel que soit le nombre entier y, y et $y+1$ sont premiers entre eux donc $2^{\alpha-2}$ divise $y(y+1)$ si et seulement si $2^{\alpha-2}$ divise y ou $y+1$. Vu la question précédente, il en découle que les nombres entiers x tels que $x^2 - 1 \equiv 0 \pmod{2^\alpha}$ sont précisément ceux de la forme $1 + 2^{\alpha-1}z$ ou $1 + 2(-1 + 2^{\alpha-2}z) = -1 + 2^{\alpha-1}z$ avec $z \in \mathbb{Z}$. Ces conditions déterminent exactement quatre classes modulo 2^α :

$$1, \quad -1, \quad 1 + 2^{\alpha-1} \text{ et } \quad -1 + 2^{\alpha-1},$$

les deux premières correspondant à z pair, les deux dernières à z impair.

Nous venons de prouver que, pour tout nombre entier $\alpha \geq 3$, l'équation $x^2 - 1 = 0$ admet exactement quatre solutions dans l'anneau $\mathbb{Z}/2^\alpha\mathbb{Z}$, c'est-à-dire $\lambda(2^\alpha) = 4$.

5. Soit n un nombre entier naturel supérieur ou égal à 2 et soit $n = 2^{v_2(n)} \prod_{p>2} p^{v_p(n)}$ la décomposition de n en produit de facteurs premiers, où l'on note $v_p(n)$ la plus grande puissance du nombre premier p divisant n.

Soit ℓ le nombre de diviseurs premiers *impairs* de n. En vertu des questions 2 et 3,

$$\begin{aligned} \lambda(n) &= \lambda(2^{v_2(n)}) \prod_{p>3} \lambda(p^{v_p(n)}) \\ &= \lambda(2^{v_2(n)}) \prod_{p \geq 3 \text{ et } p|n} 2 \\ &= \lambda(2^{v_2(n)}) 2^{\ell(n)} \end{aligned}$$

et donc, en vertu de la question 5,

$$\lambda(n) = \begin{cases} 2^{\ell(n)} & \text{si } v_2(n) \leq 1 \\ 2^{\ell(n)+1} & \text{si } v_2(n) = 2 \\ 2^{\ell(n)+2} & \text{si } v_2(n) \geq 3 \end{cases}.$$

Exemple : $440 = 2^3.5.11$, donc $\lambda(440) = 2^{2+2} = 16$.

Problème 2 — 1. (i) Soit $g \in \mathrm{N}$. Puisque $gxg^{-1} \in g\mathrm{H}g^{-1} = \mathrm{H}$, il existe un unique élément $v(g) \in \{0,1,\ldots,n-1\}$ tel que $gxg^{-1} = x^{v(g)}$. Deux éléments d'un groupe ayant le même ordre s'ils sont conjugués, $x^{v(g)}$ est d'ordre $\mathrm{ord}(x) = n$. D'autre part, quel que soit le nombre entier m, x^m est d'ordre $\frac{\mathrm{ord}(x)}{\mathrm{pgcd}(m,\mathrm{ord}(x))}$; on a donc $\mathrm{pgcd}(m,n) = 1$.

(ii) Quels que soient les éléments g et h de N,

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = gx^{v(h)}g^{-1} = (gxg^{-1})^{v(h)} = (x^{v(h)})^{v(g)} = x^{v(g)v(h)} ;$$

on a donc $x^{v(gh)} = x^{v(g)v(h)}$, soit encore $x^{v(gh)-v(g)v(h)} = 1$. Comme x est d'ordre n, il en découle $v(gh) - v(g)v(h) \equiv 0 \pmod{n}$ et l'application

$$\overline{v} : \mathrm{N} \to \mathbb{Z}/n\mathbb{Z},\ g \mapsto v(g) \pmod{n}$$

est donc un homomorphisme de groupes.

Le noyau de l'homomorphisme $\overline{v}$ est composé des éléments g de N tels que $x^{v(g)} = x$, c'est-à-dire tels que $g^{-1}xg = x$; il s'agit donc du sous-groupe C de N.

2. (i) Une permutation $\sigma \in \mathfrak{S}_m$ est un cycle de longueur ℓ si et seulement si elle possède dans $\{1,\ldots,m\}$ une orbite de cardinal ℓ et $m-\ell$ orbites réduites à un point.

Soit c un cycle de longueur ℓ et soit k un nombre entier premier à ℓ.

- Toute orbite ponctuelle de c est également une orbite ponctuelle de c^k puisque, si $c(x) = x$, alors $c^k(x) = x$.
- Soit $\mathrm{O} = \{a_1,\ldots,a_\ell\}$ l'orbite de c de cardinal ℓ et choisissons des entiers u et v tels que $1 = uk + v\ell$. Comme O est une orbite de c, il existe pour chaque $i \in \{1,\ldots,\ell\}$ un entier m tel que $a_i = c^m(a_1)$; on a alors

$$a_i = c^m(a_1) = c^{muk+mv\ell}(a_1) = c^{muk}(a_1) = (c^k)^{mu}(a_1),$$

et donc O est l'orbite de a_1 sous c^k.

Nous venons de vérifier que la permutation c^k possède $m-\ell$ orbites ponctuelles et une orbite de longueur ℓ, ce qui prouve qu'il s'agit d'un cycle de longueur ℓ.

(ii) Les générateurs du groupe cycle H sont les éléments de la forme x^k avec $\mathrm{pgcd}(k,\mathrm{ord}(x)) = 1$. Considérons la décomposition de la permuation x en un produit de cycles de supports disjoints : $x = c_1 \ldots c_r$; l'ordre de x est le plus plus petit commun multiple des ordres des cycles $c_1,\ldots,c_r$. Quel que soit le nombre entier k premier à l'ordre n de x, k est ainsi premier à l'ordre ℓ_i du cycle c_i et donc, en vertu de la question précédente, c_i^k est encore un cycle de longueur ℓ_i. Les cycles $c_1,\ldots,c_r$ ayant des supports disjoints, ils commutent deux à deux et donc $x^k = (c_1 \ldots c_r)^k = c_1^k \ldots c_r^k$. Les deux permutations x et x^k ont par suite des décompositions en produits de cycles de supports disjoints faisant intervenir des cycles de mêmes longueurs, ce qui garantit qu'elles sont conjuguées par un élément de $\mathfrak{S}_m$.

Ainsi, tout générateur du groupe cyclique H est conjugué à x.

(iii) L'homomorphisme $\overline{v} : \mathrm{N} \to (\mathbb{Z}/n\mathbb{Z})^\times$ est surjectif en vertu de la question précédente ; comme son noyau est le sous-groupe C de N (question 1, (ii)), cet homomorphisme induit un isomorphisme entre les groupes N/C et $(\mathbb{Z}/n\mathbb{Z})^\times$ par application de la propriété universelle du noyau (théorème de Noether).

(iv) Supposons que x soit un cycle de longueur m et soit g un élément de $\mathfrak{S}_m$ tel que $gx = xg$. Si l'on écrit x sous la forme $x = (a_1,\ldots,a_m)$, $gxg^{-1} = (g(a_1),\ldots,g(a_m))$ et donc les cycles $(a_1,\ldots,a_m)$ et $(g(a_1),\ldots,g(a_m))$ sont égaux. Définissant s comme l'unique élément de $\{1,\ldots,m\}$ tel que $g(a_1) = a_s$, on a

$$g(a_i) = \begin{cases} a_{i+(s-1)} & \text{si } i+s-1 \leq m \\ a_{i+s-1-m} & \text{si } i+s-1 > m \end{cases}$$

Comme d'autre part

$$x^r(a_i) = \begin{cases} a_{i+r} & \text{si } i+r \leq m \\ a_{i+r-m} & \text{si } i+r > m \end{cases},$$

pour tout nombre entier $r \in \{0,\ldots,m-1\}$, nous obtenons $g = x^{s-1}$ et donc finalement $\mathrm{C} = \mathrm{H}$.

Comme les groupes N/C et $(\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes, $|\mathrm{N}/\mathrm{C}| = \varphi(n)$ (fonction indicatrice d'Euler) et donc $|\mathrm{N}| = |\mathrm{C}||\mathrm{N}/\mathrm{C}| = \varphi(n)|\mathrm{C}|$. Dans le cas que l'on considère, H est le sous-groupe cyclique de $\mathfrak{S}_m$ engendré par un cycle de longueur m et $\mathrm{H} = \mathrm{C}$; on a donc $|\mathrm{C}| = |\mathrm{H}| = m$, d'où $|\mathrm{N}| = \varphi(n)m$.

Problème 3 — 1. Si une permutation σ est écrite comme un produit $c_1 \dots c_r$ de cycles de supports disjoints, $\varepsilon(\sigma) = \varepsilon(c_1)\dots\varepsilon(c_r) = (-1)^{\ell(c_1)-1+\dots+\ell(c_r)-1}$ et donc σ appartient au sous-groupe $\mathfrak{A}_n$ de $\mathfrak{S}_n$ si et seulement si $\ell(c_1)+\dots+\ell(c_r)-r$ est un nombre pair.

Pour chaque $n \in \{2,3,4,5\}$, les suites $(\ell(c_1),\dots,\ell(c_r))$ convenables sont les suivantes :
- $(1,1)$ si $n=2$,
- $(1,1,1)$ et (3) si $n=3$,
- $(1,1,1,1)$, $(1,3)$ et $(2,2)$ si $n=4$,
- $(1,1,1,1,1)$, $(1,1,3)$, $(1,2,2)$ et (5) si $n=5$.

Autrement dit, $\mathfrak{A}_2 = \{1\}$, $\mathfrak{A}_3$ est constitué de l'identité et des cycles de longueur 3, $\mathfrak{A}_4$ est constitué de l'identité, des cycles de longueur 3 et des produits de deux transpositions de supports disjoints, $\mathfrak{A}_5$ est constitué de l'identité, des cycles de longueurs 3 et 5 et des produits de deux transpositions de supports disjoints.

2. (i) D'après ce qui précède, $\mathfrak{A}_3 = \{1,(1,2,3),(1,3,2)\}$ et il s'agit du groupe cyclique engendré par le cycle $(1,2,3)$. L'application $\mathbb{Z} \to \mathfrak{A}_3$, $m \mapsto (1,2,3)^m$ induit donc un isomorphisme entre les groupes $\mathbb{Z}/3\mathbb{Z}$ et $\mathfrak{A}_3$.

(ii) Le groupe $\mathfrak{S}_4$ agit naturellement sur l'ensemble $\{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$ des partitions de $\{1,2,3,4\}$ en réunion de deux sous-ensembles disjoints à deux éléments en posant $\sigma\big(\{\{a,b\},\{c,d\}\}\big) = \{\{\sigma(a),\sigma(b)\},\{\sigma(c),\sigma(d)\}\}$.

On peut vérifier directement que H est stable par multiplication et inversion, de sorte qu'il s'agit bien d'un sous-groupe de $\mathfrak{S}_4$; il s'agit en fait d'un sous-groupe de $\mathfrak{A}_4$ car tous les éléments de H sont des permuations paires. Enfin, comme le conjugué d'un produit de cycles de supports disjoints et de longueurs $\ell_1,\dots,\ell_r$ est un produit de cycles de supports disjoints et de longueurs $\ell_1,\dots,\ell_r$, H est stable par conjugaison et il s'agit donc d'un sous-groupe distingué de $\mathfrak{A}_5$.

Le groupe quotient $\mathfrak{S}_4/\mathrm{H}$ est de cardinal $|\mathfrak{S}_4|/|\mathrm{H}| = \frac{12}{4} = 3$ et donc est nécessairement isomorphe au groupe $\mathbb{Z}/3\mathbb{Z}$.

3. (i) Supposons $n \geq 3$ et soient t, t' deux transpositions distinctes dans $\mathfrak{S}_3$.
- Si les supports de t et t' ne sont pas disjoints, ils ont exactement un élément un commun et donc ces transpositions sont de la forme $t = (a,b)$, $t' = (b,c)$ avec $c \neq a$. On a alors $tt' = (a,b)(b,c) = (a,b,c)$ et donc tt' est un cycle de longueur 3.
- Si les supports de t et t' sont disjoints, $t = (a,b)$ et $t' = (c,d)$ avec $\{a,b\} \cap \{c,d\} = \varnothing$ et alors $tt' = (a,b)(c,d) = (a,b)(b,c)^2(c,d) = (a,b,c)(b,c,d)$ est le produit de deux cycles de longueur 3.

(ii) Comme les cycles de longueur 3 sont des permutations de signatures 1, le sous-groupe de $\mathfrak{S}_n$ engendré par les cycles de longueur 3 est contenu dans $\mathfrak{A}_n$.

Réciproquement, les transpositions engendrant le groupe symétrique, toute permutation $\sigma \in \mathfrak{S}_n$ s'écrit comme un produit de r transpositions et, comme $\varepsilon(\sigma) = (-1)^r$, r est pair si σ appartient au groupe alterné $\mathfrak{A}_n$. Tout élément σ de $\mathfrak{A}_n$ s'écrit par conséquent sous la forme $\sigma = \sigma_1 \dots \sigma_m$, où $\sigma_1,\dots,\sigma_m$ sont des produits de deux transpositions ; vu la question précédente, σ s'écrit alors également sous la forme d'un produit de cycles de longueur 3.

Nous avons ainsi prouvé que le sous-groupe alterné $\mathfrak{A}_n$ de $\mathfrak{S}_n$ est engendré par les cycles de longueur 3 dès que $n \geq 3$.

4. Soit N un sous-groupe distingué de $\mathfrak{A}_5$.

(i) Tous les cycles de longueur 3 sont conjugués dans le groupe $\mathfrak{A}_5$ (attention, c'est plus restrictif que la conjugaison dans $\mathfrak{S}_5$!). En effet, étant donnés deux cycles c et c' de longueur 3, on sait tout d'abord qu'il existe une permutation $\sigma \in \mathfrak{S}_5$ telle que $c' = \sigma c \sigma^{-1}$. Si $\sigma \in \mathfrak{A}_5$, il n'y a plus rien à faire ; sinon, il faut modifier σ pour obtenir une conjugaison par un élément de $\mathfrak{A}_5$. Supposons donc que l'on ait $\varepsilon(\sigma) = -1$. Comme le support du cycle c est de cardinal 3, il existe deux éléments distincts a et b de $\{1,\dots,5\}$ n'appartenant pas au support de c ; on a alors $(a,b)c = c(a,b)$ et, posant $\sigma' = \sigma(a,b)$,

$$\begin{aligned} \sigma' c \sigma'^{-1} &= \sigma(a,b)c(a,b)\sigma^{-1} \\ &= \sigma c \sigma^{-1} \\ &= c'. \end{aligned}$$

Comme $\varepsilon(\sigma') = -\varepsilon(\sigma) = 1$, nous avons obtenu la conjugaison par un élément de $\mathfrak{A}_5$.

Maintenant, si le sous-groupe N de $\mathfrak{A}_5$ contient un cycle c de longueur 3, il contient tous les conjugués de c puisque N est distingué dans $\mathfrak{A}_5$. Comme tous les cycles de longueur 3 sont conjugués dans $\mathfrak{A}_5$, N contient alors tous les cycles de longueur 3 et, vu la question 3, cela implique aussitôt $\mathrm{N} = \mathfrak{A}_5$.

(ii) La permutation $g = (2,5)(3,4)$ appartient au groupe alterné $\mathfrak{A}_5$ et $g\sigma g^{-1} = (g(1),g(2))(g(3),g(4)) = (1,5)(4,3) = \tau$.

Si l'on suppose que N contient σ, N contient alors τ et donc également $\sigma\tau = (1,5,2)$.

(iii) La permutation $h = (2,3)(4,5)$ appartient au groupe alterné $\mathfrak{A}_5$ et $h\sigma h^{-1} = (h(1),h(2),h(3),h(4),h(5)) = (1,3,2,5,4) = \tau$.

Si l'on suppose que N contient σ, N contient alors τ et donc également $\sigma\tau = (1,4,2)$.

(iv) Si le sous-groupe distingué N de $\mathfrak{A}_5$ n'est pas réduit à l'identité, N contient une permutation $\sigma \neq 1$ de signature 1. Les possibilités sont : un cycle de longueur 3, le produit de deux transpositions de supports disjoints ou encore un cycle de longueur 5. Dans chaque cas, il découle des deux dernières questions que N contient nécessairement un cycle de longueur 3 et donc $\mathrm{N} = \mathfrak{A}_5$ en vertu de (i).

Les seuls sous groupes distingués du groupe $\mathfrak{A}_5$ sont donc $\{1\}$ et $\mathfrak{A}_5$, ce qui prouve que ce groupe est *simple*.

Problème 4 — Dans tout cet exercice, p et q sont deux nombres premiers distincts.

1. On a effectivement

$$(\mathrm{X}-1)(\mathrm{X}^{q-1}+\ldots+\mathrm{X}+1) = (\mathrm{X}^q+\ldots+\mathrm{X}^2+\mathrm{X}) - (\mathrm{X}^{q-1}+\ldots+\mathrm{X}+1) = \mathrm{X}^q - 1.$$

Comme $f(1) = q \neq 0$ dans $\mathbb{F}_p$, 1 n'est pas une racine de f dans $\mathbb{F}_p$.

2. (i) L'anneau quotient $\mathbb{F}_p[\mathrm{X}]/(g)$ est un corps car le polynôme g est irréductible. Rappelons la démonstration : un élément non nul x de $\mathbb{F}_p[\mathrm{X}]/(g)$ est la classe d'un polynôme $h \in \mathbb{F}_p[\mathrm{X}]$ non divisible par g ; comme g est irréductible, h et g sont alors premiers entre eux et satisfont par conséquent à une identité de Bézout $1 = ug + vh$ avec $u, v \in \mathbb{F}_p[\mathrm{X}]$. Notant y la classe de v dans l'anneau quotient $\mathbb{F}_p[\mathrm{X}]/(g)$, cette identité fournit la relation $1 = yx$ dans $\mathbb{F}_p[\mathrm{X}]/(g)$ et ceci prouve que x est inversible. Tout élément non nul étant inversible, l'anneau $\mathbb{F}_p[\mathrm{X}]/(g)$ est un corps.

(ii) Par division euclidienne, tout polynôme $h \in \mathbb{F}_p[\mathrm{X}]$ s'écrit sous la forme $h = qg + r$ avec $q, r \in \mathbb{F}_p[\mathrm{X}]$ et $\deg(r) \leq \deg(g) - 1 = d - 1$; comme g divise $h - r$, h et r définissent la même classe dans $\mathbb{F}_p[\mathrm{X}]/(g)$ et donc chaque classe contient effectivement un polynôme de degré au plus $d-1$.

D'autre part, deux polynômes $r, r' \in \mathbb{F}_p[\mathrm{X}]$ de degrés au plus $d-1$ définissent la même classe si et seulement s'ils sont égaux : en effet, comme $\deg(r - r') \leq d - 1 < \deg(g)$, $r - r' = 0$ si $g | r - r'$.

(iii) D'après la question précédente, le cardinal du corps $\mathrm{K} = \mathbb{F}_p[\mathrm{X}]/(g)$ est le nombre de polynômes de degré au plus $d-1$ dans $\mathbb{F}_p[\mathrm{X}]$, ou encore le nombre de d-uplets $(a_0, \ldots, a_{d-1})$ d'éléments de $\mathbb{F}_p$; on a donc $\mathrm{Card}(\mathrm{K}) = p^d$.

3. Soit x la classe de X dans K.

(i) Puisque g divise f, g divise $\mathrm{X}^q - 1$ et donc $x^q - 1 = 0$ dans K ; cela montre que x est un élément de $\mathrm{K}^\times$ dont l'ordre divise q. Puisque q est un nombre premier, x est donc d'ordre 1 ou d'ordre q.

Dire que x est d'ordre 1, c'est dire que $x - 1 = 0$ dans K et cela équivaut à $g | \mathrm{X} - 1$. Ceci conduit à une contradiction car alors $g = \mathrm{X} - 1$ et donc $\mathrm{X} - 1 | f$, ce qui n'est pas le cas en vertu de la question 1. Ainsi, l'élément x de $\mathrm{K}^\times$ est d'ordre q.

(ii) Le groupe multiplicatif $\mathrm{K}^\times = \mathrm{K} - \{0\}$ est d'ordre $p^d - 1$ en vertu de la question 2, (iii). Comme l'ordre de x divise l'ordre de $\mathrm{K}^\times$ (théorème de Lagrange), $q | p^d - 1$ et donc $p^d \equiv 1 \pmod{q}$.

4. Soit n l'ordre de p dans le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$.

(i) Comme $p^d \equiv 1 \pmod{q}$, l'ordre de p dans $(\mathbb{Z}/q\mathbb{Z})^\times$ divise d : $n | d$.

(ii) Quels que soient $a, b \in \mathrm{K}$, $\mathrm{F}(ab) = (ab)^p = a^p b^p = \mathrm{F}(a)\mathrm{F}(b)$ car K est commutatif. D'autre part, comme $p | \binom{p}{i}$ pour tout $i \in \{1, \ldots, p-1\}$, $\binom{p}{i} = 0$ dans le sous-corps $\mathbb{F}_p$ de K, donc $\binom{p}{i} = 0$ dans K et

$$\mathrm{F}(a+b) = (a+b)^p = a^p + \sum_{1 \leq i \leq p-1} \binom{p}{i} a^{p-i} b^i + b^p = a^p + b^p = \mathrm{F}(a) + \mathrm{F}(b).$$

Il reste à vérifier que F est une bijection. Pour cela, il suffit d'observer que F est un endomorphisme du groupe additif $(\mathrm{K}, +)$ dont le noyau, constitué des éléments a de K tels que $a^p = 0$, est réduit à 0 puisque K est un corps ; F est par suite une injection, et donc bijection puisque l'ensemble K est fini.

Ainsi, F est un automorphisme du corps K.

(iii) Par définition de l'entier n, q divise p^n-1 et donc $x^{p^n}=x$ puisque $x^q=1$. On a donc $\mathrm{F}^n(x)=x^{p^n}=x$.

En vertu de la question 2 (ii), tout élément z de K s'écrit (de manière unique) sous la forme $a_0+a_1x+\ldots+a_{d-1}x^{d-1}$ avec $a_i\in\mathbb{F}_p$. Comme F est un automorphisme de corps,

$$\mathrm{F}(z)=\mathrm{F}(a_0+a_1x+\ldots+a_{d-1}x^{d-1})=\mathrm{F}(a_0)+\mathrm{F}(a_1)\mathrm{F}(x)+\ldots+\mathrm{F}(a_{d-1})\mathrm{F}(x)^{d-1}$$

et donc $\mathrm{F}(z)=z$ car $\mathrm{F}(x)=x$ et $\mathrm{F}(a)=a$ pour tout $a\in\mathbb{F}_p$ en vertu du petit théorème de Fermat.

Ainsi, $\mathrm{F}^n=\mathrm{id}_\mathrm{K}$.

(iv) D'après la question précédente, tout élément du corps K est racine du polynôme $\mathrm{T}^{p^n}-\mathrm{T}$.

(v) Le polynôme $\mathrm{T}^{p^n}-\mathrm{T}$ ayant au plus p^n racines dans le corps K, $p^d\leq p^n$ et donc $d\leq n$. Comme d'autre part $n|d$ (question 4,(i)), $n\leq d$ et donc finalement $d=n$.

À l'issue de ces questions, nous avons démontré que chaque facteur irréductible de f dans $\mathbb{F}_p[\mathrm{X}]$ est de degré égal à l'ordre de p dans $(\mathbb{Z}/q\mathbb{Z})^\times$; en particulier, *tous* les facteurs irréductibles de f dans $\mathbb{F}_p[\mathrm{X}]$ ont le *même* degré.

5. Nous fixons dans cette question un nombre premier q.

(i) Soit a un nombre entier et soit p un nombre premier distinct de q qui divise $a^{q-1}+\ldots+a+1$. Dans ces conditions, la classe $\overline{a}$ de a dans $\mathbb{F}_p$ est une racine du polynôme $f=\mathrm{X}^{q-1}+\ldots+\mathrm{X}+1$ et donc $\mathrm{X}-\overline{a}$ est un facteur irréductible de f dans $\mathbb{F}_p[\mathrm{X}]$. En vertu de la question 4, ceci implique que la classe de p dans $(\mathbb{Z}/q\mathbb{Z})^\times$ soit d'ordre 1, c'est-à-dire $p\equiv 1\pmod q$. En outre, tous les facteurs irréductibles de f dans $\mathbb{F}_p[\mathrm{X}]$ ayant le même degré, tous sont de degré 1 et le polynôme f est scindé sur $\mathbb{F}_p$.

(ii) Étant donné un nombre entier $m\geq 2$ et un facteur premier p de $(m!)^{q-1}+\ldots+(m!)+1$, p ne divise pas $m!$ et donc $p\geq m+1$.

(iii) Le nombre entier $(q!)^{q-1}+\ldots+q!+1$ est supérieur ou égal à $q+1\geq 3$ donc est divisible par un nombre premier p_1 ; comme $p_1\geq q+1$ en vertu de la question précédente, p_1 et q sont distincts et il découle alors de la question (i) que l'on a $p_1\equiv 1\pmod q$.

On définit alors par induction une suite strictement croissante $(p_n)_{n\geq 1}$ de nombres premiers comme suit : p_1 est choisi comme ci-dessus et p_{n+1} est un nombre premier divisant $(p_n!)^{q-1}+\ldots+p_n+1>1$; on a bien $p_{n+1}>p_n$ en vertu de la question (ii), donc $p_{n+1}>p_1>q$, et $p_{n+1}\equiv 1\pmod q$ en vertu de la question (i).

Quel que soit le nombre premier q, nous avons ainsi démontré l'existence d'une infinité de nombres premiers p tels que $p\equiv 1\pmod q$.

Remarque et exercice. *Soit p un nombre premier supérieur ou égal à 3. En remplaçant le polynôme X^q-1 (resp. f) par X^4-1 (resp. X^2+1) et en suivant le même raisonnement que précédemment, on prouve que tous les facteurs irréductibles de X^2+1 ont le même degré, égal à l'ordre de p dans $(\mathbb{Z}/4\mathbb{Z})^\times$. On en déduit alors comme à la question 5 qu'il existe une infinité de nombres premiers de la forme $1+4k$, $k\in\mathbb{N}$.*

Plus généralement, une variante de cet exercice permet de démontrer qu'il existe, pour tout entier naturel $n\geq 2$, une infinité de nombres premiers p tels que $p\equiv 1\pmod n$.