Devoir libre $n°01$
Correction

N'hésitez pas de me signaler les erreurs rencontrées.

•••••••••

Exercice 1 :

1. $\sigma \circ \tau \circ \sigma^{-1} = (2\ 3)$, $\sigma^2 \circ \tau \circ \sigma^{-2} = (3\ 4)$, puis par récurrence, $\forall k \in \mathbb{N}$, $\sigma^k \circ \tau \circ \sigma^{-k} = (k+1\ k+2)$.
2. On sait que toute permutation de $\mathscr{S}_n$ peut s'écrire comme produit de transpositions de la forme $(k\ k+1)$. Ces dernières peuvent s'écrire comme produit de σ, de τ , et de σ^{-1}. Or $\sigma^n = Id$ et donc $\sigma^{-1} = \sigma^{n-1}$ et par conséquent, σ^{-1} peut s'écrire comme produit de σ.

Exercice 2 :

1. Pour $a \in \mathbb{Z}$ et $m \in \mathbb{N}$, on a $a \equiv 1[a-1]$, donc $a^m \equiv 1[a-1]$. De même $a \equiv -1[a+1]$, donc si m est impair, alors $a^m \equiv -1[a+1]$.
   Si k est un diviseur de n, prenant $a = 2^k$, on en déduit que $2^k - 1$ divise $2^n - 1$, donc si $2^n - 1$ est premier, on a $2^k - 1 = 1$ (c'est-à-dire $k = 1$) ou $2^k - 1 = 2^n - 1$, donc $k = n$. Autrement dit n est premier.
   Écrivons $n = 2^k m$ avec $k \in \mathbb{N}$ et m impair. Alors $2^{2^k} + 1$ divise $2^n + 1$, donc, si $2^n + 1$ est premier, alors $m = 1$.
2. On a $2^{2^k} \equiv -1[F_k]$, donc $2^{2^l} = (2^{2^k})^{2^{l-k}} \equiv 1[F_k]$. Enfin $F_l \equiv 2[F_k]$. Le pgcd de F_k et F_l divise 2 et, puisque F_l est impair, F_k et F_l sont premiers entre eux.
3. Puisque q divise M_p, on a $2^p \equiv 1[q]$. Donc l'ordre de 2 dans $\mathbf{F}_q^*$ divise p, ce ne peut être que p. Or l'ordre de p divise l'ordre du groupe $\mathbf{F}_q^*$ [1], donc p divise $q-1$. Comme q est impair $2p$ divise $q-1$.
4. Si M_{13} n'était pas premier, son plus petit diviseur [2] non nul q serait $< \sqrt{M_{13}} < 64\sqrt{2} < 100$ et un nombre premier de la forme $26k+1$. Comme 27 n'est pas premier, il reste à teste 53 et 79.
   Or $2^6 \equiv 11[53]$, donc $2^{12} \equiv 121 \equiv 15[53]$ et enfin $M_{13} \equiv 2 \times 15 - 1 = 29 \neq 0[53]$, de même $2^6 \equiv -15[79]$, donc $2^{12} \equiv 225 \equiv -12[79]$ et enfin $M_{13} \equiv -2 \times 12 - 1 = -25 \neq 0[79]$.
5. (a) On a $2^{2^l} \equiv -1[q]$, donc $2^{2^{l+1}} \equiv 1[q]$. L'ordre de 2 dans le groupe $\mathbf{F}_q^*$ divise 2^{l+1} et ne divise pas 2^l : c'est 2^{l+1}.
   (b) L'ordre de 2 dans le groupe $\mathbf{F}_q^*$ divise l'ordre de $\mathbf{F}_q^*$, donc 2^{l+1} divise $q-1$.
   (c) Comme w^4 est la classe de 2^{2^l}, on a $w^4 = -1$, donc $w^2 + w^{-2} = 0$, donc $(w + w^{-1})^2 = 2$. On a $(w + w^{-1})^{2^{l+1}} = -1$, donc l'ordre de $w + w^{-1}$ divise 2^{l+2} et ne divise pas 2^{l+1} : c'est 2^{l+2}. On en déduit que 2^{l+2} divise $q-1$.
   (d) Si q est le plus petit nombre premier divisant F_5, alors $q \equiv 1[2^7]$. Or 3 divise 129 et $4 \times 128 + 1 = 513$ et 5 divise $3 \times 128 + 1 = 385$. Enfin, $2 \times 128 + 1 = 257 = F_3$ est un nombre de Fermat donc premier à F_5. Le premier nombre à tester est donc $5 \times 128 + 1 = 641$.
   (e) On a $2^4 \equiv -5^4[641]$, donc $F_5 = 2^{28}2^4 + 1 \equiv 1 - 5^4 2^{28}[641]$.
   (f) On a $5 \times 2^7 = 640 \equiv -1[641]$, donc $5^4 2^{28} = (5 \times 2^7)^4 \equiv 1[641]$ et 641 divise F_5. On a en fait $F_5 = 641 \times 6700417$.

Exercice 3 :

1. Comme $(\mathbb{Z}/2\mathbb{Z})^*$ est un groupe à un élément, $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^*$. Si m est impair, $(\mathbb{Z}/2m\mathbb{Z})^*$ est donc isomorphe à $(\mathbb{Z}/m\mathbb{Z})^*$ (voir la série des exercices).
2. (a) On a $\varphi(1) = \varphi(2) = 1$. Si un nombre premier $p \neq 2$ divise n, alors $p - 1 = \varphi(p)$ divise $\varphi(n)$ donc $\varphi(n)$ est pair. Enfin, pour $k > 2$, $\varphi(2^k) = 2^{k-1}$ est pair. Bref, les seuls n tels que $\varphi(n)$ soit impair sont 1 et 2.

1. **Théorème de Lagrange :** Dans un groupe fini, le cardinal de chaque sous-groupe divise le cardinal du groupe.
2. Soit $n \geq 2$ un entier. S'il n'est pas premier, il admet un diviseur $p \leq \sqrt{n}$ qui est premier

(b) Posons $k = \text{ppcm}(\varphi(m), \varphi(n))$. Les nombres $\varphi(m)$ et $\varphi(n)$ sont pairs donc ne sont pas premiers entre eux, donc $k < \varphi(m)\varphi(n) = \varphi(mn)$. Soit $x \in (\mathbb{Z}/mn\mathbb{Z})^*$, notons $(y, z) \in (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ son image par l'isomorphisme $(\mathbb{Z}/mn\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. Comme $\varphi(m)$ et $\varphi(n)$ divisent k, on a $y^k = 1$ dans $(\mathbb{Z}/m\mathbb{Z})$ et $z^k = 1$ dans $(\mathbb{Z}/n\mathbb{Z})$. On en déduit que $x^k = 1$, donc l'ordre de x divise k et n'est donc pas égal à $\varphi(mn)$. Donc x n'est pas générateur de $(\mathbb{Z}/mn\mathbb{Z})^*$. Comme c'est vrai pour tout $x \in (\mathbb{Z}/mn\mathbb{Z})^*$, le groupe $(\mathbb{Z}/mn\mathbb{Z})^*$ n'est pas cyclique.

(c) Les éléments du groupe $(\mathbb{Z}/8\mathbb{Z})^*$ vérifient tous $x^2 = 1$, puisque $3^2 - 1, 5^2 - 1$ et $7^2 - 1$ sont multiples de 8. Donc $(\mathbb{Z}/8\mathbb{Z})^*$ n'a pas d'éléments d'ordre 4 : il n'est pas cyclique.

(d) Pour $m = 1$ ou 2, les groupes $(\mathbb{Z}/m\mathbb{Z})^*$ réduits à un élément sont cycliques, le groupe $(\mathbb{Z}/4\mathbb{Z})^*$ a deux éléments : il est cyclique.
Supposons que $k \geq 3$. Le groupe $(\mathbb{Z}/2^k\mathbb{Z})^*$ est l'ensemble des classes modulo 2^k des nombres impairs l avec $1 \leq l < 2^k$, il a 2^{k-1} éléments. Notons $H \subset (\mathbb{Z}/2^k\mathbb{Z})^*$ l'ensemble des classes modulo 2^k des nombres de la forme $8l + 1$ ($0 \leq l < 2^{k-3}$). C'est un sous-groupe de $(\mathbb{Z}/2^k\mathbb{Z})^*$ à 2^{k-3} éléments. Pour tout $x \in (\mathbb{Z}/2^k\mathbb{Z})^*$, on a $x^2 \in H$. D'après le théorème de Lagrange, il vient $(x^2)^{2^{k-3}} = 1$ soit $x^{2^{k-2}} = 1$. En particulier, x n'engendre pas $(\mathbb{Z}/2^k\mathbb{Z})^*$. On en déduit que le groupe $(\mathbb{Z}/2^k\mathbb{Z})^*$ n'est pas cyclique.

3. Notons m l'ordre de $\ker f$ et n celui de $f(G)$. En particulier, G est d'ordre mn [3]. Soit $a \in G$ tel que $f(a)$ soit un générateur de $f(G)$. Les générateurs de $f(G)$ sont les $f(a)^k = f(a^k)$ pour k premier avec n. En particulier, puisque m et n sont supposés premiers entre eux, $f(a^m)$ est un générateur de $f(G)$. Soit aussi b un générateur de $\ker f$.
Démontrons que $u = ba^m$ est un générateur de G. Notons k son ordre, il divise l'ordre mn de G.
• Comme $u^k = 1$, il vient $f(u)^k = f(u^k) = 1$. Comme $f(u) = f(a^m)$ est un générateur de $f(G)$, il est d'ordre n, on en déduit que n divise k.
L'ordre de a, qui divise l'ordre mn de G, divise mk et $(a^m)^k = 1$.
• Or $1 = u^k = b^k a^{mk}$, donc $b^k = 1$ et donc l'ordre m de b divise aussi k.
• Comme m et n sont premiers entre eux, mn divise k, puisque k divise mn, il vient $k = mn$ donc u est bien un générateur de G.

4. Remarquons que, pour $a \in \mathbb{Z}$, $\text{pgcd}(a, p^k)$ est une puissance de p, donc a est premier avec p^k si et seulement s'il n'est pas multiple de p.

(a) On raisonne par récurrence sur k.
• Pour $k = 1$, on a :

$$(1+p)^p = \sum_{j=0}^{p} p^j = 1 + p.p + p\frac{p-1}{2}p^2 + p^3 \sum_{j=3}^{p} \mathsf{C}_p^j p^{j-3} = 1 + p^2 + p^3 m$$

où $m = \dfrac{p-1}{2} + \displaystyle\sum_{j=3}^{p} \mathsf{C}_p^j p^{j-3}$.

• Soit $k \geq 1$. Supposons qu'on sache que $(1+p)^{p^k} = 1 + p^{k+1} + m_k p^{k+2}$. Alors

$$\begin{aligned}
(1+p)^{p^{k+1}} &= (1 + p^{k+1} + m_k p^{k+2})^p && (1)\\
&= \sum_{j=0}^{p} \mathsf{C}_p^j p^{(k+1)j} (1 + pm_k)^j && (2)\\
&= 1 + pp^{k+1}(1 + pm_k) + \sum_{j=2}^{p} \mathsf{C}_p^j p^{(k+1)j} (1 + pm_k)^j && (3)
\end{aligned}$$

Remarquons que, puisque $k \geq 1$, pour $j \geq 2$, on a $j(k+1) \geq 2k + 2 \geq k + 3$. On peut donc écrire

$$(1+p)^{p^{k+1}} = 1 + p^{k+2} + m_{k+1} p^{k+3}$$

où $m_{k+1} = m_k + \displaystyle\sum_{j=2}^{p} \mathsf{C}_p^j p^{(k+1)j-(k+3)} (1 + pm_k)^j$.

3. Utiliser le théorème d'isomorphisme

(b) On suppose que $n \geq 2$: pour $n = 1$, $\ker f$ a un élément.
Les éléments de $\ker f$ sont les classes modulo p^n des $x \in \mathbb{Z}$ tels $x \equiv 1[p]$. Un tel élément est représenté par un unique $x \in \mathbb{Z}$ avec $0 \leq x < p^n$ de la forme $1 + kp$, où on a $k \in \mathbb{Z}$, $0 \leq k < p^{n-1}$. L'ordre du groupe $\ker f$ est donc p^{n-1}. Notons b la classe de $1 + p$ dans $\ker f$.
Son ordre divise p^{n-1} et est donc de la forme p^r avec $r \leq n - 1$. On a :

$$(1 + p)^{p^{n-2}} \equiv 1 + p^{n-1}[p^n],$$

donc $b^{p^{n-2}} \neq 1$ donc l'ordre de b n'est pas divisible par p^{n-2}, il vient $r > n - 2$, donc $r = n - 1$. Cela prouve que b engendre $\ker f$, qui est donc cyclique.

(c) On sait que $(\mathbb{Z}/_{p\mathbb{Z}})^*$ est cyclique et puisque les ordres p^{n-1} de $\ker f$ et $p - 1$ de $(\mathbb{Z}/_{p\mathbb{Z}})^*$ sont premiers entre eux, il résulte de la question 3 que $(\mathbb{Z}/_{p^n\mathbb{Z}})^*$ est cyclique.

5. • Pour $m = 1$ ou 2, les groupes $(\mathbb{Z}/_{mZ})^*$ réduits à un élément sont cycliques.
• Le groupe $(\mathbb{Z}/_{4Z})^*$ a deux éléments : il est cyclique.
• Si p est un nombre premier distinct de 2 et $n \geq 1$, le groupe $(\mathbb{Z}/_{p^nZ})^*$ est cyclique ainsi que $(\mathbb{Z}/_{2p^nZ})^*$ qui lui est isomorphe.
• D'après la question 2b), si m a deux diviseurs premiers impairs ou si m est divisible par 4 et n'est pas une puissance de 2, le groupe $(\mathbb{Z}/_{mZ})^*$ n'est pas cyclique.
• Enfin, pour $k \geq 3$, le groupe $(\mathbb{Z}/_{2^kZ})^*$ n'est pas cyclique (d'après la question 2d)).
Donc l'ensemble des $m \in \mathbb{N}$ tels que le groupe $(\mathbb{Z}/_{mZ})^*$ est cyclique est :

$$\{1, 2, 4\} \cup \{p^n | p \text{ premier } p \neq 2, n \in \mathbb{N}^*\} \cup \{2p^n | p \text{ premier } p \neq 2, n \in \mathbb{N}^*\}.$$

Exercice 4 :

1. f transforme une base de $\mathbb{R}^n$ à une base de $\mathbb{R}^n$, donc f est inversible.

2. Nous savons que $M^n = I_n$ et donc M est un élément d'ordre fini du groupe $(\mathbf{GL}_n(\mathbb{C}), .)$. Par calcul ou par considération de polynôme minimal, on peut affirmer que n est le plus petit exposant $p > 0$ tel que $M^p = I_n$ et donc M est un élément d'ordre exactement n. On en déduit que G est un groupe cyclique de cardinal n.

••••••••••