**Exercice 1.** [Centrale MP 2 2015]
Pour $n \geqslant 1$, on note $E_n = \{0, 1, \dots, n-1\}$ et $S_n$ le groupe des permutations de $E_n$. En PYTHON une permutation $\sigma \in S_n$ est représentée par la liste $[\sigma(0), \dots, \sigma(n-1)]$. Pour $i \in E_n$, la *période* de $i$ pour $\sigma \in S_n$ est le plus petit entier naturel non nul $p$ tel que $\sigma^p(i) = i$. On le note $Per(\sigma, i)$.

1. Justifier l'existence de $Per(\sigma, i)$ et montrer qu'elle est plus petite que $n$. Préciser l'ordre de $\sigma$ en fonction des $Per(\sigma, i)$.
2. Écrire une fonction qui retourne la période d'un élément $i$ pour une permutation $\sigma$.
3. Écrire une fonction qui retourne la liste des périodes, pour une permutation $\sigma$, des éléments de $E_n$.
   **Application :** $\sigma = [3, 6, 7, 0, 2, 1, 8, 5, 4, 9]$.

Soit $\sigma \in S_n$. On définit une relation $R_\sigma$ sur $E_n$ par : $xR_\sigma y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$.

4. Montrer que $R_\sigma$ est une relation d'équivalence.

On appelle *orbite* d'un élément $x$ de $E_n$ sa classe d'équivalence. On la note $\Omega_\sigma(x)$.

5. Montrer que $\Omega_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$ où $p = Per(\sigma, x)$.
6. Écrire une fonction qui retourne la liste des orbites d'une permutation $\sigma$.

***Solution :***

1. *Soit $\sigma \in S_n$.*
   - *Soit $i \in [\![0, n-1]\!]$. $\{\sigma^k(i) \mid 0 \leqslant k \leqslant n\}$ est un ensemble fini à $n+1$ éléments, mais pour tout $k \in [\![0, n]\!]$, $\sigma^k(i) \in [\![0, n-1]\!]$ ensemble à $n$ éléments, donc il existe $k, \ell \in [\![0, n]\!]$, $k < \ell$ tels que $\sigma^k(i) = \sigma^\ell(i)$, donc $\sigma^{\ell-k}(i) = i$ où $\ell - k \in [\![1, n]\!]$, donc $\{p \in \mathbb{N}^* \mid \sigma^p(i) = i\}$ est non vide car il contient $\ell - k$, et son minimum est $\leqslant \ell - k \leqslant n$.*
   - *Soit $i \in [\![0, n-1]\!]$. Notons $p = Per(\sigma, i)$. Soit $k \in \mathbb{Z}$ que l'on écrit $k = qp + r$ où $q, r \in \mathbb{Z}$ et $0 \leqslant r < p$. Alors $\sigma^k(i) = \sigma^r((\sigma^p)^q(i)) = \sigma^r(i)$. Par minimalité de $p$, $\sigma^k(i) \iff r = 0 \iff p|k$.*
   - *Soit $k \in \mathbb{Z}$. Alors $\sigma^k = \mathrm{id}$ si et seulement si pour tout $i \in [\![0, n-1]\!]$, $Per(\sigma, i)|k$. Ainsi l'ordre de $\sigma$ est le* PPCM *des $Per(\sigma, i)$ pour $0 \leqslant i \leqslant n-1$.*
2. *On calcule les images de $i$ par les itérés de $\sigma$.*

```python
def periode(sigma,i) :
    compteur=1 # période au moins 1
    j=sigma[i] # calcul de la première image
    while j!=i : # sortie lorsque sigma^compteur(i)=i
        compteur+=1
        j=sigma[j]
    return compteur
```

3. *On applique la fonction précédente à chaque élément de $E_n$.*

```python
def liste_periodes(sigma) :
    return [periode(sigma,i) for i in range(len(sigma))]
```

   *Pour l'exemple de l'énoncé on obtient :* [2,7,7,2,7,7,7,7,7,1]

4. — *Pour tout $x \in E_n$, $x = \sigma^0(x)$ donc la relation est réflexive ;*
   — *pour tous $x, y \in E_n$,*
$$xR_\sigma y \iff \exists k \in \mathbb{Z},\ \sigma^k(x) = y \iff \exists k \in \mathbb{Z},\ x = \sigma^{-k}(y) \iff yR_\sigma x$$

*donc la relation est symétrique;*

— *pour tous* $x, y, z \in E_n$,

$$(xR_\sigma y \text{ et } yR_\sigma z) \iff \exists\, k, \ell \in \mathbb{Z},\ y = \sigma^k(x) \text{ et } z = \sigma^\ell(y)$$

*donc* $z = \sigma^{k+\ell}(x)$, *donc* $xR_\sigma z$, *la relation est transitive.*

$R_\sigma$ *est une relation d'équivalence.*

5. *Par définition*

$$\Omega_\sigma(x) = \left\{y \in E_n \,\middle|\, \exists\, k \in \mathbb{Z},\ y = \sigma^k(x)\right\} = \left\{\sigma^k(x) \,\middle|\, k \in \mathbb{Z}\right\} = \left\{\sigma^k(x) \,\middle|\, 0 \leqslant k \leqslant Per(\sigma, x)\right\}$$

*par division euclidienne comme à la question 1.*

6. *On calcule les orbites les unes après les autres en notant les éléments déjà rencontrés.*

```
def orbites(sigma) :
    n=len(sigma)
    res=[] # initialement liste vide d'orbites
    dejavu=[False for i in range(n)] # pour retenir les cas déjà traités
    for i in range(n) : # on parcourt sigma
        if not dejavu[i] : # on ignore les cas déjà vus
            orbi=[i] # on commence à construire l'orbite de i
            dejavu[i]=True # i est traité
            j=sigma[i] # on calcule son image
            while j!=i : # tant qu'on trouve des images différentes de i
                orbi.append(j)
                dejavu[j]=True
                j=sigma[j]
            res.append(orbi) # on ajoute l'orbite à la liste des orbites
    return res
```

*Pour l'exemple de l'énoncé on obtient :* $[[0,3],[1,6,8,4,2,7,5],[9]]$ *(complexité linéaire).*

**Exercice 2.** [Mines PSI/MP]
Soit $E$ un $\mathbb{Q}$-espace vectoriel de dimension $n$. Soit $f \in \mathscr{L}(E)$ telle que $f^3 + f^2 - \mathrm{Id}_E = 0$. Montrer que $n$ est multiple de $3$.

***Solution :***
*(* corrigé non détaillé *)*
$P = X^3 + X^2 - 1$ *est annulé par* $f$. *Une étude de fonction montre qu'il existe un unique* $\alpha$ *réel racine de* $P$. *Connaissant les racines de* $P'$, *on constate que ces racines sont différentes de* $\alpha$, *donc* $\alpha$ *est racine simple de* $P$, *puis* $P$ *admet une racine complexe non réelle* $\beta$, *et comme* $P$ *est réel,* $\overline{\beta}$ *est aussi racine de* $P$. *Ainsi* $P$ *est scindé à racines simples, donc diagonalisable, et en notant* $a, b, c$ *les multiplicités respectives de* $\alpha, \beta, \gamma$, *on a* $a + b + c = n$.
*Par ailleurs,* $\mathrm{tr}(f) = a\alpha + b\beta + c\overline{\beta}$ *et comme* $\mathrm{tr}(f) \in \mathbb{R}$, *on montre que* $b = c$. *Il vient alors* $\mathrm{tr}(f) = a\alpha + b(\beta + \overline{\beta})$.
*Comme* $\alpha, \beta, \overline{\beta}$ *sont les racines de* $P$, *par relation coefficients-racines il vient* $\alpha + \beta + \overline{\beta} = -1$ *donc* $\beta + \overline{\beta} = -1 - \alpha$.
*En combinant les deux dernières relations il vient :*

$$\mathrm{tr}(f) = (a - b)\alpha - b \in \mathbb{Q} \Longrightarrow (a - b)\alpha \in \mathbb{Q}$$

*En supposant par l'absurde que* $a \neq b$, *il vient* $\alpha \in \mathbb{Q}$. *On écrit alors* $\alpha = \frac{p}{q}$ *où* $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, $p \wedge q = 1$. *On injecte* $\alpha$ *dans la relation* $P(\alpha) = 0$, *on multiplie par* $q^3$ *et par considération arithmétique on trouve quelques valeurs possibles pour* $\alpha$, *et on vérifie que ces valeurs ne sont pas racines de* $P$.
*Finalement c'est absurde, donc* $a = b = c$ *et* $n = 3a$ *est un multiple de* $3$.

**Exercice 3.** [Centrale MP 2021]

1. Soit $M \in \mathscr{M}_n(\mathbb{C})$ nilpotente. Justifier l'existence de $d = \min\{p \in \mathbb{N} \mid M^p = 0\}$ et l'inégalité $d \leqslant n$.
2. Soit $M \in \mathscr{M}_n(\mathbb{C})$ nilpotente. Montrer que $M^2 - I_n$ est inversible et donner son inverse.
3. Soit $M \in \mathscr{M}_n(\mathbb{C})$ telle que $M^4 + M^3 + M^2 + M + I_n = 0$. Montrer que $|\mathrm{Tr} M| \leqslant n$ et étudier les cas d'égalité.
4. Reprendre les questions 2. et 3. pour $M \in \mathscr{M}_n(\mathbb{R})$.

***Solution :***

1. *Minimum d'un ensemble non vide de $\mathbb{N}$.*
   *Comme $N^{d-1} \neq 0$, il existe $x_0 \in \mathbb{C}^n$ tel que $M^{d-1}x_0 \neq 0$ et on montre que la famille $(M^k x_0)_{0 \leqslant k \leqslant d-1}$ de cardinal $d$ est libre, donc $d \leqslant n$.*
2. *Soit $p = \lfloor d/2 \rfloor + 1$, alors $2p \geqslant d$ et donc*
   $$(M^2 - I_n)\Big(-\sum_{k=0}^{p-1} M^{2k}\Big) = -M^{2p} + I_n = I_n$$
   *donc $M^2 - I_n$ est inversible d'inverse $-\sum_{k=0}^{p-1} M^{2k}$.*
3. *$M$ est annulé par $P = X^4 + X^3 + X^2 + X + 1 = \prod_{k=1}^{4}(X - \omega^k)$ où $\omega = e^{\mathrm{i}2\pi/5}$, les racines de ce polynôme sont les racines 5-è de l'unité sauf 1. Ce sont les valeurs propres possibles de $M$, et comme le polynôme caractéristique de $M$ est scindé sur $\mathbb{C}$, en notant $m_k$ la multiplicité éventuellement nulle de $\omega^k$ dans $P$, on a :*
   $$|Tr(M)| = \left|\sum_{k=1}^{4} m_k \omega^k\right| \leqslant \sum_{k=1}^{p} m_k = \deg(\chi_M) = n$$
   *Le cas d'égalité correspond au cas d'égalité dans l'inégalité triangulaire (à savoir démontré, récurrence pour faire simple) : $|\mathrm{Tr}(M)| = n$ si et seulement si tous les termes de la somme ont même argument, si et seulement si un seul des $\omega^k$, $1 \leqslant k \leqslant 4$ est effectivement valeur propre, si et seulement si $M = \omega^k I_n$ où $k \in [\![1,4]\!]$.*
4. *2 est formellement identique, 3 se traite en regardant $M$ comme une matrice complexe et le cas d'égalité est impossible car $\omega^k$ n'est pas réel.*

**Exercice 4.** [Mines MP]
Soient $A$ dans $\mathcal{M}_n(\mathbb{C})$ et $P$ un polynôme tels que $P(A)$ est diagonalisable et $P'(A)$ est inversible. Montrer que $A$ est diagonalisable.

***Solution :***
*Il existe $Q$ polynôme scindé à racines simples (srs en abrégé) tel que $Q \circ P(A) = Q(P(A)) = 0$. Soit $a$ une valeur propre de $A$, c'est une racine de $\chi_A$ le polynôme caractéristique de $A$, et cela existe puisque le corps de base est $\mathbb{C}$. Alors $P(a)$ est valeur propre de $P(A)$ et racine de $Q$ puisque c'est un polynôme annulateur de $P(A)$, donc $a$ est racine de $Q \circ P$. Montrons que cette racine est simple. On calcule $(Q \circ P)' = P' \times Q' \circ P$ et on évalue en $a$ : $P'(a)Q'(P(a))$. Mais, $P(a)$ est déjà racine de $Q$ qui est srs, donc $P(a)$ n'est pas racine de $Q'$, donc $Q'(P(a))$ est différent de $0$. De même, $a$ n'est pas racine de $P'$ puisque $P'(A)$ est inversible, donc $a$ n'est pas racine de $Q \circ P'$. On a donc prouvé que $a$ est racine simple de $Q \circ P$. On a donc montré que le polynôme $R$ dont les racines sont exactement les valeurs propres de $A$ avec multiplicité $1$ divise $Q \circ P$, donc on peut écrire $Q \circ P = R * \times S$ avec $S$ polynôme de $\mathbb{C}[X]$ dont les racines ne sont pas valeurs propres de $A$, donc $S(A)$ est inversible. Finalement, on a : $0 = P \circ Q(A) \times S^{-1}(A) = R(A)$, donc il existe un polynôme srs qui annule $A$ : $A$ est diagonalisable.*
*'Une version particulière de cet exercice, qui étudie des contre-exemples aussi :*
- *Soit $A$ dans $GL_n(\mathbb{C})$, montrer que $A^3$ diagonalisable si et seulement si $A$ diagonalisable.*
- *Donner un contre-exemple lorsque $A$ n'est pas supposée inversible.*
- *Donner un contre-exemple lorsque $A$ est dans $GL_n(\mathbb{R})$.*