

*Durée : 3h. Tout document interdit.
Une rédaction claire et précise sera appréciée.*

1. Sur les groupes d'ordre 8. Soit D est le plus petit sous-groupe de $Gl_2(\mathbb{R})$ contenant les matrices $\rho = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Soit Q le plus petit sous-groupe de $Gl_2(\mathbb{C})$ contenant les matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \text{ et } C = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

1.a. Etablir les relations $\sigma\rho = \rho^3\sigma$, $\sigma\rho^2 = \rho^2\sigma$, $\sigma\rho^3 = \rho\sigma$. En déduire que D s'identifie à l'ensemble $\{\rho^m\sigma^n \mid 0 \leq m \leq 3, 0 \leq n \leq 1\}$. Déterminer l'ordre des éléments de D . Combien d'éléments d'ordre 4 y a-t-il dans D ?

1.b. Montrer que Q s'identifie à l'ensemble $\{\pm I_2, \pm A, \pm B, \pm C\}$ en établissant une table de multiplication pour les éléments A, B, C de Q . Déterminer l'ordre des éléments de Q . Combien d'éléments d'ordre 4 y a-t-il dans Q ?

1.c. Déduire de **1.a-b** que les groupes D et Q ne sont pas isomorphes.

1.d. Montrer l'existence d'un morphisme de groupes $D \rightarrow S_4$ qui applique ρ sur (1234) et σ sur (13) . (On pourra vérifier que dans le groupe symétrique S_4 des relations analogues à **1.a** sont satisfaites). En déduire que D est isomorphe au plus petit sous-groupe de S_4 contenant (1234) et (13) .

Dans la suite, G désignera un sous-groupe arbitraire d'ordre 8 de S_4 .

1.e. Montrer à l'aide du théorème de Lagrange que les éléments de G sont soit des transpositions soit des produits de transpositions à supports disjoints soit des permutations cycliques d'ordre 4.

1.f. Montrer que si G contient deux transpositions alors elles sont à supports disjoints. (On pourra raisonner par l'absurde). En déduire à l'aide de **1.e** par un argument de cardinal qu'il existe une permutation cyclique d'ordre 4. Montrer enfin que G contient exactement deux permutations cycliques d'ordre 4.

1.g. Construire à l'aide de **1.d-f** un isomorphisme de groupes entre D et G . En déduire que tous les sous-groupes d'ordre 8 de S_4 sont isomorphes.

2. Anneaux-quotient et polynômes irréductibles. Soit \mathbb{K} un corps et soit $n > 0$ un entier naturel. On notera $\mathbb{K}_n[X]$ le sous-espace vectoriel de $\mathbb{K}[X]$ engendré par les monômes $1, X, X^2, \dots, X^{n-1}$. On désignera par $P(X) \in \mathbb{K}[X]$ un polynôme de degré n .

2.a. Soit $A(X) \in \mathbb{K}[X]$. Rappeler la propriété qui caractérise le reste $R_A(X)$ de la division euclidienne de $A(X)$ par $P(X)$. En déduire que $A(X) \mapsto R_A(X)$ définit une application linéaire de $\mathbb{K}[X]$ dans $\mathbb{K}_n[X]$.

2.b. Montrer que pour tous polynômes $A(X), B(X)$ de $\mathbb{K}[X]$, on a l'identité $R_{AB}(X) = R_{R_A R_B}(X)$, où $(AB)(X)$ désigne le produit de $A(X)$ et de $B(X)$.

2.c. Dédire de **2.b** qu'il existe sur le groupe $(\mathbb{K}_n[X], +)$ une loi multiplicative

$$\begin{aligned} * : \mathbb{K}_n[X] \times \mathbb{K}_n[X] &\rightarrow \mathbb{K}_n[X] \\ (A(X), B(X)) &\mapsto R_{AB}(X) \end{aligned}$$

qui en fait un anneau commutatif.

2.d. Montrer que

$$\begin{aligned} (\mathbb{K}[X], +, \cdot) &\rightarrow (\mathbb{K}_n[X], +, *) \\ A(X) &\mapsto R_A(X) \end{aligned}$$

définit un morphisme d'anneaux dont on déterminera le noyau et l'image.

2.e. Montrer que si $P(X)$ est irréductible alors tout polynôme non nul de degré strictement inférieur à n est premier à $P(X)$. En déduire (à l'aide du théorème de Bézout) que $(\mathbb{K}_n[X], +, *)$ est alors un corps. Montrer inversement que si $P(X)$ n'est pas irréductible alors $(\mathbb{K}_n[X], +, *)$ n'est pas un corps.

2.f. On pose $n = 2$ et $P(X) = X^2 + 1$. Expliciter dans $(\mathbb{K}_2[X], +, *)$ la loi multiplicative $(a + bX) * (c + dX)$. Etudier l'irréductibilité de $P(X)$ dans les cas $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Identifier les corps ainsi construits.

2.g. On pose $n = 2$ et $P(X) = X^2 + X + 1$. Expliciter dans $(\mathbb{K}_2[X], +, *)$ la loi multiplicative $(a + bX) * (c + dX)$. Etudier l'irréductibilité de $P(X)$ dans les cas $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$. Combien d'éléments contiennent les corps ainsi construits?

3. Fonction d'Euler et racines primitives de l'unité. Pour tout entier naturel non nul n , on pose $U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{2\pi i k/n} \in \mathbb{C} \mid k = 1, \dots, n\}$. La fonction d'Euler $\phi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ est définie par $\phi(1) = 1$ et, si $n > 1$, $\phi(n)$ est égal au nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

3.a. Rappeler le théorème chinois. Que peut-on dire sur les éléments inversibles de l'anneau-produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$? En déduire que pour des entiers m et n premiers entre eux, $\phi(mn) = \phi(m)\phi(n)$. Calculer $\phi(n)$ pour $n = 1, \dots, 12$.

3.b. Montrer que dans $\mathbb{C}[X]$ on a l'identité $X^n - 1 = \prod_{k=1}^n (X - e^{2\pi i k/n})$.

3.c. Montrer que si $d|n$ alors $U_d \subset U_n$ et $X^d - 1 \mid X^n - 1$ dans $\mathbb{C}[X]$; donner une formule explicite pour $\frac{X^n - 1}{X^d - 1}$ en s'inspirant du cas $d = 1$.

3.d. On pose $V_n = \{z \in U_n \mid z \text{ est d'ordre } n \text{ dans le groupe multiplicatif } U_n\}$ et $\xi_n(X) = \prod_{z \in V_n} (X - z)$. Montrer que $e^{2\pi i k/n} \in V_n$ si et seulement si $\text{pgcd}(k, n) = 1$. En déduire $\xi_p(X)$ pour p premier.

3.e. Dédire de **3.d** que pour tout $n \geq 1$, $\phi(n) = \text{deg}(\xi_n(X))$.

3.f. Montrer que U_n est réunion disjointe des V_d tels que $d|n$. En déduire l'identité $X^n - 1 = \prod_{d|n} \xi_d(X)$ et la formule $n = \sum_{d|n} \phi(d)$.

3.g. En utilisant **3.f** de manière récurrente, calculer $\xi_n(X)$ pour $n = 1, 2, \dots, 12$. Comparer avec **3.a** à l'aide de **3.e**.

CORRIGÉ

1.a. On obtient $\rho^2 = -I_2$, $\rho^3 = -\rho$, $\rho^4 = I_2$. Il s'en suit que $\sigma\rho^2 = -\sigma = \rho^2\sigma$. De plus, $\sigma\rho = -\rho\sigma = \rho^3\sigma$, et $\sigma\rho^3 = -\sigma\rho = \rho\sigma$. Comme ρ est d'ordre 4, on a $\rho^{-1} = \rho^3$; comme σ est d'ordre 2, on a $\sigma = \sigma^{-1}$. Il s'en suit que tout élément de D s'écrit comme un produit de puissances *positives* de ρ et de σ , produit qu'on peut réécrire (grâce aux trois relations établies ci-dessus) sous la forme $\rho^m\sigma^n$ avec $(m, n) \in \mathbb{N}^2$. Comme ρ est d'ordre 4 et σ d'ordre 2, on peut choisir m tel que $0 \leq m \leq 3$ et n tel que $0 \leq n \leq 2$. Par conséquent,

$$D = \{I_2, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\} = \{\pm I_2, \pm\rho, \pm\sigma, \pm\rho\sigma\}.$$

De plus, $\text{ord}(I_2) = 1$, $\text{ord}(-I_2) = \text{ord}(\pm\sigma) = \text{ord}(\pm\rho\sigma) = 2$ et $\text{ord}(\pm\rho) = 4$. Il y a donc exactement deux éléments d'ordre 4 dans D .

1.b. On vérifie les relations $A^2 = B^2 = C^2 = -I_2$ ainsi que $AB = -BA = C$, $BC = -CB = A$, $CA = -AC = B$. Il s'en suit que $\{\pm I_2, \pm A, \pm B, \pm C\}$ est stable par multiplication. De plus, les éléments de cet ensemble sont d'ordre fini; en effet:

$$\text{ord}(I_2) = 1, \text{ord}(-I_2) = 2, \text{ord}(\pm A) = \text{ord}(\pm B) = \text{ord}(\pm C) = 4.$$

Par conséquent, les inverses de ces éléments s'identifient à certaines puissances *positives*, ce qui montre que $\{\pm I_2, \pm A, \pm B, \pm C\}$ est également stable par passage à l'inverse; c'est donc un groupe : le plus petit groupe contenant les matrices A, B, C , noté Q . En particulier, Q contient exactement six éléments d'ordre 4.

1.c. Deux groupes isomorphes contiennent le même nombre d'éléments, et les ordres de leurs éléments se correspondent sous l'isomorphisme. Comme D et Q ne contiennent pas le même nombre d'éléments d'ordre 4 selon **1.a-b**, ils ne peuvent pas être isomorphes.

1.d. Pour que l'application $\phi : D \rightarrow S_4$ définie par $\phi(\rho) = (1\ 2\ 3\ 4)$ et $\phi(\sigma) = (1\ 3)$ soit un morphisme de groupes, il suffit de vérifier les relations $\phi(\sigma)\phi(\rho) = \phi(\rho)^3\phi(\sigma)$, $\phi(\sigma)\phi(\rho)^2 = \phi(\rho)^2\phi(\sigma)$, $\phi(\sigma)\phi(\rho)^3 = \phi(\rho)\phi(\sigma)$. Or, on obtient

$$\begin{aligned} (1\ 3)(1\ 2\ 3\ 4)(1\ 3)^{-1} &= (3\ 2\ 1\ 4) = (1\ 2\ 3\ 4)^3 \\ (1\ 3)(1\ 2\ 3\ 4)^2(1\ 3)^{-1} &= (1\ 3)(1\ 3)(2\ 4)(1\ 3)^{-1} = (1\ 3)(2\ 4) = (1\ 2\ 3\ 4)^2 \\ (1\ 3)(1\ 2\ 3\ 4)^3(1\ 3)^{-1} &= (1\ 3)(3\ 2\ 1\ 4)(1\ 3)^{-1} = (1\ 2\ 3\ 4) \end{aligned}$$

ce qui donne les relations requises par multiplication par $(1\ 3)$ à droite. De plus, l'image par un morphisme de groupes est un groupe; dans notre cas, cette image contient exactement huit éléments et s'identifie à l'ensemble

$$\phi(D) = \{id_4, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (3\ 2\ 1\ 4), (1\ 3), (1\ 2)(3\ 4), (2\ 4), (2\ 3)(1\ 4)\}.$$

Il s'en suit que ϕ est un *isomorphisme* de D sur le plus petit sous-groupe de S_4 contenant $\phi(\rho)$ et $\phi(\sigma)$.

1.e. Le théorème de Lagrange montre que les éléments de G sont d'ordre 1, 2, 4 ou 8. Or, toute permutation s'écrit comme produit de permutations cycliques à supports disjoints; l'ordre d'un tel produit est le *ppcm* des ordres des facteurs. Comme S_4 ne contient que des permutations cycliques d'ordre 1, 2, 3 ou 4, les seuls ordres possibles pour les éléments de G sont 1, 2 ou 4. L'élément neutre de G est d'ordre 1; les transpositions appartenant à G sont d'ordre 2; les produits de transpositions à supports disjoints appartenant à G sont d'ordre 2; enfin, les permutations cycliques de longueur 4 appartenant à G sont d'ordre 4.

1.f. Supposons que G contienne deux transpositions (ab) et (bc) à supports non-disjoints. Comme G est un groupe, il contiendrait alors également leur produit $(ab)(bc) = (abc)$ qui est une permutation cyclique d'ordre 3, ce qui est exclu selon **1.e**. Toutes les transpositions appartenant à G sont donc à supports disjoints. Ceci limite leur nombre à 2. On observe également que dans S_4 il n'existe que 3 produits de transpositions à supports disjoints, à savoir $(12)(34)$, $(13)(24)$ et $(14)(23)$. Il s'en suit selon **1.e** que G contient (avec l'élément neutre) au plus 6 éléments qui ne sont pas des permutations cycliques d'ordre 4. Comme G contient exactement 8 éléments, il contient donc au moins 2 permutations cycliques d'ordre 4. Montrons qu'il en contient exactement 2.

En effet, S_4 contient en tout 6 permutations cycliques d'ordre 4 dont 3 sont les inverses des trois autres: $\rho_1 = (1234)$ et $\rho_1^{-1} = (1432)$; $\rho_2 = (1243)$ et $\rho_2^{-1} = (1342)$; $\rho_3 = (1423)$ et $\rho_3^{-1} = (1324)$. Si G contient ρ_k alors également ρ_k^{-1} ($k = 1, 2, 3$). Supposons que G contienne ρ_1 et ρ_2 ; alors G contiendrait également $\rho_1\rho_2 = (132)$ ce qui est exclu selon **1.e**. Le même argument montre que G ne peut contenir simultanément ni ρ_1 et ρ_3 ni ρ_2 et ρ_3 . Il s'en suit que G contient soit le couple $\{\rho_1, \rho_1^{-1}\}$ soit le couple $\{\rho_2, \rho_2^{-1}\}$ soit le couple $\{\rho_3, \rho_3^{-1}\}$.

1.g. Selon **1.f**, G contient une permutations cyclique d'ordre 4, qu'on notera $(abcd)$, ainsi que son inverse $(adcb)$. Selon **1.e**, G contient alors forcément les trois produits de transpositions $(ab)(cd)$, $(ac)(bd)$ $(ad)(bc)$, l'élément neutre id_4 , ainsi que deux transpositions à supports disjoints. Comme G est stable par multiplication, ces deux transpositions sont forcément (ac) et (bd) . On obtient donc la description suivante:

$$G = \{id_4, (abcd), (ac)(bd), (adcb), (ac), (ab)(cd), (bd), (ad)(bc)\}.$$

On construit alors comme dans **1.d** un isomorphisme de groupes $\psi : D \rightarrow G$ tel que $\psi(\rho) = (abcd)$ et $\psi(\sigma) = (ac)$. Il s'en suit que tous les sous-groupes d'ordre 8 de S_4 sont isomorphes à D , donc ils sont isomorphes entre eux.

2.a. Le reste $R_A(X)$ de la division euclidienne de $A(X)$ par $P(X)$ est uniquement déterminé par l'identité $A(X) = Q_A(X)P(X) + R_A(X)$ et le fait que $\deg(R_A(X)) < \deg(P(X))$. En particulier, comme $\deg(P(X)) = n$, le reste de la division euclidienne par $P(X)$ appartient bien à $\mathbb{K}_n[X]$.

Soient deux polynômes $A(X), B(X)$ de $\mathbb{K}[X]$. Comme $A(X) = Q_A(X)P(X) + R_A(X)$ et $B(X) = Q_B(X)P(X) + R_B(X)$, il vient

$$(A + B)(X) = A(X) + B(X) = (Q_A(X) + Q_B(X))P(X) + R_A(X) + R_B(X).$$

Par conséquent, puisque $\deg(R_A(X) + R_B(X)) < n$, on obtient $R_{A+B}(X) = R_A(X) + R_B(X)$. Pour $\lambda \in \mathbb{K}$, l'identité $\lambda A(X) = \lambda Q_A(X)P(X) + \lambda R_A(X)$ entraîne que $\lambda R_A(X) = R_{\lambda A}(X)$, puisque $\deg(\lambda R_A(X)) < n$. L'application $A(X) \mapsto R_A(X)$ est donc bien une application linéaire de $\mathbb{K}[X]$ dans $\mathbb{K}_n[X]$.

2.b. On garde les notations de **2.a.** Il vient alors

$$\begin{aligned}(AB)(X) &= ((Q_AP + R_A)(Q_BP + R_B))(X) \\ &= ((Q_AQ_BP + Q_AR_B + R_AQ_B)P)(X) + (R_AR_B)(X);\end{aligned}$$

Soit encore

$$(AB)(X) = (Q_AQ_BP + Q_AR_B + R_AQ_B + Q)(X)P(X) + R_{R_AR_B}(X),$$

où $(R_AR_B)(X) = Q(X)P(X) + R_{R_AR_B}(X)$ et $\deg(R_{R_AR_B}(X)) < n$. Il s'en suit que $R_{AB}(X) = R_{R_AR_B}(X)$, par la propriété caractéristique du reste.

2.c. Il suffit de montrer que $*$ est associatif (avec élément neutre), commutatif, et distributif par rapport à $+$. Soient $A(X), B(X), C(X)$ trois polynômes de $\mathbb{K}_n[X]$. Pour des raisons de degré, on a $A(X) = R_A(X), B(X) = R_B(X)$ et $C(X) = R_C(X)$. Il vient alors

$$\begin{aligned}(A(X) * B(X)) * C(X) &= R_{(A(X)*B(X))C(X)}(X) \\ &= R_{R_AR_BC}(X);\end{aligned}$$

ce reste s'identifie à $R_{(AB)C}(X)$, d'après **2.b.** De même, on obtient

$$A(X) * (B(X) * C(X)) = R_{A(BC)}(X).$$

Comme le produit dans $\mathbb{K}[X]$ est associatif, on obtient l'associativité de $*$. Le polynôme constant 1 est le neutre pour $*$ car $R_{1.A}(X) = R_A(X)$. La commutativité découle des identités

$$A(X) * B(X) = R_{AB}(X) = R_{BA}(X) = B(X) * A(X).$$

Enfin, la distributivité s'obtient par

$$\begin{aligned}(A(X) + B(X)) * C(X) &= R_{(A+B)C}(X) \\ &= R_{AC+BC}(X);\end{aligned}$$

vu **2.a.**, c'est aussi $R_{AC}(X) + R_{BC}(X) = (A(X) * C(X)) + (B(X) * C(X))$.

2.d. L'application $A(X) \mapsto R_A(X)$ est bien un morphisme d'anneaux: elle respecte les structures additives par **2.a.**, elle respecte les structures multiplicatives par **2.b.**; en plus, elle préserve 0 et 1 car $R_0(X) = 0$ et $R_1(X) = 1$ car $1 = 0.P(X) + 1$.

L'image de ce morphisme d'anneaux est $\mathbb{K}_n[X]$, car pour $A(X) \in \mathbb{K}_n[X]$, on a $A(X) = R_A(X)$. Le noyau de ce morphisme d'anneaux est l'idéal $P(X)\mathbb{K}[X]$ car $R_A(X)$ est nul si et seulement si $P(X)$ divise $A(X)$.

2.e. Soit $A(X)$ un polynôme non nul de degré $< n$. Le polynôme $P(X)$ est irréductible si et seulement si les seuls diviseurs de $P(X)$ sont les polynômes

$\lambda P(X)$, $\lambda \in \mathbb{K}^\times$, et les polynômes constants non nuls. Tout diviseur commun de $P(X)$ et de $A(X)$ est donc forcément un polynôme constant non nul; autrement dit, $P(X)$ et $A(X)$ sont premiers entre eux.

On en déduit l'existence de deux polynômes $B(X)$ et $C(X)$ tels que $P(X)B(X) + A(X)C(X) = 1$. On peut même supposer que $\deg(C(X)) < \deg(P(X))$ quitte à remplacer $C(X)$ par $R_C(X)$. En appliquant le morphisme d'anneaux **2.d** à cette identité, on obtient l'identité $A(X) * C(X) = 1$, ce qui montre que tout élément non nul $A(X)$ de l'anneau commutatif $(\mathbb{K}_n[X], +, *)$ possède un inverse: c'est précisément la définition d'un corps.

Supposons inversement que $P(X) = P_1(X)P_2(X)$ avec $\deg(P_1(X)) < n$ et $\deg(P_2(X)) < n$. En appliquant le morphisme d'anneaux **2.d** à cette identité, on obtient l'identité $0 = P_1(X) * P_2(X)$ dans l'anneau $\mathbb{K}_n[X]$. Comme tout corps est intègre, cela montre que $(\mathbb{K}_n[X], +, *)$ n'est pas un corps si $P(X)$ n'est pas irréductible.

2.f. Pour $P(X) = X^2 + 1$, on obtient $R_{X^2}(X) = -1$. Il s'en suit que

$$(a + bX) * (c + dX) = ac + (ad + bc)X + bdR_{X^2}(X) = ac - bd + (ad + bc)X.$$

On obtient le même résultat en effectuant une division euclidienne de $(a + bX)(c + dX)$ par $P(X)$.

Un polynôme de degré 2 de $\mathbb{K}[X]$ est irréductible si et seulement s'il n'a pas de racines dans \mathbb{K} . $P(X)$ a deux racines complexes conjuguées i et $-i$. Par conséquent, $P(X)$ est irréductible dans $\mathbb{Q}[X]$, irréductible dans $\mathbb{R}[X]$, mais réductible dans $\mathbb{C}[X]$.

Le corps $\mathbb{Q}_2[X]$ s'identifie (en évaluant en i) au plus petit sous-corps de \mathbb{C} contenant \mathbb{Q} et i ; c'est un \mathbb{Q} -espace vectoriel de base $(1, X)$, souvent noté $\mathbb{Q}[i]$. Le corps $\mathbb{R}_2[X]$ s'identifie (en évaluant en i) au corps des nombres complexes \mathbb{C} ; c'est en particulier un \mathbb{R} -espace vectoriel de base $(1, X)$, souvent noté $\mathbb{R}[i]$.

2.g. Pour $P(X) = X^2 + X + 1$ on obtient $R_{X^2}(X) = -X - 1$. Il s'en suit que

$$(a + bX) * (c + dX) = ac + (ad + bc)X + bdR_{X^2}(X) = ac - 1 + (ad + bc - 1)X.$$

On vérifie aisément que $P(X)$ n'a de racines ni dans \mathbb{F}_2 ni dans \mathbb{F}_5 ; par contre $P(1) = 0$ dans \mathbb{F}_3 et $P(2) = 0$ dans \mathbb{F}_7 . Par conséquent, $P(X)$ est irréductible dans $\mathbb{F}_2[X]$ et $\mathbb{F}_5[X]$, mais réductible dans $\mathbb{F}_3[X]$ et $\mathbb{F}_7[X]$.

Le corps $((\mathbb{F}_2)_2[X], +, *)$ est en particulier un \mathbb{F}_2 -espace vectoriel de base $(1, X)$, et contient donc 4 éléments.

Le corps $((\mathbb{F}_5)_2[X], +, *)$ est en particulier un \mathbb{F}_5 -espace vectoriel de base $(1, X)$, et contient donc 25 éléments.

3.a. Soient m et n des entiers premiers entre eux. Le *théorème chinois* donne alors un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Comme les éléments inversibles de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont précisément les couples formés d'un élément inversible de $\mathbb{Z}/m\mathbb{Z}$ et d'un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, on obtient ainsi une

correspondance bijective entre les éléments inversibles de $\mathbb{Z}/mn\mathbb{Z}$ et les couples d'éléments inversibles décrits ci-dessus; par conséquent: $\phi(mn) = \phi(m)\phi(n)$.

Remarque : L'isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est valide que pour des entiers m et n premiers entre eux. Si m et n ne sont pas premiers entre eux, il existe bien un morphisme d'anneaux injectif

$$\mathbb{Z}/\text{ppcm}(m, n)\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

mais, en général, celui-ci n'est pas surjectif !!!

Par conséquent, le théorème chinois ne se généralise pas à un couple d'entiers (m, n) quelconque !!!

Les valeurs suivantes de la fonction d'Euler découlent du théorème chinois et du fait que pour $n = p^s$ avec p premier, on a $\phi(p^s) = p^s - p^{s-1}$; en effet, dans $\mathbb{Z}/p^s\mathbb{Z}$ un élément est non-inversible si et seulement s'il est divisible par p , ce qui est le cas pour exactement p^{s-1} éléments de $\mathbb{Z}/p^s\mathbb{Z}$. Ainsi, on obtient

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \phi(7) = 6, \phi(8) = 4, \phi(9) = 6, \phi(10) = 4, \phi(11) = 10, \phi(12) = 4.$$

3.b. Tous les éléments de U_n sont racines du polynôme $X^n - 1$. Il s'en suit que $\prod_{k=1}^n (X - e^{2\pi ik/n})$ divise $X^n - 1$. Comme les degrés et les coefficients directeurs des deux polynômes sont identiques, ils coïncident.

3.c. Si $d|n$ alors $z^d = 1$ implique $z^n = (z^d)^{\frac{n}{d}} = 1^{\frac{n}{d}} = 1$, donc $z \in U_d$ implique $z \in U_n$, ce qui montre l'inclusion $U_d \subset U_n$. Il s'en suit que $\prod_{z \in U_d} (X - z)$ divise $\prod_{z \in U_n} (X - z)$. D'après **3.b**, le premier produit s'identifie à $X^d - 1$, le second produit s'identifie à $X^n - 1$.

Si $d|n$ alors $(X^d - 1)(X^{n-d} + X^{n-2d} + \dots + X^d + 1) = X^n - 1$. Il s'en suit que $\frac{X^n - 1}{X^d - 1} = (X^{n-d} + X^{n-2d} + \dots + X^d + 1)$.

3.d. D'après le théorème de Lagrange, l'ordre de $e^{2\pi ik/n}$ est un diviseur d de l'ordre n du groupe U_n . En plus, pour $d|n$, on a les équivalences suivantes:

$$(e^{2\pi ik/n})^d = 1 \Leftrightarrow e^{2\pi ikd/n} = 1 \Leftrightarrow n|kd \Leftrightarrow \frac{n}{d} \text{ est un diviseur de } k$$

La dernière propriété peut encore se reformuler en disant que $\frac{n}{d}$ est un diviseur commun de n et de k . On en déduit que $e^{2\pi ik/n}$ est d'ordre n si et seulement si n et k sont premiers entre eux. Comme corollaire on obtient pour p premier :

$$\xi_p(X) = \prod_{z \in V_p} (X - z) = \prod_{k=1}^{p-1} (X - e^{2\pi ik/p}) = \frac{X^p - 1}{X - 1} = X^{p-1} + \dots + X + 1.$$

3.e. Pour $n = 1$ on a $U_1 = V_1 = \{1\}$ et $\xi_1(X) = X - 1$, d'où $\phi(1) = \text{deg}(\xi_1(X))$. Pour $n > 1$, $\text{deg}(\xi_n(X)) = \#V_n$. D'après **3.d** et le théorème de Bézout, on a

$$\#V_n = \#\{k \in \mathbb{N} \mid 1 \leq k \leq n \text{ et } \text{pgcd}(k, n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n).$$

3.f. Soit $z \in U_n$. D'après Lagrange, l'ordre d de z divise n , et par conséquent: $V_d \subset U_d \subset U_n$, cf. **3.c**. Chaque élément $z \in U_n$ a un ordre bien définie,

et $d = \text{ord}(z)$ si et seulement si $z \in V_d$. Il s'en suit que U_n s'écrit comme une réunion disjointe des V_d où d parcourt l'ensemble des diviseurs de n . En regroupant les n facteurs de $X^n - 1$ selon cette réunion disjointe, on obtient

$$X^n - 1 = \prod_{z \in U_n} (X - z) = \prod_{d|n} \prod_{z \in V_d} (X - z) = \prod_{d|n} \xi_d(X).$$

Comme le degré d'un produit de polynômes est égal à la somme des degrés des facteurs, on obtient à l'aide de **3.e**

$$n = \text{deg}(X^n - 1) = \text{deg} \prod_{d|n} \xi_d(X) = \sum_{d|n} \text{deg}(\xi_d(X)) = \sum_{d|n} \phi(d).$$

3.g. Les formules suivantes découlent de **3.d-e** pour $n = 1$ et $n = p$ premier; dans les autres cas, elles sont obtenues en utilisant de manière récurrente **3.f** et **3.c**. Le degré de $\xi_n(X)$ correspond bien à la valeur $\phi(n)$ donnée en **3.a**.

$$\xi_1(X) = X - 1$$

$$\xi_2(X) = X + 1$$

$$\xi_3(X) = X^2 + X + 1$$

$$\xi_4(X) = \frac{X^4 - 1}{\xi_1(X)\xi_2(X)} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1$$

$$\xi_5(X) = X^4 + X^3 + X^2 + X + 1$$

$$\xi_6(X) = \frac{X^6 - 1}{\xi_1(X)\xi_2(X)\xi_3(X)} = \frac{X^3 + 1}{\xi_2(X)} = X^2 - X + 1$$

$$\xi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

$$\xi_8(X) = \frac{X^8 - 1}{\xi_1(X)\xi_2(X)\xi_4(X)} = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1$$

$$\xi_9(X) = \frac{X^9 - 1}{\xi_1(X)\xi_3(X)} = \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1$$

$$\xi_{10}(X) = \frac{X^{10} - 1}{\xi_1(X)\xi_2(X)\xi_5(X)} = \frac{X^5 + 1}{X + 1} = X^4 - X^3 + X^2 - X + 1$$

$$\xi_{11}(X) = X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

$$\xi_{12}(X) = \frac{X^{12} - 1}{\xi_1(X)\xi_2(X)\xi_3(X)\xi_4(X)\xi_6(X)} = \frac{X^6 + 1}{\xi_4(X)} = X^4 - X^2 + 1$$

Remarque : Les polynômes $\xi_n(X)$, $n > 0$, s'appellent *polynômes cyclotomiques*. On peut montrer qu'ils sont irréductibles dans $\mathbb{Q}[X]$.

Barème : L'examen a été noté sur 26 :

le premier exercice a été noté sur $9 = 1, 5 + 1, 5 + 1 + 1, 5 + 1 + 1, 5 + 1$,

le deuxième exercice a été noté sur $9 = 1 + 0, 5 + 1, 5 + 1, 5 + 1, 5 + 1 + 2$,

le troisième exercice a été noté sur $8 = 1, 5 + 0, 5 + 1 + 1 + 1 + 1, 5 + 1, 5$.