Université de Strasbourg
MPA Algèbre S1
P. Guillot, bureau 314, guillot@math.unistra.fr

Partie II : algèbre

Nombres complexes

Exercice 1. Donner la partie réelle et la partie imaginaire de chacun des nombres complexes suivants :

a) $(2+3i)^2$ b) $(1+i)^3$ c) $\dfrac{1}{1+2i}$

d) $\dfrac{2+i}{1+i}$ e) i^{41} f) $\dfrac{(2+i)^2}{(2-i)^2}$

g) $(1+i)^{-3}$

Exercice 2.

1. Mettre l'expression $e^{i\theta}+e^{i\theta'}$ sous la forme $\rho e^{i\phi}$ avec ρ et ϕ réels.
2. Mettre sous forme trigonométrique : $1+e^{\frac{i\pi}{3}}$ et $e^{\frac{4i\pi}{3}}-1$.
3. Soient A, B, C trois points sur le cercle unité (en d'autres termes, les affixes a, b, et c de A, B, C sont des nombres complexes de module 1). Montrer par le calcul que si B et C sont diamétralement opposés, alors ABC est rectangle en A. (Résultat de géométrie déjà connu, normalement.)
4. Montrer la réciproque : si B et C sont sur le cercle unité, diamétralement opposés, et si ABC est rectangle en A, alors A est aussi sur le cercle unité.

   Conseils : le calcul se ramène à montrer que si une expression de la forme $(z-1)/(z+1)$ est imaginaire pure, alors z est de module 1 ; pour ceci, montrer d'abord que $(\bar{z}-1)(z+1)$ est également imaginaire pur.

Exercice 3. Calculer les racines carrées de 1, i, $3+4i$, $8-6i$, et $7+24i$.

Exercice 4. Résoudre dans $\mathbb{C}$ les équations suivantes :

$z^2+z+1=0$; $z^2-(1+2i)z+i-1=0$; $z^2-\sqrt{3}z-i=0$;

$z^2-(5-14i)z-2(5i+12)=0$; $z^2-(3+4i)z-1+5i=0$;

$4z^2-2z+1=0$; $z^4+10z^2+169=0$; $z^4+2z^2+4=0$.

Exercice 5. On appelle *demi-plan de Poincaré* l'ensemble $\mathcal{P}$ des nombres complexes z tels que $\mathrm{Im}z>0$, et *disque unité* l'ensemble $\mathcal{D}$ des nombres complexes z tels que $|z|<1$. Démontrer que $z \mapsto \frac{z-i}{z+i}$ est une bijection de $\mathcal{P}$ sur $\mathcal{D}$.

Autour de $\mathbb{Z}/n\mathbb{Z}$

Exercice 6. Ecrire la table de multiplication de $\mathbf{Z}/6\mathbf{Z}$, celle de $\mathbf{Z}/7\mathbf{Z}$.

Exercice 7. Résoudre l'équation $x^2=1$ dans $\mathbf{Z}/8\mathbf{Z}$. Commentaire ?

Exercice 8. Déterminer, pour chaque élément non nul de $\mathbf{Z}/13\mathbf{Z}$, son inverse. Calculer le produit de tous éléments non nuls de $\mathbf{Z}/13\mathbf{Z}$. En déduire la congruence : $12! \equiv -1 \pmod{13}$.

Exercice 9. On veut généraliser l'exercice précédent en remplaçant 13 par un nombre premier $p \geq 3$. Montrer que $\bar{1}$ et $-\bar{1}$ sont les deux seuls éléments de $\left(\mathbf{Z}/p\mathbf{Z}\right)^* = \left(\mathbf{Z}/p\mathbf{Z}\right) \setminus \{0\}$ qui coïncident avec leur inverse. On résoudra pour cela l'équation $x^2=1$ dans $\mathbf{Z}/p\mathbf{Z}$.

En déduire la valeur du produit de tous éléments non nuls de $\mathbf{Z}/p\mathbf{Z}$ puis la congruence : $(p-1)! \equiv -1 \pmod{p}$.

Exercice 10. (« Critère de Wilson » – utilise le précédent). Montrer que p premier $\iff$ p divise $(p-1)!+1$

Exercice 11. Résoudre dans $\mathbb{Z}/37\mathbb{Z}$:

1. $$\begin{cases} \bar{3}x+\bar{7}y=\bar{3} \\ \bar{6}x-\bar{7}y=\bar{0}. \end{cases}$$
2. $x^2-\overline{31}x+\overline{18}=\bar{0}$.

Exercice 12. (Plus difficile.) Montrer qu'il existe un corps possédant 4 éléments, et qu'il est unique.

Polynômes : premiers calculs

Exercice 13 (Somme et produit de polynômes et leur degrés)**.** Étant donnés deux polynômes $P, Q \in \mathbb{K}[X]$ exprimer les degrés de $(-10)P$, de $P+Q$ et $P \cdot Q$ en fonction de $deg(P)$ et $deg(Q)$.

Exercice 14. Montrer que, si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau intègre.

Exercice 15. Soit $P_n(X) = (1+X)(1+X^2)(1+X^4)(1+X^8)\cdots(1+X^{2^n})$. Calculer les coefficients de P_n. Pouvez-vous le faire sans récurrence ?

Exercice 16. Pour $n \neq 0$, trouver toutes les racines du polynôme $P_n(X) = 1 - X + \frac{X(X-1)}{2!} - \cdots + (-1)^n \frac{X(X-1)\cdots(X-n+1)}{n!}$.

Indication : commencer par regarder $P_n(n)$.

Division euclidienne de polynômes

Exercice 17. Trouvez le quotient et le reste des divisions suivantes : $(2X+5)$ par $(3X+1)$, (X^2-2X) par $(X-2)$, (X^2+6X+9) par $(X+3)$, (X^3-2X+3) par (X^2-1), (X^3-4X^2+2) par (X^2+i), $(X^4-2X^2+17X-10)$ par (X^4-3X^2+1).

Exercice 18. Déterminer p et q dans $\mathbb{R}$ pour que $P = X^3 + pX + q$ soit divisible par $Q = X^2 + 3X - 1$.

Exercice 19. Soit P un polynôme tel que les restes de la division euclidienne de P par $(X-1), (X-2)$ et $(X-3)$ soient $3, 7$ et 13 respectivement. Déterminer le reste de la division euclidienne de P par $(X-1)(X-2)(X-3)$.

Exercice 20. Soit $t \in \mathbb{R}$ un paramètre, $n \in \mathbb{N}$, et $P_n(X) = (\sin(t)X + \cos(t))^n$. Déterminer le reste de la division euclidienne de P par (X^2+1) .

Dérivées de polynômes

Par définition, si

$$P = a_0 + a_1X + \cdots + a_nX^n\,,$$

sa dérivée est

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1}\,.$$

Les règles habituelles s'appliquent, notamment $(PQ)' = P'Q + PQ'$, comme vous pouvez le montrer à titre d'exercice (pour les polynômes à coefficients dans $\mathbb{C}$ ou $\mathbb{Z}/p\mathbb{Z}$, on ne peut pas le déduire de ce qu'on sait déjà des dérivées...).

Exercice 21. Déterminer tous les polynômes P de $\mathbb{R}[X]$, non nuls, tels que $(X^2+1)P''(X) - 6P = 0$ et $P(1) = 2$.

Exercice 22. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \geq 0$ un entier. Montrer que les deux énoncés ci-dessous sont équivalents :

1. m est le plus grand entier tel que $(X-a)^m$ divise P.
2. On peut écrire $P = (X-a)^m Q$ avec $Q(a) \neq 0$.

Dans ce cas on dit que a est une racine de multiplicité m de P ; lorsque $m \geq 2$ on dit souvent que a est une « racine multiple ». On note que, avec ce vocabulaire, une « racine de multiplicité 0 » est un nombre qui n'est pas une racine du tout (attention).

Montrer ensuite que, si a est une racine de multiplicité $m \geq 1$ de P, alors a est une racine de multiplicité $m-1$ de P'.

Est-il vrai, réciproquement, que si $m \geq 1$ et si a est une racine de multiplicité $m-1$ de P', alors a est une racine de multiplicité m de P ? *Attention !*

On retiendra en particulier par cœur que a est une racine multiple de P si et seulement si $P(a) = 0 = P'(a)$. Vérifiez que l'on a bien montré ça !

Exercice 23. Soit $n \in \mathbb{N}$, montrer que le polynôme $P_n = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$ n'a pas de racine multiple.

Exercice 24. Déterminer $a, b \in \mathbb{Z}$ de façon à ce que le polynôme $aX^{n+1} - bX^n + 1$ soit divisible par $(X-1)^2$.

Factorisations

Exercice 25. Décomposer dans $\mathbb{R}[X]$, sans déterminer ses racines, le polynôme $P = X^4 + 1$, en produit de facteurs irréductibles.

Exercice 26. Dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$, décomposer les polynômes suivants en facteurs irréductibles.

1. $X^3 - 3$.
2. $X^{12} - 1$.
3. $X^9 + X^6 + X^3 + 1$.

Calculs de PGCD

Exercice 27. Calculer $pgcd(1001, 221)$. Idem pour 33055 et 12621.

Exercice 28. Calculer $pgcd(P, Q)$ dans chaque cas : $(P = 2X+2, Q = 3X+4)$; $(P = X^2-3X, Q = X-4)$; $(P = X^2+6X+1, Q = X-3)$; $(P = X^4-3X^2+3; Q = X^3-2)$; $(P = X^5-4X^2+2, Q = X^3+i)$; $(P = X^6-3X^2+7X-11, Q = X^4-3X^2+1)$.

Exercice 29. Soient $P = X^5 + X^4 - 6X^3 - X^2 - X + 6$ et $Q = X^4 + 2X^3 - X - 2$. Déterminer $pgcd(P, Q)$ et en déduire les racines communes de P et Q.

Exercice 30. Soient $n, p \in \mathbb{N}$.

1. Trouver quotient et reste de la division de $(X^n - 1)$ par $X^p - 1$.
2. Trouver une condition nécéssaire et suffisante pour que $X^p - 1$ divise $X^n - 1$.
3. Trouver le $pgcd$ de $X^n - 1$ et $X^p - 1$.

Théorème de Bézout

Exercice 31. Soient $P = 2X^4 + X^3 - 2X - 1$ et $Q = 2X^4 - X^3 - 3X^2 + X + 1$. Trouver $U, V \in \mathbb{C}[X]$ tels que $UP + QV = pgcd(P, Q)$. Quelles sont les racines communes de P et de Q ?

Exercice 32. Soit $n \in \mathbb{N}$. Déterminer $pgcd((X-1)^n, X^n - 1)$ en pensant aux racines communes. Pour $n = 3$ trouver $U, V \in \mathbb{C}[X]$ tels que $(X-1)^3V + (X^3-1)U = X - 1$.

Exercice 33.

1. Soient $P, Q \in \mathbb{K}[X]$ et U, V tels $PU + QV = 1$. Montrer qu'alors $pgcd(P, Q) = 1 = pgcd(U, V)$.
2. Soient $P, Q \in \mathbb{K}[X]$ et U, V tels que $PU + QV = pgcd(P, Q)$. Montrer qu'alors $pgcd(U, V) = 1$.

Ces résultats sont-ils valables avec $\mathbb{Z}$ plutôt que $\mathbb{K}[X]$?

Exercice 34. Montrer que $2^n + 1$ et $2^{n+1} + 1$ sont premiers entre eux, pour $n \in \mathbb{N}$.

Exercice 35. Trouver tous les entiers u, v tels que $12u + 8v = 1$. Puis, faire de même avec l'équation $12u + 7v = 1$.

Exercice 36. Résoudre

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 11 \bmod 16\,. \end{cases}$$

Exercice 37. (Extrait examen 2018.) 11 pirates ont trouvé un trésor composé de pièces d'or. Ils essaient de partager en parts égales, et il reste 3 pièces. Cette déception engendre une bagarre et un pirate meurt.

Les 10 pirates restant essaient de partager le trésor en parts égales, et il reste 7 pièces. À nouveau, la tension monte, et un pirate meurt lors d'une bagarre.

Les 9 pirates restant parviennent à partager les pièces d'or de manière équitable.

Trouver le nombre minimum de pièces dans le trésor.

Exercice 38. Soient A, B deux polynômes premiers entre eux. Prouver qu'il existe un unique couple (U, V) tel que $AU+BV = 1$ avec $deg(U) < deg(B)$ et $deg(V) < deg(A)$.

Que dire sur $\mathbb{Z}$?

Exercice 39. Soit

$$(E) \quad (X+1)^2A + (X-1)^2B = 1.$$

1. Trouver une solution particulière A_0, B_0 de (E) avec $A_0, B_0 \in \mathbb{R}[X]$.
2. En déduire toutes les solutions de (E).
3. Déterminer tous les polynômes P tels que $P-1$ soit un multiple de $(X+1)^2$ et que $P+1$ soit un multiple de $(X-1)^2$.

Petit théorème de Fermat

Exercice 40. Soit p un nombre premier, et k un entier tel que $1 \leq k \leq p-1$. Montrer que p divise $\binom{p}{k}$. Quelles sont les conséquences pour la formule du binôme ?

Plus difficile : montrer que

$$\binom{p-1}{k} \equiv (-1)^k \bmod p\,.$$

On pourra calculer de deux manières différentes les coefficients du polynôme $(X-1)^{p-1} \in \mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 41 (Petit théorème de Fermat)**.** Soit p un nombre premier. Montrer, si l'entier x vérifie $x^p \equiv x \bmod p$, alors $(x+1)^p \equiv x+1 \bmod p$. Conclusions ?

Exercice 42 (Petit théorème de Fermat, deuxième démonstration)**.** *Cette deuxième démonstration peut paraître plus compliquée la première fois qu'on la voit, mais c'est un argument très général, qui reviendra souvent. Voir le dernier chapitre, sur les « groupes », et notamment le « théorème de Lagrange ».*

Soit p un nombre premier, et soit $t \in (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.

1. Montrer qu'il existe un plus petit entier $k > 0$ tel que $t^k = \bar{1}$. *On dit que k est l'ordre de t.*
2. Pour $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$ on va noter $x \sim y$ lorsqu'il existe un entier $i \in \mathbb{Z}$ tel que $y = xt^i$. Montrer que $\sim$ est une relation d'équivalence.
3. Calculer la taille des classes d'équivalence.
4. En déduire que $t^{p-1} = \bar{1}$. Puis, retrouver les conclusions de l'exercice précédent.

Exercice 43. Quel est le reste de la division euclidienne de 2^{49} par 7 ? de 28^{1000} par 13 ?

Matrices : premiers calculs

Exercice 44. On considère les trois matrices suivantes :

$$A = \begin{pmatrix} 2 & -3 & 1 & 0 \\ 5 & 4 & 1 & 3 \\ 6 & -2 & -1 & 7 \end{pmatrix} \qquad B = \begin{pmatrix} 7 & 2 \\ -5 & 2 \\ 3 & 1 \\ 6 & 0 \end{pmatrix}$$

et

$$C = \begin{pmatrix} -1 & 2 & 6 \\ 3 & 5 & 7 \end{pmatrix}.$$

1. Calculer AB puis $(AB)C$.
2. Calculer BC puis $A(BC)$.
3. Que remarque-t-on ?

Exercice 45. On considère les deux matrices suivantes :

$$A = \begin{pmatrix} 2 & 3 & -4 & 1 \\ 5 & 2 & 1 & 0 \\ 3 & 1 & -6 & 7 \\ 2 & 4 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & -1 & -3 & 7 \\ 4 & 0 & 2 & 1 \\ 2 & 3 & 0 & -5 \\ 1 & 6 & 6 & 1 \end{pmatrix}$$

1. Calculer AB.
2. Calculer BA.
3. Que remarque-t-on ?

Exercice 46. Soit $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. Calculer A^2 et vérifier que $A^2 = A + 2I_3$, où I_3 est la matrice identité 3×3. En déduire que A est inversible et calculer son inverse.

Exercice 47. Mettre les matrices de l'exercice 44 sous forme bien échelonnée. Puis, faire de même avec

$$D = \begin{pmatrix} 1 & -3 & -6 & 7 \\ -3 & 4 & 8 & -11 \\ -4 & 2 & 5 & -8 \\ 1 & -2 & -4 & 5 \end{pmatrix}, \quad E = \begin{pmatrix} -1 & -3 & 7 \\ 7 & 2 & -11 \\ -2 & -2 & 6 \\ 14 & 5 & -24 \end{pmatrix}.$$

Opérations sur les lignes

Exercice 48. Mettre sous forme matricielle et résoudre les systèmes suivants.

1. $\left\{\begin{array}{rcl} 2x+y+z &=& 3\\ 3x-y-2z &=& 0\\ x+y-z &=& -2\\ x+2y+z &=& 1 \end{array}\right.$

2. $\left\{\begin{array}{rcl} x+y+z+t &=& 1\\ x-y+2z-3t &=& 2\\ 2x+4z+4t &=& 3\\ 2x+2y+3z+8t &=& 2\\ 5x+3y+9z+19t &=& 6 \end{array}\right.$

3. $\left\{\begin{array}{rcl} 2x+y+z+t &=& 1\\ x+2y+3z+4t &=& 2\\ 3x-y-3z+2t &=& 5\\ 5y+9z-t &=& -6 \end{array}\right.$

4. $\left\{\begin{array}{rcl} x-y+z+t &=& 5\\ 2x+3y+4z+5t &=& 8\\ 3x+y-z+t &=& 7 \end{array}\right.$

5. $\left\{\begin{array}{rcl} x+2y+3z &=& 0\\ 2x+3y-z &=& 0\\ 3x+y+2z &=& 0 \end{array}\right.$

Exercice 49. Les matrices suivantes sont-elles inversibles ? Si oui, calculer leurs inverses.

$$\begin{pmatrix} 1 & 2 & 3\\ 2 & 3 & 1\\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1\\ 2 & 0 & 1\\ 1 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 1 & -1\\ 0 & 3 & 0\\ 0 & 2 & 1 \end{pmatrix}.$$

Exercice 50. Calculer l'inverse de la matrice suivante :

$$A = \begin{pmatrix} 4 & 8 & 7 & 4\\ 1 & 3 & 2 & 1\\ 1 & 2 & 3 & 2\\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Exercice 51. Pour quelles valeurs de a la matrice

$$A = \begin{pmatrix} 1 & 1 & 1\\ 1 & 2 & 4\\ 1 & 3 & a \end{pmatrix}$$

est-elle inversible ? Calculer dans ce cas son inverse.

Exercice 52. Résoudre les systèmes dépendant d'un paramètre réel a :

$$\left\{\begin{array}{rcl} ax + y &=& 2\\ (a^2+1)x + 2ay &=& 1 \end{array}\right.$$

et

$$\left\{\begin{array}{rcl} (a+1)x + (a-1)y &=& 1\\ (a-1)x + (a+1)y &=& 1 \end{array}\right.$$

Matrices : autres exercices

Exercice 53 (Une remarque à garder en tête)**.** Soit A une matrice carrée. On suppose que le système

$$AX = 0$$

(où X est un vecteur-colonne contenant les inconnues, et 0 désigne le vecteur nul) ne possède que la solution $X = 0$. Montrer que A est inversible.

Exercice 54. On considère les matrices :

$$A = \begin{pmatrix} 1 & 2 & 3\\ 0 & 1 & 2\\ 0 & 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 2 & 3\\ 0 & 0 & 2\\ 0 & 0 & 0 \end{pmatrix}$$

1. Pour chaque entier $n \geq 1$ calculer B^n.
2. En déduire A^n.
3. Soient (u_n), (v_n) et (w_n) trois suites définies par la donnée de u_0, v_0, w_0 et par la relation de récurrence :

$$\left\{\begin{array}{rcl} u_{n+1} &=& u_n + 2v_n + 3w_n\\ v_{n+1} &=& v_n + 2w_n\\ w_{n+1} &=& w_n \end{array}\right.$$

Calculer (u_n), (v_n) et (w_n) en fonction de u_0, v_0, w_0.

Exercice 55. On note N la matrice carrée de taille $m \times m$ dont les coefficients n_{ij} sont donnés par : $n_{ij} = 1$ si $j = i+1$ et $n_{ij} = 0$ sinon.

1. Ecrire explicitement la matrice N, d'abord pour $m = 3$ puis « avec des pointillés » en général. Ensuite, faire de même avec $A = I + N$ (avec I la matrice identité $m \times m$).
2. Calculer les puissances de N.
3. En déduire que A est inversible et calculer son inverse. On utilisera pour cela une identité remarquable bien connue.

Exercice 56 (Défi)**.** Soient A et B des matrices carrées telles que $AB = A + B$. Montrer que $AB = BA$.

Exercice 57. Dans cet exercice, les matrices considérées sont carrées, de taille $n \times n$. On définit la *trace* d'une matrice comme étant la somme des coefficients sur la diagonale ; en d'autres termes, si $A = (a_{ij})_{i,j}$, alors

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}\,.$$

1. Soit $A = (a_{ij})_{i,j}$ et $B = (b_{ij})_{i,j}$. Exprimer $\mathrm{Tr}(AB)$ en fonction des coefficients a_{ij} et b_{ij}.
2. En déduire que $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.
3. Soit P une matrice inversible, et M une matrice quelconque. Montrer que $\mathrm{Tr}(P^{-1}MP) = \mathrm{Tr}(M)$.

Exercice 58 (Cayley-Hamilton pour les matrices 2×2)**.** Soit $A \in \mathrm{M}_2(\mathbb{K})$. Montrer que

$$A^2 - \mathrm{Tr}(A) \cdot A + \det(A) \cdot I = 0\,.$$

Ici I est la matrice identité 2×2. On rappelle que, si

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

alors $\det(A) = ad - bc$.

Exercice 59 (Suite de Fibonacci)**.** Soit

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})\,.$$

1. Montrer que $A^2 - A - I = 0$.
2. Trouver λ_1 et λ_2 tels que
$$X^2 - X - 1 = (X - \lambda_1)(X - \lambda_2).$$
Puis, trouver des scalaires $s, t \in \mathbb{R}$ tels que
$$s(A - \lambda_1 \cdot I) + t(A - \lambda_2 \cdot I) = I\,.$$
3. Soit $v \in \mathrm{M}_{2,1}(\mathbb{R})$ un vecteur, c'est-à-dire une matrice-colonne. Déduire de la question précédente que l'on peut trouver deux vecteurs v_1 et v_2 tels que $v = v_1 + v_2$ et
$$Av_1 = \lambda_1 v_1\,, \qquad Av_2 = \lambda_2 v_2\,.$$
4. Donner une formule pour $A^n v_1$, $A^n v_2$ et $A^n v$, pour tout $n \geq 1$. Pour
$$v = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$
déterminer explicitement v_1 et v_2, puis $A^n v$.
Conseils de calcul. Garder λ_1 et λ_2 le plus longtemps possible, plutôt que leurs expressions avec une racine carrée. Exploiter les identités $\lambda_1 + \lambda_2 = 1$, $\lambda_1\lambda_2 = -1$, $\lambda_2 - \lambda_1 = \pm\sqrt{5}$ (préciser), et $\lambda_i^2 = 1 + \lambda_i$ pour $i = 1, 2$. La réponse finale fait intervenir la quantité $\lambda_2^{n+1} - \lambda_1^{n+1}$.
5. La *suite de Fibonacci* est la suite $(x_n)_{n\geq 0}$ définie par récurrence par $x_0 = x_1 = 1$ et $x_{n+1} = x_n + x_{n-1}$ pour $n \geq 1$. On introduit
$$v_n = \begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix}.$$
Exprimer v_{n+1} en fonction de v_n. Puis, à l'aide des questions précédentes, trouver une formule pour x_n. En déduire
$$\lim_{n\to\infty} \frac{x_{n+1}}{x_n}\,.$$

Exercice 60. On va généraliser la question (2) de l'exercice précédent. Soit $A \in \mathrm{M}_n(\mathbb{K})$ une matrice carrée, et $P \in \mathbb{K}[X]$ tel que $P(A) = 0$. On suppose que $P = P_1 P_2$ et que $pgcd(P_1, P_2) = 1$.

1. À l'aide du théorème de Bézout, montrer que tout vecteur $v \in \mathrm{M}_{n,1}(\mathbb{K})$ peut s'écrire $v = v_1 + v_2$, avec $P_i(A)v_i = 0$, pour $i = 1, 2$.
2. Montrer que cette décomposition est unique.
Indication. Si $v = v_1 + v_2 = v_1' + v_2'$, introduire $w := v_1 - v_1' = v_2' - v_2$, calculer $P_i(A)w$ pour $i = 1, 2$, et ré-utiliser la relation de Bézout.

Groupes

Exercice 61. Décrire complètement les groupes $(\mathbb{Z}/3\mathbb{Z})^*$, $(\mathbb{Z}/5\mathbb{Z})^*$ et $(\mathbb{Z}/8\mathbb{Z})^*$. (C'est-à-dire, multiplier tous les éléments possibles.) Sont-ils tous les trois cycliques ?

Exercice 62. On définit deux matrices dans $GL_2(\mathbb{R})$:

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

1. Si $v = \begin{pmatrix} x \\ y \end{pmatrix}$ est un vecteur, calculer Rv et Sv. Interpréter géométriquement les applications $v \mapsto Rv$ et $v \mapsto Sv$, et expliquer l'emploi des lettres R et S.
2. Montrer que R est d'ordre 4, et S est d'ordre 2. En déduire R^{-1} et S^{-1}.
3. Montrer que $SR = R^{-1}S$.
4. Montrer que
$$G = \{R^i S^j \mid 0 \leq i < 4,\ 0 \leq j < 2\}$$
est un sous-groupe de $GL_2(\mathbb{R})$. Quel est son ordre ?
5. Sans écrire de matrice, calculer l'ordre de chaque élément de G. Est-ce que G est cyclique ?

Exercice 63. Soit G un groupe d'ordre 4. On suppose que G n'est pas cyclique. Décrire G le plus complètement possible.

En particulier, on va observer que G est abélien. Donc cet exercice montre que tout groupe d'ordre 4 est abélien.

Exercice 64. Décrire tous les sous-groupes du groupe G de l'exercice 62.

Il y en a 10, dont 7 sont cycliques.

Exercice 65. Dans cet exercice, G est un groupe, et on note $o(g)$ l'ordre de $g \in G$.

1. Montrer que $o(g^k)$ divise $o(g)$, pour tout $k \in \mathbb{Z}$.
2. Si $n = o(g)$ et $pgcd(k, n) = 1$, montrer que $o(g^k) = n$.
3. Soit $h \in G$ et $m = o(h)$. On suppose que $pgcd(n, m) = 1$. Montrer que, si $g^k = h^\ell$ pour des entiers k, ℓ, alors $g^k = h^\ell = 1$.
4. On suppose maintenant que $gh = hg$ (et toujours que $pgcd(n, m) = 1$). Montrer que $o(gh) = nm$.

Exercice 66.

1. Dresser la liste de tous les sous-groupes de $G = \mu_{12}$.

2. Pour chaque sous-groupe H, on définit le polynôme

$$P_H = \prod_{h \in H} (X - h) \in \mathbb{C}[X] \,.$$

Donner une formule (très) simple pour P_H.

3. Vérifer que P_H divise $P_{H'}$ si et seulement si $H \subset H'$, si et seulement si $|H|$ divise $|H'|$.
4. Déduire des questions précédentes l'expression développée de

$$\Psi_d = \prod_{\substack{g \in G \\ o(g)=d}} (X - g) \,.$$

Ici d divise 12. On vous demande de considérer chaque diviseur d, en commençant par les plus petits, et en faisant un minimul de calculs.

On appelle Ψ_d un « polynôme cyclotomique ». Nous allons voir que $\Psi_d \in \mathbb{Q}[X]$, et en fait après cet exercice vous devriez avoir deviné une relation entre les polynômes Ψ_d et les polynômes P_H de la question 1.

On peut montrer (mais c'est sensiblement plus difficile !) que Ψ_d est un polynôme irréductible de $\mathbb{Q}[X]$.

Exercice 67. Soit $\phi\colon G \to H$ un homomorphisme. On définit

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1\} \,,$$

que l'on appelle le *noyau* de ϕ.

1. Montrer que $\ker(\phi)$ est un sous-groupe de G.
2. Montrer que ϕ est injective si et seulement si $\ker(\phi) = \{1\}$.

C'est très utile, d'un point de vue pratique, pour montrer qu'un homomorphisme est injectif.

Exercice 68.

1. Soit G un groupe, soit $g \in G$ un élément d'ordre d, et soit n un multiple de d. Montrer que $x \mapsto g^x$ définit un homomorphisme $\mathbb{Z}/n\mathbb{Z} \to G$.

Procéder comme dans le cours. Il est utile d'écrire $\oplus$ pour l'addition sur $\mathbb{Z}/n\mathbb{Z}$, dans ce cas.

2. Décrire l'image, puis le noyau de cet homomorphisme.
3. Traduire en notation additive, puis dans le cas $G = \mathbb{Z}/d\mathbb{Z}$ et $g = \bar{1}$.

On dit souvent que cet homomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ est « l'application naturelle ».

Exercice 69. Si G_1 et G_2 sont des groupes, leur produit $G_1 \times G_2$ est aussi un groupe, avec l'opération

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2') \,.$$

L'élément neutre est $(1, 1)$. En notation additive, c'est

$$(g_1, g_2) + (g_1', g_2') = (g_1 + g_1', g_2 + g_2') \,,$$

avec l'élément neutre $(0, 0)$.

Montrer le *lemme chinois* : si $pgcd(n, m) = 1$, alors il existe un isomorphisme

$$\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \,.$$

Indication : on utilise l'exercice précédent pour construire un homomorphisme entre ces deux groupes.
