ALGÈBRE GÉNÉRALE

DOSSIER D'EXERCICES (1)

1. Thème : théorie des groupes

1. Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble des parties de E. L'*intersection* ($\cap$) et la *réunion* ($\cup$) sont des lois internes sur $\mathcal{P}(E)$. Montrer que ni ($\mathcal{P}(E)$,$\cap$) ni ($\mathcal{P}(E)$,$\cup$) ne sont des groupes. On définit une troisième loi interne, notée $\triangle$ et appelée la *différence symétrique*, par la relation

$$A\triangle B = (A \setminus B) \cup (B \setminus A),$$

où $X \setminus Y$ est égal par définition à l'ensemble des éléments de X qui n'appartiennent pas à Y, $X \setminus Y$ est donc l'intersection de X avec le complémentaire de Y (dans E). Faire un schéma illustrant $A\triangle B$. Montrer que ($\mathcal{P}(E)$,$\triangle$) est un groupe commutatif. Faire la table du groupe lorsque E contient 2 éléments.

---

2. On note $\mathcal{A}$ l'ensemble des applications affines non constantes de $\mathbb{R}$ dans $\mathbb{R}$, autrement dit,

$$\mathcal{A} = \left\{ f \,:\, \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax+b \end{array} \,:\, a \in \mathbb{R}^\star, b \in \mathbb{R} \right\}.$$

Montrer que la loi de composition des fonctions est une loi interne sur $\mathcal{A}$ et que ($\mathcal{A}$,$\circ$) est un groupe. Le groupe ($\mathcal{A}$,$\circ$) est-il commutatif?

Montrer que l'ensemble $\mathcal{H}$ formé des éléments $f \in \mathcal{A}$ tels que $|f(x) - f(y)| = |x - y|$ pour tous x,$y \in \mathbb{R}$ forme un sous-groupe de $\mathcal{A}$. En préciser les éléments.

---

3. Soit (G,$*$) un groupe. On définit le sous-ensemble $Z(G)$ par

$$Z(G) = \{u \in G : gu = ug \text{ pour tout } g \in G\}$$

Autrement dit, u est un élément de $Z(G)$ s'il commute avec *tous* les éléments de G.

a. Montrer que $Z(G)$ est un sous-groupe de G. (On l'appelle *le centre* de G.) A quelle(s) condition(s) a-t-on G=Z(G)?

b. Dans cette partie, on cherche $Z(\mathbf{GL}_2(\mathbb{R}))$.

i) Soit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathbf{GL}_2(\mathbb{R})).$$

En utilisant le fait que A commute avec les matrices J et K données par

$$I = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

montrer qu'on a nécessairement $a = d$ et $b = 0 = c$.

ii) En déduire $Z(\mathbf{GL}_2(\mathbb{R}))$.

c. Montrer que si ϕ est un isomorphisme de (G,$*$) sur (G',.) alors $\phi(Z(G)) = Z(G')$.

---

4. On note $\mathbf{SL}(2,\mathbb{R})$ l'ensemble des matrices 2×2 à coefficients réels dont le déterminant est égal à 1.

a. Montrer que $\mathbf{SL}(2,\mathbb{R}) < \mathbf{GL}(2,\mathbb{R})$. (Naturellement, $\mathbf{GL}(2,\mathbb{R})$ est muni de la loi multiplication des matrices.)

On définit les trois ensembles de matrices suivant.

(1) $K := \left\{ k_\theta := \begin{pmatrix} \cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & \cos\theta/2 \end{pmatrix} \ : \ \theta \in \mathbb{R} \right\}$,

(2) $A := \left\{ a_t := \begin{pmatrix} \exp t/2 & 0 \\ 0 & \exp -t/2 \end{pmatrix} \ : \ t \in \mathbb{R} \right\}$,

(3) $N := \left\{ n_\xi := \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \ : \ \xi \in \mathbb{R} \right\}$.

b. Montrer que K,A et N sont des sous-groupes de $\mathbf{SL}(2,\mathbb{R})$. Montrer que A et N sont isomorphes au groupe $(\mathbb{R},+)$: on explicitera un isomorphisme. En déduire un isomorphisme explicite $\phi : N \to A$. Donner une formule explicite pour ϕ^{-1}. Trouver un morphisme surjectif de $(\mathbb{R},+)$ dans K dont le noyau soit $4\pi\mathbb{Z}$.

c. *Décomposition d'Iwasawa.* Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On définit les réels θ_g, t_g et ξ_g par les relations

$$\exp(i\theta_g/2) = \frac{a-ic}{|a-ic|},\ \exp t_g = a^2+c^2 \text{ et } \xi_g = \frac{ab+cd}{a^2+c^2},$$

où i désigne le nombre complexe habituel. Montrer que

$$g = k_{\theta_g} \cdot a_{t_g} \cdot n_{\xi_g}.$$

En déduire que l'ensemble $K \cup A \cup N$ engendre $\mathbf{SL}(2,\mathbb{R})$.

---

5. On rappelle que $\mathbb{Z}^2 = \{(n,m) : n \in \mathbb{Z}, m \in \mathbb{Z}\}$ et que $(\mathbb{Z}^2,+)$ est un groupe avec $(n_1,m_1)+(n_2,m_2) = (n_1+n_2,m_1+m_2)$. Trouver une condition nécessaire et suffisante sur les éléments $a = (a_1,a_2)$ et $b = (b_1,b_2)$ pour que $\mathbb{Z}^2 = \langle a,b\rangle$. Donner une méthode générale pour construire de tels éléments.

---

6. Montrer que si m et n sont premiers entre eux alors $\mathbf{U}_{nm} \simeq \mathbf{U}_n \times \mathbf{U}_m$. Le résultat demeure-t-il si m et n ne sont plus supposés premiers entre eux ?

---

7. Soient A et B deux groupes et $G = A \times B$ le produit (direct) de ces deux groupes. On considère A_1 un sous-groupe distingué de A et B_1 un sous-groupe distingué de B.

a. Montrer que $A_1 \times B_1$ est un sous-groupe distingué de G.

b. Montrer en utilisant un morphisme bien choisi que

$$G/(A_1 \times B_1) \simeq (A/A_1) \times (B/B_1).$$

c. Est-il légitime d'écrire $G/A \simeq B$?

---

8. Ce problème fait intervenir les groupes:
   a) $(\mathbf{GL}_2(\mathbb{R}),.)$ formé de l'ensemble des matrices 2×2 inversibles à coefficients réels que l'on munit de la multiplication habituelle des matrices,
   b) $(\mathbb{C}^*,.)$ formé des nombres complexes *non nuls* que l'on munit de la multiplication habituelle des nombres complexes,
   c) $(\mathbb{R}^{\star+},.)$ formé de l'ensemble des nombres réels *strictement positifs* que l'on munit de la multiplication habituelle des nombres réels. On a d'ailleurs $\mathbb{R}^{\star+} < (\mathbb{C}^*,.)$.

On rappelle que

$$\text{si } A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \mathbf{GL}_2(\mathbb{R}) \text{ alors } A^{-1}=\frac{1}{ad-bc}\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}.$$

---

a. Soit G l'ensemble des matrices **inversibles** M de la forme

$$M=\begin{pmatrix} \alpha & \beta\\ -\beta & \alpha\end{pmatrix}$$

où α et β sont des nombres **réels**. (On a donc $G\subset \mathbf{GL}_2(\mathbb{R})$.)

(1) Montrer que G est un sous-groupe de $(\mathbf{GL}_2(\mathbb{R}),.)$.

(2) Montrer que l'application ψ définie par

$$\psi(M)=\alpha+i\beta \quad \text{si} \quad M=\begin{pmatrix} \alpha & \beta\\ -\beta & \alpha\end{pmatrix}$$

est un **isomorphisme** de $(G,.)$ sur $(\mathbb{C}^*,.)$. (On vérifiera d'abord qu'elle prend bien ses valeurs dans $\mathbb{C}^*$.)

(3) Soit $n\in\mathbb{N}^*$. On définit $M_n\in G$ par

$$M_n=\begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n})\\ -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n})\end{pmatrix}.$$

Quel est l'ordre de M_n ? Donner la liste (en justifiant votre réponse) des éléments du groupe $\langle M_n\rangle$. (On pourra utiliser la question précédente et calculer notamment $\psi(M_n^k)$. On rappelle que

$$M_n^k =_{def} \underbrace{M_n.M_n\ldots.M_n}_{k\,fois}.)$$

b. On considère $S=\begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix}\in\mathbf{GL}_2(\mathbb{R})$ et H, le sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ engendré par S et $M_4=\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}$. Autrement dit, $H=\langle S,M_4\rangle$.

(1) Quel est l'ordre de S? Montrer que $M_4^3=M_4^{-1}$.

(2) Montrer que $M_4.S=S.M_4^{-1}$. Que dire de $M_4^{-1}.S$?

(3) Donner la liste (en justifiant votre réponse) de tous les éléments de H. (Indication. On devra montrer que H contient **huit et seulement huit** éléments.)

c. On rappelle que pour un groupe $(W,.)$ quelconque, $Aut(W)$ désigne l'ensemble des automorphismes du groupe $(W,.)$, c'est-à-dire les morphismes bijectifs de $(W,.)$ dans lui-même. Cet ensemble $Aut(W)$ devient un groupe lorsqu'on le munit de la loi de composition des applications. L'élément neutre de ce groupe $(Aut(W),\circ)$ est l'application identité. *Ces propriétés sont admises, on ne demande pas de les démontrer.*

(1) Les trois applications suivantes sont-elles des **automorphismes** de $(\mathbb{C}^*,.)$?

$$\phi_1:\begin{array}{ccc}(\mathbb{C}^*,.) & \longrightarrow & (\mathbb{C}^*,.)\\ z & \longmapsto & \overline{z}\end{array},\quad \phi_2:\begin{array}{ccc}(\mathbb{C}^*,.) & \longrightarrow & (\mathbb{C}^*,.)\\ z & \longmapsto & z^2\end{array},\quad \phi_3:\begin{array}{ccc}(\mathbb{C}^*,.) & \longrightarrow & (\mathbb{C}^*,.)\\ z & \longmapsto & \frac{z}{|z|^2}\end{array}$$

(2) On considère à présent le groupe $(\mathbb{R}^{*+},.)$. Montrer que si $f \in Aut(\mathbb{R}^{*+})$ alors $\phi_f \in Aut(\mathbb{C}^\star)$ où ϕ_f est définie par

$$\phi_f : \begin{array}{ccc} (\mathbb{C}^*,.) & \longrightarrow & (\mathbb{C}^*,.) \\ z & \longmapsto & f(|z|) \cdot \frac{z}{|z|} \end{array}$$

(3) Montrer que $Aut(\mathbb{C}^*)$ contient une infinité d'éléments.

(4) Montrer que les groupes $Aut(\mathbb{C}^*)$ et $Aut(G)$ sont isomorphes. (On pourra construire un isomorphisme Ψ entre $Aut(\mathbb{C}^*)$ et $Aut(G)$ en utilisant l'isomorphisme ψ de I) b).)

(Partiel avril 2004)

---

9. Dans $\mathbf{S}_9$ on considère les permutations σ_1 et σ_2 suivantes :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 8 & 5 & 4 & 3 & 7 & 1 & 9 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 4 & 5 & 7 & 6 & 9 & 1 \end{pmatrix}$$

a. Décomposer chacune des permutations en produit de cycles, calculer leur ordre et leur signature.

b. Calculer σ_1^{50} et σ_2^{121}.

---

10. **Générateurs des groupes symétriques et alternés.** Soit $n \geq 2$.

a. Montrer que tout cycle $(a_1,a_2,\cdots,a_p)$ $(p \geq 2)$ s'écrit comme un produit de transpositions.

b. Montrer que toute permutation (i,j) avec $i < j$ vérifie

$$(i,j) = (i,i+1)(i+1,i+2)\cdots(j-1,j)(j-2,j-1)(j-3,j-2)\cdots(i,i+1).$$

c. Montrer que

$$(k,k+1) = (1,k)(1,k+1)(1,k).$$

d. Montrer les égalités suivantes

(1) $\mathbf{S}_n = \langle (1,2),(1,3),\ldots,(1,n) \rangle$.

(2) $\mathbf{S}_n = \langle (1,2),(1,2,\ldots,n) \rangle$

Indication : Posant $\sigma = (1,2,\ldots,n)$, on pourra montrer que

$$\sigma^k (12) \sigma^{-k} = (k+1,k+2).$$

e. Soit $n \geq 3$. Montrer que $(a,b)(a,c) = (a,c,b)$ et $(a,b)(c,d) = (a,c,b)(a,c,d)$. En déduire

(3) $\mathbf{A}_n$ est engendré par l'ensemble des 3-cycles.

---

11. On considère les éléments suivants du groupe de permutation $\mathbf{S}_4$: $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$, $\sigma_3 = (14)(23)$. On rappelle que e désigne l'élément neutre de $(\mathbf{S}_4,\cdot)$, autrement dit e est la bijection *identité*.

(1) Déterminer l'ordre de chaque élément de $H := \{e,\sigma_1,\sigma_2,\sigma_3\}$.
(2) Montrer que H est un sous-groupe de $\mathbf{S}_4$. (On pourra construire une table.) H est-il commutatif?
(3) Déterminer tous les sous-groupes de H. (Justifier votre réponse.)
(4) (a) Soit $f \in \mathbf{S}_4$. Montrer que
$$f \cdot (12)(34) \cdot f^{-1} = \big(f(1)f(2)\big)\big(f(3)f(4)\big).$$
(b) Montrer que H est un sous-groupe *distingué* de $\mathbf{S}_4$.
(5) Montrer que H est isomorphe à $\big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,,\,+\big)$. (On pourra construire un isomorphisme explicite entre H et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

(Contrôle terminal juin 2005)

---

12. **Le théorème de Cayley.** Soit $(G,*)$ un groupe à n éléments, $G = \{a_1,\ldots,a_n\}$. Pour tout $a \in G$, on définit l'application σ_a de $\{1,\ldots,n\}$ dans lui-même par la relation
$$\sigma_a(i) = j \iff a * a_i = a_j.$$

a. Montrer que $\sigma_a \in \mathbf{S}_n$.

b. Dans cette partie, on prend $(G,*) = (\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}},\bar{+})$ dont les quatre éléments sont $a_1 = (\bar{0},\,\bar{0})$, $a_2 = (\bar{1},\bar{0})$, $a_3 = (\bar{0},\bar{1})$ et $a_4 = (\bar{1},\bar{1})$. Déterminer σ_a pour tout $a \in G$.

c. Montrer dans le cas général que l'application $\Sigma : (G,*) \to (\mathbf{S}_n,\cdot)$ définie par $\Sigma(a) = \sigma_a$ est un morphisme de groupe.

d. En déduire que tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathbf{S}_n$.

2. THÈME : ANNEAUX ET CORPS

1. Soit p un nombre premier. Montrer que $\mathbb{Q}_p$ est un sous-anneau de $(\mathbb{Q}, +, \cdot)$. On rappelle que $\mathbb{Q}_p =_{def} \left\{ \frac{m}{p^n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$. Déterminer $(\mathbb{Q}_p)^*$.

---

2. On définit $\mathbb{Z}[i] =_{def} \{m + in : m,n \in \mathbb{Z}\} \subset \mathbb{C}$.

a. Montrer que $(\mathbb{Z}[i], +, \cdot)$ est un anneau commutatif unitaire (on montrera que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \cdot)$).

b. On définit sur $\mathbb{Z}[i]$ l'application N par $N(n + im) = n^2 + m^2$. Montrer que pour tous α et β dans $\mathbb{Z}[i]$, on a $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$. Montrer que si α est inversible alors $N(\alpha) = 1$ en déduire $(\mathbb{Z}[i])^*$, le groupe des éléments inversibles de $\mathbb{Z}[i]$. A quel groupe déjà rencontré $((\mathbb{Z}[i])^*, \cdot)$ est-il isomorphe ?

---

3. Soit A un sous-anneau de $(\mathbb{R}, +, \cdot)$. On appelle $\mathcal{A}$ l'ensemble des matrices de $M_2(\mathbb{R})$ dont tous les coefficients appartiennent à A.

(1) Montrer que $\mathcal{A}$ est un sous-anneau unitaire de $(M_2(\mathbb{R}), +, \cdot)$.
(2) Montrer que si $M \in \mathcal{A}$ alors $\det M \in A$.
(3) Montrer que $M \in \mathcal{A}^\star$ si et seulement si $\det M \in A^\star$.
(4) Lorsque $A = \mathbb{Z}[i]$, $\mathcal{A}^\star$ contient-il une infinité d'éléments ?

---

4. Soit $d \in \mathbb{Z}$ tel que $\sqrt{|d|} \notin \mathbb{Q}$. Lorsque $d < 0$ on pose $\sqrt{d} =_{def} i\sqrt{|d|}$. On définit $\mathbb{Q}(\sqrt{d})$ par

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} : x,y \in \mathbb{Q}\}.$$

a. Montrer que $\mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{C}$.

b. Déterminer tous les isomorphismes f de $\mathbb{Q}(\sqrt{d})$ qui coïncident avec l'identité sur $\mathbb{Q}$, autrement dit tels que $f(x) = x$ pour tout $x \in \mathbb{Q}$.

c. Justifier l'assertion suivante : $\mathbb{Q}(\sqrt{d})$ *est le plus petit sous-corps de* $\mathbb{C}$ *qui contienne à la fois* $\mathbb{Q}$ *et* $\sqrt{d}$.

d. Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{5})$ sont-ils isomorphes ?

---

5. On appelle A l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}/3\mathbb{Z}$,

$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}/3\mathbb{Z} \right\}.$$

On munit A des lois $+$ et $\cdot$ définies par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \cdot a' + b \cdot c' & a \cdot b' + b \cdot d' \\ c \cdot a' + d \cdot c' & c \cdot b' + d \cdot d' \end{pmatrix}$$

Par exemple, on a

$$\begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{0} \end{pmatrix} + \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{2} & \overline{1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{1} & \overline{2} \end{pmatrix} \cdot \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{1} & \overline{2} \end{pmatrix} = \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix}.$$

On remarquera que, formellement, ce sont exactement les mêmes règles de calculs que pour les matrices usuelles. Il faut cependant prendre garde que tous les coefficients sont des éléments de $\{\overline{0},\overline{1},\overline{2}\}$.

On **admet** que $(A,+,\cdot)$ est un anneau unitaire. On a

$$0_A = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix} \quad \text{et} \quad 1_A = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Nota Bene. Nous ne définissons pas d'application déterminant *sur A. L'emploi d'une telle application dans l'exercice est* interdit.

---

(1) Propriétés élémentaires de l'anneau A.

(a) Montrer que A contient 81 éléments.

(b) Soit $M = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$. Vérifier que $M^3 = M$. A t-on $M \in A^\star$?

(c) Montrer que A n'est pas intègre.

(2) On considère B le sous-ensemble de A formé des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec a,b quelconques dans $\mathbb{Z}/3\mathbb{Z}$.

(a) Montrer que B est un sous-anneau de $(A,+,\cdot)$.

(b) Donner la liste des éléments de B.

(c) Déterminer l'ensemble des couples $(a,b) \in (\mathbb{Z}/3\mathbb{Z})^2$ tels que a^2+b^2 soit non inversible.

(d) Soient $a,b \in \mathbb{Z}/3\mathbb{Z}$. Calculer

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

(e) En déduire que B est un corps.

(f) Existe-t-il $n \in \mathbb{N}^\star$ tel que B soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$?

---

6. Soit $(A,+,\cdot)$ un anneau commutatif unitaire et I un idéal de A. le radical de I, noté $\sqrt{I}$ est défini par

$$a \in \sqrt{I} \iff_{def} \text{il existe } m \in \mathbb{N}^\star \text{ tel que } a^m \in I$$

a. Montrer que $\sqrt{I}$ est un idéal de A. (On utilisera convenablement la formule du binôme de Newton.)

b. On prend $A = \mathbb{Z}$ et $I = 36\mathbb{Z}$. Déterminer $\sqrt{I}$. Plus généralement, comment peut-on déterminer $\sqrt{m\mathbb{Z}}$ pour tout $m \in \mathbb{Z}$?

---

7. Soit $m \in \mathbb{N}/\{0,1\}$. Montrer que $\overline{r} \in (\mathbb{Z}/m\mathbb{Z})^*$ si et seulement si m et r sont premiers entre eux. On note $\phi(m)$ le cardinal de $(\mathbb{Z}/m\mathbb{Z})^*$. Calculer $\phi(m)$ pour $m = 2,3,4,5,6$. Que vaut $\phi(p)$ lorsque p est un nombre premier? Que vaut $\phi(m)$ lorsque $m = p^s$ avec p premier?

Remarque. L'application ϕ s'appelle l'indicatrice d'Euler.

8.

a. Soient $(A,\oplus_A,\odot_A)$ et $(B,\oplus_B,\odot_B)$ deux anneaux commutatifs unitaires. On définit sur $A\times B$ les lois $+$ et $\cdot$ de la manière suivante

$$(a,b)+(a',b')=(a\oplus_A a'\,,b\oplus_B b')\quad\text{et}\quad(a,b).(a',b')=(a\odot_A a'\,,b\odot_B b').$$

1) Montrer que $(A\times B,+,\cdot)$ est un anneau commutatif unitaire. Est-il intègre ?

2) Déterminer les éléments inversibles de $A\times B$ en fonction des éléments inversibles de A et de B.

b. Dans cette partie on prend $A=\frac{\mathbb{Z}}{m\mathbb{Z}}$ et $B=\frac{\mathbb{Z}}{n\mathbb{Z}}$ où m et n sont deux entiers premiers entre eux.

1) Montrer que l'application f ci-dessous est bien définie :

$$f:\begin{array}{ccc}\mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\\ \mathbf{cl}_{mn}(a) & \longmapsto & (\mathbf{cl}_m(a)\,,\mathbf{cl}_n(a))\end{array}$$

où on utilise la notation $\mathbf{cl}_s(a)$ pour représenter la classe de a dans $\mathbb{Z}/s\mathbb{Z}$.

2) L'application f est-elle un isomorphisme d'anneau ?

3) Utiliser f, la partie a — et l'exercice précédent pour démontrer que lorsque m et n sont premiers entre eux on a $\phi(mn)=\phi(m)\phi(n)$.

4) En déduire, en utilisant l'exercice précédent, une formule générale pour le calcul de $\phi(m)$, m entier positif quelconque.