Algèbre

AI 2015/2016

Exercice 1 :
Soient a et b deux éléments d'un groupe $(G,.)$, vérifiant $ab = ba$. Si a est d'ordre m, b d'ordre n, et si m et n sont premiers entre eux, montrer que ab est d'ordre mn.

Exercice 2 :

1. Soit $(G,.)$ un groupe, A une partie de G. On note $< A >$ le sous-groupe de G engendré par A, i.e le plus petit sous-groupe de G qui contient A.

   Si $A = \varnothing$, remarquer que $< A >= \{e\}$. On suppose désormais A non vide. On pose alors $A^{-1} := \{a^{-1}, a \in A\}$.

   Montrer que $< A >$ est constitué des éléments de G qui peuvent s'écrire comme produit d'un nombre fini d'éléments de $A \cup A^{-1}$.

   Exemples :

   (a) Soit $x \in G$, $A = \{x\}$. On note $< A >$, $< x >$. C'est un groupe monogène. Montrer que $< x >= \{x^n, n \in \mathbb{Z}\}$. Quelle est la notation pour un groupe abélien ?

   (b) Soit $(x,y) \in G^2$ tel que $xy = yx$. Montrer que $< A >= \{x^m y^n, (m,n) \in \mathbb{Z}^2\}$. Pour un groupe abélien, que trouve-t-on ?

   (c) Soit $(G,+)$ un groupe abélien, et A une partie de G, non vide, et stable par $+$. Montrer que $< A >= \{x - y; (x,y) \in A^2\}$.

2. Soit $\varphi : G \longrightarrow G$ un morphisme de groupes. Montrer que $\varphi(< A >) =< \varphi(A) >$.

   Applications :

   (a) Si G est un groupe monogène, alors $\varphi(G)$ est un groupe monogène.

   (b) Si G est un groupe cyclique, $\varphi(G)$ est cyclique.

Exercice 3 :
Soit $(G,.)$ un groupe. On note $Aut(G)$ l'ensemble des automorphismes de G.

1. Montrer que $Aut(G)$ muni de la loi de composition $\circ$ est un groupe.

2. Soit $a \in G$. On définit l'application φ_a de G dans G par $\varphi_a(x) = axa^{-1}$. Montrer que $\varphi_a \in Aut(G)$.

3. Montrer que $\varphi_{ab} = \varphi_a \circ \varphi_b$.

4. Soit H un sous-groupe de $Aut(G)$ et

   $$\begin{array}{rll} \varphi : & G & \longrightarrow \mathcal{P}(G) \\ & x & \longmapsto \{f(x); f \in H\} \end{array}$$

   $\varphi(x)$ est appelé l'orbite de x sous H. Vérifier que $\varphi(G)$ est une partition de G.

5. Soit Φ l'application de G dans $Aut(G)$ qui à tout $a \in G$ associe φ_a. Montrer que Φ est un homomorphisme de groupes. Déterminer son noyau noté $Ker\Phi$.

Exercice 4 :
Quels sont les sous-groupes de $\mathbb{Z}$? De $\mathbb{R}$?

Exercice 5 :
Soient $f : G \longrightarrow G'$ un morphisme de groupes, et x un élément d'ordre fini n de G. Montrer que $f(x)$ et d'ordre fini dans G', et que son ordre m divise n. Exprimer $\frac{n}{m}$ à l'aide de $Ker f$ et de $< x >$.

Exercice 6 :

1. Soit $(G, .)$ un groupe. Montrer que les deux assertions suivantes sont équivalentes :
   (a) G est un groupe monogène.
   (b) Il existe un morphisme surjectif du groupe $(\mathbb{Z}, +)$ sur le groupe $(G, .)$.
2. En déduire que tout sous-groupe et tout groupe quotient d'un groupe monogène (respectivement cyclique) est monogène (respectivement cyclique).

Exercice 7 :
Soient $(G_1, .)$ et $(G_2, .)$ deux groupes et $G = G_1 \times G_2$ le groupe muni de la loi produit.

1. Soient $x_1 \in G_1$ (resp $x_2 \in G_2$) d'ordre n_1 (resp n_2) ; quel est l'ordre de $x := (x_1, x_2)$ dans G ?
2. On suppose que G_1 (resp G_2) est cyclique d'ordre n_1 (resp n_2). Montrer que si $n_1 \wedge n_2 = 1$, alors $G := G_1 \times G_2$ est cyclique d'ordre $n_1 n_2$.

   Remarquons que la réciproque de cette dernière propriété est eaxcte : si G est cyclique, alors $n_1 \wedge n_2 = 1$.
3. Applications :
   (a) Montrer le théorème chinois : si n_1 et n_2 sont premiers entre eux, alors $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n_1 n_2\mathbb{Z}$.
   Donner une autre preuve de ce lemme en utilisant le morphisme de groupes suivant:

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \\ & k & \longmapsto & (\dot{k}, \overline{k}) \end{array}$$

   où $\dot{(k)}$ désigne la classe *modulo* n_1 de k, et $\overline{k}$ celle *modulo* n_2.
   (b) Déduire la propriété suivante : si A_1 (resp A_2) est une classe d'entiers *modulo* n_1 (resp *modulo* n_2), alors $A_1 \cap A_2$ est non vide, et est une classe d'entiers *modulo* $n_1 n_2$.
   Retrouver ce résultat à l'aide du théorème de Bezout.
4. Etendre les résultats précèdents à p entiers premiers entre eux deux à deux.

Exercice 8 :
Soit $n \in \mathbb{N}^*$, on appelle indicateur d'Euler le nombre

$$\varphi(n) := Card(\{k \in [\![1, n]\!] / k \wedge n = 1\}).$$

Soit $G = \mathbb{Z}/n\mathbb{Z}$. Pour k entier, on note $\overline{k}$ la classe de k *modulo* n.

1. (a) Quel est l'ordre de $\overline{k}$ dans G ?
   (b) Donner une condition nécessaire et suffisante pour que $\overline{k}$ engendre G.
   (c) Quel est le nombre de générateur de G ?
2. Soient N_1, n_2 deux entiers naturels premiers entre eux. Montrer que $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$. Généraliser ce résultat.
3. Soit p un nombre premier. Soit $k \in \mathbb{N}^*$. Calculer $\varphi(p)$, puis $\varphi(p^k)$.
4. Soit $n \in \mathbb{N}, n \geq 2$. On considère la décomposition enfacteurs premiers de n : $\prod_{i=1}^{r} p_i^{\alpha_i}$.
   Etablir l'égalité :
   $$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Exercice 9 :
Soit $(G, .)$ un groupe cyclique d'ordre n, et x un générateur de G.
Soit d un diviseur de n, et $G_d := \{g \in G / g^d = e\}$.

1. Montrer que G_d est un groupe cyclique d'ordre d.
   Montrer que G_d est l'unique sous-groupe d'ordre d de G.
2. Montrer que G contient $\varphi(d)$ éléments d'ordre d. Donner des exemples.
3. Soit D_n l'ensemble des diviseurs de n. Montrer que
   $$\sum_{d \in D_n} \varphi(d) = n$$
4. Etablissons la réciproque de la propriété précèdente :
   Soit $(G, .)$ un groupe fini d'ordre n tel que, pour tout diviseur d de n, G contient au plus d éléments g tels que $g^d = e$.
   Pour $d \in D_n$, on note $\Psi(d)$ le cardinal de l'ensemble des éléments de G d'ordre d. Montrer que $\Psi(d) = 0$ ou $\Psi(d) = \varphi(d)$.
   En déduire que G est cyclique.
5. Application : Soit $\mathbb{K}$ un corps commutatif, $\mathbb{K}^*$ le groupe multiplicatif des éléments non nuls de $\mathbb{K}$.
   Montrer que tout sous-groupe fini de $\mathbb{K}^*$ est cyclique.
   (Indication : si G est un sous-groupe fini de $\mathbb{K}^*$, d'ordre n, et si $d \in D_n$, utiliser le polynôme $X^d - 1$ à coefficients dans $\mathbb{K}$).

Exercice 10 : Trouver tous les éléments nilpotents de $\mathbb{Z}/36\mathbb{Z}$.

Exercice 11 : Montrer qu'un anneau A est un corps si et seulement si ses seuls idéaux sont $\{0_A\}$ et lui même.

Exercice 12 : Soit A un anneau, $x \in A$, et $(\alpha, \beta) \in \mathbb{Z}^2 / \alpha x = \beta x = 0$.
Montrer que $(\alpha \wedge \beta).x = 0$.
On pourra remarquer que c'est encore vrai pour un pseudo-anneau (anneau non unitaire).

Exercice 13 : [Formule du multinôme de Newton] Soit A un pseudo-anneau, $(n,p) \in \mathbb{N} \times \mathbb{N}^*$, et $(x_1, x_2, ..., x_p) \in A^p$, montrer que

$$(x_1 + x_2 + ... + x_p)^n = \sum_{k_1+k_2+...+k_p=n} \frac{n!}{k_1!k_2!...k_p!} x_1^{k_1} x_2^{k_2} ... x_p^{k_p}.$$

Exercice 14 : Soit A un anneau. On dit qu'un élément $a \in A$ est *nilpotent* s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

(i) Montrer que si a est nilpotent, alors $1 - a$ est inversible et calculer son inverse.
(ii) Si a et b sont nilpotents et permutables, montrer que ab et $a + b$ sont nilpotents. Que peut-on dire de l'ensemble des éléments nilpotents d'un anneau?
(iii) Soit $a \in A$. On définit l'application $u : \left\{ \begin{array}{lll} A & \to & A \\ x & \to & u(x) = ax - xa \end{array} \right.$.
Calculer $u^p(x)$. Montrer que si a est nilpotent , il existe $p \in \mathbb{N}^*$ tel que $u^p \equiv 0$.
(iv) Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$?

Exercice 15 : Montrer qu'un anneau intègre fini est un corps.

Exercice 16 : Un idéal M d'un anneau commutatif A est dit maximal si $M \neq A$ et si M et A sont les seuls idéaux de A qui contiennent M.

1. Si I est un idéal de l'anneau commutatif A tel que A/I est un corps, alors I est un idéal maximal.
2. Si M est un idéal maximal de l'anneau commutatif A, alors A/M est un corps.

Exercice 17 : Un idéal P d'un anneau commutatif A est dit premier si

$$\left\{ \begin{array}{c} ab \in P \\ b \notin P \end{array} \right\} \Longrightarrow a \in P.$$

1. Montrer que P premier équivaut à : l'anneau quotient A/P est intègre.
2. Montrer que tout idéal maximal d'un anneau commutatif est premier.
3. Dans $\mathbb{R}[X]$, que peut-on dire de l'idéal engendré par $X^2 + 1$?
   Conclusion ?

Exercice 18 : Dans $\mathbb{Z}[X]$, l'idéal engendré par X^2+1 et $2X$ est-il principal ?

Exercice 19 : On note A l'anneau des applications continues de $[0,1]$ dans $\mathbb{R}$.

1. Soit $x \in [0,1]$. Montrer que $M(x) = \{f \in A / f(x) = 0\}$ est un idéal maximal de A.
2. On va montrer que tout idéal maximal J de A s'écrit $M(x_0)$, où x_0 est un élément convenablement choisi de $[0,1]$.
   (a) Soit I un idéal de A tel que $E_I = \bigcap_{f \in I} f^{-1}(0)$ soit vide. Montrer qu'il existe un élément de I ne prenant la valeur 0 en aucun point de $[0,1]$. En déduire $I = A$.
   (b) Conclure.