chapitre 1

Structures algébriques (compléments)

1. Comment montrer qu'un élément d'un groupe est d'ordre fini ?
2. Comment montrer qu'un sous-groupe est engendré par une partie non vide ?
3. Comment montrer qu'un groupe est monogène ?
4. Comment montrer qu'un groupe est cyclique ?
5. Comment montrer qu'un sous-groupe d'un groupe est distingué (ou invariant) ?
6. Comment déterminer la signature d'une permutation ?
7. Comment montrer qu'un élément d'un anneau est nilpotent ?
8. Comment montrer qu'une partie d'un anneau est un idéal ?
9. Comment calculer dans $\mathbf{Z}/n\mathbf{Z}$?

méthode 1

Comment montrer qu'un élément d'un groupe est d'ordre fini ?

Soit $(G,\cdot)$ un groupe d'élément neutre e et soit $a \in G$.

Pour montrer que a est d'ordre fini, on montre qu'il existe $n \in \mathbf{N}^*$ tel que $a^n = e$.

On appelle *ordre* de a, le plus petit entier naturel non nul n tel que $a^n = e$.

Exemple

Soit $G_4 = \{z \in \mathbf{C},\ z^4 = 1\} = \{-1, i, -i, 1\}$. On sait que G_4 muni de la multiplication est un groupe. Trouver l'ordre de chacun des éléments de G_4.

On a : $(-1)^4 = 1$, donc -1 est d'ordre fini, ici $\text{ordre}(-1) = 2$;
$i^4 = 1$, donc i est d'ordre fini, ici $\text{ordre}(i) = 4$;
$(-i)^4 = 1$, donc $(-i)$ est d'ordre fini, ici $\text{ordre}(-i) = 4$.

Exercices

- **Ex. 1.** Soit $(G,\cdot)$ un groupe d'élément neutre e et soit x un élément de G tel que $x^n = e$ pour un entier naturel n.
  Montrer que l'ordre de x divise n.
- **Ex. 2.** Soient $(G,\cdot)$ un groupe, x et y deux éléments de G.
  a. Montrer que si x, y et xy sont d'ordre 2, alors $xy = yx$;
  b. Montrer que si x est d'ordre fini, alors x^{-1} est d'ordre fini, de plus x et x^{-1} ont le même ordre ;
  c. Montrer que si x est d'ordre fini alors yxy^{-1} est d'ordre fini, de plus x et yxy^{-1} ont le même ordre ;
  d. Montrer que si xy est d'ordre fini alors yx est d'ordre fini, de plus xy et yx ont le même ordre.
- **Ex. 3.** Soient G, G' deux groupes, $f : G \to G'$ un morphisme de groupes, x un élément de G d'ordre fini et n l'ordre de x.
  Montrer que $f(x)$ est d'ordre fini dans G' et que l'ordre de $f(x)$ divise n.
- **Ex. 4.** Soit $(G,+)$ un groupe commutatif et T l'ensemble des éléments de G d'ordre fini.
  Montrer que T est un sous-groupe de G.
- **Ex. 5.** Trouver l'ordre de chacun des éléments de $\left(\mathbf{Z}/11\mathbf{Z} \setminus \{\overline{0}\}, \times\right)$.

Comment montrer qu'un sous-groupe est engendré par une partie non vide ?

méthode 2

Soient $(G,*)$ un groupe, A une partie non vide de G et H un sous-groupe de G.

Pour montrer que H est engendré par A, on montre que pour tout $x \in H$, il existe $n \in \mathbf{N}^*$, $a_1,\cdots,a_n \in A$ et $\varepsilon_1,\cdots,\varepsilon_n \in \{-1,1\}$ tels que $x = a_1^{\varepsilon_1}\cdots a_n^{\varepsilon_n}$.
Autrement dit : $H = \left\{x = a_1^{\varepsilon_1}\cdots a_n^{\varepsilon_n},\ a_1,\cdots,a_n \in A, \varepsilon_1,\cdots,\varepsilon_n \in \{-1,1\}\right\}$.

Exemple

Soient A,B deux sous-groupes d'un groupe G, on considère le sous-groupe S engendré par $A \cup B$. Montrer que tout élément de S est obtenu comme produit d'une suite finie d'éléments appartenant alternativement à A et à B.

Soit $x \in S$, il existe donc $c_1,\cdots,c_n \in A \cup B$, $\varepsilon_1,\cdots,\varepsilon_n \in \{-1,1\}$ tels que $x = c_1^{\varepsilon_1}c_2^{\varepsilon_2}\cdots c_n^{\varepsilon_n}$.
On peut supposer que $c_1 \in A$, soit i_1 le plus grand entier de l'ensemble $\{1,\cdots,n\}$ tel que $c_{i_1} \in A$; si $i_1 = n$ donc $x \in A$, sinon soit i_2 le plus grand entier de $\{i_1+1,\cdots,n\}$ tel que $x \in B$; si $i_2 = n$ alors $x = \alpha_1 \cdot \alpha_2$ avec $\alpha_1 = c_1^{\varepsilon_1}\cdots c_{i_1}^{\varepsilon_{i_1}}$ et $\alpha_2 = c_{i_1+1}^{\varepsilon_{i_1+1}}\cdots c_n^{\varepsilon_n} \in B$, sinon soit i_3 le plus grand entier de $\{i_2+1,\cdots,n\}$ tel que $c_{i_3} \in A$; si $i_3 = n$ alors $x = \alpha_1 \cdot \alpha_2 \cdot \alpha_3$ avec $\alpha_3 = c_{i_{2+1}}^{\varepsilon_{i_{2+1}}}\cdots c_n^{\varepsilon_n} \in A$ et ainsi de suite.
Il existe donc $\alpha_1,\alpha_3,\cdots,\alpha_{2p+1} \in A$, $\alpha_2,\alpha_4,\cdots,\alpha_{2p} \in B$ tels que $x = \alpha_1\alpha_2\alpha_3\cdots\alpha_{2p}$ ou $x = \alpha_1 \cdot \alpha_2 \cdots \alpha_{2p-1} \cdot \alpha_{2p} \cdot \alpha_{2p+1}$.

Exercices

- **Ex. 1.** Soit $n \in \mathbf{N}^*$, montrer que le groupe S_n des permutations de $\{1,\cdots,n\}$ est engendré par les cycles de S_n.
- **Ex. 2.** Soit $n \in \mathbf{N}^*$, montrer que S_n est engendré par les transpositions.
- **Ex. 3.** Soit $n \in \mathbf{N}^*$, montrer que S_n est engendré par les $n-1$ transpositions suivantes : $(1,2)$, $(2,3)$, $\cdots$, $(n-1,n)$.
- **Ex. 4.** Soit $n \in \mathbf{N}^*$, montrer que S_n est engendré par $H = \{\tau, s\}$ où $\tau = (1,2)$ et $s = (1,2,\cdots,n)$.

méthode 3

Comment montrer qu'un groupe est monogène ?

Soit $(G,\cdot)$ un groupe.

Pour montrer que G est *monogène*, on montre qu'il existe $a \in G$ tel que G soit le sous-groupe engendré par $\{a\}$.
Autrement dit : Il existe $a \in G$ tel que $G = \{a^n,\ n \in \mathbf{Z}\}$.
On remarque que tout *groupe monogène* est *commutatif*.

Exemple

Soit $n \in \mathbf{N}^*$ et notons par $U_n = \{z \in \mathbf{C},\ z^n = 1\}$. On sait que U_n muni de la multiplication des nombres complexes est un groupe. Montrer que U_n est monogène.

U_n est l'ensemble des racines $n^{\text{ièmes}}$ de l'unité.

On a donc : $U_n = \left\{e^{i\frac{2k\pi}{n}}, k \in \{0,\cdots,n-1\}\right\}$.

Posons $a = e^{i\frac{2\pi}{n}}$, on a pour tout $k \in \{0,\cdots,n-1\}$, $e^{i\frac{2k\pi}{n}} = a^k$, d'où $U_n = \{a^k, k \in \mathbf{Z}\}$.

Par suite U_n est un groupe monogène.

Exercices

- **Ex. 1.** Soient G, G' deux groupes et f un morphisme de groupes de G dans G'. Montrer que si G est monogène et f est surjectif, alors G' est un groupe monogène.
- **Ex. 2.** Soit G un groupe monogène engendré par un élément a de G. Montrer que si H est un sous-groupe de G non réduit à $\{0\}$, alors H est monogène et engendré par un élément a^m, où m est un entier positif.
- **Ex. 3.** Montrer que l'ensemble des entiers relatifs multiples de n est un groupe monogène engendré par n.
- **Ex. 4.** Montrer que $\left(\mathbf{Z}/n\mathbf{Z}, +\right)$ est un groupe monogène.

Comment montrer qu'un groupe est cyclique ?

Soit $(G,\cdot)$ un groupe.

Pour montrer que G est *cyclique*, on montre que G est monogène et fini.
Autrement dit :

$$\exists n \in \mathbf{N}^*,\ \exists a \in G \text{ tels que : } G = \left\{e, a, a^2, \cdots, a^n\right\}.$$

Exemple

Montrer que $\left(\left(\mathbb{Z}/5\mathbb{Z}\right)\setminus\{\overline{0}\},\times\right)$ *est un groupe cyclique.*

Remarquons que $\overline{3}=\overline{8}=\overline{2}\times\overline{2}\times\overline{2}=\left(\overline{2}\right)^3$ et $\overline{4}=\overline{2}\times\overline{2}=\left(\overline{2}\right)^2$, il existe donc $n=3$ tel que $\left(\left(\mathbb{Z}/5\mathbb{Z}\right)\setminus\{\overline{0}\}=\left\{\overline{1},\overline{2},\left(\overline{2}\right)^2,\left(\overline{2}\right)^3\right\}\right.$.

Par suite $\left(\left(\mathbb{Z}/5\mathbb{Z}\right)\setminus\{\overline{0}\},\times\right)$ est un groupe cyclique.

Exercices

- **Ex. 1.** Soient G, G' deux groupes et f un morphisme de groupes de G dans G'. Montrer que si G est cyclique et f est surjectif, alors G' est un groupe cyclique.

- **Ex. 2.** Soit G un groupe fini. On appelle *ordre* de G, le nombre d'éléments de G. Montrer que si G est d'ordre un nombre premier alors G est cyclique.

- **Ex. 3.** Soient $(G_1,*_1)$, $(G_2,*_2)$ deux groupes et $*$ la loi définie sur $G_1\times G_2$ par :

$$\forall (g_1,g_2),\ (h_1,h_2)\in G_1\times G_2,\ (g_1,g_2)*(h_1,h_2)=(g_1*_1 h_1, g_2*_2 h_2)$$

  a. Montrer que $(G_1\times G_2,*)$ est un groupe ;

  b. Montrer que si G_1 est cyclique d'ordre n_1, G_2 est cyclique d'ordre n_2 et si n_1 et n_2 sont premiers entre eux, alors $G_1\times G_2$ est cyclique d'ordre n_1n_2.

- **Ex. 4.** Montrer que $\left(\left(\mathbb{Z}/7\mathbb{Z}\right)\setminus\{\overline{0}\},\times\right)$ est un groupe cyclique.

méthode 5

Comment montrer qu'un sous-groupe d'un groupe est distingué (ou invariant) ?

Soient $(G,\cdot)$ un groupe et H un sous-groupe de G.

Pour montrer que H est *invariant* ou *distingué*, on montre que pour tout $a \in G$, $aHa^{-1} \subset H$.
Autrement dit : $\forall a \in G$, $\forall x \in H$, $axa^{-1} \in H$.

Remarque
Si $(G,\cdot)$ est un groupe commutatif, tout sous-groupe de G est distingué.

Exemple

Soit $(G,\cdot)$ un groupe tel qu'il existe un entier $n \in \mathbf{N}^*$ tel que pour tous $x,y \in G$, $(xy)^n = x^n y^n$. On note $G^{(n)} = \{x^n, x \in G\}$.
a. Montrer que $G^{(n)}$ est un sous-groupe de G ;
b. Montrer que $G^{(n)}$ est distingué dans G.

a. Soient $x,y \in G^{(n)}$, montrons que $xy \in G^{(n)}$. Il existe $u,v \in G$ tel que $x = u^n$, $y = v^n$, comme $xy = u^n v^n = (uv)^n$ et $uv \in G$ car G est un groupe, donc $xy \in G^{(n)}$.
Soit $x \in G^{(n)}$ et montrons que $x^{-1} \in G^{(n)}$. Il existe $u \in G$ tel que $x = u^n$, d'autre part comme $(u^n)^{-1} \cdot (u^n) = e_G$ et $(u^{-1})^n \cdot u^n = (u^{-1}u)^n = e_G$ (e_G étant l'élément neutre de G), donc $(u^n)^{-1} = (u^{-1})^n$ d'où $x^{-1} = (u^n)^{-1} = (u^{-1})^n$ et par suite $x^{-1} \in G^{(n)}$.
Par conséquent $G^{(n)}$ est un sous-groupe de G.

b. Soient $a \in G$ et $x \in G^{(n)}$, il existe donc $u \in G$ tel que $x = u^n$, et comme $axa^{-1} = au^n a^{-1} = (aua^{-1})(aua^{-1}) \cdots (aua^{-1}) = (aua^{-1})^n$ donc $axa^{-1} \in G^{(n)}$ et par suite $G^{(n)}$ est un sous-groupe distingué de G.

Exercices

• **Ex. 1.** Soient G, G' deux groupes et $f : G \to G'$ un morphisme de groupes.

a. Montrer que pour tout sous-groupe distingué H' de G', $f^{-1}(H')$ est un sous-groupe distingué de G ;

b. Montrer que si f est surjective, pour tout sous-groupe distingué H de G, $f(H)$ est un sous-groupe distingué de G.

➲ *Pour les exercices complémentaires, se reporter page 215.*

Comment déterminer la signature d'une permutation ?

Soit σ une permutation (un élément de S_n).

Pour déterminer la signature de σ, on décompose d'abord σ en produit de cycles dont les supports sont deux à deux disjoints (cette décomposition est unique), soit m le nombre de cycles formant cette décomposition.

La signature de σ est alors $(-1)^{n-m}$.

Exemple

Déterminer la signature de la permutation σ de S_{10} définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 5 & 2 & 1 & 4 & 7 & 9 & 8 & 10 \end{pmatrix}.$$

Décomposons d'abord σ en produit de cycles dont les supports sont deux à deux disjoints. Pour cela, considérons les cycles suivants

$$s_1 = (1,3,5),\ s_2 = (2,6,4),\ s_3 = (7),\ s_4 = (8,9) \text{ et } s_5 = (10)$$

On a : $\sigma = s_1 \circ s_2 \circ s_3 \circ s_4 \circ s_5$.

La signature de σ est alors $\text{sig}(\sigma) = (-1)^{10-5} = (-1)^5 = -1$.

Exercices

• **Ex. 1.** Soit σ la permutation de S_5 définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

a. Décomposer σ en produit de cycles à supports deux à deux disjoints ;

b. En déduire la signature de σ.

• **Ex. 2.** Calculer la signature de chacune des permutations suivantes :

a. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

b. $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 2 & 4 & 3 & 1 \end{pmatrix}$

c. $\sigma_n = \begin{pmatrix} 1 & 2 & 3 & \cdots & (n-1) & n \\ n & (n-1) & (n-2) & \cdots & 2 & 1 \end{pmatrix}$ avec $n \in \mathbf{N}^*$.

méthode 7

Comment montrer qu'un élément d'un anneau est nilpotent ?

Soit $(A,+,\times)$ un anneau et soit $a \in A$.

Pour montrer que a est *nilpotent*, on montre qu'il existe $n \in \mathbf{N}^*$ tel que $a^n = 0_A$.
(0_A étant l'élément neutre de $(A,+)$).

Exemple

Soit $M_2(\mathbf{R})$ l'ensemble des matrices carrées d'ordre 2, à coefficients dans $\mathbf{R}$.

On sait que $(M_2(\mathbf{R}),+,\times)$ est un anneau.

Montrer que la matrice $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est nilpotente.

Comme $A^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_{M_2(\mathbf{R})}$ donc il existe $n = 2 \in \mathbf{N}^*$ tel que $A^n = 0_{M_2(\mathbf{R})}$ et par suite A est nilpotente.

Exercices

- **Ex. 1.** Soient $(A,+,\times)$ un anneau et $x,y \in A$.
  a. Montrer que si x est nilpotent alors $1-x$ est inversible et calculer son inverse ;
  b. Montrer que si xy est nilpotent alors yx l'est aussi.
  c. Montrer que si x et y sont nilpotents et commutent alors $x+y$ est nilpotent.

- **Ex. 2.** Soient A, A' deux anneaux, f un morphisme d'anneau (cf. tome 1) et $a \in A$.
  Montrer que si a est nilpotent dans A alors $f(a)$ est nilpotent dans A'.

- **Ex. 3.** On considère l'anneau $\left(\mathbf{Z}/8\mathbf{Z},+,\times\right)$.
  Déterminer les éléments nilpotents dans $\left(\mathbf{Z}/8\mathbf{Z},+,\times\right)$.

- **Ex. 4.** Dans l'anneau $(M_3(\mathbf{R}),+,\times)$, on considère les matrices suivantes

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} -9 & 7 & 13 \\ -13 & 10 & 4 \\ 4 & -3 & -1 \end{pmatrix}.$$

  Montrer que A et B sont nilpotentes.