Exercices du CH03 : Structures algébriques usuelles

Exercices de la banque INP à étudier : ex 84 (racines n-ièmes de l'unité), 85 (factorisation de polynômes), 86 (démonstration petit théorème de Fermat), 89 (nombres complexes), 94 (système de congruences).

I TD du mardi 22/09

Sauf mention du contraire, les lois de groupe seront notées multiplicativement.

Exercice 1 (*Noyau)
Soient $(G, *)$ et $(G', \bullet)$, deux groupes, et $f : G \to G'$ un morphisme de groupes. Soient $x \in G$ et $y \in \ker f$. Montrer que $x * y * x^{-1} \in \ker f$.

Exercice 2 (*Exemples de morphismes de groupes)
Montrer que chacune des applications suivantes est un morphisme de groupes (en précisant les lois considérées). Déterminer leurs noyaux et images respectifs. Sont-ils injectifs ? surjectifs ? bijectifs ?

$$\begin{array}{rcl} f : \mathbb{C} & \to & \mathbb{C}, \\ z & \mapsto & \overline{z} \end{array} \qquad \begin{array}{rcl} g : \mathbb{C} & \to & \mathbb{C}^*, \\ z & \mapsto & e^z \end{array} \qquad \begin{array}{rcl} h_n : \mathbb{C}^* & \to & \mathbb{C}^*, \ n \in \mathbb{N}^* \\ z & \mapsto & z^n \end{array}$$

Exercice 3 (Exemples de groupes isomorphes ou non)**

1. Les groupes $(\mathbb{Z}/6\mathbb{Z})$ et $\mathbb{U}_6$ sont-ils isomorphes ? Et les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{U}_6$? On justifiera soigneusement.
2. Les groupes $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$ sont-ils isomorphes ?

Exercice 4 (Ordres et sous-groupes)**

1. Que dire de l'ordre des éléments dans un groupe fini de cardinal p premier ? Par conséquent, quels sont les sous-groupes d'un groupe fini G de cardinal p premier ?
2. Déterminer tous les sous-groupes de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. *Indication : On raisonnera sur les ordres possibles des éléments, compte tenu du cardinal du groupe...*
3. Sans effort, déterminer tous les sous-groupes de $\mathbb{U}_4$, $\mathbb{U}_5$ et $\mathbb{U}_6$.

Exercice 5 (Morphismes entre groupes additifs)**

1. Déterminer tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$. *Regarder l'image de* $1 \ldots$
2. Démontrer que les groupes additifs $\mathbb{Z}$ et $\mathbb{Z}^2$ ne sont pas isomorphes.
3. Montrer que le seul morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est le morphisme nul.

Exercice 6 (Conjugaison)**
Soit G un groupe. Pour $a \in G$, on note $f_a : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & axa^{-1} \end{array} \right.$.
Cette application est appelée *morphisme de conjugaison.*

1. Justement, montrer que pour tout $a \in G$, f_a est un automorphisme de G.
2. Montrer que $\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ a & \longmapsto & f_a \end{array} \right.$ est un morphisme de groupes, où $Aut(G)$ désigne l'ensemble des automorphismes du groupe G.
3. Est-ce que φ est injective ?

II TD du mercredi 23/09

1) MPI* seulement

Exercice 7 (*Théorème de Lagrange et ordre d'un élément dans un groupe fini)**
Soit G un groupe fini et H un sous-groupe de G.

1. Montrer que la relation définie par $x\mathcal{R}y \iff x^{-1}y \in H$ est une relation d'équivalence sur G, puis que toutes les classes d'équivalence de cette relation ont même cardinal.
2. En déduire que $Card(H)$ divise $Card(G)$ (c'est le *théorème de Lagrange*).
3. Application : en déduire que tout élément $x \in G$ vérifie $x^{Card(G)} = e$.
   On a donc ainsi démontré le théorème correspondant du cours.

Exercice 8 (*Orbite et stabilisateur)**
Soient $n \geq 2$ et G un sous-groupe de S_n. Pour tout $x \in \{1, \dots, n\}$, on note $\Omega(x) = \{\sigma(x),\ \sigma \in G\}$ (cet ensemble est appelé *l'orbite de x sous l'action de G*).

1. Démontrer : $\forall (x, y) \in \{1, \dots, n\}^2$, $\Omega(x) \cap \Omega(y) = \emptyset$ ou $\Omega(x) = \Omega(y)$.
2. Démontrer que l'ensemble $G_x = \{\sigma \in G,\ \sigma(x) = x\}$ est un sous-groupe de G.
   On l'appelle *stabilisateur de x*.
3. À l'aide de l'application $f : \left\{ \begin{array}{ccc} G & \longrightarrow & \Omega(x) \\ \sigma & \longmapsto & \sigma(x) \end{array} \right.$, en déduire : $Card\ \Omega(x) = \dfrac{Card\ G}{Card\ G_x}$.
4. Soit G un sous-groupe de S_n de cardinal p^k, avec $k \geq 1$ et p un nombre premier ne divisant pas n. Montrer qu'il existe $x \in \{1, \dots, n\}$ tel que : $\forall \sigma \in G$, $\sigma(x) = x$.

2) MPI/MPI*

Exercice 9 (*Un exemple)
Décomposer la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 7 & 8 & 2 & 6 & 3 & 4 & 5 \end{pmatrix} \in S_9$ en produit de cycles disjoints et déterminer sa signature.

Exercice 10 (Conjugaison d'un cycle)**
Soit $p \in \{1, \dots, n\}$ et $\sigma = (a_1\ \dots\ a_p)$ un p-cycle de S_n. Étant donné un élément quelconque $\rho \in S_n$, déterminer $\rho \circ \sigma \circ \rho^{-1}$ (élément dit « conjugué de σ par ρ »).

Exercice 11 (*Générateurs de S_n)**
Soit un entier $n \geq 2$. Montrer que le groupe symétrique S_n est engendré par :

1. les transpositions $\tau_{i,j} = (i\ j)$ avec $1 \leq i < j \leq n$;
2. les transpositions $\tau_{i,i+1}$ avec $1 \leq i \leq n-1$;
3. la paire $\{\tau_{1,2},\ (1\ 2\ \cdots\ n)\}$.
4. les transpositions $\tau_{1,k}$ avec $2 \leq k \leq n$.

Exercice 12 (Injectivité d'un morphisme de corps)**
Montrer que tout morphisme de corps est injectif.

Exercice 13 (Anneau intègre fini)**

1. Soit A un anneau intègre et soit $a \neq 0$ un élément de A.
   On définit les applications $\gamma_a : A \to A$ et $\delta_a : A \to A$ par : $\forall x \in A,\ \gamma_a(x) = ax$ et $\delta_a(x) = xa$.
   Montrer que γ_a et δ_a sont injectives.
2. En déduire que dans un anneau intègre fini, tout élément non nul est inversible.
   Ainsi, si l'on suppose A de plus commutatif, on obtient le résultat suivant : tout anneau intègre fini et commutatif est un corps.
   *En fait on peut même prouver que tout anneau intègre fini est un corps, sans supposer la commutativité, mais cela fait appel à un résultat connu sous le nom de **théorème de Wedderburn**.*

III A faire pour lundi 28/09

1) Groupes, anneaux, corps

Exercice 14 (*Groupe de matrices)
Par un argument rapide, établir que l'ensemble $H = \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},\ n \in \mathbb{Z}\right\}$ est un sous-groupe de $GL_2(\mathbb{R})$, et qu'il est monogène.

Exercice 15 (*Sous-corps de $\mathbb{Q}$)
Soit K un sous-corps de $\mathbb{Q}$.

1. Montrer qu'on a $\mathbb{Z} \subset K$.
2. En déduire qu'on a $K = \mathbb{Q}$. *Ainsi $\mathbb{Q}$ n'admet pas d'autre sous-corps que lui-même.*

Exercice 16 (Sous-anneaux de $\mathbb{Z}^2$)**
Pour $d \in \mathbb{N}$, on note $A_d = \{(x, y) \in \mathbb{Z}^2,\ y \equiv x\ [d]\}$.

1. Montrer que, pour tout $d \in \mathbb{N}$, A_d est un sous-anneau de $\mathbb{Z}^2$.
2. (a) Réciproquement, soit A un sous-anneau de $\mathbb{Z}^2$.
   Démontrer que $H = \{x \in \mathbb{Z},\ (x, 0) \in A\}$ est un sous-groupe de $\mathbb{Z}$.
   (b) En déduire qu'il existe $d \in \mathbb{N}$ tel que $A = A_d$.

2) Idéaux

Exercice 17 (Eléments nilpotents)**
Soit $(A, +, \times)$ un anneau commutatif.
On dit d'un élément a de A qu'il est **nilpotent** lorsqu'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$.
Montrer que l'ensemble des éléments nilpotents de A est un idéal de A.

Exercice 18 (Produit de deux idéaux)**
Soit A un anneau commutatif et I et J deux idéaux de A.

1. On note $IJ = \left\{\sum_{k=1}^{n} a_k b_k,\ n \in \mathbb{N}^* \text{ et } \forall k \in \mathbb{N},\ a_k \in I \text{ et } b_k \in J\right\}$.
   Montrer que IJ est un idéal de A (dit autrement, c'est l'idéal engendré par les produits d'éléments de I et de J).
2. On suppose qu'on a $I + J = A$. Montrer que $IJ = I \cap J$.
3. Soit $(m, n) \in \mathbb{N}^2$. On se place dans $A = \mathbb{Z}$ avec $I = m\mathbb{Z}$ et $J = n\mathbb{Z}$. Déterminer IJ.

Exercice 19 (Idéaux maximaux)**
Soit A un anneau. Un idéal I de A est dit maximal lorsqu'il est distinct de A et que les deux seuls idéaux de A contenant I sont I et A.

1. Déterminer les idéaux maximaux de $\mathbb{Z}$.
2. Montrer que $I = \{f \in C(\mathbb{R}, \mathbb{R}),\ f(0) = 0\}$ est un idéal maximal de $C(\mathbb{R}, \mathbb{R})$.

3) Arithmétique et anneaux $\mathbb{Z}/n\mathbb{Z}$

Exercice 20 (*Triplets pythagoriciens)
Soient 3 entiers non nuls a, b et c tels que $a^2 + b^2 = c^2$.

1. Montrer que a et b ne peuvent pas être tous deux impairs.
2. Si c est pair, que dire de a et b ? Illustrer ce cas par un exemple.

Exercice 21 (Nombres de Mersenne)**
Soient a et p deux entiers strictement supérieurs à 1. Montrer que si $a^p - 1$ est un nombre premier, alors $a = 2$ et p est premier.

Exercice 22 (Nombres premiers congrus à 3 modulo 4)**
En s'inspirant de la preuve de l'infinité des nombres premiers, montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Exercice 23 (*Calculs d'inverses modulo n)
Déterminer, selon s'il existe ou pas, l'inverse de :

- 6 modulo 17.
- 12 modulo 30.
- 11 modulo 25.

Exercice 24 (*Equations linéaires modulo n)

1. Résoudre l'équation $9x \equiv 3$ [16].
2. Résoudre l'équation $10x \equiv 4$ [78].

Exercice 25 (*Système dans $\mathbb{Z}/n\mathbb{Z}$)
Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ le système $\begin{cases} \overline{6}x + \overline{7}y = \overline{20} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases}$.

4) Polynômes

Exercice 26 (*Factorisation)
Factoriser au maximum les polynômes $X^4 + X^2 + 1$ et $X^6 + 1$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 27 (*CNS pour que deux polynômes soient premiers entre eux)
Soient A et B dans $\mathbb{C}[X]$. Montrer que A et B sont premiers entre eux si et seulement si ils n'ont pas de racine commune dans $\mathbb{C}$. Est-ce vrai dans $\mathbb{R}$?

IV TD du lundi 28/09

1) MPI* seulement

Exercice 28 (*Polynômes cyclotomiques)**
Pour un entier $n \geq 1$, on dit qu'une racine n-ième de l'unité z est primitive lorsque $z^d \neq 1$ pour tout entier d tel que $1 \leq d < n$. On note $\mathbb{P}_n$ l'ensemble des racines primitives n-ièmes de 1.
On définit $\Phi_n \in \mathbb{C}[X]$ par $\Phi_n = \prod_{z \in \mathbb{P}_n} (X - z)$.

1. Déterminer $\mathbb{P}_1$, $\mathbb{P}_2$, $\mathbb{P}_3$ et $\mathbb{P}_4$.
   Quel est le degré de Φ_n ?
2. Montrer que pour tout $n \geq 1$, on a $X^n - 1 = \prod_{d \geq 1,\ d|n} \Phi_d$.
3. Montrer que si p est un nombre premier et si k est un entier ≥ 1, alors :
$$\Phi_{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1.$$
4. Calculer Φ_n pour $n = 1, 2, 3, 4, 5, 6$.
5. Montrer que $\Phi_n \in \mathbb{Z}[X]$.

2) MPI/MPI*

Exercice 29 (Critère de divisibilité par 11)**

1. Pour $k \in \mathbb{N}$, déterminer le reste de la division euclidienne de 10^k par 11.
2. En déduire le critère de divisibilité par 11 d'un entier.

Exercice 30 (Théorème de Wilson)**

1. Soit p un nombre premier. Combien l'équation $x^2 = 1$ possède-t-elle de solutions dans $\mathbb{Z}/p\mathbb{Z}$?
2. Montrer qu'un nombre p est premier si et seulement si on a $(p-1)! \equiv -1\ [p]$.
   C'est le théorème de Wilson.
3. *Application* : calculer le reste de la division euclidienne de $(103!)^{109}$ par 107.

Exercice 31 (Exemple d'un groupe d'inversibles)**
Déterminer le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ et trouver un groupe additif qui lui soit isomorphe.
Indication : une fois calculé le cardinal de $(\mathbb{Z}/8\mathbb{Z})^\times$, on cherchera parmi les groupes additifs connus celui ou ceux de même cardinal. On aura ainsi les groupes candidats.

Exercice 32 (Equation du second degré dans $\mathbb{Z}/n\mathbb{Z}$)**
Résoudre l'équation $x^2 + \overline{2}x - \overline{3} = \overline{0}$ dans $\mathbb{Z}/7\mathbb{Z}$ et dans $\mathbb{Z}/91\mathbb{Z}$.

Exercice 33 (Diviseur premier d'un nombre de Mersenne)**
Soient p premier impair et k un diviseur premier de $2^p - 1$. Montrer que $k \equiv 1\ [2p]$.
Indication : examiner l'ordre de $\overline{2}$ dans $(\mathbb{Z}/k\mathbb{Z})^\times$.

Exercice 34 (PGCD, PPCM)**
On rappelle que $a \wedge b$ désigne le PGCD de a et b, et $a \vee b$ le PPCM de a et b.

1. Montrer que $(a+b) \wedge (a \vee b) = a \wedge b$ pour tout $(a, b) \in (\mathbb{N}^*)^2$.
2. Déterminer les $(a, b) \in \mathbb{N}^2$ tels que $\begin{cases} a + b = 144 \\ a \vee b = 420 \end{cases}$.

Exercice 35 (Existence de racine entière)**
Soient $P \in \mathbb{Z}[X] \setminus \{0\}$ unitaire et $r \in \mathbb{Q}$ tel que $P(r) = 0$. Montrer qu'on a en fait $r \in \mathbb{Z}$.