TD Nº 1

Structures algébriques usuelles

1 Groupes

Exercice 1. Dans chaque cas, montrer que H est un sous-groupe de G.

1. $H = \mathbb{U}_n = \left\{z \in \mathbb{C},\ \ z^n = 1\right\}$, $G = \left(\mathbb{C}^*, \times\right)$.
2. $H = \left\{a+b\sqrt{3},\ (a,b) \in \mathbb{N}\times\mathbb{Z} \text{ tq } a^2-3b^2 = 1\right\}$, $G = \left(\mathbb{R}_+^*, \times\right)$.
3. $H = \left\{\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix},\ (x,y,z) \in \mathbb{R}^3\right\}$, $G = \left(\mathcal{GL}_3(\mathbb{R}), \times\right)$.

Exercice 2. Soit G un groupe tel que $x^2 = e$ pour tout $x \in G$. Montrer que G est abélien.

Exercice 3. `Table du groupe` $(\mathcal{S}_3, \circ)$. L'ensemble $\mathcal{S}_3$ possède 6 éléments :

- l'application identité : $\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.
- trois transpositions : $(12) := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $(13) := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; $(23) := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.
- deux cycles de longueur 3 : $(123) := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $(132) := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

1. Dresser la table du groupe $(\mathcal{S}_3, \circ)$.

$\sigma \circ \sigma'$	$\sigma = \mathrm{Id}$	$\sigma = (12)$	$\sigma = (13)$	$\sigma = (23)$	$\sigma = (123)$	$\sigma = (132)$
$\sigma' = \mathrm{Id}$						
$\sigma' = (12)$						
$\sigma' = (13)$						
$\sigma' = (23)$						
$\sigma' = (123)$						
$\sigma' = (132)$						

2. En déduire l'inverse de chacun des éléments du groupe $(\mathcal{S}_3, \circ)$.
3. Le groupe $(\mathcal{S}_3, \circ)$ est-il abélien ? décrire tous les sous-groupes du groupe symétrique $(\mathcal{S}_3, \circ)$.

Exercice 4. 1. Soit $n \in \mathbb{N}^*$. Montrer que $\varphi : \begin{array}{ccc} \left(\mathbb{Z}/n\mathbb{Z}, +\right) & \longrightarrow & \left(\mathbb{U}_n, \times\right) \\ \overline{k} & \longmapsto & \mathrm{e}^{2ik\pi/n} \end{array}$ est un isomorphisme de groupes.

2. Montrer que $\varphi : \begin{array}{ccc} \left(\mathbb{R}, +\right) & \longrightarrow & \left(\mathcal{GL}_2(\mathbb{R}), \times\right) \\ \theta & \longmapsto & \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{array}$ est un morphisme de groupes. Quel est son noyau ?

Exercice 5. `Morphismes de` $(\mathbb{Q}, +)$ `dans` $(\mathbb{Z}, +)$. Soit $f : \mathbb{Q} \longrightarrow \mathbb{Z}$ un morphismes de groupes.

1. Montrer que $f(n) = nf(1)$ et $f\left(\frac{1}{m}\right) = \frac{1}{m}f(1)$ pour tout $(m,n) \in \mathbb{N}^* \times \mathbb{N}$.
2. Montrer alors que f est le morphisme nul.

Exercice 6. Montrer que les groupes produits $\left(\left\{-1,1\right\} \times \left\{-1,1\right\}, \times\right)$ et $\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +\right)$ sont isomorphes et déterminer explicitement l'isomorphisme. **Indication :** commencer par dresser la table de multiplication de chaque groupe.

Exercice 7. `Sous-groupe engendré par deux éléments.` Soient a, b deux éléments d'un groupe G et

$$H = \left\{a^{i_1}b^{j_1}a^{i_2}b^{j_2}\dots a^{i_n}b^{j_n},\ \ n \in \mathbb{N}^*, i_1, j_1, i_2, j_2, \dots, i_n, j_n \in \mathbb{Z}\right\}.$$

1. Montrer que H est le sous-groupe engendré par a et b.
2. Simplifier la description de H lorsque a et b commutent.

3. Quel est le sous-groupe de $\left(\mathcal{GL}_3(\mathbb{R}),\times\right)$ engendré par $A=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$ et $B=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$?

Exercice 8. Montrer que $\frac{1}{3}\mathbb{Z}+\frac{3}{5}\mathbb{Z}$ est un sous-groupe monogène de $\left(\mathbb{Q},+\right)$.

Exercice 9. Montrer que le groupe additif $\left(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+\right)$ n'est pas cyclique. **Indication :** raisonner par l'absurde.

Exercice 10. `Parties génératrices de` $\mathcal{S}_n$. Soit r un entier compris entre 2 et n, $\sigma=(x_1\ x_2\ \dots\ x_r)\in\mathcal{S}_n$ un cycle de longueur r et τ une permutation de $\mathcal{S}_n$.

1. Montrer $\tau\circ\sigma\circ\tau^{-1}=\left(\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_r)\right)$.

2. En déduire que $\mathcal{S}_n$ est engendré par :

a. les $n-1$ transpositions $(1\ k)$ avec $2\leq k\leq n$.

b. les $n-1$ transpositions $(k\ k+1)$ avec $1\leq k\leq n-1$. **Indication :** calculer $(k-1\ k)(1\ k-1)(k-1\ k)^{-1}$ pour $k\geq 3$.

c. $(1\ 2)$ et $(1\ 2\ \dots\ n)$. **Indication :** calculer $(1\ 2\ \dots\ n)(k\ k+1)(1\ 2\ \dots\ n)^{-1}$ pour $1\leq k\leq n-1$.

Exercice 11. `Propriétés d'isomorphismes.` Soit $\varphi:(G,\star)\longrightarrow(H,\top)$ un isomorphisme de groupes.

1. Montrer que G est abélien si, et seulement si, H est abélien.

2. Montrer que G est monogène de générateur a si, et seulement si, H est monogène de générateur $\varphi(a)$.

3. En déduire que G est cyclique si, et seulement si, H est cyclique.

4. Soit $(k,b)\in\mathbb{Z}\times G$ fixé. Montrer que l'équation $x^k=b$ a le même nombre de solutions dans G que $x^k=\varphi(b)$ dans H.

5. Les groupes suivants sont-ils isomorphes : $\left(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+\right)$ et $\left(\mathbb{Z}/4\mathbb{Z},+\right)$; $\left(\mathbb{Z}/6\mathbb{Z},+\right)$ et $\left(\mathcal{S}_3,\circ\right)$; $\left(\mathbb{R}^*,\times\right)$ et $\left(\mathbb{C}^*,\times\right)$?

2 Ordre d'un élément dans un groupe

Exercice 12. `Pour commencer.`

1. Quel est l'ordre de $\overline{3}$ dans $\left(\mathbb{Z}/12\mathbb{Z},+\right)$?

2. Soit j le complexe $\mathrm{e}^{2i\pi/3}$. Dans le groupe $\left(\mathcal{GL}_3(\mathbb{C}),\times\right)$, quel est l'ordre de la matrice $\operatorname{diag}\left(1,j,j^2\right)$.

Exercice 13. `Éléments ayant même ordre.` Soient a,b deux éléments d'un groupe G.

1. Montrer que b et aba^{-1} ont même ordre. Même question pour a et a^{-1}.

2. On suppose ab d'ordre fini égal à n. Quel est l'ordre de ba ?

Exercice 14. `Ordre d'une rotation plane.` Soit $\theta\in\mathbb{R}$. On pose $R_\theta=\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}\in\mathcal{GL}_2(\mathbb{R})$.

1. Montrer que R_θ est d'ordre fini si, et seulement si, $\frac{\theta}{2\pi}\in\mathbb{Q}$.

2. Si $\frac{\theta}{2\pi}=\frac{p}{q}$ avec $(p,q)\in\mathbb{Z}\times\mathbb{N}^*$ tels que $p\wedge q=1$. Déterminer l'ordre de R_θ.

Exercice 15. `Calcul de l'ordre dans un groupe.`

1. Soit G un groupe et a un élément de G d'ordre fini égal à n.

a. Soit $m\in\mathbb{N}^*$. Montrer que l'ordre de a^m est égal à $\frac{n}{m\wedge n}$.

b. En déduire l'ordre de $\overline{m}$ dans $\mathbb{Z}/n\mathbb{Z}$.

2. Soient G, H deux groupes et $a\in G$, $b\in H$ d'ordres respectifs p et q.

a. Montrer que l'ordre de (a,b) dans $G\times H$ est égal à $p\vee q$.

b. Déterminer les éléments d'ordre 3 dans le groupe $\left(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z},+\right)$.

Exercice 16. `Produit de groupes cycliques.` Soit G et H deux groupes cycliques.
Démontrer que $G\times H$ est cyclique si, et seulement si, les ordres de G et H sont premiers entre eux.

Exercice 17. `Signature et ordre d'un cycle.` Soit $n\geq 2$ et $\sigma=(i_1\ i_2\ \dots\ i_r)\in\mathcal{S}_n$ un cycle de longueur r avec $2\leq r\leq n$.

1. Démontrer que la signature de σ est égale à $(-1)^{r-1}$.

2. Montrer que l'ordre de σ est égal à r.

Exercice 18. `Ordre d'un élément et isomorphisme.` Soit $f : G \longrightarrow H$ un morphisme de groupes.

1. Soit $a \in G$ d'ordre fini. Comparer l'ordre de a et celui de $f(a)$. Que peut-on dire si f est injectif ?

2. Supposons f bijectif et G est fini. Montrer que G et H ont exactement le même nombre d'éléments de chaque ordre.

3. **Application :** les groupes $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont-ils isomorphes ?

Exercice 19. `Ordre du produit d'éléments dans un groupe.` Soit a et b deux éléments d'un groupe G tels que $ab = ba$. Soit p l'ordre de a et q l'ordre de b.

1. Montrer que l'ordre de ab est fini et divise $p \vee q$. Le résultat est-il vrai si a et b ne commutent pas ?

2. Supposons $p \wedge q = 1$. Montrer que l'ordre de ab est égal à $p \vee q$. Le résultat est-il vrai si p et q ne sont pas premiers entre eux ?

3. Soit $k \geq 3$. Généraliser le résultat de la question précédente au produit des a_i, $1 \leq i \leq k$ avec $a_i a_j = a_j a_i$ pour tout $i \neq j$.

4. **Application :** décomposer en cycles disjoints la permutation suivante : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 7 & 4 & 6 & 5 & 8 & 1 & 3 & 13 & 9 & 12 & 10 & 11 \end{pmatrix}$. Calculer son ordre, sa signature.

Exercice 20. `Groupe d'ordre un nombre premier.`

1. Soit G un groupe d'ordre p un nombre premier. Montrer que G est cyclique.

2. Soit H un groupe non trivial d'élément neutre e. On suppose que H n'admet pas de sous-groupes non triviaux.

a. Soit $a \in H \setminus \{e\}$. Justifier que $H = < a >$.

b. Montrer que H est cyclique d'ordre un nombre premier. **Indication :** utiliser le théorème de classification des groupes monogènes.

3 Anneaux, corps et algèbres

Exercice 21. `Pour commencer.`

1. Montrer que l'ensemble $\mathbb{Z}[\sqrt{2}] = \left\{a + \sqrt{2}b, \quad (a,b) \in \mathbb{Z}^2\right\}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

2. Montrer que l'ensemble $\mathcal{A} = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad (a,b) \in \mathbb{R}^2\right\}$ est un corps isomorphe à $\mathbb{C}$.

Exercice 22. `Anneau des entiers de Gauss.` Montrer que $\mathbb{Z}[i] = \left\{a + ib, \quad (a,b) \in \mathbb{Z}^2\right\}$ est un sous-anneau de $(\mathbb{C}, +, \times)$ et préciser ses éléments inversibles.

Exercice 23. `Élément nilpotent dans un anneau.` Soit A un anneau et $a \in A$.

1. On suppose qu'il existe $p \in \mathbb{N}^*$ tel que $(1-a)^p = 0$.

a. Montrer que a est inversible, puis calculer son inverse.

b. Montrer que $\left(1 - a^{-1}\right)^p = 0$.

2. **Application :** montrer que la matrice $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est inversible, puis calculer son inverse.

3. Supposons A commutatif et posons $\mathcal{N} = \left\{a \in A, \quad \exists p \in \mathbb{N}^* \text{ tel que } a^p = 0\right\}$ l'ensemble des éléments nilpotents de A.

a. Montrer que $\mathcal{N}$ est un idéal de A. Le résultat reste vrai si A n'est pas commutatif ?

b. Déterminer $\mathcal{N}$ lorsque $A = \mathbb{Z}/n\mathbb{Z}$ avec $n \geq 2$.

Exercice 24. `Morphismes d'anneaux de` $\mathbb{R}$. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ un morphisme d'anneaux.

1. Démonter que, pour tout $n \in \mathbb{Z}$, $f(n) = n$. En déduire que $f(r) = r$ pour tout $r \in \mathbb{Q}$.

2. Démonter que f est croissante.

3. En déduire que $f = \mathrm{Id}_{\mathbb{R}}$. **Indication :** pour $x \in \mathbb{R}$, utiliser l'encadrement : $\forall n \in \mathbb{N}^*, \quad \dfrac{\lfloor x.10^n \rfloor}{10^n} \leq x < \dfrac{\lfloor x.10^n \rfloor + 1}{10^n}$.

Exercice 25. `Les inversibles de` $\mathbb{Z}/8\mathbb{Z}$ `et` $\mathbb{Z}/11\mathbb{Z}$.

1. Déterminer les inversibles de le l'anneau $\mathbb{Z}/8\mathbb{Z}$. Le groupe des inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$ est-il cyclique ?

2. Montrer que les inversibles de l'anneau $\mathbb{Z}/11\mathbb{Z}$ forment un groupe cyclique. **Indication :** calculer les puissances de $\overline{2}$.

Exercice 26. `Idéaux d'un corps / Cas d'égalité : anneau - idéal.` Soit A un anneau commutatif non nul.

1. Soit I un idéal de A. Démontrer que : $I \cap \mathbb{U}(A) \neq \varnothing \implies I = A$.

2. On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A. Démontrer que A est un corps.

3. On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.

4. Montrer que les seuls idéaux d'un corps K sont $\{0_K\}$ et lui-même.

Exercice 27. Soit $A \in \mathcal{M}_n(\mathbb{R})$. On note $\mathscr{C}_A = \{M \in \mathcal{M}_n(\mathbb{R}),\ \ AM = MA\}$. Montrer que $\mathscr{C}_A$ est une algèbre.

Exercice 28. Montrer que l'ensemble $\mathcal{A} = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix},\ (a,b,c) \in \mathbb{R}^3 \right\}$ est une algèbre, et en donner une base en tant qu'espace vectoriel.

Exercice 29. Résoudre les systèmes de congruence suivants : $\begin{cases} x \equiv 1\,[6] \\ x \equiv 2\,[7] \end{cases}$, $\begin{cases} 3x \equiv 2\,[5] \\ 5x \equiv 1\,[6] \end{cases}$ et $\begin{cases} x \equiv 3\,[4] \\ x \equiv 4\,[5] \\ x \equiv 1\,[3] \end{cases}$.

Exercice 30. Résoudre l'équation $x^2 - \overline{4}x + \overline{3} = \overline{0}$ dans $\mathbb{Z}/11\mathbb{Z}$ et dans $\mathbb{Z}/8\mathbb{Z}$.

Exercice 31. `Théorème de Wilson.` Soit $n \geq 2$ un entier. Le but est de montrer le théorème de Wilson :

$$n \text{ premier} \iff (n-1)! \equiv -1\,[n].$$

1. Soit p un nombre premier. Combien de solutions l'équation $x^2 = \overline{1}$ admet-elle dans $\mathbb{Z}/p\mathbb{Z}$. En déduire que $(p-1)! \equiv -1\,[p]$.

2. Supposons n divise $(n-1)!+1$. Montrer que $\forall k \in [\![1, n-1]\!]$, k est inversible dans $\mathbb{Z}/n\mathbb{Z}$. En déduire que n est premier.

Exercice 32. Calculer le pgcd et les coefficients de Bézout des pôlynomes $A = X^4 - 4X^3 + 2X^2 + X + 6$ et $B = X^4 - 3X^3 + 2X^2 + X + 5$.

Exercice 33. Soit $P \in \mathbb{C}[X]$. Montrer P est à racines simples si, et seulement si, $P \wedge P' = 1$.

Exercice 34. `Irréductible versus avoir une racine.` Soit $P \in \mathbb{K}[X]$.

1. Montrer que, si P admet une racine dans $\mathbb{K}$ alors P n'est pas irréductible sur $\mathbb{K}$.

2. Supposons $\deg P = 2$ ou 3. Démontrer la réciproque de la question précédente.

3. La réciproque de la première question reste vraie pour $\deg P \geq 4$? **Indication :** considérons $P = X^4 + 1$ dans $\mathbb{R}[X]$.

4. Montrer que les polynômes $X^2 - X - 1$ et $X^3 - X - 1$ sont irréductibles sur $\mathbb{Z}$.

5. Montrer que $8X^3 - 6X - 1$ est irréductible sur $\mathbb{Q}$. En déduire que $\cos\left(\dfrac{\pi}{9}\right)$ est irrationnel.

Exercice 35. Soit $n \in \mathbb{N}^*$. On considère le polynôme $P = \prod_{k=1}^{n} \left(X^k - 1\right)^{\alpha_k}$. Soit $q \in [\![1, n]\!]$ et $\omega_q = \mathrm{e}^{2i\pi/q}$.

Montrer que la multiplicité de ω_q en tant que racine de P vaut $\sum_{\substack{k=1 \\ q|k}}^{n} \alpha_k$.

Exercice 36. Trouver tous les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P.

Exercice 37. Décomposer en facteurs du premier degré le polynôme $P = (1+X)^m - \mathrm{e}^{2i\pi\alpha}(1-X)^m$, $\dfrac{\alpha}{\pi} \in \mathbb{R} \setminus \mathbb{Q}$.

Exercice 38. Factoriser dans $\mathbb{C}[X]$ le polynôme $X^n - 1$, puis calculer $\prod_s = \prod_{k=0}^{n-1} \sin\left(x + \dfrac{k\pi}{n}\right)$ et $\prod_c = \prod_{k=0}^{n-1} \cos\left(x + \dfrac{k\pi}{n}\right)$, $x \in \mathbb{R}$.

Exercice 39. On considère l'équation $(\star) : a_n x^n + \ldots + a_1 x + a_0 = 0$ où les coefficients sont dans $\mathbb{Z}$. Montrer que si $\dfrac{p}{q}$ est racine de $(\star)$ avec $p \wedge q = 1$ alors $p \mid a_0$ et $q \mid a_n$.