STRUCTURES ALGÉBRIQUES, POLYNÔMES

- Il faut connaître la définition d'un groupe, d'un anneau, d'un corps, mais on ne s'en sert directement que rarement.
- La plupart du temps, pour montrer qu'on a un groupe, on montre plutôt que c'est un sous-groupe d'un groupe connu, en reconnaissant une partie d'un groupe connu et
  - ⋆ en utilisant la caractérisation d'un sous-groupe, c'est ce qui sert le plus dans la pratique,
  - ⋆ en faisant apparaître l'ensemble comme image directe ou réciproque d'un sous-groupe par un morphisme de groupe,
  - ⋆ en voyant l'ensemble comme image d'un groupe par une bijection vérifiant la propriété des morphismes de groupes.
- Attention à l'erreur très classique consistant à appliquer la formule du binôme dans un anneau sans vérifier que les deux éléments commutent.
- Attention aussi à bien penser à vérifier, pour un sous-anneau la présence de 1_A et pour un morphisme d'anneaux l'image de 1_A.

Vrai ou faux

1. $(\mathbb{N},+)$ est un groupe abélien.
2. $(\mathbb{R},\times)$ est un groupe abélien.
3. Si H sous-groupe de G, alors l'élément neutre de G est aussi celui de H.
4. La réunion d'une famille de sous-groupes de G est un sous-groupe de G.
5. Si $(G,\star)$ groupe, $a,b,c\in G$, $a\star b=a\star c\iff b=c$.
6. Si $(A,+,\times)$ est un anneau, $(A,+)$ et $(A,\times)$ sont des groupes.
7. Si $(\mathbb{K},+,\times)$ est un corps, $(\mathbb{K},+)$ et $(\mathbb{K},\times)$ sont des groupes.
8. $\{\pm 1\}$ est un sous groupe de $(\mathbb{R}^*,\times)$.
9. 1 est le seul élément inversible de $(\mathbb{Z},+,\times)$.
10. Tout anneau intègre est un corps.
11. $\mathbb{Z}^2$ est intègre.
12. Dans un anneau, si a différent de zéro, alors a est un diviseur de zéro.
13. Dans un anneau, $a^2-b^2=(a-b)\times(a+b)$.
14. Dans un anneau, $a^2=b^2\iff a=\pm b$.
15. Deux polynômes qui n'ont pas de racine commune sont premiers entre eux.
16. $\mathbb{R}$ est une sous-algèbre de la $\mathbb{C}$-algèbre $\mathbb{C}$.

1. Exercices traités en cours

1 Soient E et F deux ensembles et $f\in F^E=\mathscr{F}(E,F)$. Montrer que

1. f est injective si et seulement s'il existe $g\in E^F$ telle que $g\circ f=\mathrm{id}_E$.
2. f est surjective si et seulement s'il existe $h\in E^F$ telle que $f\circ h=\mathrm{id}_F$.

2 Soit $(G,\star)$ un groupe, H,K sont des sous groupes de $(G,\star)$. Montrer que

$$H\cup K \text{ sous-groupe de } G\iff H\subset K \text{ ou } K\subset H.$$

3 1. Montrer que $f:\left|\begin{array}{ccc}\mathbb{R}&\longrightarrow&\mathbb{C}^*\\ x&\longmapsto&\mathrm{e}^{\mathrm{i}x}\end{array}\right.$ est un morphisme de groupes.
Déterminer son image et son noyau.

2. Montrer que $f:\left|\begin{array}{ccc}\mathbb{R}^*&\longrightarrow&\mathbb{R}^*\\ x&\longmapsto&\frac{x}{|x|}\end{array}\right.$ est un morphisme de groupes.
Déterminer son image et son noyau.

3. Même question pour $g:\left|\begin{array}{ccc}\mathbb{C}^*&\longrightarrow&\mathbb{C}^*\\ z&\longmapsto&\frac{z}{|z|}\end{array}\right.$.

4 Montrer que si $f:(A,+,\times)\to(A',\oplus,\otimes)$ est un morphisme d'anneaux :

- L'image réciproque d'un sous-anneau de A' est un sous-anneau de A.
- L'image directe d'un sous-anneau de A est un sous-anneau de A'.
- L'image réciproque d'un idéal de A' par f est un idéal de A.
- L'image directe d'un idéal de A par f est un idéal de $f(A)$.

2. Structure de groupe

5 Soit E un ensemble muni d'une loi interne $*$ associative. Montrer que l'ensemble des éléments réguliers à gauche (c'est-à-dire $x\in E$ tels que $\forall\, a,b\in E,\quad x*a=x*b\Rightarrow a=b$) (respectivement réguliers à droite) est stable pour $*$.

6 Soit $G=]-1,1[$ et pour $(x,y)\in G^2$, $x\star y=\dfrac{x+y}{1+xy}$.
Montrer que $(G,\star)$ est un groupe. Est-il commutatif ?

7 **Transport de structure**

Soient G un ensemble muni d'une loi de composition interne $\star$, $(H,\times)$ un groupe et f une application surjective de H vers G telle que

$$\forall\, x,y\in H,\quad f(x\times y)=f(x)\star f(y).$$

Montrer que $(G,\star)$ est un groupe, et que si f est bijective, $(G,\star)$ isomorphe à $(H,\times)$.
Applications :

- Montrer que $(\mathbb{R},\star)$ est un groupe isomorphe à $(\mathbb{R},+)$, avec $a\star b=\sqrt[2021]{a^{2021}+b^{2021}}$
- Montrer que $(]-1,1[,\triangle)$ est un groupe isomorphe à $(\mathbb{R},+)$ avec $a\triangle b=\dfrac{a+b}{1+ab}$ (Utiliser th).

8 Soit G un groupe tel que pour tout $x \in G$, $x^2 = e$.

1. Montrer que G est abélien.
2. Soient H un sous-groupe strict de G, $a \in G \setminus H$. Montrer que $H \cup aH$ est un sous-groupe de G.
3. Si G est fini, en créant par récurrence un suite de sous-groupe de G de cardinal une puissance de 2, montrer que le cardinal de G est une puissance de 2.

9 Centre d'un groupe

Soit G un groupe. On appelle *centre* de G, noté $Z(G)$, l'ensemble des éléments de G qui commutent avec tous les autres. Montrer qu'il s'agit d'un sous-groupe commutatif de G.

10 Soit $(G, \star)$ un groupe commutatif de neutre e. On pose $T(G) = \{x \in G \mid \exists\, n \in \mathbb{N}^*,\ \ x^n = e\}$.

Montrer que $T(G)$ est un sous-groupe de $(G, \times)$.

11 Théorème de Lagrange

Soit $(G, *)$ un groupe d'**ordre** (c'est-à-dire de cardinal) fini, H un sous-groupe de G.

1. Montrer que la relation définie par $x \mathscr{R} y \iff x^{-1} * y \in H$ est une relation d'équivalence sur G.
2. Vérifier que les classes d'équivalence ont toutes le même cardinal.
3. Démontrer le théorème de Lagrange : $|H|$ divise $|G|$.

12 Pour tout $x \in \mathbb{R}$, on pose $M(x) = \begin{pmatrix} 1 & 0 & x \\ -x & 1 & -\frac{x^2}{2} \\ 0 & 0 & 1 \end{pmatrix}$.

Soit $G = \{M(x), x \in \mathbb{R}\}$. Montrer que $(G, \times)$ est un groupe. Est-il abélien ?

13 Soit G un ensemble et $\star$ une loi de composition interne associative sur G telle qu'il existe $e \in G$ tel que

- $\forall\, x \in G,\ \ x \star e = x$
- $\forall\, x \in G,\ \ \exists\, x' \in G,\ \ x \star x' = e$

Montrer que $(G, \star)$ est un groupe.

14 Soit $(G, \times)$ un groupe, $a \in G$ et H un sous-groupe de $(G, \times)$. On note $aHa^{-1} = \left\{aha^{-1}, h \in H\right\}$.

Montrer que aHa^{-1} est un sous-groupe de $(G, \times)$.

15 Automorphismes intérieurs

Soit $(G, *)$ un groupe. Pour tout $a \in G$, on note $\varphi_a : \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a * x * a^{-1} \end{array} \right.$

1. Soit $a \in G$. Montrer que φ_a est un automorphisme du groupe $(G, *)$.
2. On note $\mathrm{Int}(G) = \{\varphi_a, a \in G\}$. Montrer que $(\mathrm{Int}(G), \circ)$ est un groupe.

16 Sous-groupes distingués

Soit $(G, \times)$ un groupe. On dit qu'un sous-groupe H de $(G, \times)$ est distingué si

$$\forall\, (a, h) \in G \times H,\ \ aha^{-1} \in H.$$

1. Soit f un morphisme du groupe $(G, \times)$ vers un groupe $(G', *)$. Montrer que $\mathrm{Ker}\, f$ est un sous-groupe distingué de $(G, \times)$.
2. Soit H un sous-groupe distingué de $(G, \times)$ et K un sous-groupe de $(G, \times)$.
   On note $HK = \{x \times y, x \in H, y \in K\}$.
   Montrer que HK est un sous-groupe de $(G, \times)$.

3. Anneaux et idéaux, corps

17 Soit A un anneau commutatif et M une partie de A. On appelle **annulateur** de M l'ensemble des éléments $a \in A$ tels que $am = 0_A$ pour tout $m \in M$. Montrer qu'il s'agit d'un idéal de A.

18 Soit A un anneau commutatif et I un idéal de A. On dit que l'idéal I est **premier** si pour tout $a, b \in A$, $ab \in I \Longrightarrow a \in I$ ou $b \in I$.

1. Quels sont les idéaux premiers de $\mathbb{Z}$?
2. Montrer que si f est un morphisme d'anneaux de A dans A', l'image réciproque d'un idéal premier de A' est un idéal premier de A.

19 Quels sont les idéaux d'un corps ?

Montrer que si un anneau commutatif ne possède que $\{0_1\}$ et A comme idéaux, c'est un corps.

20 Nilpotents d'un anneau

On dit qu'un élément a d'un anneau A est *nilpotent* lorsqu'il existe $n \in \mathbb{N}$ tel que $a^n = 0_A$. Le plus petit $n \in \mathbb{N}$ vérifiant cette propriété est alors appelé **indice de nilpotence** de a.

1. Quels sont les éléments nilpotents d'un anneau intègre ?
2. Montrer que si $a, b \in A$ nilpotents qui commutent, $a + b$ et ab le sont. Que peut-on dire de leurs indices de nilpotence ?
3. Montrer que si A est commutatif, l'ensemble des éléments nilpotents est un idéal de A.
4. Montrer que si ab est nilpotent, ba l'est aussi. Comparer leurs indices de nilpotence.
5. Soit a nilpotent. Montrer que $1_A - a$ est inversible dans A et préciser son inverse.

21 Montrer que tout anneau fini intègre est un corps.

On pourra vérifier qu'une translation $x \mapsto ax$ est bijective.

22

Montrer que $\mathbb{Q}$ ne possède qu'un sous-corps.

23

Déterminer les endomorphismes de l'anneau $\mathbb{Z}$, puis de l'anneau $\mathbb{Q}$ et enfin de l'anneau $\mathbb{R}$.

Indication : pour le passage de $\mathbb{Q}$ à $\mathbb{R}$, on pourra vérifier que l'image d'un nombre positif l'est encore et en déduire qu'un endomorphisme est croissant puis utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$

24

Déterminer les endomorphismes de l'anneau $\mathbb{C}$ laissant $\mathbb{R}$ globalement invariant.

25

Soit A un anneau.

1. Justifier que les endomorphismes du groupe $(A,+)$ forment un anneau pour les lois $+$ et $\circ$, noté $\mathrm{Endo}(A)$.
2. Pour $a \in A$, on note $f_a : \left|\begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array}\right.$. Montrer que l'application $\phi : \left|\begin{array}{ccc} A & \longrightarrow & \mathrm{Endo}(A) \\ a & \longmapsto & \phi(a) = f_a \end{array}\right.$ est bien définie et est un morphisme d'anneau.

26 Entiers de Gauss

On définit l'ensemble des entiers de Gauss[1] comme étant l'ensemble des nombres complexes à coordonnées entières $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + \mathrm{i}\mathbb{Z} = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$.

1. Montrer qu'il s'agit d'un anneau intègre.
2. On définit, pour $z \in \mathbb{C}$, $N(z) = |z|^2$. Déterminer le groupe des inversibles de $\mathbb{Z}[\mathrm{i}]$ en utilisant N.
3. Un élément a de $\mathbb{Z}[\mathrm{i}]$ est dit irréductible dans $\mathbb{Z}[\mathrm{i}]$ lorsque

$$(\exists\, u, v \in \mathbb{Z}[\mathrm{i}],\ \ a = uv) \Rightarrow u \text{ est inversible ou } v \text{ est inversible.}$$

Montrer que 2 n'est pas irréductible dans $\mathbb{Z}[\mathrm{i}]$.

4. Soit $\varphi : \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}[\mathrm{i}]$ un endomorphisme d'anneaux.

   4.a) Calculer les deux valeurs possibles pour $\varphi(\mathrm{i})$.

   4.b) Quels sont les endomorphismes d'anneaux de $\mathbb{Z}[\mathrm{i}]$?

On définit l'ensemble des rationnels de Gauss comme étant l'ensemble des nombres complexes à coordonnées rationnelles $\mathbb{Q}[\mathrm{i}] = \mathbb{Q} + \mathrm{i}\mathbb{Q} = \{a + \mathrm{i}b \mid a, b \in \mathbb{Q}\}$.

5. Montrer qu'il s'agit d'un corps.
6. Quels sont les endomorphismes de corps de $\mathbb{Q}[\mathrm{i}]$?

1. 

Carl Friedrich Gauss (Brunswick 1777 - Göttingen 1855) est un mathématicien, astronome et physicien allemand. Surnommé *le prince des mathématiciens*, il est considéré comme l'un des plus grands mathématiciens de tous les temps. Gauss était un génie particulièrement précoce : à 7 ans (ou 10 selon les sources), il donne la formule calculant $1 + 2 + \cdots + 100$. À 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse en 1799, l'invention de la théorie des congruences, la résolution de problèmes de construction à la règle et au compas…Il est considéré comme le fondateur de la géométrie différentielle.

27 Anneau de Boole

On considère $(A,+,\times)$ un anneau de Boole cest-à-dire un anneau non nul tel que tout élément est idempotent pour la 2e loi ce qui signifie $\forall\, x \in A,\ \ x^2 = x$.

1. Montrer que $\forall\,(x,y) \in A^2,\ \ xy + yx = 0_A$ et en déduire que $\forall\, x \in A,\ \ x + x = 0_A$.
   En déduire que lanneau A est commutatif.
2. Montrer que la relation binaire définie sur A par $x \preccurlyeq y \iff yx = x$ est une relation d'ordre.
3. Montrer que $\forall\,(x,y) \in A^2,\ \ xy(x+y) = 0_A$.
   En déduire qu'un anneau de Boole intègre ne peut avoir que deux éléments.

28

Soit E un ensemble. On note $\mathscr{P}(E)$ l'ensemble des parties de E.

Soit A et B deux parties de E. On appelle différence symétrique de A et B l'ensemble

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

1. Montrer que Δ est une loi associative à l'aide d'une table de vérité dont les entêtes sont $x \in A$, $x \in B$, $x \in C$, $x \in A\Delta B$, $x \in (A\Delta B)\Delta C$, $x \in B\Delta C$ et $x \in A\Delta(B\Delta C)$
2. Montrer que $(\mathscr{P}(E), \Delta)$ est un groupe abélien.
3. Montrer que $\cap$ est distributive sur Δ
4. Montrer que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau commutatif.
5. Montrer que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau de Boole (voir exercice précédent).

29

Soient $\alpha \in \mathbb{Q}_*^+$ tel que $\sqrt{\alpha} \notin \mathbb{Q}$ et $\mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q} + \sqrt{\alpha}\mathbb{Q} = \{r + r'\sqrt{\alpha}\ ;\ r, r' \in \mathbb{Q}\}$.

1. Montrer que $(\mathbb{Q}(\sqrt{\alpha}), +, \times)$ est un corps.
2. Montrer que les anneaux $\mathbb{Q}(\sqrt{\alpha})$ et $\mathbb{Q}^2$ ne sont pas isomorphes[2].
3. Montrer que les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ ne sont pas isomorphes[3].

2.

Si c'était le cas, calculer $f(r)$ pour $r \in \mathbb{Q}$ puis $f(\sqrt{\alpha})$…

3.

Si c'était le cas, considérer le carré de l'image de $\sqrt{2}$, puis l'image elle-même… On pourra utiliser que $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{R} \setminus \mathbb{Q}$.