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.
- Lorsque l'on utilise deux polynômes, ne pas les appeler P et P' (sauf si le deuxième est effectivement le polynôme dérivé du premier.
- a est racine de P se traduit par $\tilde{P}(a) = 0$ mais aussi $(X - a)|P$, cela peut être bien pratique.
- Savoir traduire la multiplicité des racines à l'aide des polynômes dérivés.
- Pour se débarrasser d'un terme polynomial, une bonne idée peut être d'évaluer en une racine de celui-ci (calcul de restes de divisions euclidiennes...)
- Pour justifier qu'un polynôme est nul, il suffit de vérifier qu'il a trop de racines.
- Attention au polynôme nul dans les discussions faisant intervenir le degré, il faut souvent le traiter à part.
- L'arithmétique sur $\mathbb{K}[X]$ est semblable à celle sur $\mathbb{Z}$, mais l'utilisation des racines peut parfois court-circuiter les raisonnements.
- Bien connaître les relation cœfficients-racines, mais ne les appliquer qu'aux polynômes scindés. Il suffit par exemple de les considérer à cœfficients complexes.

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 $f(A)$.

5 Soit $A = X^5 - X^4 + 2X^3 + 1$ et $B = X^4 - X^3 + 3X^2 - 2X + 2$.

1. À l'aide de l'algorithme d'Euclide, déterminer $D = A \wedge B$.
2. En déduire $(U, V) \in \mathbb{R}[X]^2$ tel que $AU + BV = D$.

6 Factoriser dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ le polynôme $X^4 + 1$.

2. Travaux dirigés

7 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 $\forall\, a, b \in E,\ \ x * a = x * b \Rightarrow a = b$) (respectivement réguliers à droite) est stable pour $*$.

8 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 ?

9 **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

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

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).

10 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.

11 **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.

12 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 $(G, \times)$.

13 **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 $|G|$.

14 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.

15 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.

16 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.

17 **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 $a^n = 0_A$.

1. Quels sont les éléments nilpotents d'un anneau intègre ?
2. Soient $a, b \in A$ nilpotents qui commutent. Montrer que $a+b$ et ab le sont.
3. Montrer que si ab est nilpotent, ba l'est aussi.
4. Soit a nilpotent. Montrer que $1_A - a$ est inversible dans A et préciser son inverse.

18 Montrer que tout anneau fini intègre est un corps.

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

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

20 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 $\mathbb{R}$

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

22 Soit $(a,b) \in \mathbb{K}^2$ tel que $a \neq b$. Quel est le reste de la division euclidienne de P par $(X-a)(X-b)$? Que devient-il si $a = b$?

23 **Polynômes de Legendre** [1]

On considère pour $n \in \mathbb{N}$, le polynôme $L_n = \dfrac{\left((X^2-1)^n\right)^{(n)}}{2^n n!}$.

1. Déterminer le degré et le cœfficient dominant de L_n.
2. Soit $P_n = (X^2-1)^n$. Montrer que $(X^2-1)P_n' = 2nXP_n$. En déduire une relation entre L_n, L_n' et L_n''.
3. Montrer que L_n est scindé à racines simples toutes dans $]-1,1[$.

24 Résoudre dans $\mathbb{R}^3$ $\begin{cases} x+y+z=1 \\ x^2+y^2+z^2=9 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \end{cases}$

25 Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme à cœfficients dans $\mathbb{Z}$. Démontrer que si $\frac{p}{q}$ est une fraction irréductible racine de P alors p divise a_0 et q divise a_n.

Exemples : déterminer les racines rationnelles de $6X^4 - 11X^3 - X^2 - 4$.

26 Soit $A = X^3 - 3X + 1$.

1. A est-il irréductible dans $\mathbb{C}[X]$? dans $\mathbb{R}[X]$? dans $\mathbb{Q}[X]$?
2. A est-il scindé sur $\mathbb{C}$? sur $\mathbb{R}$? sur $\mathbb{Q}$?

27
1. Donner une condition nécessaire et suffisante sur les racines d'un polynôme pour qu'il soit scindé à racines simples.
2. Soit $P \in \mathbb{R}[X]$ scindé simple avec $\deg P \geqslant 2$. Montrer que P' est scindé simple.
3. Est-ce encore vrai sur $\mathbb{C}[X]$?
4. Soit $P \in \mathbb{R}[X]$ scindé avec $\deg P \geqslant 2$. Montrer que P' est scindé.

---

1. 

Adrien Marie Legendre (Paris 1752 - 1833) Pour les opérations géodésiques organisées par les observatoires de Paris et de Greenwich, il élabora de nombreux résultats de trigonométrie. Ses Éléments de géométrie (1794) se sont imposés pendant plus d'un siècle dans l'enseignement secondaire. Dans la Théorie des nombres (1798), il énonça la loi de distribution des nombres premiers et formula algébriquement la loi de réciprocité des résidus quadratiques, démontrée par Gauss. Sa classification des intégrales elliptiques en trois espèces distinctes prépare les travaux d'Abel et de Jacobi.

3. Groupes, anneaux, corps

28 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 ?

29 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.

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

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

31 **Automorphismes intérieurs**

Soit $(G,*)$ un groupe. Pour tout $a \in G$, on note φ_a l'application de G vers G définie par $\forall\, x \in G,\ \ \varphi_a(x) = a * x * a^{-1}$.

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.

32 **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 $(G,\times)$.

33 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.

34 Entiers de Gauss

On définit l'ensemble des entiers de Gauss[2] 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

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

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 $\mathbb{Q}[\mathrm{i}]$?

35 Anneau de Boole

On considère $(A, +, \times)$ un anneau de Boole c'est-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 l'anneau 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.

36

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).

2. 

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.

4. Polynômes

37

Quel est le reste de la division euclidienne de $X^{2n+1} + (X+1)^{n+2}$ par $X^2 + X + 1$, où $n \in \mathbb{N}$?

38

Factoriser sur $\mathbb{R}[X]$ les polynômes $X^4 + X^2 + 1$ et $(X^2 - X + 1)^2 + 1$.

39

Soit, pour $n \in \mathbb{N}^*$, $P_n = \dfrac{(X+\mathrm{i})^{2n+1} - (X-\mathrm{i})^{2n+1}}{2\mathrm{i}}$.

1. Montrer que P_n est un polynôme à cœfficients réels. Quel est son degré et son cœfficient dominant ?

2. Déterminer les racines de P_n. En déduire la décomposition en facteurs irréductibles de P_n sur $\mathbb{R}[X]$.

3. Montrer qu'il existe $Q_n \in \mathbb{R}[X]$ tel que $P_n = Q_n(X^2)$. Quel est le degré et le cœfficient dominant de Q_n ? Trouver les racines de Q_n.

4. Calculer $S_n = \displaystyle\sum_{k=1}^{n} \operatorname{cotan}^2 \frac{k\pi}{2n+1}$ puis $T_n = \displaystyle\sum_{k=1}^{n} \frac{1}{\sin^2 \frac{k\pi}{2n+1}}$.

5. Montrer que pour $x \in \left]0, \frac{\pi}{2}\right[$, $\sin x \leqslant x \leqslant \tan x$.

6. En déduire la limite de $u_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k^2}$.

40 Théorème de Bezout[3] avec degrés

Soient A et B deux polynômes non constants premiers entre eux. Montrer qu'il existe un unique couple de polynômes (U, V) tel que $AU + BV = 1$ avec $\deg U < \deg B$ et $\deg V < \deg A$.
Indication : $\deg AU = \deg BV$. *Utiliser le lemme de Gauß.*

41

Soient a et b deux entiers naturels dont le pgcd est d. Montrer que le pgcd de $X^a - 1$ et $X^b - 1$ est $X^d - 1$.

3. 

Étienne Bezout (Nemours 1730 - Avon 1783) Éminent mathématicien, adjoint mécanicien à l'Académie des sciences en mars 1758, il fut nommé en 1763 professeur et examinateur des gardes-marine et composa pour eux un Cours de mathématiques en 4 volumes. Membre de l'Académie de marine, il est l'auteur de nombreux ouvrages dont un Traité de navigation (1769) et une Théorie générale des équations algébriques (1779). Bézout contribua beaucoup à orienter dans un sens mathématique la formation des jeunes officiers pour les rendre aptes aux calculs astronomiques les plus savants. Un tel système, où la théorie l'emportait trop souvent sur la pratique, contrairement à ce qui se faisait en Angleterre, provoqua d'assez vives polémiques.