Préparation à l'agrégation externe de Mathématiques 2026-2027
Université Paris Cité-Grands Moulins

Structures algébriques

Muriel Livernet

Table des matières

1. Introduction aux structures algébriques

Etant donné un ensemble E on peut rajouter ce que l'on appelle une "structure algébrique" sur cet ensemble, par exemple des opérations (comme une somme, un produit) internes à l'ensemble ou des opérations externes. Les notions de

— groupes
— anneaux
— $\mathbb{K}$-espaces vectoriels
— $\mathbb{K}$-algèbres

sont des structures algébriques sur un ensemble. Pour cette introduction on dira "truc" pour l'une des 4 notions ci-dessus. Puis on pourra spécifier lorsque "truc=groupe" ou "truc=anneau".

Soient E et E' deux trucs.

— On définira la notion de morphisme de trucs de E dans E' : c'est une application $f : E \to E'$ qui respecte la structure algébrique. On montrera le
Théorème A- *La composée de deux morphismes de trucs est un morphisme de trucs. Pour tout morphisme de trucs $f : E \to E'$ bijectif , sa réciproque f^{-1} est aussi un morphisme de trucs.*
Un morphisme de trucs bijectif s'appelle un *isomorphisme de trucs*. S'il existe un isomorphisme de trucs entre E et E' on dira que E et E' sont des trucs *isomorphes*. Les ensembles sous-jacents sont en particulier équipotents.
— On montrera le

Théorème de transport de structures- *Si $f : E \to E'$ est une application surjective et E est un truc, alors il existe au plus une structure de trucs sur E' tel que f soit un morphisme de trucs. Si f est bijective et E (resp. E') est un truc, alors il existe une unique structure de truc sur E' (resp. E) tel que f soit un isomorphisme de trucs.*

— Soit F un sous ensemble de E, à quelles conditions sur F, F est-il un truc ? On dira alors que F est un sous-truc (sous-groupe, sous-anneau, sous-espace vectoriel, sous-algèbre). Dans le cas où F est un sous-truc l'inclusion canonique $i : F \to E$ sera un morphisme de trucs. On montrera le

Théorème B- *L'image directe d'un sous-truc de E par un morphisme de trucs $f : E \to E'$ est un sous-truc de E'. L'image réciproque d'un sous-truc de E' par f est un sous-truc de E.*

— On montrera le

Théorème C- *Si $\{F_i\}_{i\in I}$ est une famille de sous-trucs de E alors $\cap_{i\in I}F_i$ est un sous-truc de E.*

Cela permettra de montrer l'existence pour S sous-ensemble de E du plus petit sous-truc de E contenant S. On dira que c'est le *sous-truc de E engendré par l'ensemble S* (par exemple sous-espace vectoriel engendré par un ensemble, sous-groupe engendré par un ensemble).

— Soit $\mathcal{R}$ une relation d'équivalence sur l'ensemble E. On sait par le théorème de transport de structures que l'ensemble quotient $E/\mathcal{R}$ est muni d'au plus une structure de truc telle que l'application quotient canonique $E \to E/\mathcal{R}$ soit un morphisme de trucs. A quelles conditions sur $\mathcal{R}$ cette structure existe ? Si elle existe, on parlera de "truc quotient" (groupe quotient, anneau quotient, espace vectoriel quotient). Dans le cas où $E/\mathcal{R}$ est un truc, la surjection canonique $E \to E/\mathcal{R}$ est un morphisme de trucs et tout morphisme de trucs $f : E \to E'$ induit un isomorphisme de trucs $E/\mathcal{R}_f \to f(E)$. (**Théorème d'isomorphisme**)

2. Groupes

2.1. **Généralités sur la structure de groupe.** Cette section est consacrée à l'élaboration de la notion de groupe comme présentée dans l'introduction.

Définition 2.1.1. Un *groupe* est un ensemble G muni d'une loi de composition interne $\star : G \times G \to G$ associative, possédant un élément neutre e_G et tel que tout $x \in G$ possède un élément symétrique, noté $x^{\star -1}$ ou x^{-1} s'il n'y a pas de confusion. On dit que le groupe est *abélien* ou *commutatif* si pour tous $x, y \in G$ on a

$$x \star y = y \star x.$$

Dans le cas abélien la loi de composition interne est souvent notée "+" et appelée notation additive.

Notation 2.1.2. Pour $n \geq 0$ on définit par récurrence $x^{\star 0} = e_G$ et $x^{\star (n+1)} = x^{\star n} \star x$ et pour $n < 0$ $x^{\star n} = (x^{\star -1})^{\star (-n)}$. Si la notation est additive ($\star = +$) alors $x^{\star n}$ est noté nx.

Définition 2.1.3. Soient $(G, \star)$ et $(G', \star')$ deux groupes. Une application $f : G \to G'$ est appelée *morphisme de groupes* (ou *homomorphisme*) si pour tous $x, y \in G$ on a

$$f(x \star y) = f(x) \star' f(y).$$

Remarque 2.1.4. Si $f : G \to G'$ est un morphisme de groupes, on a nécessairement $f(e_G) = e_{G'}$.

Exercice 2.1.5. Montrer le théorème A et le théorème de transport de structures.

Proposition 2.1.6. *Soit H un sous-ensemble non vide d'un groupe $(G, \star)$. Si pour tous $h, h' \in H$ on a $h \star h' \in H$ et $h^{-1} \in H$ alors $(H, \star)$ est un groupe d'élément neutre $e_G \in H$. On dit que H est un* sous-groupe de G.

Exercice 2.1.7. Montrer les théorèmes B et C.

Soit G un groupe et S une partie de G. On notera $\langle S \rangle$ le sous-groupe de G engendré par S. Si $S = \{x\}$ est un singleton, par abus de notation on notera $\langle x \rangle$ le sous-groupe engendré par $\{x\}$. On rappelle que G est *monogène* s'il est engendré par un élément :

$$\exists x \in G, G = \langle x \rangle.$$

On rappelle que *le noyau* d'un morphisme de groupes $f : G \to G'$, noté $\mathrm{Ker} f$ est l'image réciproque de l'élément neutre de G'. Plus précisément

$$\mathrm{Ker} f = \{x \in E \mid f(x) = e_{G'}\}.$$

Proposition 2.1.8. *Un morphisme de groupes $f : G \to G'$ est injectif si et seulement si* $\mathrm{Ker} f = \{e_G\}$.

Proposition 2.1.9. *Soit $f : G \to G'$ un morphisme de groupes surjectif. Soit $H = \mathrm{Ker} f$. On a*

$$x \mathcal{R}_f y \iff xy^{-1} \in H \iff x^{-1}y \in H$$

Démonstration. On a $x \mathcal{R}_f y$ ssi $f(x) = f(y)$ ssi $f(xy^{-1}) = e_{G'}$ ssi $f(x^{-1}y) = e_{G'}$. □

On a vu dans le cours sur les ensembles que toute surjection d'ensembles $f : G \to G'$ induit une bijection $\bar{f} : G/\mathcal{R}_f \to G'$. La proposition ci-dessus dit que si f est un morphisme de groupes, les classes d'équivalence pour la relation $\mathcal{R}_f$ sont de la forme $xH = Hx$ avec $H = \mathrm{Ker} f$. Le théorème de transport de structures permet de dire que

le quotient par cette relation d'équivalence, noté G/H est muni d'une unique structure de groupes telle que la surjection canonique $G \to G/H$ est un morphisme de groupes.

On rappelle qu'un sous-groupe H de G est *distingué dans* G si l'une des équivalences suivantes est satisfaite

$$\begin{aligned} &\forall x \in G, \forall h \in H,\ xhx^{-1} \in H \\ \iff &\forall x \in G,\ xHx^{-1} = H \\ \iff &\forall x \in G,\ xH = Hx \end{aligned}$$

Proposition 2.1.10. *Soit $f : G \to G'$ un morphisme de groupes. Le sous-groupe* $\mathrm{Ker} f$ *est distingué dans G.*

Proposition 2.1.11. *Soit G un groupe et H un sous-groupe distingué de G. La relation sur G définie par $x\mathcal{R}y \iff xH = yH \iff Hx = Hy$ est une relation d'équivalence sur G et le quotient par cette relation est noté G/H. Il existe une unique structure de groupes sur G/H telle que la projection canonique $\pi : G \to G/H$ (définie par $\pi(x) = xH$), soit un morphisme de groupes.*

Démonstration. Le fait que la relation soit une relation d'équivalence est laissé en exercice (ou voir la section suivante classes à gauche, classes à droite modulo un sous-groupe). S'il existe une loi de groupe, nécessairement, comme π doit être un morphisme de groupes on doit avoir $xH \star x'H = xx'H$. Il faut cependant vérifier que si $xH = yH$ et $x'H = y'H$ alors $xx'H = yy'H$ pour définir la loi de composition interne sur G/H. On suppose que $x = yh$ et $x' = y'h'$. Alors $xx' = yhy'h' = yy'kh'$ pour un certain $k \in H$, puisque H est distingué dans G. Donc la loi est bien définie et elle est associative d'élément neutre $e_G H = H$. □

Exercice 2.1.12. En déduire le théorème d'isomorphisme.

2.2. **Exemples de groupes.**

2.2.1. *Groupes abéliens.*

(1) L'ensemble des nombres complexes muni de l'addition $(\mathbb{C}, +)$ et ses sous-groupes $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$. Remarquer que $\mathbb{N}$ n'est pas un sous-groupe car 4 ne possède pas de symétrique (opposé).

(2) L'ensemble des nombres complexes non nuls muni de la multiplication $(\mathbb{C}^*, \times)$ et ses sous groupes $\mathbb{R}^*, \mathbb{Q}^*$. Remarquer que $\mathbb{Z} \setminus 0$ n'est pas un sous-groupe de $(\mathbb{C}^*, \times)$ car 2 ne possède pas de symétrique (d'inverse) dans $\mathbb{Z}$.

(3) Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ pour $n \geq 0$: ce sont des groupes quotient de $\mathbb{Z}$ par le sous-groupe distingué $n\mathbb{Z}$.

Tout sous-groupe d'un groupe abélien est distingué.

2.2.2. $\mathbb{Z}$ *et* $\mathbb{Z}/n\mathbb{Z}$. Ce sont des groupes à part car ils sont monogènes et $\mathbb{Z}/n\mathbb{Z}$ est cyclique (monogène fini). Grâce à la division euclidienne on montre que les sous-groupes de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$ avec $n \geq 0$ et l'on montre que les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments de la forme $\bar{k}$ avec k premier avec n.

Soit G un groupe et $x \in G$, il existe un unique morphisme de groupes $\varphi_x : \mathbb{Z} \to G$ qui à 1 associe x. On a précisément

$$\varphi_x(n) = x^{\star n} \text{ et } \varphi_x(\mathbb{Z}) = \{x^{\star n}, n \in \mathbb{Z}\} \text{ est un sous-groupe de } G.$$

Définition 2.2.1. Un groupe G est monogène s'il existe $x \in G$ tel que $G = \langle x \rangle = \varphi_x(\mathbb{Z})$.

Théorème 2.2.2. *Tout groupe monogène G est soit infini et isomorphe à $\mathbb{Z}$ soit fini et isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n = |G|$.*

Démonstration. Le noyau de φ_x est un sous-groupe de $\mathbb{Z}$ donc de type $n\mathbb{Z}$. Le théorème d'isomorphisme permet de conclure

$$\bar{\varphi}_x : \mathbb{Z}/n\mathbb{Z} \to G$$

est un isomorphisme de groupes. □

Le morphisme caractéristique φ_x permet de défnir *l'ordre d'un élément $x \in G$* : c'est le cardinal du groupe $\varphi_x(\mathbb{Z})$ qui est monogène, soit infini, soit fini. Par la division euclidienne, on montre que

Proposition 2.2.3. *Soit $x \in G$ un élément d'ordre fini n. L'entier n est le plus petit entier tel que $x^{\star n} = e_G$. Si $x^{\star k} = e_G$ alors n divise k.*

2.2.3. *Exemples de groupes non abéliens.* Ils sont principalement issus de sous-groupes de bijection, ou de sous-groupes d'isomorphismes.

(1) Le groupe symétrique S_n est le groupe des bijections d'un ensemble à n éléments. Les éléments de ce groupe sont appelées permutation. Les p-cycles sont des permutations particulières, les 2-cycles sont appelés transposition. Revoir la signature d'une permutation, la décomposition en cycles à support disjoint, le groupe alternée A_n des permutations de signature paire : c'est aussi le noyau du morphisme de groupes $\mathrm{sgn} : S_n \to \{\pm 1\}$, donc c'est un sous-groupe distingué de S_n. Le groupe S_n est non abélien pour $n \geq 3$

(2) Le groupe des matrices inversibles $\mathrm{GL}_n(\mathbb{K})$ pour $\mathbb{K}$ un corps, éventuellement à coefficients dans $\mathbb{Z}$, muni de la multiplication matricielle et ses sous-groupes :
   (a) $\mathrm{GL}_n(\mathbb{Q})$, l'ensemble des matrices à coefficients rationnels de déterminant non nul est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ et de $\mathrm{GL}_n(\mathbb{C})$.
   (b) $\mathrm{SL}_n(\mathbb{R})$ est le groupe *spécial linéaire* formé des matrices de déterminant 1 ;
   (c) $\mathrm{O}(n)$ est le *groupe orthogonal*, formé des matrices orthogonales (les matrices $A \in M_n(\mathbb{R})$ vérifiant ${}^tAA = I_n$) ;
   (d) $\mathrm{SO}(n)$ est le *groupe spécial orthogonal*, le sous-groupe de $\mathrm{O}(n)$ formé des matrices de déterminant 1 ;
   (e) $\mathrm{SL}_n(\mathbb{Z})$ est le groupe des matrices à coefficients entiers de déterminant 1.

   Tous ces exemples peuvent se traduire au niveau des isomorphismes d'espace vectoriels $f : E \to E$ avec E un $\mathbb{K}$-espace vectoriel de dimension n.

(3) Pour G un groupe, le groupe $(\mathrm{Aut}(G), \circ)$ des isomorphismes de groupes $f : G \to G$ (appelés *automorphismes de G*).

2.3. **Relations d'équivalence associées à un sous-groupe.** Soit G un groupe et soit $H \subset G$ un sous-groupe. Sur G on définit deux relations d'équivalence, notées $\equiv_g$ et $\equiv_d$ par

$$x \equiv_g y \iff x^{-1} \star y \in H \iff xH = yH$$
$$x \equiv_d y \iff y \star x^{-1} \in H \iff Hx = Hy.$$

La classe de x pour $\equiv_g$ est xH. La classe de x pour $\equiv_d$ est Hx. On note G/H l'ensemble quotient par la relation $\equiv_g$ et $H\backslash G$ l'ensemble quotient par la relation $\equiv_d$. G/H est l'ensemble des *classes à gauche modulo H* et $H\backslash G$ l'ensemble des *classes à droite modulo H* . On notera $\pi : G \to G/H$ la projection canonique.

Exemples 2.3.1. Pour $H = \{e_G\}$, on a $xH = Hx = \{x\}$, donc $G/H = H\backslash G$ et la projection canonique $G \to G/H$ est bijective.

Pour $H = G$, on a $xH = Hx = G$, donc $G/H = H\backslash G = \{G\}$.

Théorème 2.3.2 (Théorème de Lagrange)**.** *Soit $(G, \star)$ un groupe fini et soit H un sous-groupe de G. On a $|G| = |H|\times|G/H| = |H|\times|H\backslash G|$. En particulier, le nombre d'éléments de H divise le nombre d'éléments de G.*

Notation 2.3.3. Lorsque G/H est fini, son nombre d'éléments s'appelle l'*indice* de H dans G et se note $[G : H]$. Si G/H est infini, on dit que l'indice de H dans G est infini.

Le théorème de Lagrange est très utile pour avoir une idée de l'ordre des éléments dans un groupe.

Corollaire 2.3.4. *Soit $(G, \star)$ un groupe fini d'ordre n. L'ordre d'un élément de G divise l'ordre de G. En particulier, pour tout $x \in G$ on a $x^n = e_G$. Si $f : G \to G'$ est un morphisme de groupes et x est un élément d'ordre n dans G alors $f(x)$ est d'ordre fini divisant n.*

Corollaire 2.3.5. *Un groupe fini d'ordre premier est cyclique.*

Proposition 2.3.6. *Soit $(G, \star)$ un groupe et soient $x, y \in G$. On suppose que x et y sont d'ordre fini $\omega(x)$ et $\omega(y)$ respectivement. On suppose que $\omega(x)$ et $\omega(y)$ sont premiers entre eux. Alors*

(1) $\langle x\rangle \cap \langle y\rangle = \{e_G\}$;

(2) Si de plus $x \star y = y \star x$, alors $\omega(x \star y) = \omega(x)\omega(y)$ et $\langle x \star y\rangle = \langle\{x, y\}\rangle$.

Remarque 2.3.7. En général, pour H sous-groupe de G on n'a pas de structure de groupes sur G/H et sur $H\backslash G$. Il faut que H soit distingué dans G, pour avoir une structure de groupes, et dans ce cas on a $G/H = H\backslash G$. On rappelle que si G est abélien alors tout sous-groupe est distingué.

2.4. **Exercices sur les groupes.**

Exercice 2.4.1.
(1) Donner l'ordre de tous les éléments de $\mathbb{Z}/12\mathbb{Z}$.
(2) Donner tous les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.
(3) Est-ce que $\mathbb{Z}^2$ est monogène ?
(4) Le groupe $\mathbb{Z}/9\mathbb{Z}$ est-il isomorphe au groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?
(5) Le groupe $(\mathbb{R}^*, \times)$ est-il isomorphe au groupe $(\mathbb{C}^*, \times)$?
(6) Le groupe $(\mathbb{C}, +)$ est-il isomorphe au groupe $(\mathbb{C}^*, \times)$?
(7) Trouver tous les endomorphismes de $(\mathbb{Q}, +)$.
(8) Trouver tous les morphismes de $\mathbb{Z}$ dans $\mathbb{Q}$.

Exercice 2.4.2. Dans le groupe $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ on considère les matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.

Calculer l'ordre de A, de B et de $C := AB$. Que remarque-t-on ?

Exercice 2.4.3. Montrer que $H = \{(x, y) \in \mathbb{Z}^2,\ x + y \in 2\mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}^2$ et qu'il est isomorphe à $\mathbb{Z}^2$.

Exercice 2.4.4. On considère les sous-groupes de $\mathrm{GL}_2(\mathbb{R})$ suivants :

$G = \{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \in M_2(\mathbb{R})\ ;\ b \neq 0\}$, $H = \{\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \in M_2(\mathbb{R})\ ;\ b \neq 0\}$ et $K = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\ ;\ a \in \mathbb{R}\}$.

Montrer que :

(1) $f : G \to \mathbb{R}^*,\ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mapsto b$ est un morphisme et que $K = \mathrm{Ker} f$.

(2) $g : G \to \mathbb{R},\ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mapsto a$ n'est pas un morphisme.

(3) $h : \mathbb{R}^* \to H,\ b \mapsto \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$ est un isomorphisme.

(4) $\varphi : \mathbb{R} \to K,\ a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ est un isomorphisme.

Exercice 2.4.5. Soit G un groupe. Soient $m, n \in \mathbb{N}\backslash\{0\}$.

(1) Déterminer tous les homomorphismes de $\mathbb{Z}$ dans G.

(2) Déterminer tous les homomorphismes de $\mathbb{Z}/n\mathbb{Z}$ dans G.

(3) En déduire tous les homomorphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ (resp. les automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$)

Exercice 2.4.6. Soit G un groupe et soit X une partie génératrice de G.

(1) Soit $f : G \to H$ un morphisme. Montrer que $f(X)$ engendre l'image de f.

(2) Montrer que $\mathrm{Im}(f)$ est cyclique d'ordre divisant $|G|$ lorsque G est cyclique.

On suppose dans la suite de l'exercice que X est fini, $X = \{x_1, x_2, .., x_n\}$.

(3) On suppose que $x_i x_j = x_j x_i$, $i, j = 1, \ldots, n$.

(a) Montrer que le groupe G est abélien.

(b) Montrer que l'application $\varphi : (m_1, m_2, ..., m_n) \mapsto x_1^{m_1} x_2^{m_2} ... x_n^{m_n}$ est un morphisme surjectif du groupe $\mathbb{Z}^n$ sur le groupe G.

(4) L'application φ est-elle encore un morphisme si G n'est pas abélien ?

Exercice 2.4.7. On considère le groupe S_3 des six permutations de trois éléments.

(1) Déterminer tous les sous-groupes de S_3.

(2) Lesquels de ces sous-groupes sont distingués dans S_3 ?

(3) Donner la liste complète de tous les groupes quotients de S_3.

Exercice 2.4.8. On considère le groupe quotient $(\mathbb{Q}/\mathbb{Z}, +)$.

(1) Montrer que l'application $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $\varphi(x) = e^{2i\pi x}$ est un homomorphisme de groupes.

(2) Calculer son noyau et son image, et en déduire que $\mathbb{R}/\mathbb{Z} \simeq \mathbb{U} := \{z \in \mathbb{C}; |z| = 1\}$.

(3) On note ϕ la restriction de φ au sous-groupe $\mathbb{Q}$. Montrer (par double inclusion) que l'image de ϕ est égale à

$$\mathbb{U}_\infty = \{z \in \mathbb{C};\ \text{il existe } n \in \mathbb{N}^* \text{ tel que } z^n = 1\} = \cup_{n \in \mathbb{N}^*} \mathbb{U}_n.$$

(4) En déduire que $\mathbb{Q}/\mathbb{Z} \simeq \mathbb{U}_\infty$.

Exercice 2.4.9. Soit G un groupe.

(1) Rappeler la définition du centre $Z(G)$ de G.

(2) Montrer que $Z(G)$ est un sous-groupe distingué de G.

(3) Quel est le centre d'un groupe abélien ?

(4) On suppose que $G/Z(G)$ est cyclique. Montrer que G est abélien et donc $Z(G) = G$.

Exercice 2.4.10. Soit $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, (a,b,c) \in \mathbb{R}^3 \right\}$, $H = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, (b,c) \in \mathbb{R}^2 \right\}$ et $K = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a \in \mathbb{R} \right\}$.

(1) Montrer que G est un sous-groupe non-abélien de $GL_3(\mathbb{R})$, que H est un sous-groupe abélien et distingué de G et que G/H est isomorphe à $\mathbb{R}$.

(2) Montrer que K est un sous-groupe non distingué dans G.

(3) Déterminer le centre $Z(G)$ de G, puis montrer que $G/Z(G)$ est isomorphe à $\mathbb{R}^2$.

Exercice 2.4.11. Soient G un groupe et H un sous-groupe distingué d'indice n.

(1) Montrer que pour tout $a \in G$, on a $a^n \in H$.

(2) Donner un exemple de sous-groupe H non distingué de G pour lequel il existe $a \in G$ avec $a^n \notin H$.

Exercice 2.4.12. Soient G un groupe fini et H un sous-groupe distingué d'ordre n et d'indice m. On suppose que m et n sont premiers entre eux. Montrer que H est l'unique sous-groupe de G d'ordre n. On pourra considérer la surjection canonique $G \to G/H$.

Exercice 2.4.13. Soit G un groupe. Notons $\mathrm{Aut}(G)$ le groupe de ses automorphismes.

(1) Considérons l'application $G \to \mathrm{Aut}(G)$ qui à g associe la conjugaison par g. Montrer que c'est un morphisme. Déterminer son noyau.

(2) Montrer que son image $\mathrm{Int}(G)$ (le groupe des *automorphismes intérieurs* de G) est distingué dans $\mathrm{Aut}(G)$. Le groupe quotient $\mathrm{Aut}(G)/\mathrm{Int}(G)$ s'appelle le groupe des *automorphismes extérieurs* de G.

(3) Déterminer $\mathrm{Aut}(G)$ et $\mathrm{Int}(G)$ lorsque G est le groupe des isométries du triangle équilatéral.

3. Anneaux

3.1. **Généralités sur la structure d'anneau.** Cette section est consacrée à l'élaboration de la notion d'anneau comme présentée dans l'introduction.

Définition 3.1.1. Un *anneau* est un ensemble A muni de deux lois de composition interne $+, \times : A \times A \to A$ et d'un élément neutre 1_A pour la loi $\times$ tels que : $(A, +)$ est un groupe abélien ; la loi $\times$ est associative et distributive par rapport à la loi $+$.

Remarque 3.1.2. On note souvent $(A, +, \times, 1_A)$ pour indiquer les lois de l'anneau A. On peut trouver dans la littérature la précision que l'anneau est *unitaire* (un anneau non-unitaire ne possède pas nécessairement d'élément neutre 1_A pour la loi $\times$). Dans la majorité des cas traités les anneaux considérés sont des anneaux commutatifs (la loi $\times$ est commutative).

Définition 3.1.3. Soient $(A, +, \times, 1_A)$ et $(A', +, \times, 1_{A'})$ deux anneaux. Une application $f : A \to A'$ est appelée *morphisme d'anneaux* si f est un morphisme de groupes (pour les lois $+$), si $f(1_A) = 1_{A'}$ et si pour tous $x, y \in A$ on a

$$f(x \times y) = f(x) \times f(y).$$

Exercice 3.1.4. Montrer le théorème A et le théorème de transport de structures.

Proposition 3.1.5. *Soit B un sous-ensemble non vide d'un anneau $(A, +, \times, 1_A)$. Si pour tous $b, b' \in B$ les trois conditions suivantes sont satisfaites :*

(1) $b - b' \in B$,

(2) $b \times b' \in B$,

(3) $1_A \in B$,

alors $(B, +, \times, 1_A)$ est un anneau. On dit que B est un sous-anneau de A.

Exercice 3.1.6. Montrer les théorèmes B et C.

Remarque 3.1.7. On remarque que tout morphisme d'anneaux $f : A \to A'$ est un morphisme de groupes (pour la loi $+$). Le noyau de f n'est pas un sous-anneau de A en général ! En effet si $f(1_A) = 0_{A'}$ comme f est un morphisme d'anneaux on doit avoir nécessairement $1_{A'} = 0_{A'}$ or ceci n'est possible que si $A' = \{0_{A'}\}$. On appelle cet anneau *l'anneau trivial*.

Comme dans le cas des groupes on a :

Proposition 3.1.8. *Un morphisme d'anneaux $f : A \to A'$ est injectif si et seulement si* $\mathrm{Ker} f = \{0_A\}$.

Ainsi pour étudier les quotients on a besoin d'une autre notion, la notion d'idéal. Pour la suite on suppose que A est **un anneau commutatif**.

Définition 3.1.9. Soit $(A, +, \times, 1_A)$ un anneau commutatif. Un *idéal* de A est un sous-ensemble I de A tel que I est un sous-groupe de A et

$$\forall a \in A, \forall i \in I, a \times i \in I.$$

Proposition 3.1.10. *Soit $f : A \to A'$ un morphisme d'anneaux.* $\mathrm{Ker} f$ *est un idéal de A.*

Proposition 3.1.11. *Soit A un anneau commutatif et H un sous-groupe de $(A, +)$. Il existe une unique structure d'anneau sur le groupe quotient A/H telle que la projection canonique $A \to A/H$ soit un morphisme d'anneaux si et seulement si H est un idéal de A.*

Démonstration. On a déjà vu que la loi + sur A/H est donnée par $(x+H)+(y+H) = (x+y)+H$ (le groupe $(A,+)$ étant abélien, tout sous-groupe H de A est distingué). On a également vu que si la structure d'anneau existe sur la quotient A/H alors elle est unique et donnée par $(x+H)\times(y+H) = (x\times y)+H$. Il faut montrer que cette définition a un sens si et seulement si H est un idéal de A. Mais

$$(x+h)\times(y+k) = x\times y + \underbrace{(h\times y + x\times k + h\times k)}_{=:u(h,k)}$$

et $u(h,k)\in H$ pour tous $h,k\in H$ si et seulement si H est un idéal de A. Notons que nécessairement, $1_{A/H} = 1_A + H$. □

Exercice 3.1.12. En déduire le théorème d'isomorphisme.

3.2. **Théorie des anneaux.**

Définition 3.2.1. Soit $(A,+,\times,1_A)$ un anneau commutatif. Un élément $x\in A$ est dit *inversible* s'il admet un inverse pour la multiplication : un élément $x'\in A$ tel que $x'\times x = x\times x' = 1_A$. Cet inverse se note en général x^{-1}. A est un *corps* si tout élément non nul ($\neq 0_A$) est inversible.

Proposition 3.2.2. *L'ensemble des éléments inversibles de A est un groupe pour la multiplication, noté $A^\times$.*

Exemples 3.2.3. Les anneaux $\mathbb{Q}$, $\mathbb{R},\mathbb{C}$, sont des corps ; l' anneau $\mathbb{Z}$ n'est pas des corps.

Définition 3.2.4. Un anneau commutatif $(A,+,\times,1_A)$ est *intègre* si l'égalité $x\times y = 0_A$ implique $x = 0_A$ ou $y = 0_A$.

Proposition 3.2.5. *Tout corps est intègre.*

Proposition 3.2.6. *Soient $n,k\in\mathbb{N}^*$. Les propriétés suivantes sont équivalentes.*

(1) $\bar{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

(2) $\bar{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times,\bar{1})$

(3) k est premier avec n.

Corollaire 3.2.7. *Soit $n\in\mathbb{N}^*$. Les propriétés suivantes sont équivalentes.*

(1) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

(2) Le nombre n est premier.

(3) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Pour $m\in\mathbb{N}$, notons $\pi_m : \mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ l'application quotient.

Théorème 3.2.8. (lemme chinois) *Soient $m,n\in\mathbb{N}^*$ premiers entre eux. Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ sont isomorphes. Plus précisément, l'application $\pi_{mn}(x)\mapsto(\tilde{\pi}_m(x),\tilde{\pi}_n(x))$ est bijective. C'est un isomorphisme d'anneaux.*

Corollaire 3.2.9. *Soit $n\in\mathbb{N}^*$. Écrivons $n = \prod_{i=1}^r p_i^{k_i}$ sa décomposition en nombres premiers. Alors on a un isomorphisme d'anneaux*

$$\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/p_1^{k_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_r^{k_r}\mathbb{Z}.$$

3.3. **Caractéristique d'un anneau.**

Proposition 3.3.1. *Soit $(A, +, \times, 1_A)$ un anneau commutatif. L'application $\kappa : \mathbb{Z} \to A$ donnée par $\kappa(k) = k1_A$ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A.*

Définition 3.3.2. La caractéristique d'un anneau A est l'unique entier $n \geq 0$ tel que $\mathrm{Ker}\kappa = n\mathbb{Z}$. On dit qe A est de caractéristique n.

Proposition 3.3.3. *La caractéristique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est n ($n \geq 2$).*

Proposition 3.3.4. *Soit $n \geq 2$. Il existe au plus un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to A$. Un tel morphisme existe si et seulement si la caractéristique de A divise n.*

Proposition 3.3.5. *Soit A un anneau. Si A est intègre alors sa caractéristique est soit 0 soit un nombre premier. En particulier la caractéristique d'un corps est soit 0 soit un nombre premier.*

3.4. **Exemples d'anneaux et propriétés arithmétiques.**

— On a vu que l'anneau commutatif $(\mathbb{Z}, +, \times, 1)$ et ses quotients $\mathbb{Z}/n\mathbb{Z}$ sont des anneaux incontournables, essentiellement car ce sont des groupes monogènes.
— Un exemple fondamental est donné par l'anneau $A[X]$ des polynomes à coefficients dans un anneau commutatif.
— D'autres exemples sont donnés par l'ensemble des matrices carrées à coefficients dans un anneau commutatif $(M_n(A), +, \times, \mathrm{id})$ ce sont des anneaux non-commutatifs !

Les propriétés arithmétiques (anneaux euclidiens, principaux, factoriels) seront étudiés plus en détails pendant l'année.

3.5. **Exercices sur les anneaux.**

Exercice 3.5.1. Les ensembles suivants sont-ils des anneaux (avec les lois $+$ et $\times$ évidentes). Déterminer leurs éléments inversibles.

(1) L'ensemble des nombres réels de la forme $a + b\sqrt{2}$, avec a et b rationnels.
(2) L'ensemble des nombres réels de la forme $a + b\pi$, avec a et b rationnels.

Exercice 3.5.2. Soit A l'ensemble des applications de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$. On le munit des deux opérations suivantes :

$$\forall (f, g) \in A^2, \forall x \in \mathbb{Z}/n\mathbb{Z}, (f + g)(x) = f(x) + g(x),$$
$$\forall (f, g) \in A^2, \forall x \in \mathbb{Z}/n\mathbb{Z}, (f * g)(x) = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} f(x - k)g(k).$$

Montrer que $(A, +, *)$ est un anneau.

Exercice 3.5.3. Quels sont les morphismes d'anneaux :

(1) de $\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$?
(2) de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$?
(3) de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$?

Donner une condition nécessaire et suffisante pour qu'il existe un morphisme d'anneaux de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$ (avec $a, b \in \mathbb{N} \setminus \{0\}$).

Exercice 3.5.4. Soit A un anneau intègre et $x \neq 0 \in A$. Montrer que l'application $\phi : A \to A$ définie par $\phi(a) = ax$ est un morphisme de groupe injectif. En déduire que si A est fini, alors A est un corps.

Exercice 3.5.5. Soit $\phi : A \to B$ un morphisme d'anneaux et soit $a \in A$. On dit que $a \neq 0_A$ est *irréductible* si a est non inversible et si

$$\forall b, c \in A, a = bc \Rightarrow b \text{ ou } c \text{ est inversible.}$$

Parmi les énoncés suivants, certains sont vrais et certains sont faux. Selon le cas, donner une preuve ou un contre-exemple.

(1) Si a est inversible, alors $a \notin Ker(\phi)$.

(2) Si $\phi(a)$ est inversible, alors a est inversible.

(3) Si ϕ est bijectif et a est irréductible, alors $\phi(a)$ est irréductible.

(4) Si a est inversible alors $\phi(a)^2$ est inversible.

(5) Si ϕ est injectif et a irréductible, alors $\phi(a)$ est irréductible.

(6) Si ϕ est surjectif et $\phi(a)$ irréductible, alors a est irréductible.

Exercice 3.5.6. Soit A un anneau commutatif et I un idéal de A.

On dit que I est un *idéal premier* si $I \neq A$ et $xy \in I \Rightarrow x \in I$ ou $y \in I$.

On dit que J est un *idéal maximal* s'il n'existe aucun idéal K contenant strictement J et différent de A.

(1) Montrer que I est premier si et seulement si A/I est intègre.

(2) Montrer que I est maximal si et seulement si A/I est un corps.

(3) Montrer que si A est un anneau principal (tout idéal est principal, i.e. engendré par un élément), I est premier si et seulement si I est maximal.

Exercice 3.5.7. Soit $A = C^\infty(]-1, +1[, \mathbb{R})$, et soit $I_n = \{f \in A, f(0) = f'(0) = \cdots = f^{(n)}(0) = 0\}$. Montrer que I_n est un idéal de A et que I_0 est maximal.

Exercice 3.5.8. Soit A un anneau et notons $A^\times = \{x \in A,\ x \text{ inversible}\}$. On rappelle que $A^\times$ est un groupe pour la multiplication dans A.

(1) Soit $p \in \mathbb{Z}$ un nombre premier. Déterminer l'ordre du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ et en déduire une nouvelle démonstration du petit théorème de Fermat ($n^p \equiv n\ [p]$).

(2) Soit $\alpha > 0$ un entier. Déterminer l'ordre du groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

(3) Soient a, b deux entiers premiers entre eux. En utilisant le théorème Chinois, montrer que $(\mathbb{Z}/ab\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$.

(4) Soit n un entier. Soit $n = \prod_{i=1}^r p_i^{\alpha_i}$ sa décomposition en un produit de nombres premiers. Calculer l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$.

4. Espaces vectoriels et $\mathbb{K}$-algèbres

Cette petite section donne uniquement les définitions des objets, en suivant la démarche de l'introduction. On fixe $\mathbb{K}$ un corps.

4.1. Espaces vectoriels sur un corps $\mathbb{K}$.

Définition 4.1.1. Un $\mathbb{K}$-*espace vectoriel* est un ensemble E muni d'une loi de composition interne $+ : E \times E \to E$ telle que $(E, +)$ est un groupe abélien et une loi de composition externe $\cdot : \mathbb{K} \times E \to E$ vérifiant les propriétés suivantes, pour tous $\lambda, \mu \in \mathbb{K}, x, y \in E$,

- $1_{\mathbb{K}} \cdot x = x$
- $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$
- $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
- $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$.

Remarque 4.1.2. Ces conditions impliquent : $0_{\mathbb{K}} \cdot x = 0_E$ et $\lambda \cdot 0_E = 0_E$. De même, nécessairement on a $(-1_{\mathbb{K}}) \cdot x = -x$.

Définition 4.1.3. Soient E et E' deux $\mathbb{K}$-espaces vectoriels. Une application $f : E \to E'$ est appelée *morphisme de $\mathbb{K}$-espaces vectoriels* (ou application $\mathbb{K}$-linéaire) si pour tous $x, y \in E, \lambda, \mu \in K$ on a

$$f(\lambda \cdot x + y) = \lambda \cdot f(x) + \mu \cdot f(y).$$

Exercice 4.1.4. Montrer le théorème A et le théorème de transport de structures.

Proposition 4.1.5. *Soit F un sous-ensemble non vide d'un $\mathbb{K}$-espace vectoriel E. Si pour tous $x, x' \in F, \lambda, \lambda' \in \mathbb{K}$ on a $\lambda \cdot x + \lambda' \cdot x' \in F$ alors $(F, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel. On dit que F est un* sous-espace vectoriel de E.

Exercice 4.1.6. Montrer les théorèmes B et C.

Soit E un $\mathbb{K}$-espace vectoriel et S une partie de E. On notera $\langle S \rangle$ le sous-espace vectoriel de E engendré par S.

Proposition 4.1.7. *Soit S une partie d'un $\mathbb{K}$-espace vectoriel E. On a*

$$\langle S \rangle = \{\sum_{i \in I} \lambda_i \cdot s_i \mid I \text{ fini }, s_i \in S, \lambda_i \in \mathbb{K}\}.$$

Proposition 4.1.8. *Soit E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Le groupe quotient E/F est muni d'une unique structure de $\mathbb{K}$-espace vectoriel telle que la projection canonique $\pi : E \to E/F$ soit une application linéaire.*

Exercice 4.1.9. En déduire le théorème d'isomorphisme.

4.2. $\mathbb{K}$-algèbre. .

Définition 4.2.1. Une $\mathbb{K}$-*algèbre* est un ensemble R muni d'une loi de composition interne $+ : R \times R \to R$, d'une loi de composition externe $\cdot : \mathbb{K} \times R \to R$ telles que $(R, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel et d'une loi de composition interne $\times : R \times R \to R$ distributive par rapport à $+$ et vérifiant, pour tous $\lambda \in \mathbb{K}, x, y \in R$,

$$\lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y).$$

Remarque 4.2.2. Dans la pratique, la loi $\times$ est associative (on parle de $\mathbb{K}$-algèbre associative) et unitaire. Dans ce cas $(R, +, \times, 1_R)$ est un anneau, $(R, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel, et ces lois satisfont la condition de la définition ci-dessus. Les deux exemples typiques sont $\mathbb{K}[X]$ et $M_n(\mathbb{K})$.

Définition 4.2.3. Soient R et R' deux $\mathbb{K}$-algèbres. Une application $f : R \to R'$ est appelée *morphisme de $\mathbb{K}$-algèbres*, si f est une application $\mathbb{K}$-linéaire vérifiant de plus, pour tous $x, y \in E$ on a

$$f(x \times y) = f(x) \times f(y).$$

Exercice 4.2.4. Montrer le théorème A et le théorème de transport de structures.

Proposition 4.2.5. *Soit U un sous-ensemble non vide d'une $\mathbb{K}$-algèbre R. Si U est un sous-espace vectoriel de R et pour tous $x, x' \in U, x \times x' \in U$, alors $(U, +, \cdot, \times)$ est une $\mathbb{K}$-algèbre. On dit que U est une* sous-algèbre de R.

Exercice 4.2.6. Montrer les théorèmes B et C.

Exercice 4.2.7. Décrire les sous-espaces vectoriels U d'une $\mathbb{K}$-algèbre R vérifiant qu'il existe une unique structure de $\mathbb{K}$-algèbre sur R/U telle que la projection canonique $R \to R/U$ soit un morphisme de $\mathbb{K}$-algèbre.

L'exercice suivant est important pour parler de polynômes d'endomorphismes, de fonctions polynômes etc...

Exercice 4.2.8. Soit R un $\mathbb{K}$-algèbre associative et unitaire. Soit $a \in R$. Montrer qu'il existe un unique morphisme de $\mathbb{K}$-algèbres $\varphi_a : \mathbb{K}[X] \to R$ vérifiant $\varphi_a(X) = a$.
Indication : on pourra procéder par analyse et synthèse : s'il existe alors nécessairement $\varphi_a(\sum_{i=0}^n \lambda_i X^i) = \sum_{i=0}^n \lambda_i \cdot a^i$ et démontrer que, ainsi défini, c'est un morphisme de $\mathbb{K}$-algèbre.