Julien Rouyer

Concours externe et interne

Réviser les bases pour l'agrégation de mathématiques

- Rappels fondamentaux
- Exercices d'annales corrigés

ellipses

Chapitre 1

Algèbre et arithmétique : groupes, anneaux, corps, idéaux et algèbres

Le gros pavé de plus de mille pages de Berhuy [Ber18] permet une immersion complète dans le très vaste domaine qu'est l'algèbre de niveau licence et master. On pourra aussi se reporter à l'indispensable Cours d'algèbre de Perrin [Per96] et au tome d'exercices qui lui est associé [Ort04], rédigé par Ortiz. Citons également le classique tome d'algèbre [Gou21] du *Maths en tête* de Gourdon.

Les recueils d'exercices d'algèbre du trio Francinou, Gianella & Nicolas [FGN01] proposent d'innombrables exemples pertinents et d'une grande qualité sur ce domaine.

L'excellent recueil de contre-exemples de Hauchecorne [Hau07] permet d'apprécier certaines subtilités.

1.1 Structures algébriques usuelles

Définitions

Un **groupe** est un ensemble non vide $\mathbb{A}$ muni d'une loi de composition interne (addition, multiplication ou composition), un **anneau** (resp. un **corps**) est un ensemble non vide $\mathbb{A}$ muni de deux lois de composition interne (addition et multiplication le plus souvent, parfois remplacée par la composition des applications), un **espace vectoriel** est un ensemble non vide $\mathbb{A}$ muni d'une loi de composition interne (addition) et d'une loi de composition externe (multiplication par un scalaire) et une **algèbre** est un ensemble non vide $\mathbb{A}$ muni de

deux lois de composition internes et d'une loi de composition externe. Les lois en question satisfont, *grosso modo*, toutes les conditions qu'on peut raisonnablement attendre d'elles et dont voici la liste.

Les propriétés sont à entendre pour tous $x, y, z \in \mathbb{A}$. Les symboles $+$ et $\times$ représentent des lois de composition internes : ce ne sont pas nécessairement l'addition ni la multiplication usuelles mais elles en possèdent un grand nombre de caractéristiques :

- $\mathbb{A}$ est non vide.
- $+$ est associative ($(x + y) + z = x + (y + z)$), possède un élément neutre qu'on notera $0_{\mathbb{A}} \in \mathbb{A}$ ($x + 0_{\mathbb{A}} = 0_{\mathbb{A}} + x = x$) et chaque $x \in \mathbb{A}$ admet dans $\mathbb{A}$ un symétrique pour $+$ qu'on notera $-x \in \mathbb{A}$ et vérifiant $x + (-x) = 0_{\mathbb{A}}$.
- quand $\mathbb{A}$ possède toutes les propriétés ci-dessus, $(\mathbb{A}, +)$ est un **groupe**.
- $+$ est commutative ($x + y = y + x$)
- quand $(\mathbb{A}, +)$ possède toutes les propriétés ci-dessus, $(\mathbb{A}, +)$ est un **groupe abélien** (on dit aussi groupe commutatif).
- $\times$ est associative ($(x \times y) \times z = x \times (y \times z)$), distributive par rapport à $+$ ($x \times (y + z) = x \times y + x \times z$ et $(x + y) \times z = x \times z + y \times z$).
- quand $(\mathbb{A}, +, \times)$ possède toutes les propriétés ci-dessus, c'est un **anneau**.
- quand $x \times y = 0_{\mathbb{A}} \Rightarrow x = 0_{\mathbb{A}}$ ou $y = 0_{\mathbb{A}}$, l'anneau $(\mathbb{A}, +, \times)$ est dit **intègre**.
- quand $\times$ possède un élément neutre qu'on notera $1_{\mathbb{A}}$, on dit de l'anneau $(\mathbb{A}, +, \times)$ qu'il est **unitaire**.
- tout élément non nul $x \in \mathbb{A}$ admet dans $\mathbb{A}$ un symétrique qu'on notera $x^{-1} \in \mathbb{A}$ et vérifiant $x \times x^{-1} = 1_{\mathbb{A}}$ (ce qui signifie en particulier que $\mathbb{A}$ est supposé unitaire). $(\mathbb{A}, +, \times)$ est alors automatiquement intègre.
- quand $(\mathbb{A}, +, \times)$ possède toutes les propriétés ci-dessus, c'est un **corps** et en particulier $(\mathbb{A}^*, \times)$ est un groupe.
- quand $\times$ est commutative, on dit d'un anneau $(\mathbb{A}, +, \times)$ qu'il est commutatif.
- quand $(\mathbb{A}, +, \times)$ possède toutes les propriétés ci-dessus, c'est un **corps commutatif** et en particulier $(\mathbb{A}^*, \times)$ est un groupe abélien.
- $(\mathbb{A}, +, \cdot)$ est un **espace vectoriel** sur un corps $\mathbb{K}$ donné, si $(\mathbb{A}, +)$ est un groupe abélien et $\cdot$ est la multiplication des éléments de $\mathbb{A}$ par les éléments de $\mathbb{K}$ (appelés *scalaires*). Cette multiplication doit être associative ($\alpha \cdot (\beta \cdot x) = (\alpha\beta) \cdot x$), distributive par rapport à $+$ ($\alpha \cdot (x + y) = \alpha \cdot x + \beta \cdot y$) et l'élément unité de $\mathbb{K}$ doit être neutre : $\forall x \in \mathbb{A}, 1_{\mathbb{K}} \cdot x = x$.

— $(\mathbb{A}, +, \times, \cdot)$ est une **algèbre** (resp. une **algèbre commutative**) sur un corps $\mathbb{K}$ donné si $(\mathbb{A}, +, \times)$ est un anneau (resp. un anneau commutatif) et $(\mathbb{A}, +, \cdot)$ est un espace vectoriel.

Il y aurait bien quelques subtilités à dire (notamment sur les algèbres), mais nous garderons un silence courtois à ce sujet.

Quand il n'y a pas d'ambiguïté sur les lois de composition, on peut se permettre de parler du groupe (resp. anneau, corps, espace vectoriel, algèbre) $\mathbb{A}$ plutôt que d'écrire lourdement $(\mathbb{A}, +)$ (resp. $(\mathbb{A}, +, \times)$, $(\mathbb{A}, +, \cdot)$, $(\mathbb{A}, +, \times, \cdot)$), noter xy pour $x \times y$ et αx pour $\alpha \cdot x$, voire, parfois (et seulement quand l'énoncé nous y incite), fg pour $f \circ g$.

Dans la suite, la loi d'un groupe sera notée multiplicativement (on écrira ab et non pas $a+b$, a^{-1} et non pas $-a$) quand elle n'est pas explicitement une addition.

Sous-structures

Un sous-groupe $\mathbb{B}$ d'un groupe $\mathbb{A}$ est une partie non vide de $\mathbb{A}$ stable par la loi de composition interne de $\mathbb{A}$, c'est-à-dire $a, b \in \mathbb{B} \Rightarrow ab \in \mathbb{B}$ et $a^{-1} \in \mathbb{B}$.

Les notions similaires de sous-anneau, sous-corps, sous-espace vectoriel et sous-algèbre désignent à chaque fois des parties non vides et stables pour l'ensemble des lois de composition (y compris par opposé ou inverse quand l'une de ces notions a un sens) de la structure initiale.

Sous-groupe normal (ou distingué)

Un sous-groupe $\mathbb{B}$ d'un groupe $\mathbb{A}$ est dit normal ssi $\forall a \in \mathbb{A}, aB = Ba$. L'intérêt des sous-groupes normaux est de permettre de définir le groupe quotient $\mathbb{A}/\mathbb{B}$ (il est nécessaire que $\mathbb{B}$ soit distingué dans $\mathbb{A}$ pour pouvoir définir la loi de composition interne du quotient à partir de celle de $\mathbb{A}$).

Idéal

Un idéal $\mathbb{I}$ d'un anneau $(\mathbb{A}, +, \times)$ est un sous-groupe de $(\mathbb{A}, +)$ absorbant pour $\times$.

Si $\forall a \in \mathbb{A}, \forall i \in \mathbb{I}, ai \in \mathbb{I}$ on dira de $\mathbb{I}$ que c'est un idéal à gauche.

Si $\forall a \in \mathbb{A}, \forall i \in \mathbb{I}, ia \in \mathbb{I}$ on dira de $\mathbb{I}$ que c'est un idéal à droite.

Si $\mathbb{I}$ vérifie les deux propriétés ci-dessus, c'est un idéal bilatère.

Dans un anneau commutatif, les trois notions ci-dessus se confondent. L'intérêt des idéaux est de permettre de définir l'anneau quotient $\mathbb{A}/\mathbb{I}$ (il est nécessaire que $\mathbb{I}$ soit un idéal de $\mathbb{A}$ pour pouvoir définir les lois de composition interne du quotient à partir de celles de $\mathbb{A}$).

Un idéal $\mathbb{I}$ est dit **maximal** quand les seuls idéaux le contenant sont lui-même et $\mathbb{A}$ et c'est le cas ssi $\mathbb{A}/\mathbb{I}$ est un corps.

Un idéal $\mathbb{I}$ est dit **premier** quand $\mathbb{I} \neq \mathbb{A}$ et $ab \in \mathbb{I} \Rightarrow (a \in \mathbb{I}$ ou $b \in \mathbb{I})$ et c'est le cas ssi $\mathbb{A}/\mathbb{I}$ est intègre.

Un idéal $\mathbb{I}$ est dit **principal** quand il est engendré par un seul élément, c'est-à-dire $\exists\, a \in \mathbb{A}, \mathbb{I} = a\mathbb{A} = \{ab \,|\, b \in \mathbb{A}\}$.

Les idéaux triviaux d'un anneau $\mathbb{A}$ sont $0_{\mathbb{A}}\mathbb{A} = \{0_{\mathbb{A}}\}$ et $1_{\mathbb{A}}\mathbb{A} = \mathbb{A}$.

Les idéaux de $\mathbb{Z}$ sont tous principaux et en particulier les idéaux non triviaux de $\mathbb{Z}$ sont les groupes du type $n\mathbb{Z}$ pour $n \in \mathbb{N}^*$, $n \neq 1$. Les idéaux du type $p\mathbb{Z}$ pour $p \in \mathbb{P}$ sont maximaux. Dans $\mathbb{Z}$ les notions d'idéal premier et d'idéal maximal sont confondues, à l'exception de l'idéal $\{0\}$ qui est premier (comme c'est toujours le cas dans un anneau intègre) mais pas maximal.

1.2 Groupes

1.2.1 Bestiaire

On rappelle ici succinctement quelques-uns des groupes les plus courants, à l'exception notable des groupes projectifs.
Soit E un espace vectoriel, $\mathbb{K}$ un corps commutatif, G et H deux groupes, $n \in \mathbb{N}^*$.

Le groupe $\mathbb{Z}/n\mathbb{Z}$

Ses éléments sont les classes de congruence modulo n. C'est un groupe abélien pour l'addition et plus précisément le groupe quotient du groupe abélien $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$.

Le groupe linéaire $\mathrm{GL}(E)$ ou $\mathrm{GL}_n(\mathbb{K})$

$(\mathrm{GL}(E), \circ)$ est le groupe des automorphismes (c'est-à-dire les endomorphismes bijectifs) de E.

$(\mathrm{GL}_n(\mathbb{K}), \times)$ est le groupe des matrices inversibles de $\mathscr{M}_n(\mathbb{K})$.

Le groupe spécial linéaire $\mathrm{SL}(E)$ ou $\mathrm{SL}_n(\mathbb{K})$

Si E est de dimension finie, $\mathrm{SL}(E)$ est le sous-groupe de $\mathrm{GL}(E)$ constitué des endomorphismes de E de déterminant 1.

$\mathrm{SL}_n(\mathbb{K})$ est le sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ constitué des matrices de déterminant 1.

Le groupe orthogonal $\mathrm{O}(E)$ ou $\mathrm{O}_n(\mathbb{K})$ ou $\mathrm{O}(E,q)$

Si E est un espace euclidien, $\mathrm{O}(E)$ est le sous-groupe de $\mathrm{GL}(E)$ constitué des isométries de E. Si $u \in \mathrm{GL}(E)$, cela revient à écrire :

$$u \in \mathrm{O}(E) \Leftrightarrow \forall x \in E, ||u(x)|| = ||x||.$$

De même on note $\mathrm{O}_n(\mathbb{K})$ le sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ constitué des matrices qui conservent la norme.

Les vecteurs colonnes (resp. lignes) d'un élément de $\mathrm{O}_n(\mathbb{K})$ forment une base orthonormée de $\mathbb{K}^n$.

L'inverse d'un élément de $\mathrm{O}_n(\mathbb{K})$ est égal à sa transposée.

Plus généralement, si E est un e.v. quelconque et q une forme quadratique sur E, le groupe orthogonal de q, $\mathrm{O}(E,q)$ est constitué des automorphismes $u \in \mathrm{GL}(E)$ laissant q invariante, c'est-à-dire tels que $\forall x \in E, q(u(x)) = q(x)$.

Le groupe spécial orthogonal $\mathrm{SO}(E)$ ou $\mathrm{SO}_n(\mathbb{K})$ ou $\mathrm{SO}(E,q)$

$\mathrm{SO}(E) = \mathrm{SL}(E) \cap \mathrm{O}(E)$ est le sous-groupe de $\mathrm{GL}(E)$ constitué des isométries de déterminant 1.

De même on note $\mathrm{SO}_n(\mathbb{K})$ le sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ constitué des matrices de déterminant 1 qui conservent la norme.

Plus généralement, $\mathrm{SO}(E,q) = \mathrm{SL}(E) \cap \mathrm{O}(E,q)$ est le sous-groupe de $\mathrm{GL}(E)$ constitué des endomorphismes de déterminant 1 laissant la forme quadratique q invariante.

Le groupe diédral $\mathbb{D}_n$

Le groupe diédral est constitué des $2n$ isométries du plan (n rotations dont l'identité et n réflexions) laissant invariant le polygone régulier à n côtés.

$\mathbb{D}_n$ est engendré par la rotation d'angle $\dfrac{2\pi}{n}$ et une réflexion.

Le groupe symétrique $\mathfrak{S}_n$

Le groupe symétrique, constitué de l'ensemble des permutations d'un ensemble à n éléments (par exemple $\{1, 2, \ldots, n\}$), est noté $\mathfrak{S}_n$ ou encore S_n pour ceux qui sont fâchés avec la graphie gothique. Il contient $n!$ éléments.

Par exemple, $\mathfrak{S}_3 = \{id, (12), (13), (23), (123), (132)\}$.

Les éléments de $\mathfrak{S}_n$ peuvent toujours s'exprimer comme composées (on dit aussi produits) de cycles à supports disjoints mais aussi comme produit de transpositions (une transposition est un cycle de longueur 2).

Par exemple, (abc) désigne le cycle de longueur 3 qui à a associe b, à b associe c et à c associe a.

Le groupe alterné A_n

Le groupe alterné est le sous-groupe de $\mathfrak{S}_n$ constitué des permutations paires (c'est-à-dire celles dont la signature vaut 1).

A_n est le noyau de l'application signature $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$. Celle-ci étant un morphisme de groupes surjectif quand $n \geqslant 2$, le premier théorème d'isomorphisme permet d'obtenir que le cardinal de A_n est $\dfrac{n!}{2}$.

En tant que noyau d'un morphisme de groupes (mais aussi en tant que sous-groupe d'indice 2, quand $n \geqslant 2$), A_n est distingué dans $\mathfrak{S}_n$.

Par exemple, $A_3 = \{id, (123), (132)\}$.

Le groupe de Klein

Le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est le plus petit exemple de groupe (additif) non cyclique. C'est aussi le plus petit anneau non intègre.

Le groupe des quaternions $\mathbb{Q}_8$

C'est, avec les règles $i^2 = j^2 = k^2 = ijk = -1$, le groupe multiplicatif

$$\mathbb{Q}_8 = \{1, -1, i, j, k, -i, -j, -k\}.$$

On en déduit $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$.

Ne pas confondre $\mathbb{Q}_8$ avec le corps des quaternions $\mathbb{H}$.

Centre d'un groupe

Le centre $Z(G)$ d'un groupe G est constitué des éléments de G qui commutent avec tous les éléments de G :

$$z \in Z(G) \Leftrightarrow \forall g \in G, zg = gz.$$

Sous-groupe distingué (ou normal)

H est un sous-groupe distingué (ou normal) de G et on note $H \lhd G$ ssi

$$H \subset G \qquad \text{et} \qquad \forall g \in G, gHg^{-1} \subset H,$$

ce qui revient à montrer que $\forall g \in G, gHg^{-1} = H$ ou encore $\forall g \in G, gH = Hg$.

Les sous-groupes distingués de G sont ceux qui sont stables par l'action de conjugaison de G sur lui-même. Ce sont plus précisément les points fixes de l'action de conjugaison de G sur l'ensemble des sous-groupes de G.

L'intérêt des sous-groupes distingués est de permettre de définir la notion de groupe quotient (il est nécessaire que H soit un sous-groupe distingué de G pour pouvoir définir les lois de composition interne du quotient G/H à partir de celles de G).

Groupe quotient

Si H est un sous-groupe distingué de G, l'ensemble quotient G/H a pour éléments les classes d'équivalence modulo H, c'est-à-dire les parties de G du type $gH = \{gh; h \in H\}$ pour les éléments g de G. G/H est muni d'une structure de groupe induite naturellement par celle de G.

Groupe dérivé

Le groupe dérivé $D(G)$ de G est le sous-groupe de G engendré par les commutateurs $[g,h] = ghg^{-1}h^{-1}$, pour $g, h \in G$.

$D(G)$ est un sous-groupe distingué de G et c'est le plus petit sous-groupe distingué H de G tel que G/H soit abélien.

Groupe monogène

G est monogène si il est engendré par un de ses éléments g. On note

$$G = \langle g \rangle = \left\{ g^k, k \in \mathbb{Z} \right\}.$$

Tout groupe monogène infini est isomorphe à $\mathbb{Z}$, tout sous-groupe d'un groupe monogène est monogène.

Groupe cyclique

Si G est monogène et fini, il est dit cyclique.

Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, tout sous-groupe d'un groupe cyclique est cyclique.

Sous-groupe de Sylow ou p-Sylow

Si G est un groupe fini d'ordre $|G| = n$ et si $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}$ sont tels que $p^\alpha \mid n$ et $p^{\alpha+1} \nmid n$ (c'est-à-dire qu'on peut écrire $n = p^\alpha m$ avec m premier avec p), un sous-groupe de G d'ordre p^α est appelé p-Sylow.

1.2.2 Résultats majeurs

Des trois théorèmes d'isomorphismes, on doit surtout connaître parfaitement le premier ainsi que sa démonstration. Donnés ici pour des groupes, ils peuvent se généraliser à d'autres structures (les anneaux et les espaces vectoriels par exemple).

Théorèmes d'isomorphisme

Premier théorème d'isomorphisme. Soit G et H deux groupes et $f : G \to H$ un morphisme de groupes.

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$$

et l'isomorphisme de $G/\mathrm{Ker}(f) = \{g\mathrm{Ker}(f), g \in G\}$ à $\mathrm{Im}(f) = \{f(g), g \in G\}$ est fourni par le morphisme de groupes $\hat{f}$ défini à partir de f par

$$\begin{array}{rccc} & G/\mathrm{Ker}(f) & \to & \mathrm{Im}(f) \\ \hat{f} : & g\mathrm{Ker}(f) & \mapsto & \hat{f}(g\mathrm{Ker}(f)) = f(g) \end{array}$$

si G est noté multiplicativement (si G était un groupe additif, il conviendrait d'écrire $g + \mathrm{Ker}(f)$ au lieu de $g\mathrm{Ker}(f)$).

Il faut bien sûr vérifier que $\hat{f}$ est ainsi (1) bien défini (c'est-à-dire que si $g_1\mathrm{Ker}(f) = g_2\mathrm{Ker}(f)$ on a bien $f(g_1) = f(g_2)$), (2) un morphisme de groupes, (3) injectif et (4) surjectif.

Deuxième théorème d'isomorphisme. Soit G un groupe, N un sous-groupe distingué de G et H un sous-groupe de G. Alors $H \cap N$ est un sous-groupe distingué de H et

$$H/(H \cap N) \simeq HN/N.$$

Il faut pour cela s'assurer que HN est un groupe et N un sous-groupe distingué de HN. On utilise ensuite le premier théorème d'isomorphisme avec $f : h \in H \mapsto hN \in HN/N$.