Présentation des chapitres de mathématiques de MP

Structures algébriques

Vous avez vu en 1re année différentes structures algébriques : groupes, anneaux, corps, espaces vectoriels, avec l'accent mis plus particulièrement sur cette dernière structure. Nous revenons sur les autres, surtout sur les groupes.

1 Théorie des groupes et des anneaux

La théorie des groupes est infiniment profonde et possède des motivations riches qui lui sont propres (même si l'algébriste finit par découvrir qu'un groupe n'est réellement intéressant que lorsqu'il *agit* sur un ensemble, de la même manière qu'une permutation σ dans S_n ne s'étudie pas en soi, mais à travers son action sur $[\![1,n]\!]$, et malheureusement le programme de MPSI/MP ne met pas en valeur cet aspect). Cependant, le point de départ de ma motivation, dans ce document, puise dans une analogie avec l'algèbre linéaire ; non pas parce que c'est le plus pertinent, mais parce que c'est le plus parlant pour vous, à ce stade de votre formation mathématique.

Vous avez pu juger de l'intérêt des bases en algèbre linéaire de deux manières :

— un certain nombre de résultats, valables pour tout vecteur d'un espace vectoriel de dimension finie, se démontrent en se contentant de vérifier ces résultats pour tout vecteur d'une base ;

— une base de E permet d'exprimer tout vecteur de E à l'aide d'un n-uplet de *coordonnées* qui le caractérise entièrement ; or raisonner avec n-uplet revient à raisonner dans K^n, qui est un espace vectoriel très simple d'étude (là où E ne l'était pas forcément).

Le dernier point se formule de façon plus savante en disant que le choix d'une base permet d'obtenir un isomorphisme d'espaces vectoriels $f : K^n \to E$: comme un isomorphisme préserve tout ce qui est relatif à la structure, on peut raisonner indifféremment avec E ou K^n (de même avec $\mathrm{L}(E)$: le choix d'une base permet de raisonner indifféremment avec $\mathrm{M}_n(K)$).

Exercice 1.

1. Démontrer cette affirmation : quel est l'isomorphisme $f : K^n \to E$ obtenu en fixant une base ?
2. Et si l'on remplace la base par une famille libre, que devient l'application linéaire f de la question précédente ? Et si l'on considère une famille génératrice ?

Étant donné le succès de la notion dans le cadre de l'algèbre linéaire, on peut se demander si on peut la transposer à d'autres structures, à commencer par les groupes. Même si la notion de base se transpose assez mal (et d'ailleurs nous n'en parlerons pas), l'exercice suivant expliquant le type de souci que l'on peut rencontrer :

Exercice 2. Pour comprendre ce qui coince lorsqu'on veut transposer la notion de base à des groupes, étudions le cas particulier de $\mathbb{Z}$. On dit qu'une famille de $\mathbb{Z}$ est libre, génératrice, une base si elle vérifie les propriétés qu'on attend d'une telle famille dans un K-espace vectoriel, mais en remplaçant K par $\mathbb{Z}$ (attention à ne pas vouloir généraliser cela à tout groupe, cela n'aurait en général aucun sens).

1. Montrer que les seules bases de $\mathbb{Z}$ sont (1) et (-1).
2. Montrer que la famille (2,3) est une famille génératrice de $\mathbb{Z}$, mais qu'aucune de ses familles extraites n'est une base de $\mathbb{Z}$.
3. Montrer que le théorème de la base incomplète ne se généralise pas aux groupes, en montrant que pour tout $n \in \mathbb{Z} \setminus \{-1,0,1\}$ la famille (n) est libre (mais n'est pas une base, ce qui contredit un autre résultat classique d'algèbre linéaire : lequel ?) et ne peut pas être complétée en une base de $\mathbb{Z}$.

Mais ce n'est pas si grave : nous allons tout de même définir ce qu'est une partie génératrice d'un groupe. Dans l'idée : si S est une partie de G, alors nous dirons que S engendre G si tout élément $g \in G$ s'écrit comme produit d'éléments de S et de leurs inverses :

$$\forall g \in G,\ \exists r \in \mathbb{N},\ \exists (g_1,\dots,g_r) \in S^r,\ \exists (\varepsilon_1,\dots,\varepsilon_r) \in \{-1,1\}^r,\quad g = g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r}.$$

Si G est commutatif et sa loi notée additivement, alors la dernière égalité devient : $g = \sum_{i=1}^{r} \varepsilon_i g_i$. Mieux : si $S = \{s_1, \dots, s_k\}$ est une partie finie de G (toujours supposé commutatif), alors le terme général de la somme précédente est de la forme $\pm s_i$ pour tout i et, quitte à regrouper les termes qui sont égaux, on peut réécrire de manière équivalente la propriété d'être une partie génératrice ainsi :

$$\forall g \in G,\ \exists (a_1, \dots, a_k) \in \mathbb{Z}^k,\ g = \sum_{i=1}^{k} a_i s_i.$$

C'est le point de vue de l'exercice 2.

Exercice 3. Soit $n \in \mathbb{N} \setminus \{0\}$.

1. Justifier que $\mathbb{Z}$ admet $\{1\}$ et $\{-1\}$ comme parties génératrices.
2. Montrer que $\mathbb{U}_n$ admet $\left\{e^{\frac{2i\pi}{n}}\right\}$ comme partie génératrice. En proposer d'autres à un seul élément.
3. Soit C l'ensemble des cycles dans S_n. Justifier que S_n admet C comme partie génératrice.
4. Soit T l'ensemble des transpositions dans S_n. Justifier que S_n admet T comme partie génératrice.

Comme en algèbre linéaire, un certain nombre de résultats peuvent se démontrer en raisonnant uniquement sur une partie génératrice :

Exercice 4. Soit G un groupe dont on note S une partie génératrice.

1. Soit H un sous-groupe de G. Montrer : $H = G \iff S \subseteq H$.
2. Soit $f : K \to G$ un morphisme de groupes. Montrer que f est surjective si et seulement si : $S \subseteq \mathrm{im}(f)$.
3. Soient $f : G \to K$ et $g : G \to K$ deux morphismes de groupes. Montrer : $f = g \iff f_{|S} = g_{|S}$.

En vérité, la définition de partie génératrice donnée ci-dessus n'est pas la plus commode pour traiter cet exercice. Pour la théorie, on privilégiera une autre définition : on définira le sous-groupe engendré par S, noté $\langle S \rangle$, comme le plus petit sous-groupe de G contenant les éléments de S (plus petit au sens de l'inclusion), et on dira que S engendre G si : $\langle S \rangle = G$. Vérifiez que cela simplifie grandement les raisonnements de cet exercice en les affranchissant de calculs.

Nous donnerons des exemples de parties génératrices : l'exercice 3 en donne quelques-uns, mais nous en donnerons davantage, surtout dans le cas particulier du groupe symétrique S_n. Une partie génératrice est en effet d'autant plus intéressante qu'elle a peu d'éléments, et nous pouvons faire mieux que les parties génératrices C et T proposées. Le cas le plus favorable est bien sûr celui où un groupe admet une partie génératrice avec **un seul** élément : dans ce cas, il suffit la plupart du temps de raisonner sur cet unique générateur pour obtenir un résultat valable pour tout le groupe ! Cette situation est si appréciable qu'elle mérite qu'on lui donne un nom : on parle dans ce cas de groupe *monogène*, et plus particulièrement de groupe *cyclique* s'il est en plus de cardinal fini.

Le groupe monogène infini par excellence est $\mathbb{Z}$ (voir l'exercice 3). Nous montrerons en effet que tout autre groupe monogène infini est isomorphe à $\mathbb{Z}$; comme un isomorphisme de groupes conserve tout ce qui est relatif à la structure de groupe, étudier $\mathbb{Z}$ permet d'étudier tous les groupes monogènes infinis. Mais il n'est d'aucune utilité pour les groupes cycliques, qui sont pourtant bien plus nombreux dans la nature (à commencer par les groupes $\mathbb{U}_n$ des racines n^{es} de l'unité). Pour leur étude spécifique, nous aurons besoin d'introduire :

— la notion très importante *d'ordre* d'un élément : si g est un élément d'un groupe G, alors on dit que g est d'ordre fini si le groupe engendré par g est fini, et dans ce cas son cardinal est appelé *l'ordre de* g (de manière équivalente, l'ordre de g est le plus petit entier naturel non nul k tel que : $g^k = 1_G$, s'il en existe) ;

— les groupes $\mathbb{Z}/n\mathbb{Z}$, qui sont informellement « le groupe $\mathbb{Z}$ où l'on a "posé $n = 0$" ».

Au vu de tout ce que l'on a raconté, un groupe G est cyclique s'il admet une partie génératrice de la forme $\{g\}$ avec g d'ordre fini : $\exists g \in G,\ G = \langle g \rangle$. De la même manière que $\mathbb{Z}$ décrit tous les groupes monogènes infinis à isomorphisme près, nous montrerons que $\mathbb{Z}/n\mathbb{Z}$ décrit tous les groupes

cycliques (toujours à isomorphisme près). Par conséquent, en étudiant $\mathbb{Z}/n\mathbb{Z}$, nous connaîtrons tous les groupes cycliques. C'est très important, parce qu'il y en a partout ! Pour tout groupe fini G et tout $g \in G$, le groupe engendré par g est nécessairement cyclique, par définition.

Exercice 5. Vérifier l'équivalence entre les deux définitions données de l'ordre d'un élément $g \in G$.

Exercice 6. Sans chercher à être rigoureux : avec la description qu'on a donnée de $\mathbb{Z}/n\mathbb{Z}$, justifier que c'est un groupe pour l'addition à n éléments, et en donner un générateur.

Même dans le cas d'un groupe non monogène, les éléments d'ordre fini sont utiles parce qu'ils donnent des informations sur la structure du groupe (le cardinal, notamment), et permettent d'avoir des isomorphismes avec des groupes plus simples d'étude. En effet, pour expliciter un groupe fini compliqué G, une première piste est éventuellement de considérer un élément non trivial $g_1 \in G$ et ses puissances : 1_G, g_1, g_1^2, etc., jusqu'à ce que cela boucle (et ce sera le cas à partir du moment où l'on obtient $g_1^k = 1_G$: c'est là qu'intervient l'ordre de g) ; puis passe à un second élément g_2, dont on considère toutes les puissances ainsi que les produits par les puissances de g_1 (cela revient à considérer le groupe engendré par g_1 et g_2), et ainsi de suite, espérant ainsi finir par obtenir tout le groupe pour des raisons de cardinalité. Plus les éléments ainsi considérés sont d'ordre élevé, plus on va obtenir d'éléments par ce procédé, et donc plus on est susceptible de reconstituer une grande partie de G. Cette observation est naïve, mais on peut même faire mieux, puisqu'il s'avère qu'il y a des relations de divisibilité très fortes entre les ordres des éléments et le cardinal de G. Imaginons par exemple, pour simplifier, que G soit commutatif, non cyclique, mais admette tout de même une partie génératrice relativement petite $\{g_1, g_2\}$, avec g_1 et g_2 distincts, respectivement d'ordres d_1 et d_2. Il est alors facile de montrer que l'application :

$$f : \begin{cases} \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} & \to & G \\ (k, \ell) & \mapsto & g_1^k g_2^\ell \end{cases}$$

est bijective ; elle conserve donc les cardinaux, et on a : $\text{card}(G) = d_1 d_2$, donc les ordres de g_1 et g_2 divisent G ; nous verrons en fait que dans un groupe fini, même sans hypothèse de commutativité ni sur les parties génératrices, l'ordre d'un élément divise l'ordre de G (cas particulier du théorème de Lagrange) : c'est un résultat fort, qui impose beaucoup de contraintes sur les ordres de G (quand on connaît le cardinal de G) ou sur G (quand on connaît l'ordre de certains de ses éléments) ! Il nous aidera énormément à expliciter des groupes par de simples raisonnements arithmétiques : voir l'exercice 8 pour une démonstration de cette efficacité, et du lien que cela implique entre le cardinal d'un groupe et sa structure.

Exercice 7. Vérifier que l'application ci-dessus est bien bijective, sous les hypothèses effectuées.

Exercice 8. Soit p un nombre premier. Utiliser le résultat énoncé ci-dessus pour en déduire que tout groupe de cardinal p est cyclique.

Exercice 9. Soit G un groupe fini et commutatif de cardinal n. Soit $g \in G$ un élément d'ordre d. En exprimant le produit $\prod_{x \in G} x$ de deux manières différentes (*utiliser le fait que l'application $x \mapsto gx$ soit bijective*), montrer : $g^n = 1_G$. En déduire que d divise n. C'est un cas particulier du résultat énoncé ci-dessus.

De nombreux exercices seront consacrés aux implications de ce lien entre ordre des éléments, cardinal du groupe, et structure du groupe.

Certaines problématiques de la théorie des groupes ont leur analogue dans la théorie des anneaux. La notion qui leur est spécifique, et que nous introduirons cette année, est celle *d'idéal* d'un anneau : les idéaux sont aux anneaux ce que les sous-espaces vectoriels sont aux espaces vectoriels, et en cela ils sont plus instructifs sur la structure d'un anneau que ses sous-anneaux (ce qui peut paraître contre-intuitif). Nous ne donnerons que les définitions et propriétés de base : c'est le chapitre suivant qui en parlera plus amplement.

2 Résumé : objectif du chapitre

Nous allons d'abord donner des énoncés généraux sur les relations d'équivalence et les ensembles-quotients, qui seront pour nous d'un grand confort pour fabriquer de nouveaux groupes et anneaux, à commencer par l'anneau $\mathbb{Z}/n\mathbb{Z}$ dont nous parlions ci-dessus (qui revient à « poser $n = 0$ » dans $\mathbb{Z}$). Si le temps nous le permet, nous montrerons comment ils permettent de donner une définition rigoureuse de $\mathbb{Z}$ et $\mathbb{Q}$ (cette construction étant hors programme).

Ensuite, nous introduirons les notions de partie génératrice d'un groupe, d'ordre d'un groupe ou d'un élément d'un groupe, de groupe monogène ou cyclique, suivant ce que nous disions ci-dessus.

Les groupes sont aussi plus agréables à étudier si l'on considère les morphismes qui les relient ; les meilleurs d'entre eux étant les isomorphismes, puisqu'ils préservent tout ce qui est relatif à la structure : ainsi, ayant un isomorphisme entre un groupe compliqué (inconnu) et un groupe simple (connu), nous pourrons résoudre tout problème dans le groupe inconnu en étudiant le même problème dans le groupe connu. Cette stratégie est très fructueuse et nous ferons donc des rappels sur les morphismes.

Après avoir justifié que tout groupe monogène est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$, nous étudierons de près le groupe $\mathbb{Z}/n\mathbb{Z}$: en le connaissant, nous connaîtrons tous les groupes monogènes finis, d'après le principe formulé ci-dessus.

L'étude du nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ (et donc, par extension, de tout groupe cyclique), et plus généralement du nombre d'éléments d'ordre d dans un groupe cyclique, nous conduira à introduire l'indicatrice d'Euler qui est, par définition, le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, mais aussi le nombre d'éléments de $[\![1, n]\!]$ qui sont premiers avec n. C'est une fonction arithmétique centrale.

L'étude du groupe symétrique S_n est plus fine parce que c'est un groupe extrêmement riche. Nous donnerons entre autres des exemples de parties génératrices avec des applications du même ordre que celles données plus haut : pour démontrer certains résultats, il suffit parfois de les montrer sur tout élément d'une partie génératrice. Comme les transpositions engendrent S_n, et que de plus elles sont toutes reliées les unes aux autres assez simplement par conjugaison (nous dirons ce qu'on entend par là), cela permet à peu de frais de démontrer certains résultats sur S_n en raisonnant sur une seule transposition !

La partie consacrée aux anneaux sera brève, une étude plus approfondie étant faite au chapitre suivant. Nous introduirons simplement la notion d'idéal, en donnant quelques propriétés de base sur ces analogues annelés des sous-espaces vectoriels, ainsi que la notion d'algèbres (une K-algèbre étant un ensemble muni à la fois d'une structure d'anneau et de K-espace vectoriel).