INTRODUCTION À LA THÉORIE DES GROUPES

RUBÉN MUÑOZ--BERTRAND

Ces notes de cours contiennent les premiers chapitres du cours d'algèbre générale donné en deuxième année de licence de mathématiques à l'Université de Versailles Saint-Quentin-en-Yvelines.

Sauf mention contraire explicite, l'ensemble de ces notes fait partie du programme de l'année. Il est donc attendu que vous connaissiez les notions qui suivent en arrivant en troisième année de licence, y compris ce qui n'a pu être traité que brièvement en cours magistral.

Remerciements

Ces notes de cours sont librement inspirées d'anciennes notes de mon prédécesseur Nicolas Pouyanne, que je remercie chaleureusement.

Je remercie également mes étudiants pour leur attention et leur enthousiasme tout au long du semestre. Je salue particulièrement ceux qui ont participé à l'amélioration de ce document : Ariane Audy, Antoine Bellando, Hugo Bouzinac, Mohammed Chennig, Roman de Crécy, Alexandre Mesbah et César Pitigliano.

Je remercie enfin Bernhard Elsner pour ses commentaires sur ce document, et son soutien tout au long de l'année.

1. Lois de composition interne

Dans cette section, nous allons étudier les lois de composition interne sur un ensemble. Il faut penser à cette notion comme étant un moyen de pouvoir parler à la fois de l'addition, de la multiplication, et de toute autre opération que l'on peut avoir sur un ensemble.

Définition 1.1. *Soit E un ensemble. Une* ***loi de composition*** *sur E est une application $F \times E \to E$ pour un certain ensemble F. Lorsque $F \neq E$, on dit que la loi de composition est* ***externe****. Si $F = E$, on dit que la loi de composition est* ***interne****.*

Pour le moment, nous n'allons nous intéresser qu'aux lois de composition internes. Nous reviendrons aux lois de composition externes dans le cadre des espaces vectoriels.

Exemple 1.2. *L'addition est une loi de composition interne sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. La multiplication et la soustraction aussi.*

Exemple 1.3. *Soit E un ensemble. On peut composer deux applications $f\colon E \to E$ et $g\colon E \to E$ en $f \circ g\colon E \to E$. On obtient ainsi une loi de composition interne sur l'ensemble des fonctions de E dans E.*

Dans ce qui suit, lorsque l'on dira que $\bullet$ est une loi de composition sur E, on notera $x \bullet y$ l'image de $(x, y) \in F \times E$ dans E. Cela correspond à la notation

que l'on emploie déjà habituellement pour l'addition, la multiplication ou encore la composition.

D'ailleurs, de la même manière que vous avez pris l'habitude de remplacer des lettres représentant des variables par d'autres lettres dans vos formules, ici, vous allez remplacer le symbole $\bullet$ par la loi de votre choix : par exemple $+$, $\times$, $\circ$...

Définition 1.4. *Soit E un ensemble muni d'une loi de composition interne $\bullet$. On dit que $\bullet$ est **associative** si :*

$$\forall x, y, z \in E,\ (x \bullet y) \bullet z = x \bullet (y \bullet z).$$

Lorsqu'une loi de composition interne est associative, on voit qu'il n'est pas nécessaire de garder les parenthèses. On notera donc dans ce cas $x \bullet y \bullet z$ sans risque de confusion.

Exemple 1.5. *L'addition est une loi de composition interne associative sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. La multiplication aussi.*

Attention ! La soustraction n'est pas une loi de composition interne associative sur ces ensembles. Par exemple, on voit bien dans $\mathbb{Z}$ que :

$$(1 - 2) - 3 \neq 1 - (2 - 3).$$

Pensez donc bien à ne jamais oublier les parenthèses dans vos formules !

Exemple 1.6. *La composition est une loi de composition interne associative sur l'ensemble des fonctions d'un ensemble sur lui-même.*

Définition 1.7. *Soit E un ensemble muni d'une loi de composition interne $\bullet$. Un élément $e \in E$ est dit **neutre** pour $\bullet$ si :*

$$\forall x \in E,\ x \bullet e = e \bullet x = x.$$

Remarquons que si E est un ensemble muni d'une loi de composition interne $\bullet$, alors un élément neutre pour $\bullet$ est unique. En effet, si e et e' sont deux éléments neutres pour $\bullet$ alors on a :

$$e = e \bullet e' = e'.$$

Exemple 1.8. *Le nombre 0 est l'élément neutre pour l'addition sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.*

À nouveau, attention ! La soustraction dans $\mathbb{Z}$ ne possède pas d'élément neutre. Certes, pour tout $x \in \mathbb{Z}$ l'élément $x - 0$ est toujours égal à x, mais vous pouvez constater que $0 - 1 = -1 \neq 1$.

Exemple 1.9. *Le nombre 1 est l'élément neutre pour la multiplication sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.*

Exemple 1.10. *L'identité est l'élément neutre pour la composition sur l'ensemble des fonctions d'un ensemble sur lui-même.*

Définition 1.11. *Soit E un ensemble muni d'une loi de composition interne $\bullet$. Supposons qu'il existe un élément neutre $e \in E$ pour $\bullet$. Soit $x \in E$. On dit que $y \in E$ est le **symétrique** de x pour $\bullet$ si :*

$$x \bullet y = y \bullet x = e.$$

Exemple 1.12. *Quel que soit le nombre x dans l'un des ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, le nombre $-x$ est le symétrique de x pour l'addition.*

Remarquons que 0 n'a pas d'élément symétrique pour la multiplication dans aucun des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$... Cela provient du fait que l'on ne peut pas trouver x dans l'un de ces ensembles tel que $0 \times x = 1$. C'est bien connu, on ne peut pas diviser par zéro !

Dans tout ce cours, lorsque l'on aura un ensemble E muni d'une loi de composition interne notée additivement par $+$, on notera E^* l'ensemble E privé de l'élément neutre pour $+$. Cette notation correspond à celle que vous connaissez déjà pour $\mathbb{N}^*$ ou $\mathbb{R}^*$. Cela nous permet d'introduire l'exemple suivant.

Exemple 1.13. *Quel que soit le nombre x dans l'un des ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$, le nombre $\frac{1}{x}$ est le symétrique de x pour la multiplication.*

On rappelle qu'une fonction bijective est une fonction qui possède une réciproque. Dans le cas des bijections d'un ensemble sur lui-même, on parle plutôt de permutation. On peut reformuler cette définition avec notre nouveau vocabulaire.

Définition 1.14. *Soit E un ensemble. Une fonction $f\colon E \to E$ est une **permutation** si f possède un symétrique pour la composition. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E.*

2. Groupes

Nous avons désormais introduit tout ce qu'il faut pour définir la notion principale de ce chapitre.

Définition 2.1. *Un **groupe** est un ensemble G muni d'une loi de composition interne $\bullet$ telle que :*

(1) la loi $\bullet$ est associative ;

(2) la loi $\bullet$ possède un élément neutre ;

(3) tout élément $g \in G$ possède un élément symétrique pour $\bullet$.

On dira aussi que $(G, \bullet)$ est un groupe. Lorsque le contexte le permet, on omet parfois d'écrire la loi de composition interne, et on dit simplement que G est un groupe.

Exemple 2.2. *Les exemples vus dans la première section nous indiquent que $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes. On parle de groupes additifs, et on nomme les éléments symétriques les opposés.*

Exemple 2.3. *Nous avons également vérifié que $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes. On parle de groupes multiplicatifs, et on nomme les éléments symétriques les inverses.*

Exemple 2.4. *Notons $\{e\}$ l'ensemble réduit à un seul élément. Alors, il existe une unique loi de composition interne $\times$ sur cet ensemble, définie par $e \times e \coloneqq e$, et $(\{e\}, \times)$ est alors un groupe.*

Soit E un ensemble. Nous avons vu que l'ensemble des permutations de E est un groupe pour la composition. Ce groupe joue un rôle particulièrement important en mathématiques.

Définition 2.5. *Soit E un ensemble. Le groupe $(\mathfrak{S}(E), \circ)$ est appelé le **groupe symétrique** de E. Si le cardinal de E est un entier $n \in \mathbb{N}$, on note le groupe symétrique $\mathfrak{S}_n$.*

Dans un groupe, on demande pour chaque élément du groupe l'existence d'un élément symétrique. La proposition suivante nous dit que cet élément est unique.

Proposition 2.6. *Soit $(G, \bullet)$ un groupe, et soit $x \in G$. Si $y \in G$ et $z \in G$ sont deux éléments symétriques de x pour $\bullet$, alors $y = z$.*

Démonstration. Par définition, on a $x \bullet y = e$, où $e \in G$ désigne l'élément neutre de $\bullet$. On trouve donc $z \bullet (x \bullet y) = z \bullet e = z$. Par associativité, cela signifie que $(z \bullet x) \bullet y = z$. Or, par hypothèse sur z, on a $z \bullet x = e$, d'où $e \bullet y = z$. On vérifie donc bien que $y = z$. □

Définition 2.7. *Soit G un ensemble, et soit $\bullet$ une loi de composition interne sur G. On dit que $\bullet$ est **commutative** si l'on a :*

$$\forall x, y \in G,\ x \bullet y = y \bullet x.$$

*Si de plus $(G, \bullet)$ est un groupe, on dit dans ce cas qu'il est **commutatif**, ou de manière synonyme **abélien**.*

Le mot « abélien » est un hommage au mathématicien norvégien Niels Henrik Abel, mort à seulement 26 ans.

Exemple 2.8. *Les groupes $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont tous abéliens.*

Prenez garde au fait que $\mathfrak{S}_n$ n'est pas abélien si $n \geqslant 3$.

Définition 2.9. *Soit $(G, \bullet)$ un groupe. Un **sous-groupe** d'un groupe G est un sous-ensemble H de G tel que :*

(1) l'ensemble H n'est pas vide ;

(2) pour tout $g, h \in H$, on a $g \bullet h \in H$;

(3) pour tout $h \in H$, le symétrique de h est aussi dans H.

On note $H \leqslant G$ pour dire que H est un sous-groupe de G.

Nous aurions pu aussi définir un sous-groupe avec la proposition suivante.

Proposition 2.10. *Soit $(G, \bullet)$ un groupe. Un sous-ensemble H de G est un sous-groupe de G si et seulement si $(H, \bullet)$ est un groupe, où l'on a aussi noté $\bullet$ la restriction de la loi de composition interne de G à H.*

Démonstration. Supposons d'abord que $H \leqslant G$. Pour tout $g, h \in H$, on a $g \bullet h \in H$ par définition. Cela signifie que la restriction de $\bullet$ à $H \times H$ donne une loi de composition interne à H. L'associativité de $\bullet$ sur G implique celle de sa restriction à H. De plus, comme pour tout $h \in H$, le symétrique $s \in H$ de h est aussi dans H, on voit que l'élément neutre $e = h \bullet s \in H$. Il est alors clair que cet élément neutre est aussi celui de H, et qu'il existe un symétrique à chaque élément de H par hypothèse. Nous avons bien vérifié que $(H, \bullet)$ est un groupe.

Réciproquement, si $(H, \bullet)$ est un groupe alors H n'est pas vide car l'élément neutre e de $\bullet$ est dans H. Puisque $\bullet$ est une loi de composition interne sur H, pour tout $g, h \in H$, on a $g \bullet h \in H$, et l'existence du symétrique est donnée par définition. On a bien $H \leqslant G$. □

Exemple 2.11. *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$.*

Exemple 2.12. *Les ensembles $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.*

Exemple 2.13. *L'ensemble $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \times)$.*

Exemple 2.14. *On rappelle que $\mathbb{U}$ désigne l'ensemble des nombres complexes de module 1, et que pour tout $n \in \mathbb{N}^*$ on note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. Ces ensembles $\mathbb{U}$ et $\mathbb{U}_n$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.*

Proposition 2.15. *Les sous-groupes du groupe additif $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.*

Démonstration. Il est rapide de vérifier que les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Si G est un sous-groupe différent de $0\mathbb{Z}$, on peut poser $n \coloneqq \min\{g \in G \mid g > 0\}$. Remarquez alors que $n\mathbb{Z} = \langle n \rangle \subset G$. Si $x \in G$, soient $q, r \in \mathbb{Z}$ le quotient et le reste de la division euclidienne de x par n. Alors $x - nq = r \in G$ avec $0 \leqslant r < n$. Par minimalité de n on doit avoir $r = 0$. Ainsi, $x \in n\mathbb{Z}$. On a montré que $G = n\mathbb{Z}$. □

3. Morphismes de groupes

Définition 3.1. *Un **homomorphisme de groupes**, ou plus brièvement un **morphisme de groupes**, est une application $f\colon G \to H$ d'un groupe $(G, \bullet)$ dans un groupe $(H, \star)$ tel que :*

$$\forall g, h \in G,\ f(g \bullet h) = f(g) \star f(h).$$

*Lorsque $G = H$, on dit que f est un **endomorphisme de groupe**.*

On note $\mathrm{Hom}(G, H)$ l'ensemble des homomorphismes de groupes de G dans H, et $\mathrm{End}(G)$ l'ensemble des endomorphismes de groupe de G.

La loi de composition interne n'est pas la seule chose que préserve un homomorphisme de groupes. Les deux propositions suivantes nous assurent qu'un homomorphisme préserve également l'élément neutre, et les éléments symétriques.

Proposition 3.2. *Soient $(G, \bullet)$ et $(H, \star)$ deux groupes. Soit $f\colon G \to H$ un homomorphisme de groupes. Notons $e_G \in G$ l'élément neutre de G, et $e_H \in H$ celui de H. Alors $f(e_G) = e_H$.*

Démonstration. On a $f(e_G) = f(e_G \bullet e_G) = f(e_G) \star f(e_G)$. Si l'on note s le symétrique de $f(e_G)$, on trouve alors que $e_H = f(e_G) \star s = f(e_G) \star f(e_G) \star s = f(e_G)$. □

Proposition 3.3. *Soient $(G, \bullet)$ et $(H, \star)$ deux groupes. Soit $f\colon G \to H$ un homomorphisme de groupes. Alors pour tout $g \in G$ de symétrique $s \in G$, l'élément $f(g)$ a pour symétrique $f(s)$ dans H.*

Démonstration. Il suffit de vérifier que $f(g) \star f(s) = e_H$, où $e_H \in H$ est l'élément neutre de H. Mais $f(g) \star f(s) = f(g \bullet s) = f(e_G)$. Il ne reste alors qu'à conclure en appliquant la proposition précédente. □

Exemple 3.4. *Le module $|\bullet|\colon \mathbb{C}^* \to \mathbb{R}^*$ est un homomorphisme de groupes de $(\mathbb{C}^*, \times)$ vers $\left(\mathbb{R}_+^*, \times\right)$.*

Exemple 3.5. *Les fonctions parties réelle et imaginaire sont des homomorphismes de groupes de $(\mathbb{C}, +)$ vers $(\mathbb{R}, +)$.*

Exemple 3.6. *Le conjugué $\overline{\bullet}\colon \mathbb{C} \to \mathbb{C}$ est un endomorphisme de groupe de $(\mathbb{C}, +)$. Il induit également un endomorphisme de groupe de $(\mathbb{C}^*, \times)$.*

Exemple 3.7. *La dérivation est un endomorphisme de $(\mathbb{R}[X], +)$.*

Exemple 3.8. *Soit $(G, \bullet)$ un groupe. Soit $H \leqslant G$. Alors l'inclusion $H \subset G$ induit un homomorphisme de groupes.*

En effet, considérons l'application de H dans G qui à chaque $h \in H$ associe le même h, mais vu dans G. Vous pouvez penser à cette fonction comme une fonction identité, mais avec un ensemble d'arrivée plus gros. Il découle alors de la caractérisation d'un sous-groupe que cette application d'inclusion est un homomorphisme de groupes de H dans G.

Exemple 3.9. *Notons $\{e\}$ le groupe à un seul élément. Soit G un groupe, et soit e_G l'élément neutre de G. L'application $f\colon \{e\} \to G$ définie par $f(e) \coloneqq e_G$ et l'application $h\colon G \to \{e\}$ telle que $h(g) \coloneqq e$ pour tout $g \in G$ sont des homomorphismes de groupes.*

Dans un groupe $(G, +)$ noté additivement, d'élément neutre e, on peut définir la multiplication par un élément $n \in \mathbb{Z}$. Pour tout $g \in G$ de symétrique $s \in G$ on pose $0g \coloneqq e$ et $-1g \coloneqq s$. Si $n \geqslant 1$, on pose $ng \coloneqq \sum_{i=1}^{n} g$. Si $n \leqslant -1$, on pose $ng \coloneqq (-n)(-1g)$.

Dans ce genre de situation, on note plutôt $0 \coloneqq e$ et $-g \coloneqq -1g$, comme dans $\mathbb{R}$ par exemple.

Prenez deux secondes pour vous convaincre que cette définition, qui semble abstraite de prime abord, vous redonne la définition de la multiplication sur $\mathbb{Z}$ que vous connaissez depuis votre enfance.

Exemple 3.10. *Pour tout $n \in \mathbb{Z}$, la multiplication par n dans un groupe abélien $(G, +)$ noté additivement est un endomorphisme de groupe.*

Similairement, dans un groupe $(G, \times)$ noté multiplicativement, d'élément neutre e, on peut définir l'exponentiation par un élément $n \in \mathbb{Z}$. Pour tout $g \in G$ de symétrique $s \in G$ on pose $g^0 \coloneqq e$ et $g^{-1} \coloneqq s$. Si $n \geqslant 1$, on pose $g^n \coloneqq \prod_{i=1}^{n} g$. Si $n \leqslant -1$, on pose $g^n \coloneqq \left(g^{-1}\right)^{-n}$.

Dans ce genre de situation, on note plutôt $1 \coloneqq e$, comme dans $\mathbb{R}^*$ par exemple.

À nouveau, prenez quelques instants pour constater que cette définition coïncide avec la définition de la puissance sur $\mathbb{Q}^*$ que vous connaissez depuis votre adolescence.

Dans la suite, quand la loi $\bullet$ d'un groupe ne sera pas précisée, on gardera la notation g^n définie ci-dessus, comme si le groupe était multiplicatif. Ceci étant, la loi $\bullet$ pourra tout de même être l'addition, auquel cas g^n désignerait la multiplication par n ! Attention donc à cette subtilité.

En particulier, dans ce qui suit, on notera g^{-1} le symétrique de $g \in G$.

Remarquez, avec ces notations, que l'on a pour tout $g, h \in G$ la formule suivante :

$$(g \bullet h)^{-1} = h^{-1} \bullet g^{-1}.$$

Essayez de faire le calcul $\left(h^{-1} \bullet g^{-1}\right) \bullet (g \bullet h)$ pour vous en convaincre ! Ne vous faites donc pas avoir en croyant que le symétrique est donné par $g^{-1} \bullet h^{-1}$... Cela ne fonctionne que dans le cas abélien !

Exemple 3.11. *Pour tout $n \in \mathbb{Z}$, l'exponentiation par n dans un groupe abélien $(G, \times)$ noté multiplicativement est un endomorphisme de groupe.*

Tous les exemples ci-dessus étaient des morphismes entre des groupes ayant des lois de composition internes notées de la même manière. Mais ce n'est pas une obligation, comme nous le montre l'exemple suivant.

Exemple 3.12. *L'exponentielle* $\exp\colon \mathbb{C} \to \mathbb{C}^*$ *est un homomorphisme de groupes de* $(\mathbb{C}, +)$ *dans* $(\mathbb{C}^*, \times)$.

Proposition 3.13. *La composée de deux homomorphismes de groupes est un homomorphisme de groupes.*

Démonstration. Soient $f\colon G \to H$ et $g\colon H \to I$ deux homomorphismes de groupes. Notons $\bullet$ la loi de composition interne de G, notons $\star$ celle de H, et $\diamond$ celle de I. Il nous faut vérifier que pour tout $x, y \in G$ on a $g \circ f(x \bullet y) = g \circ f(x) \diamond g \circ f(y)$. Or, les deux termes de l'égalité sont égaux à $g(f(x) \star f(y))$ par les propriétés d'homomorphismes de groupes. □

Définition 3.14. *On dit qu'un homomorphisme de groupes est un* ***isomorphisme de groupes*** *s'il est bijectif. Lorsqu'il existe un isomorphisme de groupes* $G \to H$*, on note* $G \cong H$ *et on dit que les groupes* G *et* H *sont* ***isomorphes****.*

L'exponentielle complexe est une application surjective, mais pas bijective. En revanche, l'exponentielle réelle est un isomorphisme sur son image, comme le montre l'exemple suivant.

Exemple 3.15. *L'exponentielle* $\exp\colon \mathbb{R} \to \mathbb{R}_+^*$ *est un isomorphisme de groupes de* $(\mathbb{R}, +)$ *dans* $\left(\mathbb{R}_+^*, \times\right)$.

Le logarithme népérien $\ln\colon \mathbb{R}_+^* \to \mathbb{R}$ *est un isomorphisme de groupes de* $\left(\mathbb{R}_+^*, \times\right)$ *dans* $(\mathbb{R}, +)$.

On remarque que la réciproque de l'isomorphisme de groupes exponentiel est aussi un isomorphisme de groupes. Ce n'est pas une coïncidence, car cela découle du fait général ci-dessous.

Proposition 3.16. *Soit* $f\colon G \to H$ *un isomorphisme de groupes. Alors l'application réciproque de* f *est aussi un isomorphisme de groupes.*

Démonstration. Notons $\bullet$ la loi de composition interne de G, et $\star$ celle de H. Notons $f^{-1}\colon H \to G$ l'application réciproque de f. On cherche à démontrer que pour tout $h, h' \in H$, on a $f^{-1}(h \star h') = f^{-1}(h) \bullet f^{-1}(h')$. Puisque f est surjective, il existe $g, g' \in G$ tels que $h = f(g)$ et $h' = f(g')$.

On a alors :

$$\begin{aligned} f^{-1}(h \star h') &= f^{-1}(f(g) \star f(g')) \\ &= f^{-1}(f(g \bullet g')) \\ &= g \bullet g' \\ f^{-1}(h \star h') &= f^{-1}(h) \bullet f^{-1}(h'). \end{aligned}$$

□

Définition 3.17. *Un* ***automorphisme de groupe*** *est un endomorphisme de groupe qui est aussi un isomorphisme de groupes. On note* $\mathrm{Aut}(G)$ *l'ensemble des automorphismes de groupe d'un groupe* G*.*

De manière synonyme, un automorphisme de groupe est un homomorphisme de groupes bijectif d'un groupe sur lui-même.

Exemple 3.18. *Soit* G *un groupe. L'identité* Id_G *est un automorphisme de groupe.*

Exemple 3.19. *La racine carrée est un automorphisme du groupe* $\left(\mathbb{R}_+^*, \times\right)$.

Proposition 3.20. *Pour tout groupe G, l'ensemble* $\mathrm{Aut}(G)$ *des automorphismes de G est un sous-groupe de* $(\mathfrak{S}(G), \circ)$.

Démonstration. L'ensemble $\mathrm{Aut}(G)$ n'est pas vide car Id_G est un automorphisme de groupe. La composition de deux homomorphismes de groupes étant aussi un homomorphisme de groupes, et celle de deux bijections étant aussi une bijection, on obtient la stabilité de $\mathrm{Aut}(G)$ pour la composition. Enfin, on a vu que la réciproque d'un isomorphisme de groupes est aussi un isomorphisme de groupes, ce qui conclut la preuve. □

4. Image et noyau

Définition 4.1. *Soit $f\colon G \to H$ un homomorphisme de groupes. L'**image** de f est le sous-ensemble :*

$$\mathrm{Im}(f) \coloneqq \{f(g) \in H \mid g \in G\}.$$

Proposition 4.2. *Si $f\colon G \to H$ est un homomorphisme de groupes,* $\mathrm{Im}(f)$ *est un sous-groupe de H.*

Démonstration. L'image de f n'est pas vide, car G n'est pas vide. Notons $\bullet$ la loi de composition interne de G, et $\star$ celle de H. Si $g, h \in G$, alors $f(g) \star f(h) = f(g \bullet h)$, donc $\mathrm{Im}(f)$ est stable par $\star$.

Enfin, $f(g) \star f\big(g^{-1}\big) = f\big(g \bullet g^{-1}\big) = f(e_G) = e_H$, où $e_G \in G$ et $e_H \in H$ sont les éléments neutres respectifs de G et H. On rappelle que l'on avait introduit la notation faisant de $g^{-1} \in G$ le symétrique de g. □

Définition 4.3. *Soit $f\colon G \to H$ un homomorphisme de groupes. Notons $e_H \in H$ l'élément neutre de H. Le **noyau** de f est le sous-ensemble :*

$$\mathrm{Ker}(f) \coloneqq \{g \in G \mid f(g) = e_H\}.$$

Proposition 4.4. *Si $f\colon G \to H$ est un homomorphisme de groupes,* $\mathrm{Ker}(f)$ *est un sous-groupe de G.*

Démonstration. Le noyau de f n'est pas vide, car l'élément neutre e_G de G est dans le noyau. Notons $\bullet$ la loi de composition interne de G, et $\star$ celle de H. Notons également e_H l'élément neutre de H.

Si $g, h \in \mathrm{Ker}(f)$, alors $f(g \bullet h) = f(g) \star f(h) = e_H \star e_H = e_H$, donc $\mathrm{Ker}(f)$ est stable par $\bullet$. Enfin, on trouve que :

$$\begin{aligned} f\big(g^{-1}\big) &= f\big(g^{-1}\big) \star e_H \\ &= f\big(g^{-1}\big) \star f(g) \\ &= f\big(g^{-1} \bullet g\big) \\ &= f(e_G) \\ f\big(g^{-1}\big) &= e_H. \end{aligned}$$

□

Proposition 4.5. *Soit $f\colon G \to H$ un homomorphisme de groupes. Alors f est injectif si et seulement si* $\mathrm{Ker}(f) = \{e_G\}$*, où e_G est l'élément neutre de G.*

Démonstration. Supposons que f est injectif. Alors, il existe un unique $g \in G$ tel que $f(g) = e_H$, où e_H désigne l'élément neutre de H. Puisque e_G vérifie cette propriété, cela implique que $\mathrm{Ker}(f) = \{e_G\}$.

Supposons maintenant que $\mathrm{Ker}(f) = \{e_G\}$. Notons $\bullet$ la loi de composition interne de G, et $\star$ celle de H. Soient $g, h \in G$ tels que $f(g) = f(h)$.

$$\begin{aligned} f\big(h \bullet g^{-1}\big) &= f(h) \star f\big(g^{-1}\big) \\ &= f(g) \star f(g)^{-1} \\ f\big(h \bullet g^{-1}\big) &= e_H. \end{aligned}$$

Par hypothèse sur le noyau, cela implique que $h \bullet g^{-1} = e_G$. En d'autres termes, h est le symétrique de g^{-1}. Mais g est aussi le symétrique de g^{-1}. Par unicité du symétrique, cela signifie que $g = h$, donc que f est injectif. □

Exemple 4.6. *Le noyau de l'exponentielle complexe* $\exp\colon \mathbb{C} \to \mathbb{C}^*$ *est le groupe* $(2i\pi\mathbb{Z}, +)$.

Définition 4.7. *L'**ordre** d'un groupe G est le cardinal de son ensemble sous-jacent. On le note $|G|$. Lorsque celui-ci est fini, on dit que G est un **groupe fini**.*

Exemple 4.8. *Soit $n \in \mathbb{N}^*$. L'ordre de $\mathbb{U}_n$ est n.*

Définition 4.9. *Soit H un sous-groupe d'un groupe $(G, \bullet)$. Pour tout $g \in G$, la **classe à gauche de** g **suivant** H est l'ensemble $g \bullet H \coloneqq \{g \bullet h \mid h \in H\}$ et la **classe à droite de** g **suivant** H est l'ensemble $H \bullet g \coloneqq \{h \bullet g \mid h \in H\}$.*

Proposition 4.10. *Soit H un sous-groupe d'un groupe $(G, \bullet)$. Pour tout $g, x \in G$, on a $x \in g \bullet H$ si et seulement si $g \in x \bullet H$. Similairement, $x \in H \bullet g$ si et seulement si $g \in H \bullet x$.*

Démonstration. Faisons uniquement le cas de la classe à gauche, celui de la classe à droite fonctionnant exactement de la même manière.

Si $x \in g \bullet H$, cela signifie qu'il existe $h \in H$ tel que $x = g \bullet h$. Nous avons alors $g = g \bullet h \bullet h^{-1} = x \bullet h^{-1}$. Donc $g \in x \bullet H$.

La réciproque s'obtient en échangeant x et g dans la preuve. □

Proposition 4.11. *Soit H un sous-groupe d'un groupe $(G, \bullet)$. Alors :*

$$\forall g \in G,\ \#(g \bullet H) = \#(H \bullet g) = |H|.$$

Démonstration. Faisons uniquement le cas de la classe à gauche, celui de la classe à droite fonctionnant exactement de la même manière.

Soit $g \in G$. Il suffit de trouver une bijection entre H et $g \bullet H$. Celle-ci est donnée par l'application qui à $h \in H$ associe $g \bullet h$, la réciproque étant l'application qui à $x \in g \bullet H$ associe $g^{-1} \bullet x$. □

Proposition 4.12. *Soit H un sous-groupe d'un groupe $(G, \bullet)$. Alors :*

$$\#\{g \bullet H \mid g \in G\} = \#\{H \bullet g \mid g \in G\}.$$

Démonstration. Soient $g \in G$, et $h \in H$. Alors, le symétrique de $g \bullet h$ est $h^{-1} \bullet g^{-1}$. En particulier, l'application i qui à chaque élément de G associe son symétrique induit une bijection entre les classes $g \bullet H$ et $H \bullet g^{-1}$. La proposition en découle, puisque i est une involution sur G et sur H, c'est-à-dire une bijection qui est son propre inverse. □

Définition 4.13. *Soit H un sous-groupe d'un groupe $(G, \bullet)$. L'**indice de H dans** G est le cardinal l'ensemble des classes à gauche suivant H, ou de manière synonyme le nombre de classes à droite suivant H. On le note :*

$$[G : H] \coloneqq \#\{g \bullet H \mid g \in G\}.$$

Théorème 4.14 (Lagrange)**.** *Soient G un groupe et H un sous-groupe de G. Alors :*

$$|G| = |H| \times [G : H].$$

En particulier si G est un groupe fini, alors $|H|$ divise $|G|$.

Démonstration. Notons $\bullet$ la loi de composition interne de G. Tout d'abord, il est clair que l'union de toutes les classes à gauche suivant H est G, puisque pour tout $g \in G$ on a $g \in g \bullet H$. Puisque toutes ces classes ont toutes pour cardinal $|H|$, il suffit donc de vérifier que ces classes sont deux à deux disjointes : c'est-à-dire qu'elles forment une partition de G.

Soient $g, g' \in G$. Soit $x \in g \bullet H \cap g' \bullet H$. C'est-à-dire qu'il existe $h, h' \in H$ tels que $x = g \bullet h = g' \bullet h'$. On trouve que $g = g \bullet h \bullet h^{-1} = g' \bullet h' \bullet h^{-1}$. En particulier, $g \in g' \bullet H$, et on en déduit que $g \bullet H \subset g' \bullet H$. L'inclusion réciproque se fait de la même manière, donc deux classes sont égales dès lors que leur intersection est non nulle. Nous avons bien une partition. □

Exemple 4.15. *Il n'existe pas de sous-groupe de $\mathbb{U}_{10}$ d'ordre 4.*

Proposition 4.16. *Soit $f \colon G \to H$ un homomorphisme de groupes. On a alors $[G : \mathrm{Ker}(f)] = |\mathrm{Im}(f)|$, et :*

$$|G| = |\mathrm{Im}(f)| \times |\mathrm{Ker}(f)|.$$

Démonstration. D'après le théorème de Lagrange, il nous suffit de vérifier que $[G : \mathrm{Ker}(f)] = |\mathrm{Im}(f)|$.

Soit $g \in G$. Notons $\bullet$ la loi de composition interne de G, et $\star$ celle de H. Montrons d'abord que :

$$\{x \in G \mid f(x) = f(g)\} = g \bullet \mathrm{Ker}(f).$$

En effet, si $x \in g \bullet \mathrm{Ker}(f)$ alors $f(x) = f(g \bullet y)$ pour un certain $y \in \mathrm{Ker}(f)$, et on trouve que $f(g \bullet y) = f(g) \star f(y) = f(g) \star e_H = f(g)$, où e_H désigne l'élément neutre de H.

Réciproquement, si $x \in G$ vérifie $f(x) = f(g)$, alors on a :

$$\begin{aligned} f\big(g^{-1} \bullet x\big) &= f\big(g^{-1}\big) \star f(x) \\ &= f(g)^{-1} \star f(g) \\ f\big(g^{-1} \bullet x\big) &= e_H. \end{aligned}$$

Donc $g^{-1} \bullet x \in \mathrm{Ker}(f)$, ce qui implique que $x = g \bullet g^{-1} \bullet x \in g \bullet \mathrm{Ker}(f)$.

Maintenant, on remarque qu'il existe une bijection entre les classes à gauche suivant $\mathrm{Ker}(f)$, et $\mathrm{Im}(f)$. En effet, d'après la discussion ci-dessus, tous les éléments d'une même classe sont envoyés sur la même image, qui détermine uniquement cette classe. La proposition en découle. □

5. Sous-groupe engendré, groupe monogène

De manière analogue aux familles génératrices des espaces vectoriels, on va s'intéresser à des éléments qui engendrent un sous-groupe.

Proposition 5.1. *Soit G un groupe. L'intersection d'une famille de sous-groupes de G est un sous-groupe de G.*

Démonstration. L'élément neutre de G appartient à l'intersection. De plus, l'intersection est stable pour la loi de G, étant donné que chacun des sous-groupes l'est. De même, il est aisé de vérifier que le symétrique d'un élément de l'intersection est aussi dans l'intersection, puisqu'il est dans chacun des sous-groupes. □

Définition 5.2. *Soit E un sous-ensemble d'un groupe G. Le* ***sous-groupe engendré par*** *E est l'intersection des sous-groupes de G contenant E. On le note $\langle E\rangle$.*

Définition 5.3. *Lorsque E est un sous-ensemble de cardinal $n \in \mathbb{N}$ d'un groupe G, dont tous les éléments sont notés $x_i \in E$ pour $i \in [\![1, n]\!]$, on note $\langle x_1, \dots, x_n\rangle \coloneqq \langle E\rangle$. Si $G = \langle x_1, \dots, x_n\rangle$ pour un tel ensemble E, on dit alors G est un groupe* ***de type fini****.*

Il ne faut pas confondre groupe de type fini et groupe fini. Tout groupe fini est de type fini. En effet, un groupe est engendré par lui-même. En revanche, voici un premier exemple de groupe de type fini, mais d'ordre infini.

Exemple 5.4. *Dans $(\mathbb{R}[X], +)$, le sous-groupe $\langle 1, X\rangle$ engendré par 1 et X est $\mathbb{Z}_1[X]$, c'est-à-dire l'ensemble des polynômes à coefficients entiers de degré inférieur ou égal à 1.*

Définition 5.5. *Un groupe G est* ***monogène*** *lorsqu'il existe $x \in G$ tel que $G = \langle x\rangle$. On dit qu'un tel x est un* ***générateur*** *de G. Un groupe monogène et fini est dit* ***cyclique****.*

Proposition 5.6. *Soit G un groupe. Soit $x \in G$. Alors le sous-groupe $\langle x\rangle$ de G est abélien, et vérifie :*

$$\langle x\rangle = \left\{x^k \mid k \in \mathbb{Z}\right\}.$$

Démonstration. On considère la fonction $f\colon \mathbb{Z} \to G$ qui à chaque $n \in \mathbb{Z}$ associe $x^n \in G$. Il s'agit d'un homomorphisme de groupes. En effet, si $n, m \in \mathbb{Z}$, on peut prendre le temps de vérifier que $x^{n+m} = x^n \bullet x^m$ en suivant la définition, où $\bullet$ désigne la loi de composition interne de G.

On remarque alors que l'ensemble $\left\{x^k \mid k \in \mathbb{Z}\right\}$ est un sous-groupe de G. En effet, il s'agit de l'image de f. Or, on a vu que l'image d'un groupe est un sous-groupe, et on conclut car $\mathbb{Z}$ est abélien, donc il est rapide de vérifier que son image aussi. □

Exemple 5.7. *Soit $n \in \mathbb{N}^*$. Le groupe $\mathbb{U}_n$ est cyclique, et $\exp\left(\frac{2i\pi}{n}\right)$ est un générateur.*

Ce n'est pas le seul générateur ! Par exemple, si $n \geqslant 3$, l'élément $\exp\left(\frac{-2i\pi}{n}\right)$ est un autre générateur de $\mathbb{U}_n$.

Exemple 5.8. *Le groupe $(\mathbb{Z}, +)$ est monogène infini, et 1 est un générateur.*

Définition 5.9. *Soit G un groupe. Soit $x \in G$. L'***ordre*** de x dans G est l'ordre du sous-groupe $\langle x\rangle$.*

Remarquez que si l'ordre de x est fini, alors il vaut $\min\{n \in \mathbb{N}^* \mid x^n = e_G\}$, où $e_G \in G$ est l'élément neutre de G.

Rappelez-vous de notre convention de notation pour la puissance. Si la loi de G est notée $+$, alors lorsque l'ordre de x est fini on écrira plutôt que celui-ci vaut $\min\{n \in \mathbb{N}^* \mid nx = 0\}$. Il s'agit de la même formule, tout n'est qu'une histoire de notation.

Attention ! Il n'y a aucune formule de ce type concernant l'ordre d'un groupe. Ne confondez donc pas ordre d'un groupe, et ordre d'un élément, ce sont deux choses distinctes.

Proposition 5.10. *Si G est un groupe fini, tout élément de G a un ordre fini qui est un diviseur de $|G|$.*

Démonstration. Cela découle immédiatement du théorème de Lagrange. □

Il découle de la proposition précédente que si G est un groupe fini, alors pour tout $x \in G$ on a $x^{|G|} = e_G$, où $e_G \in G$ désigne l'élément neutre de G.

Toujours en gardant en tête que ces notations ne sont qu'une convention, si la loi de G est notée $+$, alors on préférera noter $|G|x = 0$.

Proposition 5.11. *Soit G un groupe, d'élément neutre e_G. Soient $n \in \mathbb{N}$ et $x \in G$ un élément d'ordre fini. Alors $x^n = e_G$ si et seulement si l'ordre de x divise n.*

Démonstration. Considérons l'application de $\mathbb{Z}$ dans G qui à $k \in \mathbb{Z}$ associe x^k. Nous avons vu dans une preuve précédente qu'il s'agit en fait d'un homomorphisme de groupes.

Son noyau est un sous-groupe de $\mathbb{Z}$. Or, nous avons vu qu'un sous-groupe de $\mathbb{Z}$ est de la forme $o\mathbb{Z}$, pour un certain $o \in \mathbb{Z}$.

Tout d'abord, $o \neq 0$ car l'ordre de x est fini : cet ordre est donc un entier naturel non nul appartenant à ce noyau. Ensuite, on constate que o est l'ordre de x. En effet, l'ordre est le plus petit entier strictement positif n vérifiant $x^n = e_G$, c'est-à-dire le plus petit entier strictement positif du noyau : or cet entier ici est o.

Maintenant, on voit que si $x^n = e_G$, alors n appartient à ce noyau. Donc avec la discussion ci-dessus, on voit que o divise n.

Réciproquement, $n = ok$ pour un certain $k \in \mathbb{Z}$, alors :

$$x^n = x^{ok} = (x^o)^k = {e_G}^k = e_G.$$

□

Proposition 5.12. *Soit G un groupe cyclique, de générateur $x \in G$ et d'ordre $n \in \mathbb{N}^*$. Alors, pour tout $k \in \mathbb{Z}$, l'ordre de x^k est $\frac{n}{\operatorname{pgcd}(n,k)}$.*

En particulier, x^k est un générateur du groupe G si et seulement si k est premier avec n.

Démonstration. On sait que l'ordre de x^k divise n, donc cet ordre est de la forme $\frac{n}{d}$, où $d \in \mathbb{N}^*$ divise n. On a ainsi $x^{\frac{n}{d}k} = e_G$, où e_G désigne l'élément neutre de G.

Cela implique qu'il existe $q \in \mathbb{Z}$ tel que $\frac{n}{d}k = nq$. En particulier, $k = qd$, c'est-à-dire que d divise aussi k. Afin d'avoir le $\frac{n}{d}$ le plus petit vérifiant les propriétés ci-dessus, il convient donc de prendre $d = \operatorname{pgcd}(n, k)$. On vérifie que ce d vérifie effectivement que $x^{\frac{n}{d}k} = e_G$, et on conclut. □

On peut évidemment énoncer la proposition précédente avec une notation additive.

Définition 5.13. *Le nombre de générateurs de $\mathbb{U}_n$ est noté $\varphi(n)$, et on appelle φ la* ***fonction indicatrice d'Euler****.*

Exemple 5.14. *Soit p un nombre premier. Par définition, on a $\varphi(p) = p - 1$.*

Proposition 5.15. *Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.*

Démonstration. Soit G un groupe monogène infini. Soit $x \in G$ un générateur de G.

On considère la fonction de $\mathbb{Z}$ dans G qui à chaque $n \in \mathbb{Z}$ associe $x^n \in G$. Nous avons vu dans une autre preuve que c'est un homomorphisme de groupes.

Maintenant, il est aisé de voir que ce morphisme est injectif. En effet, son noyau est $\{0\}$ car on a supposé G monogène infini. Enfin, il est surjectif car son image est un sous-groupe de G contenant x, donc il s'agit de G tout entier. □

Proposition 5.16. *Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $\mathbb{U}_n$.*

Démonstration. Soit G un groupe cyclique d'ordre n. Soit $x \in G$ un générateur du groupe G.

On considère la fonction $f : \mathbb{U}_n \to G$ qui à chaque élément $\exp\left(\frac{2i\pi k}{n}\right) \in \mathbb{U}_n$, avec $k \in [\![0, n-1]\!]$, associe $x^k \in G$. Il s'agit d'un homomorphisme de groupes.

Mais f est injective car $x^k = 1$ si et seulement si n divise k, donc ici $n = 0$. Quant à la surjectivité, elle provient du fait que l'on injecte un ensemble de cardinal n dans un ensemble étant également de cardinal n. □

6. Quotient

Nous allons définir une notion de quotient sur les groupes, de manière similaire à celle que vous connaissez sur les ensembles (par rapport à une relation d'équivalence) ou sur les espaces vectoriels (par rapport à un sous-espace vectoriel).

Contrairement aux espaces vectoriels, on ne peut pas effectuer le quotient par rapport à un sous-groupe et obtenir canoniquement un groupe. On a besoin de la définition suivante.

Définition 6.1. *Soit $(G, \bullet)$ un groupe. Un* ***sous-groupe distingué*** *H de G est un sous-groupe de G tel que pour tout $g \in G$ on ait :*

$$g \bullet H = H \bullet g.$$

On note $H \trianglelefteq G$.

Cette définition équivaut à dire que pour tout $g \in G$, les classes à droite et à gauche de g suivant H coïncident. Il existe une définition équivalente d'un sous-groupe distingué.

Proposition 6.2. *Soit $(G, \bullet)$ un groupe. Un sous-groupe H de G est distingué si et seulement si pour tout $g \in G$ on a :*

$$\forall h \in H,\ g \bullet h \bullet g^{-1} \in H.$$

Démonstration. Supposons d'abord que H est distingué. Alors, avec les notations de l'énoncé, on a $g \bullet H = H \bullet g$. En particulier, il existe $h' \in H$ tel que $g \bullet h = h' \bullet g$, d'où $g \bullet h \bullet g^{-1} = h' \bullet g \bullet g^{-1} = h' \in H$.

Réciproquement, si la condition de l'énoncé est vérifiée, alors pour tout $h \in H$ il existe $h' \in H$ tel que $g \bullet h \bullet g^{-1} = h'$, donc $g \bullet h = g \bullet h \bullet g^{-1} \bullet g = h' \bullet g$. Nous avons donc $g \bullet H \subset H \bullet g$. L'inclusion réciproque se démontre de manière similaire, en remarquant que $g^{-1} \bullet h \bullet g \in H$ pour tout $h \in H$. □

Une conséquence immédiate de la proposition précédente est que dans un groupe abélien, tout sous-groupe est distingué !

La définition et la proposition ci-dessus sont hors programme. Il n'est donc pas nécessaire d'apprendre la notion de sous-groupe distingué, à condition que vous gardiez en tête les deux choses suivantes : on ne peut pas toujours quotienter un groupe par un sous-groupe, sauf dans le cas des groupes abéliens.

Dans la suite, vous pouvez donc supposer que tous les groupes sont abéliens, et ainsi ne plus vous soucier de vérifier que le sous-groupe est distingué. Les résultats qui suivent sont quant à eux au programme.

L'intérêt de cette notion est que la loi de composition interne d'un groupe induit une loi de composition interne sur l'ensemble des classes à gauche (et donc à droite) suivant un sous-groupe distingué.

Proposition 6.3. *Soit $(G, \bullet)$ un groupe. Soit $H \trianglelefteq G$. Il existe une loi de composition interne, notée ici aussi $\bullet$, sur l'ensemble $\{g \bullet H \mid g \in G\}$ des classes à gauche suivant H vérifiant :*

$$(x \bullet H) \bullet (y \bullet H) = (x \bullet y) \bullet H,$$

où $x, y \in G$.

Démonstration. Il s'agit de vérifier que la loi de composition interne est bien définie, c'est-à-dire que cela ne va pas dépendre des choix de x et de y. Soient $x', y' \in G$ tels que $x \bullet H = x' \bullet H$ et $y \bullet H = y' \bullet H$. On veut vérifier que $(x \bullet y)H = (x' \bullet y')H$.

Soit $h \in H$. On sait qu'il existe $h_2 \in H$ tel que $y \bullet h = y' \bullet h_2$. Nous avons donc $x \bullet y \bullet h = x \bullet y' \bullet h_2$. De plus, puisque H est distingué, on peut trouver $h_3 \in H$ tel que $y' \bullet h_2 = h_3 \bullet y'$. Donc $x \bullet y \bullet h = x \bullet h_3 \bullet y'$. Or par hypothèse, on peut trouver $h_4 \in H$ tel que $x \bullet h_3 = x' \bullet h_4$. Donc $x \bullet y \bullet h = x' \bullet h_4 \bullet y'$. Toujours par l'hypothèse de distinction, on peut trouver $h_5 \in H$ tel que $h_4 \bullet y' = y' \bullet h_5$. Donc $x \bullet y \bullet h = x' \bullet y' \bullet h_5$. Nous avons donc l'inclusion $(x \bullet y)H \subset (x' \bullet y')H$.

L'inclusion réciproque se fait de la même manière. □

Une conséquence immédiate de cette proposition est que cette loi de composition interne est une loi de groupe ! On vous laisse vérifier les trois axiomes, avec un indice : l'élément neutre est donné par $e \bullet H$, où $e \in G$ est l'élément neutre de G.

Définition 6.4. *Soit G un groupe. Soit $H \trianglelefteq G$. On note G/H l'ensemble des classes à gauche (donc, de manière synonyme ici, à droite) suivant H. Muni de la loi de composition interne définie ci-dessus, on l'appelle le* ***groupe quotient de*** *G* ***par*** *H.*

Exemple 6.5. *Pour tout $n \in \mathbb{N}^*$, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe distingué du groupe additif $\mathbb{Z}$, et le groupe quotient obtenu $\mathbb{Z}/n\mathbb{Z}$, qui est un groupe cyclique d'ordre n engendré par $1 + n\mathbb{Z}$. On note ses éléments $\overline{0}$, $\overline{1}$, ...et $\overline{n-1}$.*

Exemple 6.6. *L'ensemble des multiples de $2\pi\mathbb{Z}$ est un sous-groupe du groupe additif $\mathbb{R}$. Le quotient $\mathbb{R}/2\pi\mathbb{Z}$ est en bijection en tant qu'ensemble à l'intervalle $[0, 2\pi[$, ou encore à l'intervalle $]-\pi, \pi]$. L'argument d'un nombre complexe nous donne ainsi un homomorphisme de groupes de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}/2\pi\mathbb{Z}, +)$.*

Définition 6.7. *Soit $(G, \bullet)$ un groupe. Soit $H \trianglelefteq G$. L'homomorphisme de groupes $G \to G/H$ qui à chaque $g \in G$ associe $g \bullet H$ est un homomorphisme de groupes que l'on appelle la* ***projection canonique****.*

Par exemple, on peut voir la projection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, où $n \in \mathbb{N}^*$ comme étant le reste de la division euclidienne par n, sauf que l'on considère la classe associée à ce reste (avec notre notation, on la surligne).

Théorème 6.8 (Propriété universelle du quotient)**.** *Soit G un groupe, H un sous-groupe distingué de G et $p\colon G \to G/H$ la projection canonique. Si $f\colon G \to G'$ est un homomorphisme de groupes dont le noyau contient H, il existe un unique homomorphisme de groupes $\overline{f}\colon G/H \to G'$ tel que $f = \overline{f} \circ p$.*

En algèbre, on préfère simplifier ce type d'énoncé en disant que le diagramme ci-dessous commute :

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle p}\downarrow & \nearrow_{\overline{f}} & \\ G/H. & & \end{array}$$

Démonstration. Notons $\bullet$ la loi de composition interne de G, et $\star$ celle de G'. Si une telle flèche existait, elle doit associer à chaque $g \bullet H \in G/H$ l'élément $f(g) \in G'$. Il s'agit donc ici de vérifier que cette application est bien définie, c'est-à-dire que celle-ci ne dépend pas du choix de $g \in G$.

Soit $g' \in G$ tel que $g \bullet H = g' \bullet H$. Il existe donc $h, h' \in H$ tels que $g \bullet h = g' \bullet h'$. Rappelons que $H \subset \mathrm{Ker}(f)$, donc si l'on note $e \in G'$ l'élément neutre de G' on a $f(h) = f(h') = e$. On a alors :

$$\begin{aligned} f(g') &= f(g') \star e \\ &= f(g') \star f(h') \\ &= f(g' \bullet h') \\ &= f(g \bullet h) \\ &= f(g) \star f(h) \\ &= f(g) \star e \\ f(g') &= f(g). \end{aligned}$$

□

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

Soit $n \in \mathbb{N}^*$. On rappelle que $x, y \in \mathbb{Z}$ sont congrus modulo n s'il existe $k \in \mathbb{Z}$ tel que $x = y + kn$. On note $x \equiv y[n]$. Cela équivaut à dire que x et y ont le même reste dans leur division euclidienne par n.

Proposition 7.1. *L'addition et la multiplication sont des opérations compatibles avec les congruences modulo $n \in \mathbb{N}^*$, c'est-à-dire que pour tout $x, x', y, y' \in \mathbb{Z}$ on a l'implication :*

$$\begin{cases} x \equiv y[n], \\ x' \equiv y'[n] \end{cases} \implies \begin{cases} x + x' \equiv y + y'[n], \\ xx' \equiv yy'[n] \end{cases}.$$

Démonstration. Soient $k, k' \in \mathbb{Z}$ on a $x = y + kn$ et $x' = y' + k'n$. En particulier, $x + x' = y + y' + (k + k')n$. De plus :

$$\begin{aligned} xx' &= (y + kn)(y' + k'n) \\ &= yy' + (yk' + y'k + kk'n)n. \end{aligned}$$

□

La congruence modulo $n \in \mathbb{N}^*$ définit clairement une relation d'équivalence sur $\mathbb{Z}$: elle est réflexive, symétrique et transitive. En fait, ces classes correspondent aux classes suivant $n\mathbb{Z}$. Nous avons donc une loi correspondant à la multiplication en plus de l'addition ; on parle de structure d'anneau.

Proposition 7.2. *Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Démonstration. Nous avons déjà démontré que tout groupe cyclique d'ordre n est isomorphe à $\mathbb{U}_n$. De plus, l'application $f\colon \mathbb{Z} \to \mathbb{U}_n$ qui à chaque $k \in \mathbb{Z}$ associe $\exp\left(\frac{2ik\pi}{n}\right)$ est un homomorphisme de groupes surjectif.

Remarquons que $n\mathbb{Z} \subset \mathrm{Ker}(f)$. Par la propriété universelle du quotient, f se factorise via un homomorphisme de groupes $i\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$. Cet homomorphisme est surjectif puisque f est surjectif. Il est donc bijectif, car les deux groupes ont le même ordre. □

Proposition 7.3. *Tout sous-groupe d'un groupe monogène est monogène.*

Démonstration. Nous avons déjà démontré cette proposition dans le cas d'un groupe monogène infini : il s'agissait de la proposition caractérisant les sous-groupes de $\mathbb{Z}$. Concentrons-nous donc sur le cas où le groupe monogène est fini, en d'autres termes cyclique. Soit $n \in \mathbb{N}^*$, et démontrons que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique.

Soit G un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{N}^*$ le plus petit entier naturel non nul tel que $\overline{k} \in G$. Soit $l \in \mathbb{N}^*$ n'importe quel entier vérifiant $\overline{l} \in G$.

Avec le théorème de Bézout, on trouve $u, v \in \mathbb{Z}$ tels que $\mathrm{pgcd}(k,l) = uk + vl$. En particulier, $\overline{\mathrm{pgcd}(k,l)} \in G$. Puisque l'on a $\mathrm{pgcd}(k,l) \in [\![1, k]\!]$, par minimalité de k on obtient que $\mathrm{pgcd}(k,l) = k$. Cela signifie que k divise l. Donc $\overline{l} \in \langle \overline{k} \rangle$, et $G = \langle \overline{k} \rangle$. □

Proposition 7.4. *Soit d un diviseur de $n \in \mathbb{N}^*$. Il existe un unique sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Il s'agit de $\langle \frac{\overline{n}}{d} \rangle$.*

Démonstration. Puisque tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique, il suffit de démontrer que pour tout $k \in \mathbb{Z}$, on a l'égalité $\langle \overline{k} \rangle = \left\langle \overline{\mathrm{pgcd}(k,n)} \right\rangle$. Clairement, $\langle \overline{k} \rangle \subset \left\langle \overline{\mathrm{pgcd}(k,n)} \right\rangle$. Démontrons donc l'inclusion réciproque.

Avec le théorème de Bézout, on trouve $u, v \in \mathbb{Z}$ tels que $\mathrm{pgcd}(k,n) = uk + vn$. En particulier, puisque $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n, on a $\overline{\mathrm{pgcd}(k,n)} = \overline{uk} + \overline{kn} = u\overline{k}$. Cela démontre l'inclusion réciproque. Le d de l'énoncé est donc $d = \frac{n}{\mathrm{pgcd}(k,n)}$. □

8. Structure des groupes abéliens de type fini

Nous avons maintenant tous les outils en main pour étudier le théorème principal de ce cours : la classification des groupes abéliens de type fini, à isomorphisme près.

Définition 8.1. *Soient $(G, \bullet)$ et $(H, \bullet)$ deux groupes. La loi de composition interne sur $G \times H$ définie par :*

$$(g,h) \bullet (g',h') \coloneqq (g \bullet g', h \bullet h'),$$

où $g, g' \in G$ et $h, h' \in H$ est une loi de groupe sur $G \times H$. On appelle le groupe obtenu le ***groupe produit****.*

On observe que l'élémént neutre de $G \times H$ est (e_G, e_H), où e_G et e_H sont les éléments neutres respectifs de G et de H. Le symétrique d'un couple $(g, h) \in G \times H$ est $\left(g^{-1}, h^{-1}\right)$.

On observe que l'application $f\colon G \times H \to H \times G$ qui à chaque $(g, h) \in G \times H$ associe $(h, g) \in H \times G$ est un isomorphisme de groupes.

Définition 8.2. *Soient G et H deux groupes. Les fonctions $p_G\colon G \times H \to G$ et $p_H\colon G \times H \to H$ qui à $(g, h) \in G \times H$ associent respectivement g et h sont des homomorphismes de groupes appelés les* ***projections****.*

On peut vérifier une forme de propriété d'associativité pour ce produit. En effet, si G, H et I sont trois groupes, alors $(G \times H) \times I$ et $G \times (H \times I)$ sont isomorphes, en associant à chaque $((g, h), i) \in (G \times H) \times I$ le couple $(g, (h, i))$.

On peut généraliser le produit en considérant une famille de groupes $(G_i)_{i \in I}$ indicés par un ensemble I. Sur le produit cartésien $\prod_{i \in I} G_i$, on définit une la loi de composition interne terme à terme avec la loi de groupe de chaque G_i.

Un sous-groupe du produit $(G_i)_{i \in I}$ est la somme directe $\bigoplus_{i \in I} G_i$, dont les éléments sont les familles presque nulles : c'est à dire les familles $(g_i)_{i \in I} \in (G_i)_{i \in I}$ telles que seuls un nombre fini des g_i ne soient pas l'élément neutre. Lorsque I est un ensemble fini, on remarque donc qu'il n'y a pas de différence entre le groupe produit et la somme directe. Il n'y a une différence entre les deux notions que lorsque I est un ensemble infini, mais cela ne nous intéressera pas dans cette section.

Cette différence est hors programme, et nous emploierons donc $\oplus$ et $\times$ de manière interchangeable car nous n'étudierons que des produits finis. Mais gardez bien en tête pour la suite de votre parcours que ces notions ne sont pas les mêmes !

Théorème 8.3 (dit « des restes chinois »)**.** *Soient m et n deux entiers premiers entre eux. Alors les groupes $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes.*

Démonstration. On a un homomorphisme de groupes de $\mathbb{Z}$ dans le groupe produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ qui à chaque $k \in \mathbb{Z}$ associe le couple des images par chacune des projections canoniques $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ de k. On remarque que $mn\mathbb{Z}$ est dans le noyau de cet homomorphisme. Par la propriété universelle du quotient, il se factorise donc via un homomorphisme de groupes de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/mn\mathbb{Z}$.

Cet homomorphisme est injectif, car un entier divisible par m et n est divisible par $\mathrm{ppcm}(m, n) = mn$. L'homomorphisme est donc un isomorphisme par égalité des ordres. □

Lemme 8.4. *Soit $(G, +)$ un groupe abélien. Soient H et H' deux sous-groupes de G tels que $H \cap H' = \{0\}$, et que pour tout $g \in G$ il existe $h \in H$ et $h' \in H'$ vérifiant $g = h + h'$. Alors, G est isomorphe à $H \times H'$.*

Démonstration. Remarquons tout d'abord que pour tout $g \in G$, les $h \in H$ et $h' \in H'$ tels que $g = h + h'$ sont uniques. En effet, si l'on avait d'autres éléments $x \in H$ et $x' \in H'$ tels que $g = x + x'$, on obtiendrait $h - x + h' - x' = 0$, donc $h - x = x' - h'$. En particulier, $h - x \in H'$ et $x' - h' \in H$, donc ces différences sont dans l'intersection $H \cap H'$. Par hypothèse, cela implique que $h = x$ et $h' = x'$.

On peut donc définir l'application qui à chaque $g \in G$ associe $(h, h') \in H \times H'$, où $g = h + h'$. Il s'agit d'un homomorphisme de groupes, car si $g' \in G$ égale $y + y'$ où $y \in H$ et $y' \in H'$, on a $g + g' = h + y + h' + y'$. Puisque H et H' sont des sous-groupes de G, pour tout $h \in H$ et tout $h' \in H$ on a $h + h' \in G$, donc l'isomorphisme est surjectif. Il est de plus injectif par hypothèse sur l'intersection. □

Lemme 8.5. *Soit $(G,+)$ un groupe abélien. Soit $k \in \mathbb{N}$. Soient $g_1, \dots, g_k \in G$ tels que $G = \langle g_1, \dots, g_k \rangle$. Soient $a_1, \dots, a_k \in \mathbb{N}$ tels que $\operatorname{pgcd}(a_1, \dots, a_k) = 1$. Alors il existe $x_2, \dots, x_k \in G$ tels que $G = \left\langle \sum_{i=1}^k a_i g_i, x_2, \dots, x_k \right\rangle$.*

Démonstration. On raisonne par récurrence sur $\sum_{i=1}^k a_i \in \mathbb{N}^*$. Lorsque cette somme vaut 1, il n'y a rien à démontrer.

Lorsque la somme est strictement plus grande que 1, alors par hypothèse sur le plus grand diviseur commun on a au moins deux des a_i non nuls ; quitte à permuter les générateurs, on peut supposer qu'il s'agit de a_1 et a_2, et que $a_1 \geqslant a_2$. Dans ce cas, puisque $G = \langle g_1, g_1 + g_2, \dots, g_k \rangle$, que $\operatorname{pgcd}(a_1 - a_2, a_2, \dots, a_k) = 1$, et que $a_1 - a_2 + \sum_{i=2}^k a_i < \sum_{i=1}^k a_i$, on peut appliquer l'hypothèse de récurrence et trouver $x_2, \dots, x_k \in G$ tels que $G = \left\langle (a_1 - a_2) g_1 + a_2(g_1 + g_2) + \sum_{i=3}^k a_i g_i, x_2, \dots, x_k \right\rangle$. On conclut en simplifiant le premier terme en utilisant le fait que G est abélien. □

Théorème 8.6 (Structure des groupes abéliens de type fini)**.** *Tout groupe abélien de type fini est isomorphe à $\bigoplus_{i=1}^k \mathbb{Z} \oplus \bigoplus_{j=1}^l \mathbb{Z}/{p_j}^{n_j}\mathbb{Z}$, où $k, l \in \mathbb{N}$, et où pour chaque $j \in [\![1, l]\!]$ les p_j sont des nombres premiers et les $n_j \in \mathbb{N}^*$.*

En particulier, tout groupe abélien fini est isomorphe à une somme directe finie de groupes cycliques.

Démonstration. Si l'on démontre qu'un groupe abélien de type fini est isomorphe à une somme directe finie de groupes monogènes, on peut alors conclure en employant le théorème des restes chinois. Démontrons donc ce résultat plus faible par récurrence sur le nombre minimum $k \in \mathbb{N}$ de générateurs d'un groupe abélien. Lorsqu'un groupe abélien est généré par moins d'un élément, il est monogène et le résultat est évident.

Supposons donc que $k \geqslant 2$. Soit $(G,+)$ un groupe abélien engendré par au moins k éléments. Soient $g_1, \dots, g_k \in G$ tels que $G = \langle g_1, \dots, g_k \rangle$. On suppose que l'on a choisi ces éléments de telle façon à ce que l'ordre de g_1 soit le plus petit possible. Si l'on vérifie que $\langle g_1 \rangle \cap \langle g_2, \dots, g_k \rangle = \{0\}$, alors la récurrence est terminée en appliquant l'hypothèse de récurrence sur le sous-groupe $\langle g_2, \dots, g_k \rangle$.

Si cette intersection est plus grande, quitte à prendre les symétriques des générateurs on peut trouver $a_1, \dots, a_k \in \mathbb{N}$ tels que $a_1 \neq 0$ soit plus petit que l'ordre de g_1, et que $\sum_{i=1}^k a_i g_i = 0$. Notons $d \coloneqq \operatorname{pgcd}(a_1, \dots, a_k)$. Alors d'après le lemme, il existe $x_2, \dots, x_k \in G$ tels que $G = \left\langle \sum_{i=1}^k \frac{a_i}{d} g_i, x_2, \dots, x_k \right\rangle$. Or, l'élément $\sum_{i=1}^k \frac{a_i}{d} g_i$ est d'ordre au plus $d \leqslant a_1$, ce qui contredit le choix de g_1 comme ayant le plus petit ordre possible. □

Ce résultat est faux si le groupe n'est pas de type fini : prenez par exemple $(\mathbb{Q},+)$.

Dans le cas des groupes abéliens finis, on en déduit deux types de décomposition.

Définition 8.7. *Soit G un groupe abélien fini. On appelle* ***décomposition primaire*** *l'écriture de G comme produit de groupes dont tous les éléments sont d'ordre une puissance d'un nombre premier, uniquement déterminé par le terme du produit.*

Exemple 8.8. *La décomposition primaire de $\mathbb{Z}/6\mathbb{Z}$ est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Exemple 8.9. *La décomposition primaire du groupe $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est le produit $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$.*

Exemple 8.10. *La décomposition primaire du groupe $\mathbb{Z}/21\mathbb{Z}\times\mathbb{Z}/99\mathbb{Z}$ est le produit $(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z})\times\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/11\mathbb{Z}$.*

Définition 8.11. *Soit G un groupe abélien fini. On appelle* ***décomposition en facteurs invariants*** *l'écriture de G comme produit de groupes cycliques, dont les ordres forment une suite dans laquelle chaque terme divise le suivant.*

Exemple 8.12. *Le groupe $\mathbb{Z}/6\mathbb{Z}$ est déjà décomposé en facteurs invariants.*

Exemple 8.13. *La décomposition en facteurs invariants de $\mathbb{Z}/15\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ est $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$.*

Exemple 8.14. *La décomposition en facteurs invariants de $\mathbb{Z}/21\mathbb{Z}\times\mathbb{Z}/99\mathbb{Z}$ est $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/693\mathbb{Z}$.*

9. Rappels sur les espaces vectoriels

Plus tôt dans votre cursus, vous avez étudié les espaces vectoriels. Ceux-ci sont tous des groupes, et donnent donc de très nombreux exemples. On explique dans cette section comment redéfinir les notions que vous connaissez avec notre nouveau vocabulaire.

Définition 9.1. *Soit E un ensemble, et considérons $\times$ une loi de composition $F\times E\to E$ sur E. On dit que $\times$ est* ***distributive à droite*** *par rapport à une loi de composition interne $+$ sur F si :*

$$\forall x,y\in F,\ \forall z\in E,\ (x+y)\times z=x\times z+y\times z.$$

De même, on dira que $\times$ est ***distributive à gauche*** *par rapport à une loi de composition interne $+$ sur E si :*

$$\forall x,y\in E,\ \forall z\in F,\ z\times(x+y)=z\times x+z\times y.$$

Remarquez que lorsque $\times$ est une loi de composition interne et commutative, alors les notions de distributivité à droite et à gauche sont équivalentes. On parlera dans cette situation uniquement de lois distributives, sans préciser de côté.

Définition 9.2. *Un* ***corps*** *est un ensemble k muni de deux lois de composition internes $+$ et $\times$ telles que :*

(1) le couple $(k,+)$ est un groupe abélien ;

(2) le couple $(k^*,\times)$ est un groupe abélien ;

(3) la loi $\times$ est distributive par rapport à $+$.

Attention ! Dans certains vieux livres, il est parfois demandé que $(k^*,\times)$ soit seulement un groupe, pas forcément un groupe abélien. Nous préférons ici une définition moderne. On parlera plutôt d'anneau à division dans le cas non-commutatif, qui ne nous intéressera pas dans ce cours.

Exemple 9.3. *Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition et de la multiplication usuelles sont des corps.*

Exemple 9.4. *Soit $p\in\mathbb{N}^*$. Nous avons vu que dans $\mathbb{Z}/p\mathbb{Z}$, l'ordre de $\overline{k}$ où $k\in\mathbb{Z}$ est $\frac{p}{\mathrm{pgcd}(k,p)}$. On déduit de ce fait et du théorème de Bézout que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Avec le nouveau vocabulaire des groupes, on peut désormais donner une définition plus succincte des espaces vectoriels.

Définition 9.5. *Soit k un corps. Un* ***k-espace vectoriel*** *est un ensemble E muni :*
— *d'une loi de composition interne $+$ sur E ;*
— *et d'une loi de composition externe $\cdot\colon k \times E \to E$ sur E,*
vérifiant les conditions suivantes :

(1) le couple $(E, +)$ est un groupe abélien ;

(2) la loi $\cdot$ est distributive à droite par rapport à la loi $+$ sur k ;

(3) la loi $\cdot$ est distributive à gauche par rapport à la loi $+$ sur E ;

(4) les lois $\times$ et $\cdot$ vérifient la propriété d'associativité mixte :

$$\forall x, y \in k,\ \forall z \in E,\ (x \times y) \cdot z = x \cdot (y \cdot z)\ ;$$

(5) l'élément neutre $1 \in k$ pour $\times$ vérifie :

$$\forall x \in E,\ 1 \cdot x = x.$$

Un petit exercice afin de vérifier que vous avez bien compris les définitions de ce cours est de s'assurer que cette définition est équivalente à celle que vous avez vue en étudiant les espaces vectoriels.

Remarquez que l'on demande à ce qu'un espace vectoriel soit un groupe abélien additif. Par conséquent, tous les espaces vectoriels que vous avez étudiés sont des exemples de groupes. Il suffit simplement de ne pas considérer la loi de composition externe. On dit aussi que l'on l'oublie.

Exemple 9.6. *L'ensemble des polynômes à coefficients réels $\mathbb{R}[X]$ est un $\mathbb{R}$-espace vectoriel. Par conséquent, $(\mathbb{R}[X], +)$ est un groupe.*

Exemple 9.7. *Soit k un corps, et soit $n \in \mathbb{N}^*$. Le produit direct k^n muni de l'addition et de la multiplication externe terme à terme est un k-espace vectoriel.*

Exemple 9.8. *L'ensemble des suites à coefficients dans un corps k, muni de l'addition et de la multiplication externe coefficient par coefficient est un k-espace vectoriel.*

Exemple 9.9. *Soit E un ensemble. L'ensemble des applications de E dans un corps k est un k-espace vectoriel, où les deux lois sont définies usuellement pour chaque valeur.*

Définition 9.10. *Soit k un corps, et soit E un k-espace vectoriel. Un* ***sous-espace vectoriel*** *de E est un sous-groupe additif $F \leqslant E$ tel que :*

$$\forall \lambda \in k,\ \forall x \in F,\ \lambda \cdot x \in F.$$

Nous vous laissons le soin de vérifier que cette définition correspond à celle que vous connaissez déjà. On retrouve ainsi les résultats usuels concernant les sous-espaces vectoriels, comme par exemple le fait que ces derniers sont aussi des k-espaces vectoriels.

Exemple 9.11. *Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{R}_n[X]$ des polynômes réels de degré inférieur ou égal à n est un sous-espace vectoriel de $\mathbb{R}[X]$. En particulier, c'est un sous groupe additif de $\mathbb{R}[X]$.*

Définition 9.12. *Soit k un corps. Une* ***application linéaire*** *entre deux k-espaces vectoriels E et F est un homomorphisme de groupes additifs $f\colon E \to F$ tel que :*

$$\forall \lambda \in k,\ \forall x \in E,\ f(\lambda \cdot x) = \lambda \cdot f(x).$$

L'ensemble des applications linéaires de E dans F est noté $\mathcal{L}(E,F)$, et $\mathcal{L}(E)$ lorsque $E=F$.

À nouveau, il est recommandé de vérifier que cette définition correspond avec celle que vous avez apprise auparavant.

Exemple 9.13. *Soit $x\in\mathbb{R}$. L'application qui à un polynôme $P(X)\in\mathbb{R}[X]$ associe $P(x)$ est une application linéaire. En particulier, c'est un homomorphisme de groupes de $(\mathbb{R}[X],+)$ dans $(\mathbb{R},+)$.*

On rappelle que dans un $\mathbb{R}$-espace vectoriel E de dimension finie, il existe une application $\det\colon \mathcal{L}(E)\to\mathbb{R}$ appelée le déterminant. L'ensemble des endomorphismes de E dont le déterminant n'est pas nul sont les automorphismes, ils forment un sous-groupe $\mathrm{GL}(E)$ de $(\mathfrak{S}(E),\circ)$. De plus, le déterminant est alors un homomorphisme de groupes de $\mathrm{GL}(E)$ vers $(\mathbb{R}^*,\times)$.

On rappelle que le sous-ensemble de $\mathrm{GL}(E)$ composé des applications linéaires de déterminant égal à 1 est noté $\mathrm{SL}(E)$. Il s'agit d'un sous-groupe de $\mathrm{GL}(E)$.

10. Réduction des endomorphismes

Dans toute cette section, k désigne un corps et E un k-espace vectoriel de dimension finie. On rappelle qu'étant donné un polynôme $P(X)$ à coefficients dans k et un endomorphisme $f\in\mathcal{L}(E)$, on définit $P(f)$ en substituant f à X, où les puissances de f sont pour la loi de composition.

On rappelle également le théorème de Cayley–Hamilton.

Théorème 10.1 (Cayley–Hamilton)**.** *Soit $f\in\mathcal{L}(E)$. Soit χ_f son polynôme caractéristique. Alors $\chi_f(f)$ est l'endomorphisme nul.*

Démonstration. Soit M la matrice associée à f dans une base fixée de E. Soit $n\in\mathbb{N}$ la dimension de E. On rappelle que $\chi_f(X)=\det(M-I_nX)$. Soit $\mathrm{com}(M-I_nX)$ la comatrice de $M-I_nX$ La formule de Laplace nous donne :

$$\mathrm{com}(M-I_nX)^T\times(M-I_nX)=\chi_f(X)I_n.$$

On peut conclure si en évaluant ces polynômes matriciels en M, on vérifie que le terme de gauche vaut zéro. Comme le produit matriciel n'est pas commutatif, l'évaluation en M d'un produit n'est pas le produit des évaluations en M, il convient donc d'être prudents ici.

Si l'on note N_i les uniques matrices carrées à coefficients dans k vérifiant l'égalité $\sum_{i=0}^{n-1}N_iX^i=\mathrm{com}(M-I_nX)^T$, on a alors :

$$\mathrm{com}(M-I_nX)^T\times(M-I_nX)=\sum_{i=0}^{n-1}N_iMX^i-\sum_{i=0}^{n-1}N_iX^{i+1}.$$

Le théorème en découle. □

On rappelle que les valeurs propres d'un endomorphisme linéaire sont les racines de son polynôme caractéristique. L'espace propre associé à l'une de ces valeurs propres est l'espace vectoriel des vecteurs propres associés à cette valeur propre.

On note $\mathrm{Sp}(f)$ le spectre, c'est-à-dire l'ensemble des valeurs propres, d'un endomorphisme $f\in\mathcal{L}(E)$.

Dans la suite, nous allons nous intéresser aux endomorphismes linéaires dont le polynôme caractéristique est scindé. Par exemple, sur $\mathbb{C}$, tous les polynômes sont scindés.

Définition 10.2. *Soit $f \in \mathcal{L}(E)$ un endomorphisme linéaire dont le polynôme caractéristique est scindé. Notons $\chi_f = \prod_{\lambda \in \mathrm{Sp}(f)} (X-\lambda)^{m_\lambda}$, où les $m_\lambda \in \mathbb{N}^*$ sont les multiplicités des racines du polynôme caractéristique.*

Soit $\lambda \in \mathrm{Sp}(f)$. Le ***sous-espace caractéristique de f associé à λ*** *est le sous-espace vectoriel $\ker((f - \lambda \mathrm{Id}_E)^{m_\lambda})$.*

On remarque que le sous-espace caractéristique d'un endomorphisme linéaire associé à une valeur propre contient le sous-espace propre associé à la même valeur propre.

Exemple 10.3. *Dans $\mathbb{R}^3$ muni de la base canonique, on considère l'endomorphisme linéaire f défini par la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Son polynôme caractéristique est $\chi_f(X) = (X-1)^2(X-2)$.*

L'endomorphisme $f - 2\,\mathrm{Id}_{\mathbb{R}^3}$ est représenté par la matrice $\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Son noyau est donc engendré par $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, il s'agit de l'espace propre associé à 2.

L'endomorphisme $f - 1\,\mathrm{Id}_{\mathbb{R}^3}$ est représenté par la matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Son noyau est donc engendré par $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, il s'agit de l'espace propre associé à 1.

L'endomorphisme $(f - 1\,\mathrm{Id}_{\mathbb{R}^3})^2$ est représenté par la matrice $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Son noyau est donc engendré par $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, il s'agit du sous-espace caractéristique associé à 1.

Soit $f \in \mathcal{L}(E)$ un endomorphisme linéaire dont le polynôme caractéristique est scindé. Dans ce qui suit, pour tout $\lambda \in \mathrm{Sp}(f)$, on notera :

$$P_\lambda \coloneqq \prod_{\mu \in \mathrm{Sp}(f) \setminus \{\lambda\}} (X-\mu)^{m_\mu}.$$

Ces polynômes sont premiers entre eux dans leur ensemble. On choisit une relation de Bézout, c'est-à-dire des polynômes Q_λ tels que :

$$\sum_{\lambda \in \mathrm{Sp}(f)} P_\lambda Q_\lambda = 1.$$

Ceci est possible grâce à la division euclidienne dans $k[X]$, nous admettons qu'elle se généralise dans ce contexte. En particulier, on a :

$$\sum_{\lambda \in \mathrm{Sp}(f)} P_\lambda(f) \circ Q_\lambda(f) = \sum_{\lambda \in \mathrm{Sp}(f)} Q_\lambda(f) \circ P_\lambda(f) = \mathrm{Id}_E\,.$$

Lemme 10.4. *Soit $f \in \mathrm{End}(E)$. On suppose que le polynôme caractéristique de f est scindé. Pour tout $\lambda \in \mathrm{Sp}(f)$, on note E_λ le sous-espace caractéristique associé à λ. Alors :*

(1) le sous-espace E_λ est stable par f et $E = \bigoplus_{\lambda \in \mathrm{Sp}(f)} E_\lambda$;

(2) la projection sur le sous-espace E_λ relativement à la somme directe ci-dessus est $Q_\lambda(f) \circ P_\lambda(f)$, et en particulier, ces projections commutent ;

(3) pour tous $\lambda, \mu \in \mathrm{Sp}(f)$ tels que $\lambda \neq \mu$, on a $p_\lambda^2 = p_\lambda$ et $p_\lambda \circ p_\mu = 0$.

Démonstration. Si $x \in E_\lambda$, on a :

$$(f - \lambda \mathrm{Id}_E)^{m_\lambda}(fx) = f((f - \lambda \mathrm{Id}_E)^{m_\lambda}(x)) = 0,$$

ce qui montre que E_λ est stable par f.

Pour tout $x \in E$ et pour tout $\lambda \in \mathrm{Sp}(f)$, on a $(P_\lambda(f))(x) \in E_\lambda$ en vertu du théorème de Cayley-Hamilton. Puisque $x = \sum_{\lambda \in \mathrm{Sp}(f)} P_\lambda(f)(Q_\lambda(f)(x))$, il existe une écriture de x dans la somme des E_λ.

Par ailleurs, si $\lambda, \mu \in \mathrm{Sp}(f)$ sont distincts et si $x \in E_\mu$, alors $P_\lambda(f)(x) = 0$ puisque $(X - \mu)^{m_\mu}$ divise P_λ. En particulier, si $x \in E_\lambda$, la décomposition ci-dessus qui s'écrit aussi $x = \sum_{\lambda \in \mathrm{Sp}(f)} Q_\lambda(f)(P_\lambda(f)(x))$, fournit $x = Q_\lambda(f) \circ P_\lambda(f)(x)$. Ainsi, si des vecteurs $x_\lambda \in E_\lambda$ vérifient $\sum_{\lambda \in \mathrm{Sp}(f)} x_\lambda = 0$, alors pour tout $\lambda \in \mathrm{Sp}(f)$ on a :

$$Q_\lambda(f) \circ P_\lambda(f)(0) = Q_\lambda(f) \circ P_\lambda(f)(x_\lambda) = x_\lambda.$$

On a prouvé le premier et le second point.

Le troisième point est une propriété générale des projections relatives à une décomposition en sous-espaces supplémentaires. □

Ce qu'il faut retenir, notamment, c'est que les sous-espaces caractéristiques sont supplémentaires et que les projections sont des polynômes en l'endomorphisme.

Définition 10.5. *Un endomorphisme f est **nilpotent** lorsqu'il existe $m \in \mathbb{N}$ tel que $f^m = 0$. Le plus petit entier m vérifiant cette équation est appelé l'**indice** de f. Même vocabulaire pour une matrice carrée.*

Prenez garde à ne pas confondre l'indice d'un élément et son ordre ! Ici, 0 est l'élément neutre pour la loi $+$, mais la relation $f^m = 0$ écrite ci-dessus est pour la loi $\circ$.

Exemple 10.6. *Les matrices triangulaires avec des 0 sur la diagonale sont nilpotentes.*

Exemple 10.7. *Si $f \in \mathcal{L}(E)$ est nilpotent, son polynôme caractéristique est $X^{\dim E}$. Comme ce polynôme caractéristique est scindé, cela montre, par trigonalisation, que f admet une matrice triangulaire à diagonale nulle dans une certaine base. Inversement, si f a 0 comme seule valeur propre et un polynôme caractéristique scindé, c'est-à-dire égal à $X^{\dim E}$, alors f est nilpotent.*

Exemple 10.8. *Si $f \in \mathcal{L}(E)$ a une unique valeur propre λ et un polynôme caractéristique scindé, alors $f - \lambda \mathrm{Id}_E$ est un endomorphisme nilpotent. Autrement dit, f est la somme $f = \lambda \mathrm{Id}_E + n$ d'une homothétie et d'un nilpotent qui commutent.*

Cela se généralise au cas général de la façon suivante.

Proposition 10.9. *Soit $f \in \mathcal{L}(E)$ un endomorphisme linéaire dont le polynôme caractéristique est scindé. Alors, il existe deux endomorphismes $d, n \in L(E)$ tels que :*

(1) l'endomorphisme d est diagonalisable ;

(2) l'endomorphisme n est nilpotent ;

(3) les endomorphismes n et d sont des polynômes en f, et donc commutent ;

(4) on a $f = d + n$.

Démonstration. Avec les notations du paragraphe précédent, on pose le polynôme $d \coloneqq \sum_{\lambda \in \mathrm{Sp}(f)} \lambda Q_\lambda \circ P_\lambda(f)$. Si $x \in E_\lambda$, alors $d(x) = \lambda Q_\lambda \circ P_\lambda(f)(x) = \lambda x$, ce qui montre que les E_λ sont dans les espaces propres pour d. Comme ils sont supplémentaires, cela montre que d est diagonalisable.

Soit $n \coloneqq f - d$, polynôme en f. Si $x \in E_\lambda$, alors $n^{m_\lambda}(x) = (f - \lambda \mathrm{Id}_E)^{m_\lambda}(x) = 0$ ce qui montre que n est nilpotent, d'indice inférieur ou égal à $\max\{m_\lambda \mid \lambda \in \mathrm{Sp}(f)\}$ puisque les E_λ sont supplémentaires. □

11. Dualité en dimension finie

À présent, k désignera un corps.

Définition 11.1. *Soit E un k-espace vectoriel. On appelle **dual** de E l'ensemble $E^* = \mathcal{L}(E, k)$. Un élément du dual est appelé une **forme linéaire sur** E.*

Remarquez que le dual d'un k-espace vectoriel E est également un k-espace vectoriel pour les lois usuelles $+$ et $\cdot$ définies par :

$$\forall f, g \in E^*,\ \forall x \in E,\ (f+g)(x) = f(x) + g(x),$$
$$\forall f \in E^*,\ \forall x \in E,\ \forall a \in k,\ (a \cdot f)(x) = a \times (f(x)).$$

Soit $n \in \mathbb{N}$. Une forme linéaire sur k^n est de la forme $(x_1, \cdots, x_n) \mapsto \sum_{i=1}^n a_i x_i$, où $(a_1, \cdots, a_n) \in k^n$.

Définition 11.2. *Le noyau d'une forme linéaire non nulle sur un k-espace vectoriel E est un **hyperplan** de E.*

Proposition 11.3. *Soit E un k-espace vectoriel de dimension finie d. On considère une base $(e_1, \ldots, e_d)$ de E.*

(1) Le d-uplet de formes linéaires $(e_1^*, \ldots, e_d^*)$ définies par :

$$\forall i, j \in [\![1, \ldots, d]\!],\ e_i^*(e_j) = \delta_{i,j}, \tag{1}$$

où δ est le symbole de Kronecker, est une base de E^*.

(2) Pour tout $f \in E^*$, on a la formule :

$$f = \sum_{i=1}^{d} f(e_i) e_i^*. \tag{2}$$

(3) Pour tout $x \in E$, on a la formule :

$$x = \sum_{i=1}^{d} e_i^*(x) e_i. \tag{3}$$

Démonstration. Les formules (1) définissent une famille de formes linéaires puisque toute forme linéaire est déterminée par l'image d'une base. La formule (2) est vraie car les formes linéaires à droite et à gauche de l'égalité coïncident sur la base $(e_1, \dots, e_d)$: la famille est génératrice. Enfin, si $\sum_{i=1}^{d} a_i e_i^* = 0$, alors pour chaque i, prendre la valeur en e_i et montrer que $a_i = 0$: la famille est libre. Pour montrer (3), développer $x = \sum_{i=1}^{d} x_i e_i$ dans la base et prendre les images par les e_i^*. □

Définition 11.4. *La base $(e_1^*, \dots, e_d^*)$ de la proposition précédente est appelée la* ***base duale*** *de la base $(e_1, \dots, e_d)$.*

Proposition 11.5. *Si E est un k-espace vectoriel de dimension finie, alors E et E^* ont même dimension, et sont donc des espaces vectoriels isomorphes.*

Démonstration. Cela découle de la proposition sur la base duale. □

Proposition 11.6. *Soit E un k-espace vectoriel de dimension finie. L'application linéaire $\delta\colon E \to (E^*)^*$ définie par $\delta(x)(f) = f(x)$ pour tout $x \in E$ et tout $f \in E^*$ est un isomorphisme.*

Démonstration. On prend une base $(e_1, \dots, e_d)$ de E. Dire que $x \in \ker(\delta)$ signifie que $\delta(x)(e_i^*) = e_i^*(x) = 0$ pour tout $i \in [\![1, d]\!]$. Comme ces nombres sont les coordonnées de x dans la base $(e_1, \dots, e_d)$, cela signifie que $x = 0$. Il s'agit donc d'une application linéaire injective entre deux espaces vectoriels de même dimension, c'est donc un isomorphisme. □

Contrairement à l'isomorphisme entre E et son dual, l'isomorphisme δ entre E et son bidual est canonique, c'est-à-dire que sa définition ne fait pas intervenir le choix d'une base de E.

Définition 11.7. *Soit E un k-espace vectoriel de dimension finie. Soit $x \in E$ et $f \in E^*$. Le* ***crochet de dualité*** *est l'application $E \times E^* \to k$ définie par :*

$$\langle x, f \rangle \coloneqq f(x).$$

On a donc pour tout $x \in E$ et tout $f \in E^*$ dans un k-espace vectoriel E de dimension finie d et de base $(e_1, \dots, e_d)$ les égalités :

$$x = \sum_{i=1}^{d} \langle x, e_i^* \rangle e_i,$$

$$f = \sum_{i=1}^{d} \langle e_i, f \rangle e_i^*.$$

Exemple 11.8. *On note $\mathbb{R}_d[X]$ le $\mathbb{R}$-espace vectoriel des polynômes à coefficients réels de degré au plus d. Soit $a \in \mathbb{R}$. La famille ordonnée $\left((X-a)^i\right)_{i \in [\![0,d]\!]}$ est une famille libre de $d+1$ vecteurs. C'est donc une base de $\mathbb{R}_d[X]$. Sa base duale est la famille ordonnée $(\ell_i)_{i \in [\![0,d]\!]}$ où $\ell_i \in \mathbb{R}_d[X]^*$ est définie par la formule $\langle P, \ell_i \rangle = \frac{P^{(i)}(a)}{i!}$. En effet, le développement d'un polynôme dans cette base est la formule de Taylor–Young pour les polynômes :*

$$P = \sum_{i=0}^{d} \frac{P^{(i)}(a)}{i!} (X-a)^i.$$

Sa formule duale développe toute forme linéaire f dans la base $(\ell_0, \dots, \ell_d)$ ainsi :

$$f = \sum_{i=0}^{d} f\Big((X-a)^i\Big)\ell_i.$$

Par exemple, si $a \in \mathbb{R}$, le développement de la forme linéaire $P \mapsto \int_0^a P(t)dt$ fournit la formule :

$$\forall P \in \mathbb{R}_d[X],\ \int_0^a P(t)dt = \sum_{i=0}^{d} (-1)^i \frac{a^{i+1}}{(i+1)!} P^{(i)}(a).$$

Exemple 11.9. *Dans le même $\mathbb{R}$-espace vectoriel de dimension d que l'exemple précédent, considérons $a_0, \dots, a_d \in \mathbb{R}$ des réels deux à deux distincts. Les formes linéaires $P \mapsto P(a_i)$ pour $i \in [\![0, d]\!]$ forment une base de $\mathbb{R}_d[X]^*$. En effet, le développement dans cette base est la formule d'interpolation de Lagrange.*