Math 211 - Théorie des Groupes

Les nouveaux concepts seront écrits en **gras**, et les nouvelles formules seront $\boxed{\text{encadrées}}$.

Le matériel que vous avez déjà rencontré dans Math 113 sera marqué comme tel.

Les détails dans les démonstrations que nous laissons intentionnellement de côté, pour que vous les travailliez par vous-mêmes, seront colorés en bleu. Demandez aux assistants (en personne/sur le forum) si vous avez besoin d'aide.

Table des matières :

Cours 1

1.1

Le changement est l'une des choses les plus intéressantes et importantes en mathématiques. Formellement, la façon dont nous l'abordons est de considérer un ensemble X, et d'interpréter une fonction

$$f : X \to X$$

comme une transformation de X. En termes simples, si x est un élément de l'ensemble X avant la transformation, alors $f(x) \in X$ indique comment cet élément change après la transformation. Par exemple :

- Soit $X = \{0, 1, \ldots, n-1\}$ l'ensemble des sommets d'un n-gone régulier, et soit $f : X \to X$ une rotation ou une réflexion qui préserve l'intégrité du n-gone. Cependant, f peut modifier les sommets individuels, par exemple il peut envoyer le sommet $x \in X$ vers le sommet $f(x) \in X$.

- Imaginez que vous ayez n emplacements indexés par l'ensemble $X = \{1, \ldots, n\}$, et que vous étiquetiez chaque emplacement avec un post-it. Une **permutation** est une fonction $f : X \to X$ qui contrôle comment les post-its sont déplacés d'un emplacement à un autre, mais sans qu'il y ait plus ou moins d'un post-it par emplacement. Mathématiquement, la fonction f encode le fait que nous déplaçons le post-it de l'emplacement $f(x)$ à l'emplacement x, pour chaque $x \in X$.

1.2

Alors, que se passe-t-il lorsque nous avons deux transformations

$$f : X \to X \quad \text{et} \quad g : X \to X$$

et que nous voulons les appliquer successivement ? C'est très simple : appliquer d'abord la transformation g puis f ensuite revient à appliquer directement la

$$\textbf{composition} \quad \boxed{f \circ g : X \to X} \quad \text{définie par } (f \circ g)(x) = f(g(x)),\ \forall x \in X \tag{1}$$

Dans le premier exemple de la page précédente, cela signifierait que nous appliquons

- deux rotations, ou
- deux réflexions, ou
- une rotation et une réflexion, ou
- une réflexion et une rotation

successivement. Si vous dessinez une image de cela, vous observerez que la transformation résultante dans les quatre cas ci-dessus sera une rotation, une rotation, une réflexion, une réflexion, respectivement.

1.3

Que dire de la question de savoir quand une transformation peut être "inversée", c'est-à-dire au lieu de passer de x à $f(x)$, nous passons de $f(x)$ à x, pour tout $x \in X$? Mathématiquement, cela est modélisé par la notion de transformation inversible, à savoir une fonction $f : X \to X$ qui a un **inverse**

$$\boxed{f^{-1} : X \to X} \tag{2}$$

dont la propriété définissante est que

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X \tag{3}$$

Ci-dessus et par la suite, nous écrivons

$$\boxed{\mathrm{Id}_X : X \to X} \tag{4}$$

pour désigner la fonction **identité** qui envoie chaque $x \in X$ sur lui-même. Intuitivement, l'identité ne change rien, mais nous la considérons tout de même comme une "transformation". Elle a la propriété que

$$f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f \tag{5}$$

pour toute fonction $f : X \to X$.

Lemme 1. *Si une fonction $f : X \to X$ a un inverse, alors cet inverse est unique.*

Proof. Supposons que la fonction f ait deux inverses $g_1 : X \to X$ et $g_2 : X \to X$. La formule (2) implique que

$$f(g_1(x)) = g_1(f(x)) = x \tag{6}$$

$$f(g_2(x)) = g_2(f(x)) = x \tag{7}$$

pour tout $x \in X$. Si nous appliquons la formule (6) avec x remplacé par $g_2(x)$, nous en déduisons que

$$g_1(f(g_2(x)) = g_2(x)$$

pour tout $x \in X$. Cependant, si nous appliquons la fonction g_1 des deux côtés de (7), nous en déduisons que

$$g_1(f(g_2(x)) = g_1(x)$$

pour tout $x \in X$. La comparaison des deux égalités ci-dessus implique que $g_1(x) = g_2(x)$ pour tout $x \in X$, c'est-à-dire que les "deux" inverses g_1 et g_2 sont en fait une seule et même fonction.

□

1.4

Il pourrait sembler que la preuve ci-dessus repose sur une série d'astuces mathématiques, mais ce n'est pas vraiment le cas. En fait, le Lemme 1 découle du fait qu'une fonction $f : X \to X$ est inversible si et seulement si elle est **bijective**, ce qui signifie qu'elle est à la fois

- **injective :** lorsque $x \neq x'$ sont des éléments de X, nous avons $f(x) \neq f(x')$, et

- **surjective :** pour tout $y \in X$, il existe un $x \in X$ tel que $f(x) = y$.

Si une fonction est bijective, alors pour tout y, il existe un unique x tel que $f(x) = y$. Les formules (2) nous obligent alors à définir $f^{-1}(y) = x$, ce qui implique que l'inverse est déterminé de manière unique. Cela donne un argument intuitif pour la validité du Lemme 1.

1.5

L'un des grands avantages de l'utilisation des mathématiques pour formaliser les transformations est qu'elle facilite les calculs avec elles. Par exemple, rappelons l'exemple donné dans la première puce de la sous-section 1.1 : une rotation préserve un n-gone régulier P si et seulement si nous tournons dans le sens antihoraire d'un angle de $\frac{2\pi k}{n}$ radians autour du centre de P pour un certain entier k. En termes de formules, la fonction correspondante sur l'ensemble des sommets $\{0, 1, \ldots, n-1\}$ prend la forme suivante :

$$f_k : X \to X, \qquad f_k(x) = x + k \bmod n \tag{8}$$

(rappelons que $z \bmod n$ désigne le reste de la division de l'entier z par le nombre naturel n, et que ce reste est un élément de l'ensemble $\{0, 1, \ldots, n-1\}$). Bien que l'entier k puisse être arbitraire, seule sa classe résiduelle modulo n importe dans la formule (8), puisque $f_k = f_{k+n}$ pour tout $k \in \mathbb{Z}$. Géométriquement, cela signifie que

$$\frac{2\pi k}{n} \text{ radians est le même angle que } \frac{2\pi(k+n)}{n} = \frac{2\pi k}{n} + 2\pi \text{ radians.}$$

Les réflexions qui préservent le n-gone régulier P correspondent aux fonctions

$$g_k : X \to X, \qquad g_k(x) = -x + k \bmod n \tag{9}$$

pour un certain entier k. Comme auparavant, seule la classe résiduelle de k modulo n importe, car $g_k = g_{k+n}$ pour tout $k \in \mathbb{Z}$. Ainsi, nous avons exactement n rotations et n réflexions qui préservent le n-gone régulier, et les formules (8) et (9) nous fournissent tous les outils nécessaires pour les manipuler. Par exemple, nous pouvons calculer explicitement la composition de deux réflexions g_k et g_ℓ par

$$g_k \circ g_\ell(x) = g_k(g_\ell(x)) = g_k(-x + \ell \bmod n) = x + k - \ell \bmod n$$

et le résultat est clairement une rotation (de $\frac{2\pi(k-\ell)}{n}$ radians).

1.6

Utilisons maintenant des formules pour décrire l'exemple des permutations, c'est-à-dire le deuxième point de la Sous-section 1.1. Les permutations (pour $n = 6$ dans les exemples ci-dessous) seront représentées comme

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 6 & 5 & 3 \end{pmatrix} \tag{10}$$

ce qui signifie que nous déplaçons le post-it numéro 4 à la position 1, le post-it numéro 2 à la position 2, le post-it numéro 1 à la position 3, etc. La composition des permutations est calculée en empilant les permutations les unes sur les autres. Par exemple, si nous essayons de calculer $f \circ g$ où f est donné par la formule (10) et g est donné par la formule

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

nous calculons $f \circ g$ en plaçant g au-dessus (car il est appliqué en premier) et f en dessous (car il est appliqué en second ; notez que nous réarrangeons les colonnes de f pour que sa ligne supérieure soit compatible avec la ligne inférieure de g)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 2 & 4 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix} \qquad \Rightarrow \qquad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$$

Quant à la permutation inverse f^{-1}, elle est calculée en échangeant les deux lignes de (10) puis en réordonnant les colonnes afin d'avoir les numéros sur la ligne supérieure dans l'ordre croissant :

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 5 & 4 \end{pmatrix}$$

La permutation identité est simplement $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$.

1.7

La composition des transformations possède trois propriétés importantes : l'existence de la fonction identité (4) satisfaisant la propriété (5), l'existence des inverses (2) satisfaisant la propriété (3), ainsi que

$$\boxed{f \circ (g \circ h) = (f \circ g) \circ h} \tag{11}$$

pour toutes les fonctions $f, g, h : X \to X$. En effet, les deux côtés de la formule (11) représentent la fonction $x \mapsto f(g(h(x)))$, ce qui implique qu'ils sont égaux. La propriété (11) est appelée **associativité**. Les caractéristiques des compositions de fonctions énumérées ci-dessus peuvent être abstraites, comme dans la notion suivante.

Définition 1. *Un* ***groupe*** *(comme vous l'avez appris en Math 113) est un ensemble G doté de*

- *un élément $e \in G$ appelé* ***identité***
- *pour tout élément $g \in G$, un élément $g^{-1} \in G$ appelé* ***inverse***
- *pour deux éléments quelconques $g, h \in G$, un élément $gh \in G$ appelé le* ***produit*** *de g et h.*

qui doivent satisfaire les propriétés suivantes

$$ge = eg = g, \qquad \forall g \in G \tag{12}$$

$$gg^{-1} = g^{-1}g = e, \qquad \forall g \in G \tag{13}$$

$$g(g'g'') = (gg')g'', \quad \forall g, g', g'' \in G \tag{14}$$

Deux exemples importants de groupes (qui correspondent aux deux points de la Sous-section 1.1, et que vous avez appris en Math 113) sont le **groupe diédral**

$$\boxed{D_{2n}} = \Big\{\text{rotations et réflexions qui préservent un } n\text{-gone régulier}\Big\} \tag{15}$$

et le **groupe symétrique**

$$\boxed{S_n} = \Big\{\text{permutations, c'est-à-dire bijections } \{1,\dots,n\} \to \{1,\dots,n\}\Big\} \tag{16}$$

Dans les deux cas, l'identité est la fonction identité, l'inverse est donné par les fonctions inverses, et le produit des éléments est donné par la composition des fonctions. Rappelez-vous que $|D_{2n}| = 2n$ (il y a exactement n rotations et n réflexions qui préservent un n-gone régulier) tandis que $|S_n| = n!$. Tant D_n que S_n sont des groupes **finis**, en ce sens qu'ils ont un nombre fini d'éléments.

1.8

Les formules (12), (13), (14) ne sont pas seulement similaires de manière coïncidente à (4), (2), (11), mais les premières sont modélisées après les secondes. En d'autres termes, les groupes sont simplement les structures mathématiques abstraites qui décrivent les transformations de divers ensembles X. Cette connexion est rendue encore plus concrète par la notion suivante, qui est centrale dans de nombreux domaines des mathématiques (comme la théorie de la représentation).

Définition 2. *Une action d'un groupe G sur un ensemble X est une attribution*

$$\forall g \in G \quad \rightsquigarrow \quad \textit{une bijection } \Phi_g : X \to X \tag{17}$$

qui respecte

- *l'identité, au sens où*
$$\Phi_e = \mathrm{Id}_X \tag{18}$$
- *l'inverse, au sens où*
$$\Phi_{g^{-1}} = (\Phi_g)^{-1}, \qquad \forall g \in G \tag{19}$$
- *le produit, dans le sens où*
$$\Phi_{gg'} = \Phi_g \circ \Phi_{g'}, \quad \forall g, g' \in G \tag{20}$$

Nous indiquerons une action, c'est-à-dire l'attribution (17), par le symbole

$$\boxed{G \curvearrowright X} \tag{21}$$

Bien que plutôt imprécis, nous abrégerons désormais les bijections Φ_g par le symbole

$$\boxed{\Phi_g(x) = g \cdot x}$$

pour tous $g \in G, x \in X$. Dans cet esprit, la formule (18) prend la forme $e \cdot x = x$, tandis que (20) se lit

$$(gg') \cdot x = g \cdot (g' \cdot x) \tag{22}$$

pour tous $g, g' \in G$ et tout $x \in X$.

Remarque. *Notez que les propriétés* (18) *et* (19) *sont en réalité superflues, c'est-à-dire qu'elles découlent de* (20) *et du fait que toutes les* Φ_g *sont des bijections. En effet, il suffit d'appliquer* (20) *pour* $g' = e$ *et vous obtiendrez*

$$\Phi_g = \Phi_{ge} = \Phi_g \circ \Phi_e$$

Composer avec $(\Phi_g)^{-1}$ *implique précisément* (18). *Ensuite, si nous invoquons* (22) *pour* $g' = g^{-1}$ *nous obtenons*

$$\mathrm{Id}_X = \Phi_e = \Phi_{gg^{-1}} = \Phi_g \circ \Phi_{g^{-1}}$$

ce qui implique (19).

1.9

Par leur construction même (mais vous êtes encouragé à vérifier cela rigoureusement), les exemples des deux points de la Sous-section 1.1 sont équivalents à des actions

$$D_{2n} \curvearrowright \Big\{\text{sommets d'un } n\text{-gone régulier}\Big\} \tag{23}$$

et

$$S_n \curvearrowright \{1, \ldots, n\} \tag{24}$$

respectivement. En fait, le dernier exemple peut être généralisé comme suit.

Définition 3. *Pour tout ensemble* X*, nous définissons*

$$S_X = \Big\{\textit{bijective } X \to X\Big\}$$

en le transformant en un groupe en utilisant la composition des fonctions. Il y a alors une action

$$S_X \curvearrowright X$$

simplement en faisant agir chaque bijection $\sigma \in S_X$ *sur* X *par* σ *elle-même.*

En plus des exemples d'actions ci-dessus, il y a deux actions spéciales d'un groupe sur lui-même, comme suit.

Définition 4. *Pour chaque groupe* G*, son* ***action à gauche*** $G \curvearrowright G$ *est l'attribution*

$$h \cdot g = hg, \quad \forall g, h \in G \tag{25}$$

Définition 5. *Pour chaque groupe* G*, son* ***action adjointe*** $G \curvearrowright G$ *est l'attribution*

$$h \cdot g = hgh^{-1}, \quad \forall g, h \in G \tag{26}$$

Proposition 1. *Les attributions* (25) *et* (26) *sont des actions bien définies.*

Proof. Comme nous l'avons montré à la fin de la Sous-section 1.8, il suffit de vérifier que chaque Φ_g est une bijection, et que la formule (22) est vérifiée. Nous le ferons pour l'action adjointe, et laisserons le cas analogue de l'action à gauche comme un exercice pour vous. Pour vérifier que $g \mapsto hgh^{-1}$ est une fonction bijective de g pour chaque h fixé dans G, notez que

$$hgh^{-1} = hg'h^{-1} \quad \Rightarrow \quad hg = hg' \quad \Rightarrow \quad g = g'$$

ce qui prouve l'injectivité, tandis que

$$h(h^{-1}gh)h^{-1} = (hh^{-1})g(hh^{-1}) = ege = g, \quad \forall g \in G$$

ce qui prouve la surjectivité. Enfin, pour montrer (22), nous notons que

$$(hh') \cdot g = hh'gh'^{-1}h^{-1} = h(h'gh'^{-1})h^{-1} = h \cdot (h' \cdot g)$$

pour tous $g, h, h' \in G$, comme requis. Notez que toutes ces vérifications ont fait un usage important de l'associativité.

□

1.10

Explorons maintenant comment la notion d'action interagit avec la notion d'homomorphisme de groupes, que vous avez appris en Math 113.

Définition 6. *Soit G et G' deux groupes, chacun avec ses propres notions d'élément neutre, d'inverse et de produit. Une fonction*

$$f : G \to G'$$

est appelée un ***homomorphisme*** *si elle préserve*

- *les éléments neutres, dans le sens où*
$$f(e) = e' \tag{27}$$
où e est l'unité dans G et e' est l'unité dans G'

- *les inverses, dans le sens où*
$$f(g^{-1}) = (f(g))^{-1} \tag{28}$$
avec le côté gauche impliquant l'inverse dans G et le côté droit impliquant l'inverse dans G'.

- *les produits, dans le sens où*
$$f(gh) = f(g)f(h) \tag{29}$$
avec le côté gauche impliquant le produit dans G et le côté droit impliquant le produit dans G'.

Comme auparavant, certaines des propriétés (27), (28) et (29) sont superflues : soit la première, soit la seconde d'entre elles découlent des deux autres. Essayez de prouver cela pour vous entraîner.

1.11

Un homomorphisme qui est également une fonction bijective est appelé un **isomorphisme**. S'il existe un isomorphisme entre deux groupes G et G', nous le noterons

$$\boxed{G \cong G'} \tag{30}$$

et nous dirons que G et G' sont isomorphes.

Lemme 2. *Si $f : G \to G'$ est un isomorphisme entre deux groupes G et G', alors son inverse*

$$f^{-1} : G' \to G$$

est également un isomorphisme.

Proof. L'inverse d'une bijection est une bijection, il reste donc à montrer que l'inverse est également un homomorphisme. Comme nous l'avons expliqué à la fin de la Sous-section 1.10, il suffit de vérifier (27) (ce qui est évident, puisque le fait que $f(e) = e'$ implique $f^{-1}(e') = e$) et (29). En effet, (29) découle de

$$gh = (f^{-1} \circ f)(gh) = f^{-1}(f(gh)) = f^{-1}(f(g)f(h))$$

pour tous $g, h \in G$. Si nous remplaçons g et h par $f^{-1}(g)$ et $f^{-1}(h)$ dans la relation ci-dessus, nous obtenons

$$f^{-1}(g)f^{-1}(h) = f^{-1}(f(f^{-1}(g))f(f^{-1}(h))) = f^{-1}(gh)$$

ce qui est exactement ce que nous avions besoin de prouver.

□

1.12

Le formalisme des groupes, des actions et des homomorphismes se regroupe dans le résultat suivant.

Proposition 2. *Donner une action d'un groupe G sur un ensemble X est équivalent à donner un homomorphisme*

$$G \to S_X \tag{31}$$

(rappelez-vous le groupe S_X dans la Définition 3).

Proof. Il est clair que l'attribution $g \rightsquigarrow \Phi_g$ correspond à une fonction (31). Montrer que la première attribution étant une action est équivalente à la dernière fonction étant un homomorphisme revient à montrer que les propriétés (18), (19), (22) correspondent à (27), (28), (29). Cela est une tautologie, c'est-à-dire une déclaration mathématique qui est évidente une fois déballée (bien que le déballage soit un exercice utile; essayez de le faire et demandez à un de vos assistants si vous êtes bloqué).

□

Cours 2

2.1

Soit G un groupe. Rappelons de Math 113 qu'un sous-ensemble $H \subseteq G$ est appelé un **sous-groupe**, noté

$$\boxed{H \leq G} \tag{32}$$

si H est fermé sous

- l'identité, dans le sens où $e \in H$
- l'inverse, dans le sens où $g \in H$ implique $g^{-1} \in H$
- le produit, dans le sens où $g, g' \in H$ implique $gg' \in H$

Si les conditions ci-dessus sont satisfaits, alors H est aussi un groupe, et la fonction d'inclusion

$$\iota : H \hookrightarrow G$$

est un homomorphisme. En général, pour tout homomorphisme

$$f : G \to G'$$

l'image de f est un sous-groupe de G'. De plus, si f est injectif, alors $\boxed{\text{Im } f \cong G}$.

2.2

Nous allons maintenant voir comment le langage des actions nous permet de décrire des caractéristiques générales des groupes. Le théorème suivant est dû à Cayley.

Théorème 1. *Tout groupe G est un **groupe de permutations**, c'est-à-dire un sous-groupe de S_X pour un certain ensemble X.*

Ainsi, tout groupe peut être réalisé comme vivant à l'intérieur d'un certain groupe de permutations (si G est fini, nous verrons que l'ensemble X peut être choisi fini, et donc tout groupe fini est un sous-groupe du groupe symétrique S_n pour un certain $n \in \mathbb{N}$). À cette fin, considérons toute action $G \curvearrowright X$ et rappelons l'homomorphisme (31). Le résultat suivant est facile, vous l'avez prouvé dans Math 113.

Lemme 3. *Un homomorphisme $f : G \to G'$ est injectif si et seulement si son noyau*

$$\boxed{\text{Ker } f} = \left\{ g \in G \text{ tel que } f(g) = e' \right\}$$

*est le **sous-groupe trivial** $\{e\} \leq G$.*

Avec le Lemme ci-dessus à l'esprit, nous voyons que (31) est injectif si et seulement si son noyau est trivial. Cependant, dans le contexte d'une action de groupe, ce noyau peut être décrit explicitement comme

$$\Big\{ g \in G \Big| g \cdot x = x, \forall x \in X \Big\}$$

et il est appelé le **noyau de l'action**. En d'autres termes, le noyau de l'action se compose de tous les éléments de G qui agissent sur X par la transformation identité. Ainsi, pour prouver le Théorème 1, il suffit de trouver une action de G dont le noyau est juste le sous-groupe trivial, c'est-à-dire que seul l'élément identité de G agit sur X par la transformation identité (une telle action est appelée **fidèle**). À cette fin, nous choisissons simplement l'action à gauche de G sur $X = G$ de la Définition 4 : tout élément $g \neq e$ de G agit sur G en envoyant e vers g, et donc ne peut pas agir par la transformation identité.

2.3

Toute action $G \curvearrowright X$ induit une relation d'équivalence sur X via

$$x \sim y \quad \Leftrightarrow \quad \exists g \in G \text{ tel que } g \cdot x = y \tag{33}$$

Les propriétés (18), (19) et (20) garantissent précisément que la relation d'équivalence ci-dessus est réflexive, symétrique et transitive, respectivement (essayez de le prouver vous-même, c'est un excellent exercice).

Définition 7. *Une classe d'équivalence par rapport à la relation* (33) *est appelée une* ***orbite*** *de l'action $G \curvearrowright X$. Elle peut s'écrire comme*

$$\boxed{G \cdot x} = \Big\{ g \cdot x \Big| g \in G \Big\} \tag{34}$$

et elle sera appelée l'orbite de x (bien que tout autre $y \sim x$ ait la même orbite que x).

Une action est appelée **transitive** si tous les éléments de X sont dans une seule et même orbite.

Définition 8. *Étant donné une action $G \curvearrowright X$ et tout élément $x \in X$, son* ***stabilisateur*** *est défini comme*

$$\boxed{\mathrm{Stab}_G(x)} = \Big\{ g \in G \text{ tel que } g \cdot x = x \Big\} \tag{35}$$

Prouvez par vous-même que le stabilisateur est toujours un sous-groupe de G.

Le noyau d'une action de groupe, que nous avons déjà rencontré, est par définition l'intersection des stabilisateurs de tous les éléments $x \in X$. Une action est appelée **libre** si tous les stabilisateurs sont égaux à $\{e\}$. Par exemple, l'action (23) est transitive, mais elle n'est pas libre (car il existe des sommets qui sont préservés par des réflexions). Cependant, l'action du sous-groupe des rotations dans D_{2n} sur les sommets est libre.

2.4

Comme pour toute relation d'équivalence, X peut être partitionné en l'union disjointe des orbites d'une action de groupe $G \curvearrowright X$. Cependant, nous pouvons en dire plus lorsque G est fini.

Proposition 3. *Si $G \curvearrowright X$ est une action d'un groupe fini G sur un ensemble X, alors nous avons*

$$|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|} \tag{36}$$

pour chaque $x \in X$.

Le résultat ci-dessus est appelé le **théorème orbite-stabilisateur**. Lorsque G et X sont finis, le fait que X soit l'union disjointe de ses orbites signifie que (36) implique l'équation suivante

$$|X| = \sum_{\text{orbites } G\cdot x} |G \cdot x| = \sum_{\text{orbites } G\cdot x} \frac{|G|}{|\mathrm{Stab}_G(x)|} \tag{37}$$

(tandis que l'ensemble $\mathrm{Stab}_G(x)$ peut changer lorsqu'on modifie x au sein d'une orbite donnée, sa cardinalité ne change pas ; essayez de prouver la déclaration précédente, bien que cela découle implicitement de la preuve ci-dessous).

Proof. de la Proposition 3 : rappelez-vous la description des orbites de (34). Pour un $x \in X$ fixe, la fonction

$$G \to G \cdot x, \qquad g \mapsto g \cdot x \tag{38}$$

est surjective. Calculons combien d'éléments se trouvent dans l'antécédent de tout élément $g \cdot x$ de la fonction (38). En d'autres termes, nous cherchons à compter combien de $g' \in G$ ont la propriété que

$$g' \cdot x = g \cdot x \quad \Leftrightarrow \quad g^{-1}g' \cdot x = x \quad \Leftrightarrow \quad g^{-1}g' \in \mathrm{Stab}_G(x) \quad \Leftrightarrow \quad g' \in \left\{ gh \middle| h \in \mathrm{Stab}_G(x) \right\}$$

Comme les éléments gh (à mesure que h varie) sont tous distincts (prouvez cela), il y a $|\mathrm{Stab}_G(x)|$ éléments dans l'antécédent de chaque élément par rapport à la fonction (38). Cela prouve immédiatement (36). □

2.5

Continuons à travailler dans le contexte d'une action d'un groupe G sur un ensemble X. Tandis que le stabilisateur (35) décrit l'ensemble des éléments de G qui fixent un certain élément $x \in X$, il existe la notion duale de l'ensemble des éléments de X qui sont fixés par un $g \in G$ donné par

$$\boxed{X^g} = \left\{ x \in X \middle| g \cdot x = x \right\} \tag{39}$$

En général, tout ce que nous pouvons dire est que X^g est un sous-ensemble de X. Mais lorsque X est fini, nous avons la formule suivante souvent appelée "Lemme de Burnside", bien qu'elle remonte à Cauchy et Frobenius. C'est un comptage très utile du nombre d'orbites dans une action de groupe

Lemme 4. *Si G est un groupe fini agissant sur un ensemble fini X, alors*

$$\Big|\text{orbites de } G \curvearrowright X\Big| = \sum_{g\in G} \frac{|X^g|}{|G|} \tag{40}$$

Proof. Le Lemme est un exercice combinatoire simple. En particulier, réécrivons (40) comme

$$|G| \cdot |\text{orbites de } G \curvearrowright X| = \sum_{g\in G} |X^g| \tag{41}$$

Le côté droit compte le nombre de paires

$$(g, x) \in G \times X \text{ tel que } g \cdot x = x$$

Si nous interprétons ce nombre comme une somme sur $x \in X$, nous concluons que le côté droit de (41) est

$$\sum_{x\in X} |\mathrm{Stab}_G(x)|$$

En utilisant la Proposition 3, nous voyons que le nombre ci-dessus est

$$\sum_{x\in X} \frac{|G|}{|G \cdot x|}$$

Nous pouvons remplacer la somme sur $x \in X$ par une somme sur les orbites ; cependant, chaque orbite $G \cdot x$ apparaît un nombre de $|G \cdot x|$ fois dans la somme ci-dessus, nous concluons donc que le nombre ci-dessus est

$$\sum_{\text{orbites } G\cdot x} |G|$$

ce qui est précisément le côté gauche de (41). □

2.6

Lorsque H est un sous-groupe d'un groupe G, les orbites de l'action à gauche

$$H \curvearrowright G, \qquad h \cdot g = hg$$

sont appelées **classes à droite**. La terminologie légèrement inhabituelle est due au fait que les orbites en question sont explicitement données par la formule

$$\boxed{Hg} = \Big\{hg\Big|h \in H\Big\} \tag{42}$$

où g est à droite. La notion duale correspondante provient de l'action dite **à droite**

$$H \curvearrowright G, \qquad h \cdot g = gh^{-1}$$

(veuillez vérifier que la formule ci-dessus satisfait toutes les propriétés d'une action, tout comme nous l'avons fait pour l'action à gauche de la Définition 4) dont les orbites sont appelées **classes à gauche**

$$\boxed{gH} = \Big\{gh\Big|h \in H\Big\}. \tag{43}$$

En effet, à mesure que h varie dans H, l'ensemble des éléments de la forme gh^{-1} correspond à l'ensemble des éléments de la forme gh, en raison du fait que le sous-groupe $H \leq G$ est fermé sous la prise d'inverses. Les actions à gauche et à droite sont toutes deux libres, en ce sens que

$$\text{Stab}_H(g) = \{e\}, \quad \text{car } hg = g \text{ ou } gh^{-1} = g \text{ si et seulement si } h = e \tag{44}$$

pour tout $g \in G$.

Définition 9. *Soit* $\boxed{G/H}$ *(respectivement* $\boxed{H\backslash G}$*) l'ensemble des classes à gauche (respectivement à droite) de* G *par rapport à un sous-groupe* H*.*

Supposons maintenant que G soit fini, et que $H \leq G$ soit un sous-groupe quelconque. En raison de (44), la Proposition 3 implique que chaque classe à gauche ou à droite contient exactement $|H|$ éléments. Puisque G est partitionné en classes à gauche ou à droite, nous concluons que le nombre de ces classes est exactement

$$|G/H| = |H\backslash G| = \frac{|G|}{|H|} \tag{45}$$

On désigne souvent le nombre ci-dessus par $\boxed{[G : H]}$ et on l'appelle l'**indice** du sous-groupe H de G.

2.7

Rappelez-vous de Math 113 que l'**ordre** d'un groupe fini est sa cardinalité, c'est-à-dire son nombre d'éléments. Dans ce contexte, (45) implique un résultat fondamental dans la théorie des groupes finis dû à Lagrange

l'ordre d'un groupe G est un multiple des ordres de chacun de ses sous-groupes (46)

En particulier, nous pouvons prendre n'importe quel $g \in G$ et considérer le sous-groupe de G engendré par g, c'est-à-dire

$$H := \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\} \subseteq G$$

Si nous supposons que G est fini, alors le sous-groupe H ci-dessus doit également être fini. Cela implique notamment qu'il existe des entiers $a < b$ tels que $g^a = g^b$, donc $g^{b-a} = e$. Cela implique que l'**ordre** de g, à savoir

$$\boxed{|g|} = \min\left\{d > 0 \text{ t.q. } g^d = e\right\} \tag{47}$$

est bien défini. Si g a pour ordre d, alors nous avons un isomorphisme

$$\mathbb{Z}/d\mathbb{Z} \cong H, \qquad (k \bmod d) \mapsto g^k$$

où nous rappelons que $\mathbb{Z}/d\mathbb{Z}$ est un groupe par rapport à l'addition. Dans le cas particulier qui nous intéresse, le théorème de Lagrange (46) implique que l'ordre de tout élément d'un groupe divise l'ordre de l'ensemble du groupe. Cela impose des restrictions importantes sur les groupes finis et leurs éléments.

2.8

Maintenant que nous avons étudié les orbites des actions à gauche et à droite (d'un sous-groupe sur un groupe), considérons l'action adjointe d'un groupe G sur lui-même

$$G \curvearrowright G, \qquad h \cdot g = hgh^{-1}, \ \forall g, h \in G$$

Les éléments dans la même orbite sont appelés **conjugués**, et les orbites elles-mêmes sont appelées **classes de conjugaison** (vous en avez entendu parler dans Math 113). Plus précisément, la classe de conjugaison de $g \in G$ est l'ensemble

$$\left\{ hgh^{-1} \middle| h \in G \right\} \tag{48}$$

En parallèle, le stabilisateur de g par rapport à l'action adjointe est appelé son **centralisateur**

$$\boxed{C_G(g)} = \left\{ h \in G \text{ t.q. } hg = gh \right\}. \tag{49}$$

Proposition 4. *Si g et g' sont conjugués dans un groupe G, alors leurs centralisateurs sont isomorphes.*

Proof. Si $g' = hgh^{-1}$, alors l'application $x \mapsto h^{-1}xh$ donne un isomorphisme $C_G(g') \to C_G(g)$. □

Ainsi, nous nous référerons souvent au centralisateur d'une classe de conjugaison $\widetilde{g} \subseteq G$, noté $C_G(\widetilde{g})$, comme à la classe d'isomorphisme du centralisateur de n'importe quel élément $g \in \widetilde{g}$.

2.9

Lorsque le groupe G est fini, la formule (37) pour l'action adjointe implique la formule

$$|G| = \sum_{\text{classes de conjugaison } \widetilde{g}} |\widetilde{g}| \tag{50}$$

appelée l'**équation des classes** de G. Cependant, la Proposition 3 pour l'action adjointe implique que

$$|\widetilde{g}| = \frac{|G|}{|\mathrm{Stab}_G(\widetilde{g})|}. \tag{51}$$

En gardant à l'esprit que les stabilisateurs ne sont autres que les centralisateurs, nous avons

$$|\widetilde{g}| = \frac{|G|}{|C_G(\widetilde{g})|}. \tag{52}$$

Notez que dans les formules ci-dessus, nous faisons référence au stabilisateur/centralisateur d'une classe de conjugaison. En effet, deux éléments d'une même classe de conjugaison $\widetilde{g}$ ont des centralisateurs isomorphes (selon la Proposition 4), et nous pouvons donc définir sans ambiguïté $\mathrm{Stab}_G(\widetilde{g}) = C_G(\widetilde{g})$ à un isomorphisme près. En particulier, l'ordre de ce stabilisateur/centralisateur est bien défini, quel que soit l'élément $g \in \widetilde{g}$ que nous choisissons pour le définir. En combinant les formules ci-dessus, nous obtenons la version équivalente de (50), que nous appellerons également l'équation des classes de G

$$1 = \sum_{\text{classes de conjugaison } \widetilde{g}} \frac{1}{|C_G(\widetilde{g})|} \tag{53}$$

2.10

Appliquons maintenant toutes les notions ci-dessus aux deux principaux exemples de groupes que nous avons étudiés dans la Sous-section 1.1. Rappelons le groupe diédral D_{2n} composé de rotations et de réflexions qui préservent un n-gone régulier. Le sous-ensemble des n rotations est en fait un sous-groupe de D_{2n} (essayez de justifier pourquoi : vous devez vous convaincre que l'identité est une rotation, que l'inverse d'une rotation est une rotation, et que la composition des rotations est une rotation), et en fait il n'est pas difficile de se convaincre que ce sous-groupe est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Ainsi, nous avons un homomorphisme injectif

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow D_{2n}, \qquad (k \bmod n) \mapsto \left(\text{rotation de } \frac{2\pi k}{n} \text{ radians}\right)$$

Travaillons maintenant sur les classes de conjugaison du groupe diédral dans un petit exemple, disons

$$D_6 = \Big\{ \underbrace{e, \sigma, \sigma^2}_{\text{rotations}}, \underbrace{\tau, \sigma\tau, \sigma^2\tau}_{\text{réflexions}} \Big\}$$

(recall from Math 113 que nous avons les formules $\tau^2 = \sigma^3 = e$ et $\sigma\tau = \tau\sigma^{-1}$). L'élément neutre est toujours seul dans sa classe de conjugaison

$$\{e\}$$

et son centralisateur est toujours le groupe entier, qui dans ce cas a pour ordre 6. Pendant ce temps, les deux rotations non triviales

$$\{\sigma, \sigma^2\}$$

forment leur propre classe de conjugaison, car $\sigma^2 = \sigma^{-1} = \tau^{-1}\sigma\tau$. Le centralisateur de l'une de ces rotations est le sous-groupe des rotations, qui a pour ordre 3 (vérifiez cela en utilisant les symboles σ et τ). Enfin, les réflexions

$$\{\tau, \tau\sigma, \tau\sigma^2\}$$

sont toutes conjuguées entre elles, car $\tau\sigma = \sigma\tau\sigma^{-1}$ et $\tau\sigma^2 = \sigma^{-1}\tau\sigma$. Le centralisateur de chaque réflexion est simplement le sous-groupe d'ordre 2 consistant en l'élément neutre et la réflexion elle-même (vérifiez cela en utilisant les symboles σ et τ). Avec cela à l'esprit, l'équation des classes (53) devient

$$1 = \frac{1}{6} + \frac{1}{3} + \frac{1}{2} \tag{54}$$

ce qui est assurément une affirmation vraie.

2.11

Considérons maintenant le groupe symétrique S_n. Comme vous l'avez appris dans Math 113, chaque permutation $\sigma \in S_n$ peut être écrite comme un produit disjoint de cycles, par exemple

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 8 & 6 & 5 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 6)(2\ 7)(3\ 8)(5)$$

Ainsi, à la permutation σ, nous pouvons associer son **type cyclique**, qui est l'ensemble des longueurs de ses cycles en ordre décroissant. Dans l'exemple ci-dessus, le type cyclique est $3 \geq 2 \geq 2 \geq 1$, car il y a un cycle de longueur 3, deux cycles de longueur 2, et un cycle de longueur 1.

En général, le type cyclique d'une permutation $\sigma \in S_n$ sera une **partition** de n, c'est-à-dire une collection d'entiers positifs

$$\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k)$$

avec une somme totale $|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_k$ égale à n.

Proposition 5. *Deux éléments de S_n sont conjugués si et seulement s'ils ont le même type cyclique.*

Proof. Cet exercice est plus facile qu'il n'y paraît, et il repose sur le fait que si nous considérons $\sigma, \tau \in S_n$ comme des bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$, alors

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix} \qquad \Longrightarrow \qquad \tau\sigma\tau^{-1} = \begin{pmatrix} \ldots & \tau(i) & \ldots \\ \ldots & \tau(\sigma(i)) & \ldots \end{pmatrix}$$

Ainsi, il existe une correspondance biunivoque entre les cycles $i_1 \to i_2 \to \cdots \to i_k \to i_1$ de la permutation σ et les cycles $\tau(i_1) \to \tau(i_2) \to \cdots \to \tau(i_k) \to \tau(i_1)$ de la permutation $\tau\sigma\tau^{-1}$. Cela montre immédiatement que toutes les partitions conjuguées ont le même type cyclique, mais cela montre aussi la réciproque : toute partition σ de type cyclique λ peut être écrite comme $\tau\sigma_\lambda\tau^{-1}$, où

$$\sigma_\lambda = (1\ 2\ \ldots\ \lambda_1)(\lambda_1 + 1\ \lambda_1 + 2\ \ldots\ \lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + 1\ \lambda_1 + \lambda_2 + 2\ \ldots\ \lambda_1 + \lambda_2 + \lambda_3)\ldots \quad (55)$$

et $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$ est la fonction qui envoie la séquence $(\lambda_1 + \cdots + \lambda_{i-1} + 1, \ldots, \lambda_1 + \cdots + \lambda_i)$ à l'un des cycles de σ de longueur λ_i, pour tout i.

□

Examinons maintenant l'équation des classes pour les groupes symétriques. À cette fin, nous devons déterminer l'ordre du centralisateur d'un élément donné dans chaque classe de conjugaison. Il suffit de le faire pour le représentant (55). Nous avons $\tau \in C_{S_n}(\sigma_\lambda)$ si et seulement si

$$\tau\sigma_\lambda\tau^{-1} = \sigma_\lambda$$

Comme nous l'avons vu dans la preuve de la Proposition 5, cela signifie que τ doit permuter les cycles de σ_λ de longueur i entre eux. Si nous notons $\#_\lambda^i$ le nombre de tels cycles, cela revient à $\#_\lambda^i!$ choix. Cependant, une fois que nous avons fixé le fait que τ prend un cycle γ de longueur i pour un autre cycle γ' de longueur i, nous avons la liberté supplémentaire de choisir quelle entrée particulière de γ' sera l'image de la première entrée du cycle γ. Cela équivaut à i choix pour chaque cycle de longueur i. Ainsi, nous concluons que

$$|C_{S_n}(\sigma_\lambda)| = \prod_{i \geq 1} i^{\#_\lambda^i} \#_\lambda^i!$$

Ne vous inquiétez pas du fait que le produit semble infini. Pour i assez grand, nous avons $\#_\lambda^i = 0$, et $i^0 0! = 1$. Avec cela à l'esprit, l'équation des classes (53) devient

$$1 = \sum_{\lambda \text{ une partition de } n} \frac{1}{\prod_{i \geq 1} i^{\#_\lambda^i} \#_\lambda^i!} \quad (56)$$

Par exemple, lorsque $n = 4$, la formule ci-dessus devient $1 = \frac{1}{24} + \frac{1}{4} + \frac{1}{8} + \frac{1}{3} + \frac{1}{4}$.

Cours 3

3.1

Considérons un groupe et un sous-groupe $H \leq G$. En général, les classes à gauche et à droite de G par rapport à H sont différentes. Mais dans le cas où elles sont égales, c'est-à-dire

$$\boxed{gH = Hg}, \qquad \forall g \in G \tag{57}$$

alors vous avez appris en Math 113 que nous appelons H un sous-groupe **normal** de G, et nous le notons $\boxed{H \trianglelefteq G}$.

Lemme 5. *Si $f : G \to G'$ est un homomorphisme quelconque, le noyau de f est un sous-groupe normal.*

Proof. La propriété (57) peut être réécrite comme

$$gHg^{-1} = H$$

pour tout $g \in G$. Lorsque $H = \text{Ker } f$, tout élément $h \in H$ est caractérisé par la propriété que $f(h) = e'$. Cependant, pour tout élément $g \in G$, cela équivaut à

$$f(ghg^{-1}) = f(g)e'f(g^{-1}) = f(g)f(g)^{-1} = e'$$

ce qui équivaut à $ghg^{-1} \in \text{Ker } f = H$.

□

Les propriétés importantes des sous-groupes normaux (que vous devez vérifier) sont les faits que

- si H_1 et H_2 sont normaux dans G, alors $H_1 \cap H_2$ est normal dans G
- si H est normal dans G, alors H est normal dans tout sous-groupe de G qui contient H

3.2

Vous vous souvenez peut-être de Math 113 que si $H \trianglelefteq G$ est un sous-groupe normal, alors l'ensemble des classes (à gauche ou à droite, puisqu'elles sont égales par normalité)

$$G/H$$

hérite d'une structure de groupe de G. Cette structure de groupe assure que la projection dite

$$\pi : G \to G/H, \quad g \mapsto [g]$$

est un homomorphisme. Le noyau de cet homomorphisme est évidemment H. Cela conduit à un résultat important appelé le **premier théorème d'isomorphisme**, que vous avez appris en Math 113.

Théorème 2. *Pour tout homomorphisme $f : G \to G'$, nous avons un isomorphisme*

$$G/\text{Ker } f \cong \text{Im } f \tag{58}$$

induit par $[g] \mapsto f(g)$, pour tout $g \in G$.

Exemple 1. *Prenons $G = \mathbb{Z}$ (muni de l'addition, souvent appelé le groupe **cyclique** infini) et $H = n\mathbb{Z}$ pour un certain entier naturel n. Ce dernier est un sous-groupe normal car $\mathbb{Z}$ est abélien (nous en parlerons plus tard) et tous les sous-groupes d'un groupe abélien sont normaux. Ensuite, nous avons*

$$G/H = \mathbb{Z}/n\mathbb{Z}$$

*qui est le groupe des résidus modulo n (souvent appelé le groupe **cyclique** d'ordre n). Plus généralement, vous pouvez choisir deux entiers naturels m et n et considérer l'homomorphisme*

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad f(k) = (mk \ mod \ n), \ \forall k \in \mathbb{Z}$$

Dans ce cas, Ker $f = \frac{n}{d}\mathbb{Z}$ *où* $d = \gcd(m, n)$*, donc le premier théorème d'isomorphisme* (58) *implique que le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ composé d'éléments qui sont des multiples de m est isomorphe à $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$. En particulier, si $d = 1$, tout élément de $\mathbb{Z}/n\mathbb{Z}$ est un multiple de m, ce qui implique qu'il existe $a \in \mathbb{Z}$ tel que $am \equiv 1$ modulo n. Cela implique à son tour qu'il existe $b \in \mathbb{Z}$ tel que*

$$am + bn = 1 \tag{59}$$

en tant qu'entiers, une propriété bien connue des nombres premiers entre eux m et n.

3.3

Les quotients ont une propriété importante par rapport aux actions de groupes. Supposons que nous ayons une action

$$G \curvearrowright X \tag{60}$$

et qu'un certain sous-groupe normal $H \trianglelefteq G$ agisse trivialement sur X, c'est-à-dire

$$h \cdot x = x, \qquad \forall h \in H, x \in X \tag{61}$$

(en d'autres termes, h est contenu dans le noyau de l'action). Alors, l'action (60) induit une action

$$\boxed{G/H \curvearrowright X} \tag{62}$$

donnée par la formule

$$[g] \cdot x = g \cdot x, \qquad \forall g \in G, x \in X \tag{63}$$

En effet, pour s'assurer que cette action est bien définie, il suffit de montrer que la formule (63) reste inchangée si l'on remplace g par gh pour un $h \in H$ quelconque. Cependant, cela découle immédiatement du fait que $(gh) \cdot x = g \cdot (h \cdot x)$ et de l'hypothèse (61).

Remarque. *Si nous prenons H comme noyau de l'action* (60) *(qui est normal, car il peut être interprété comme le noyau de l'homomorphisme* (31)*), alors l'action induite* (62) *est fidèle. Prouvez-le.*

3.4

Avec les définitions ci-dessus à l'esprit, nous généralisons maintenant la notion de centralisateur vue lors du cours précédent. Les notions suivantes ont déjà été rencontrées en Math 113.

Définition 10. *Pour tout sous-ensemble X d'un groupe G, on définit son* ***centralisateur*** *comme*

$$\boxed{C_G(X)} = \Big\{ g \in G \Big| gx = xg, \ \forall x \in X \Big\} \tag{64}$$

Le centralisateur de $X = G$ est appelé le **centre** du groupe G, et est noté

$$Z(G) = \Big\{ g \in G \Big| gh = hg, \forall h \in G \Big\} \tag{65}$$

Définition 11. *Pour tout sous-ensemble X d'un groupe G, on définit son* ***normalisateur*** *comme*

$$\boxed{N_G(X)} = \Big\{ g \in G \Big| gX = Xg \Big\} \tag{66}$$

Il est évident que $C_G(X) \leq N_G(X)$ pour tout ensemble $X \subseteq G$, car la propriété $gx = xg, \forall x \in X$ est plus forte que $gX = Xg$. De plus, le résultat suivant, plus fort, est vrai.

Proposition 6. *Pour tout sous-ensemble $X \subset G$, son centralisateur est un sous-groupe normal de son normalisateur*

$$C_G(X) \trianglelefteq N_G(X) \tag{67}$$

Au lieu de prouver directement la Proposition 6, nous allons l'argumenter en utilisant le langage des actions de groupes. Pour tout sous-ensemble X d'un groupe G, nous avons une action

$$N_G(X) \curvearrowright X, \qquad g \cdot x = gxg^{-1}$$

Le noyau de cette action est, par définition, le sous-groupe centralisateur $C_G(X)$. Étant donné que le noyau de toute action de groupe est normal, cela implique la Proposition 6. De plus, selon le principe général dans la Sous-section 3.3, nous obtenons une action fidèle

$$N_G(X)/C_G(X) \curvearrowright X \tag{68}$$

3.5

Nous nous spécialisons désormais au cas où X est un sous-groupe de G.

Définition 12. *Un* ***automorphisme*** *d'un groupe K est un isomorphisme $K \to K$, et nous écrivons*

$$\boxed{\mathrm{Aut}(K)} \tag{69}$$

pour le groupe des automorphismes de K, par rapport à la composition.

Définition 13. *On dit qu'un groupe L agit sur un groupe K par automorphismes, encore noté*

$$L \curvearrowright K$$

si les bijections $\Phi_\ell(k) = \ell \cdot k$ sont des homomorphismes pour tout $\ell \in L$.

Lemme 6. *Si H est un sous-groupe de G, alors l'action*

$$N_G(H)/C_G(H) \curvearrowright H \tag{70}$$

de (68) *est par automorphismes.*

Proof. C'est une conséquence immédiate de la formule

$$ghh'g^{-1} = (ghg^{-1})(gh'g^{-1})$$

pour tout $h, h' \in H$, $g \in G$.

□

Avec cela en tête, la formule (70) nous donne une inclusion

$$\boxed{N_G(H)/C_G(H) \hookrightarrow \mathrm{Aut}(H)} \tag{71}$$

pour tout sous-groupe $H \leq G$. Le fait (71) est souvent appelé le **théorème du normalisateur/centralisateur**.

3.6

Considérons maintenant deux sous-groupes H et K d'un groupe G. Nous pouvons former les sous-ensembles

$$HK = \left\{ hk \middle| h \in H, k \in K \right\}$$

et

$$KH = \left\{ kh \middle| h \in H, k \in K \right\}$$

de G, qui seront en général différents. Le résultat suivant est assez simple, et nous vous le laissons comme exercice. Vous vous en souvenez peut-être aussi de Math 113.

Proposition 7. *Soit H et K des sous-groupes d'un groupe G.*

- *Nous avons $HK = KH$ si et seulement si HK est un sous-groupe de G.*
- *Si H et K sont des sous-groupes normaux de G, alors HK est un sous-groupe normal de G.*

Par exemple, la condition $HK = KH$ dans la Proposition 7 est satisfaite si

$$K \leq N_G(H) \tag{72}$$

car dans ce cas nous avons $Hk = kH$ pour tout $k \in K$. À son tour, une source significative d'exemples pour (72) est lorsque $H \trianglelefteq G$, car dans ce dernier cas $N_G(H) = G$. La formule (72) est également le cadre du **deuxième théorème d'isomorphisme**, que vous avez également appris dans Math 113.

Théorème 3. *Si K et H sont des sous-groupes de G tels que $K \leq N_G(H)$, alors*

$$K/K \cap H \cong HK/H \tag{73}$$

(le fait que $K \cap H$ soit normal dans K et que H soit normal dans HK fait partie du Théorème).

3.7

Le résultat suivant est souvent appelé le **théorème de correspondance**. Certaines personnes l'appellent le **théorème du treillis**, tandis que pour d'autres, c'est une fusion des **troisième** et **quatrième théorèmes d'isomorphisme**.

Théorème 4. *Pour tout groupe et sous-groupe normal $H \trianglelefteq G$, il existe une correspondance biunivoque*

$$\Big\{\textit{sous-groupes } H \leq K \leq G\Big\} \leftrightarrow \Big\{\textit{sous-groupes } \bar{K} \leq \bar{G}\Big\} \tag{74}$$

où $\bar{G} = G/H$ avec projection standard $\pi : G \to \bar{G}$. La correspondance (74) est donnée par

$$\bar{K} = \pi(K) \quad \textit{et} \quad K = \pi^{-1}(\bar{K}) \tag{75}$$

et elle possède les propriétés suivantes :

1. *Nous avons $K \leq K'$ si et seulement si $\bar{K} \leq \bar{K}'$, et dans ce cas nous avons une bijection*
$$K'/K \leftrightarrow \bar{K}'/\bar{K}$$

2. *Nous avons $K \trianglelefteq K'$ si et seulement si $\bar{K} \trianglelefteq \bar{K}'$, et dans ce cas nous avons un isomorphisme*
$$\boxed{K'/K \cong \bar{K}'/\bar{K}} \tag{76}$$
En particulier, K est normal si et seulement si $\bar{K}$ est normal.

Proof. Nous vous laissons montrer que les attributions (75) sont mutuellement inverses. Le fait que K soit un sous-groupe équivaut à ce que $\bar{K}$ soit un sous-groupe, ce qui découle du résultat suivant.

Proposition 1. *Si $f : G \to G'$ est un homomorphisme, alors pour tout sous-groupe $H \leq G$ et $H' \leq G'$, nous avons*

$$f(H) \leq G' \qquad \textit{et} \qquad f^{-1}(H') \leq G$$

Nous laissons la Proposition 1 comme un exercice. La propriété 1 est une affirmation triviale, avec la bijection donnée par

$$[g \bmod K] \mapsto \Big[[g \bmod H] \bmod K/H\Big], \quad \forall g \in K' \tag{77}$$

La propriété 2 découle de

$$K \trianglelefteq K' \quad \Leftrightarrow \quad Kg = gK,\ \forall g \in K' \quad \Leftrightarrow \quad \bar{K}\bar{g} = \bar{g}\bar{K},\ \forall \bar{g} \in \bar{K}' \quad \Leftrightarrow \quad \bar{K} \trianglelefteq \bar{K}'$$

où l'équivalence du milieu n'est autre que la correspondance (74). Si K est normal dans K', alors la bijection (77) est facilement vue comme un homomorphisme, ce qui donne ainsi l'isomorphisme (76).

□

Cours 4

4.1

Nous allons maintenant approfondir la notion de sous-groupes et de groupes quotients.

Définition 14. *Une **suite exacte courte** (de groupes)*

$$1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1 \tag{78}$$

est la donnée de deux homomorphismes f et g comme ci-dessus, où f est injectif, g est surjectif, et

$$\text{Im } f = \text{Ker } g \tag{79}$$

Le "1" à gauche et à droite de la suite (78) représente le groupe trivial.

Une conséquence immédiate de la définition est que f induit un isomorphisme entre K et un sous-groupe normal $H \trianglelefteq G$, tandis que le premier théorème d'isomorphisme implique que g induit un isomorphisme entre L et le groupe quotient G/H. Pour cette raison, s'il existe une suite exacte courte (78), nous appellerons G une **extension** de L par K.

Exemple 2. *La suite exacte courte par excellence est*

$$1 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{f} \mathbb{Z}/mn\mathbb{Z} \xrightarrow{g} \mathbb{Z}/n\mathbb{Z} \to 1 \tag{80}$$

pour tout $m, n \in \mathbb{N}$, où f est la multiplication par n et g est la réduction modulo n.

4.2

Pour tous groupes K et L, rappelons de Math 113 leur **produit direct**

$$K \times L$$

qui est fait pour devenir un groupe via l'opération $(k, \ell)(k', \ell') = (kk', \ell\ell')$ (essayez par vous-même de deviner l'identité et l'inverse, et de vérifier tous les axiomes du groupe). Ensuite, nous avons une suite exacte courte

$$1 \to K \xrightarrow{f} K \times L \xrightarrow{g} L \to 1 \tag{81}$$

où $f(k) = (k, e)$ et $g(k, \ell) = \ell$, pour tout $k \in K$ et $\ell \in L$. Vous pouvez vérifier que les applications f et g sont des homomorphismes, et que (79) est satisfaite. Cependant, les suites exactes courtes prennent aussi en compte les produits semi-directs de groupes que vous avez appris dans Math 113.

Définition 15. *Si un groupe L agit sur un groupe K par automorphismes (avec la notation de la Définition 13), alors le **produit semi-direct** correspondant*

$$K \rtimes L = \left\{ (k, \ell) \middle| k \in K, \ell \in L \right\} \tag{82}$$

est fait pour devenir un groupe avec l'élément neutre (e, e) via

$$(k, \ell)(k', \ell') = (k\Phi_\ell(k'), \ell\ell')$$

Les produits directs sont le cas particulier des produits semi-directs pour $\Phi_\ell = \text{Id}_K$, pour tout $\ell \in L$.

Proposition 8. *Étant donné un produit semi-direct* (82)*, nous avons une suite exacte courte*

$$1 \to K \xrightarrow{f} K \rtimes L \xrightarrow{g} L \to 1 \tag{83}$$

où $f(k) = (k, e)$ *et* $g(k, \ell) = \ell$*, pour tout* $k \in K$ *et* $\ell \in L$*.*

Proof. Il est immédiat de voir que f est injectif, g est surjectif, et que Im f = Ker g (en fait, la démonstration de ces énoncés est équivalente au cas du produit direct, que nous avons déjà traité). La seule chose qu'il reste à montrer est que f et g sont des homomorphismes. Montrons qu'ils respectent le produit. Pour f, cela découle du fait que

$$(k, e)(k', e) = (k\Phi_e(k'), ee) = (kk', e), \qquad \forall k, k' \in K$$

tandis que pour g, cela découle du fait que

$$(k, \ell)(k', \ell') = (\text{un élément quelconque de } K, \ell\ell'), \quad \forall k, k' \in K, \ell, \ell' \in L$$

□

4.3

Nous allons maintenant montrer que de nombreuses suites exactes courtes sont de la forme (83), bien que pour ce faire, nous devons d'abord formuler ce que cela signifie pour deux suites exactes courtes d'être "identiques".

Définition 16. *Deux suites exactes courtes*

$$1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$$

et

$$1 \to K \xrightarrow{f'} G' \xrightarrow{g'} L \to 1$$

sont dites ***équivalentes*** *s'il existe un homomorphisme* $s : G \to G'$ *qui fait commuter les carrés dans le diagramme suivant*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & \mathrm{Id}_K \downarrow & & s \downarrow & & \mathrm{Id}_L \downarrow & & \\ 1 & \longrightarrow & K & \xrightarrow{f'} & G' & \xrightarrow{g'} & L & \longrightarrow & 1 \end{array} \tag{84}$$

Notez que l'équivalence des suites exactes courtes est une relation d'équivalence, c'est-à-dire qu'elle est réflexive, symétrique et transitive (vérifiez ces faits, s'il vous plaît).

Lemme 7. *Si deux suites exactes courtes sont équivalentes, alors l'homomorphisme* s *dans la Définition 16 doit être un isomorphisme.*

Proof. Nous utiliserons la notation de la Définition 16 et la commutativité du diagramme (84). Supposons que $s(x) = e$ pour un certain $x \in G$. Alors $g'(s(x)) = e$, donc par la commutativité du carré le plus à droite, nous devons avoir $g(x) = e$. Cependant, cela implique qu'il existe $y \in K$ tel que $x = f(y)$. Ensuite, nous avons $e = s(x) = s(f(y))$, ce qui, par la commutativité du carré le plus à gauche, implique que $f'(y) = e$. Comme f' est injectif, cela implique $y = e$, donc $x = e$. Cela établit l'injectivité de s.

Considérons un $x' \in G'$. Comme g est surjectif, nous pouvons choisir $x \in G$ tel que $g(x) = g'(x')$. Cependant, par la commutativité du carré le plus à droite dans (84), nous avons $g = g' \circ s$. Ainsi, nous avons

$$g'(s(x)) = g'(x') \quad \Rightarrow \quad g'(s(x)^{-1}x') = e$$

donc il existe $y' \in K$ tel que $f'(y') = s(x)^{-1}x'$. Cependant, la commutativité du carré le plus à gauche dans (84) dit que $f' = s \circ f$, et donc nous avons

$$x' = s(x)f'(y') = s(x)s(f(y')) = s(xf(y'))$$

Cela établit la surjectivité de s.

□

4.4

Nous allons maintenant donner des critères pour savoir quand une suite exacte courte est équivalente à (81) ou à (83).

Proposition 9. *Une suite exacte courte* $1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$ *est équivalente à* (81) *si et seulement s'il existe un homomorphisme*

$$\phi : G \to K \tag{85}$$

tel que $\phi \circ f = \mathrm{Id}_K$.

Proof. Nous vous laissons déduire l'énoncé "si" à partir du fait que la suite (81) possède effectivement un homomorphisme (85) (si $G = K \times L$, alors vous définissez simplement ϕ comme étant la projection sur le premier facteur). Quant à l'énoncé "seulement si", supposons que nous avons un homomorphisme (85). Ensuite, le diagramme commutatif

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Id}_K} & & \downarrow{\scriptstyle \phi\times g} & & \downarrow{\scriptstyle \mathrm{Id}_L} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \times L & \longrightarrow & L & \longrightarrow & 1 \end{array}$$

(avec les morphismes sur la ligne du bas étant $k \mapsto (k, e)$ et $(k, \ell) \mapsto \ell$) donne l'équivalence requise des suites exactes courtes.

□

Proposition 10. *Une extension* $1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$ *est équivalente à* (83) *si et seulement s'il existe un homomorphisme*

$$\psi : L \to G \tag{86}$$

tel que $g \circ \psi = \mathrm{Id}_L$.

Proof. Nous vous laissons déduire l'énoncé "si" à partir du fait que la suite (83) possède effectivement un homomorphisme (86) (si $G = K \rtimes L$, alors vous définissez $\psi(\ell) = (e, \ell), \forall \ell \in L$). Quant à l'énoncé "seulement si", supposons que nous avons un homomorphisme (86). Cela nous permet de définir une action

$$L \curvearrowright K$$

comme suit : pour chaque $k \in K$ et $\ell \in L$, le fait que $\text{Im } f = \text{Ker } g$ et que $g \circ \psi = \text{Id}_L$ implique que

$$\psi(\ell) f(k) \psi(\ell)^{-1} \in G$$

se trouve dans $\text{Ker } g = \text{Im } f$, et peut donc être écrit de manière unique comme $f(x)$ pour un certain $x \in K$. Définissez la fonction

$$\Phi_\ell : K \to K, \qquad k \mapsto \text{ sur l'élément } x \text{ mentionné ci-dessus.}$$

Il y a plusieurs choses à vérifier, toutes sont faciles, mais nous vous recommandons de parcourir vous-mêmes les étapes :

- $\Phi_e = \text{Id}_K$,
- Φ_ℓ est une bijection pour tout $\ell \in L$,
- Φ_ℓ est un homomorphisme pour tout $\ell \in L$,
- $\Phi_\ell \circ \Phi_{\ell'} = \Phi_{\ell\ell'}$ pour tout $\ell, \ell' \in L$.

Ainsi, les Φ_ℓ définies ci-dessus donnent lieu à un produit semi-direct $K \rtimes L$. Nous affirmons que le diagramme

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & \text{Id}_K \uparrow & & f\times\psi \uparrow & & \text{Id}_L \uparrow & & \\ 1 & \longrightarrow & K & \longrightarrow & K \rtimes L & \longrightarrow & L & \longrightarrow & 1 \end{array}$$

(avec les morphismes sur la ligne du bas étant $k \mapsto (k, e)$ et $(k, \ell) \mapsto \ell$, et la flèche verticale au centre étant $(k, \ell) \mapsto f(k)\psi(\ell)$) donne l'équivalence requise. En effet, pour démontrer cela, nous devons vérifier deux faits : le premier est que le diagramme commute, ce qui est évident. Le second fait est que la flèche verticale au centre est un homomorphisme, ce qui découle de l'égalité

$$\begin{aligned}(f \times \psi)((k, \ell)(k', \ell')) &= (f \times \psi)(k\Phi_\ell(k'), \ell\ell') = f(k\Phi_\ell(k'))\psi(\ell\ell') = \\ &= f(k)f(\Phi_\ell(k'))\psi(\ell)\psi(\ell') = f(k)\psi(\ell)f(k')\psi(\ell') = (f \times \psi)(k, \ell)(f \times \psi)(k', \ell')\end{aligned}$$

□

4.5

Rappelons la définition suivante importante de Math 113.

Définition 17. *Un groupe est dit* ***abélien*** *si tous ses éléments commutent deux à deux, c'est-à-dire*

$$gh = hg, \quad \forall g, h \in G \tag{87}$$

Pour un groupe abélien, il est habituel de noter le produit en notation "additive", c'est-à-dire

$$g + h \quad \textit{au lieu de} \quad gh \tag{88}$$

et l'identité par 0 *au lieu de* e.

Le centre $Z(G)$ de tout groupe G est abélien. D'autres exemples de groupes abéliens sont les groupes cycliques $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$. Considérons maintenant des suites exactes courtes (78) avec K, G, L abéliens.

Lemme 8. *Soient K et L des groupes abéliens, et considérons une action $L \curvearrowright K$ par homomorphismes. Alors*

$$K \rtimes L$$

est abélien si et seulement si l'action est triviale, c'est-à-dire que $\Phi_\ell(k) = k$ pour tout $k \in K$, $\ell \in L$.

Proof. L'énoncé "si" est évident. Pour l'énoncé "seulement si", notez que $K \rtimes L$ étant abélien implique que

$$k + \Phi_\ell(k') = k' + \Phi_{\ell'}(k)$$

pour tous $k, k' \in K$ et $\ell, \ell' \in L$. En prenant k et ℓ' comme les éléments neutres dans la formule ci-dessus, cela implique que $\Phi_\ell(k') = k'$ pour tout $k' \in K$ et $\ell \in L$.

□

Le Lemme 8 implique que pour les suites exactes courtes de groupes abéliens (notez que lorsqu'on travaille avec des groupes abéliens, il est habituel de noter le groupe trivial par 0 au lieu de 1 ; cela devrait clarifier quand une de nos suites exactes courtes concerne des groupes abéliens ou généraux)

$$0 \to K \xrightarrow{f} G \xrightarrow{g} L \to 0 \tag{89}$$

les contextes des Propositions 9 et 10 sont en fait les mêmes. Ainsi, lorsque tous les groupes impliqués sont abéliens, nous concluons que l'existence d'un homomorphisme

$$\phi : G \to K \qquad \text{tel que} \qquad \phi \circ f = \mathrm{Id}_K$$

est équivalente à l'existence d'un homomorphisme

$$\psi : L \to G \qquad \text{tel que} \qquad g \circ \psi = \mathrm{Id}_L$$

Dans ces deux cas équivalents, nous appelons la suite exacte courte (89) **scindée**, l'application ϕ est appelée une **rétraction** et l'application ψ est une **section**.

Exemple 3. *Lorsque* $\gcd(m, n) = 1$*, nous affirmons que la suite exacte courte* (80) *est scindée. En effet, une rétraction explicite est donnée par $\phi =$ "multiplication par b et réduction modulo m" et une section par $\psi =$ "multiplication par am", où les entiers a et b sont choisis comme dans* (59)*. En particulier, nous avons*

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \tag{90}$$

chaque fois que $\gcd(m, n) = 1$.

Cours 5

5.1

Nous aimerions classifier les groupes abéliens. Cependant, nous ne pouvons pas espérer le faire pour tous les groupes abéliens, car il y en a tout simplement trop. A la place, nous allons classifier ceux qui sont de type fini, selon la définition suivante.

Définition 18. *Nous disons que les éléments $g_1, \dots, g_k$ **engendrent** un groupe abélien G si tout élément de G peut être écrit (pas nécessairement de manière unique) comme une combinaison linéaire*

$$a_1 g_1 + \cdots + a_k g_k$$

pour divers $a_1, \dots, a_k \in \mathbb{Z}$. Ici, nous rappelons que nous utilisons une notation additive, donc ag signifie la même chose que g^a signifiait précédemment (c'est-à-dire l'opération de groupe de g avec lui-même répétée a fois).

Si un groupe abélien admet un ensemble fini de générateurs, alors nous le dirons **de type fini**. Notre principal résultat dans les Cours 5 et 6 sera la classification de tels groupes, à savoir la preuve du résultat suivant. Nous écrivons

$$\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ fois}}$$

pour tout nombre $r \geq 0$, et nous définissons $\mathbb{Z}^0 = 0$, le groupe trivial.

Théorème 5. *Tout groupe abélien de type fini G est isomorphe à un produit direct*

$$\boxed{\mathbb{Z}^r \times \mathbb{Z}/p_1^{d_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{d_k}\mathbb{Z}} \tag{91}$$

*pour certains $r \geq 0$ (appelé le **rang** de G) et divers nombres premiers élevés à des puissances $p_1^{d_1}, \dots, p_k^{d_k}$ (appelés les **diviseurs élémentaires** de G). La décomposition (91) est unique à permutation des facteurs près.*

Tous les groupes abéliens (et en fait, très peu d'entre eux) ne sont pas de type fini, comme le montre le résultat suivant.

Proposition 11. *Le groupe des nombres rationnels $\mathbb{Q}$ par rapport à l'addition n'est pas de type fini.*

Proof. Supposons par l'absurde que $\mathbb{Q}$ soit de type fini. Alors, il existe des nombres rationnels

$$\frac{b_1}{c_1}, \dots, \frac{b_k}{c_k}$$

(pour divers $b_1, \dots, b_k \in \mathbb{Z}$ et $c_1, \dots, c_k \in \mathbb{N}$) tels que tout élément de $\mathbb{Q}$ puisse être écrit comme

$$a_1 \frac{b_1}{c_1} + \cdots + a_k \frac{b_k}{c_k} \tag{92}$$

pour divers $a_1, \dots, a_k \in \mathbb{Z}$. Mais le dénominateur de (92) doit diviser le nombre naturel fixe $c_1 \dots c_k$, il est donc impossible que tous les nombres rationnels soient de la forme (92).

□

5.2

Pour tout groupe abélien G et tout $n \in \mathbb{Z}$, la fonction

$$G \to G, \qquad g \mapsto ng, \ \forall g \in G \tag{93}$$

est un homomorphisme (Je vous recommande de vérifier cela). Le noyau de cet homomorphisme, à savoir

$$\boxed{\mathrm{Tors}_n(G)} = \Big\{ g \in G \Big| ng = 0 \Big\} \tag{94}$$

est appelé le **n-ième sous-groupe de torsion** de G. Il est facile de voir que le n-ième sous-groupe de torsion est le même que le $(-n)$-ième sous-groupe de torsion. Par ailleurs, le 0-ième sous-groupe de torsion de G est tout G, donc ce n'est pas un concept intéressant. Ainsi, nous ne travaillerons qu'avec la n-ième torsion pour les nombres naturels n.

Lemme 9. *Pour tout groupe abélien G, l'ensemble*

$$\boxed{\mathrm{Tors}(G)} = \bigcup_{n=1}^{\infty} \mathrm{Tors}_n(G) \tag{95}$$

est un sous-groupe. Il sera appelé le ***sous-groupe de torsion*** *de G.*

Proof. Puisque chaque $\mathrm{Tors}_n(G)$ est un sous-groupe de G, cela implique que $\mathrm{Tors}(G)$ contient l'élément neutre et qu'il est fermé pour la prise d'inverses. Il reste à montrer que le produit de deux éléments quelconques dans $\mathrm{Tors}(G)$ appartient à $\mathrm{Tors}(G)$. À cette fin, notons le fait évident que

$$\mathrm{Tors}_n(G) \subseteq \mathrm{Tors}_{mn}(G)$$

pour tous $m, n \in \mathbb{N}$. Ainsi, si nous prenons un élément $g \in \mathrm{Tors}_m(G) \subset \mathrm{Tors}(G)$ et un élément $h \in \mathrm{Tors}_n(G) \subset \mathrm{Tors}(G)$, alors g et h appartiennent tous deux à $\mathrm{Tors}_{mn}(G)$. Comme ce dernier est un sous-groupe de G, cela implique que $g + h \in \mathrm{Tors}_{mn}(G) \subset \mathrm{Tors}(G)$, comme nous devions le montrer.

□

Un aspect important de la torsion est qu'aucun élément (sauf l'élément neutre) ne peut appartenir simultanément à la m-ième torsion et à la n-ième torsion si $\gcd(m, n) = 1$. En d'autres termes

$$\{0\} = \mathrm{Tors}_m(G) \cap \mathrm{Tors}_n(G) \tag{96}$$

pour tout groupe abélien G, dès lors que $\gcd(m, n) = 1$. Pour voir cela, nous invoquons l'existence des entiers a, b de (59). Si un élément $g \in G$ appartient à la fois aux sous-groupes de la m-ième et de la n-ième torsion, alors

$$mg = ng = 0 \quad \Rightarrow \quad (am + bn)g = 0 \quad \Rightarrow \quad g = 0$$

5.3

Un groupe abélien dans lequel le seul élément de torsion est 0 (c'est-à-dire tel que $ng = 0$ pour un certain $n \in \mathbb{N}$ implique $g = 0$) est appelé **sans torsion**. Il est clair que $\mathbb{Z}^r$ est sans torsion, tout comme ses sous-groupes. Par ailleurs, aucun groupe fini (autre que le groupe trivial) ne peut être sans torsion, puisque tous ses éléments sont d'ordre fini.

Lemme 10. *Pour tout groupe abélien G, le groupe quotient*

$$G/\mathrm{Tors}(G)$$

est sans torsion.

Proof. Supposons que $g \in G$ ait la propriété que $n[g] = 0$ dans $G/\mathrm{Tors}(G)$ pour un certain $n \in \mathbb{N}$. Alors

$$ng \in \mathrm{Tors}(G)$$

ce qui implique qu'il existe un certain $m \in \mathbb{N}$ tel que $mng = 0$. Cela implique que $g \in \mathrm{Tors}(G)$, donc $[g] = 0$ dans $G/\mathrm{Tors}(G)$.

□

Si G est un groupe de la forme de (91), alors montrez par vous-même que

$$\mathrm{Tors}(G) \cong \mathbb{Z}/p_1^{d_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{d_k}\mathbb{Z}$$

et $G/\mathrm{Tors}(G) \cong \mathbb{Z}^r$. Ainsi, comme une étape intermédiaire pour prouver le Théorème 5, nous prouverons le résultat suivant.

Proposition 12. *Tout groupe abélien de type fini et sans torsion G est **libre**, c'est-à-dire*

$$\boxed{G \cong \mathbb{Z}^r}$$

pour un certain $r \geq 0$.

5.4

La Proposition 12 est une conséquence immédiate des Propositions 13 et 14.

Proposition 13. *Tout groupe abélien finiment engendré et sans torsion G est isomorphe à un sous-groupe de $\mathbb{Z}^k$, pour un certain $k \geq 0$.*

Proof. Adaptant la notion d'indépendance linéaire de l'algèbre linéaire au contexte des groupes abéliens, on dit que $g_1, \ldots, g_k \in G$ sont **linéairement indépendants** si pour tous $a_1, \ldots, a_k \in \mathbb{Z}$,

$$a_1 g_1 + \cdots + a_k g_k = 0 \quad \Rightarrow \quad a_1 = \cdots = a_k = 0$$

Supposons maintenant que G est un groupe abélien sans torsion finiment engendré. Considérons un ensemble de générateurs $g_1, \ldots, g_{k+\ell}$ de G, et supposons que $g_1, \ldots, g_k$ sont un sous-ensemble

maximal d'éléments linéairement indépendants parmi les générateurs mentionnés (cela est toujours possible en renumérotant les g). Par conséquent, l'homomorphisme suivant est injectif

$$\mathbb{Z}^k \xrightarrow{\gamma} G, \qquad (a_1, \ldots, a_k) \mapsto a_1 g_1 + \cdots + a_k g_k$$

Cependant, le fait que l'ensemble $g_1, \ldots, g_k$ soit maximal par rapport à l'indépendance linéaire signifie que les éléments $g_1, \ldots, g_k, g_i$ sont linéairement dépendants, pour tous $i \in \{k+1, \ldots, \ell\}$. Par conséquent, il existe des entiers $a_i^1, \ldots, a_i^k, b_i$ (avec $b_i \neq 0$ en raison de l'indépendance linéaire de $g_1, \ldots, g_k$) tels que

$$b_i g_i = a_i^1 g_1 + \cdots + a_i^k g_k$$

pour tous $i \in \{k+1, \ldots, \ell\}$. Soit m le plus petit commun multiple de $b_{k+1}, \ldots, b_\ell$. Ainsi, $mg_{k+1}, \ldots, mg_{k+\ell}$ peuvent être écrits comme des combinaisons linéaires de $g_1, \ldots, g_k$; puisque $g_1, \ldots, g_{k+l}$ génèrent G, nous concluons donc que mg peut être écrit comme une combinaison linéaire de $g_1, \ldots, g_k$, pour tout $g \in G$. Par conséquent, l'image de l'homomorphisme

$$G \xrightarrow{\delta} G, \qquad g \mapsto mg$$

est contenue dans l'image de l'homomorphisme injectif γ. Cela implique que δ se factorise comme

$$\delta : G \to \mathbb{Z}^k \xrightarrow{\gamma} G$$

Cependant, δ est injectif car G est sans torsion, ce qui implique que l'homomorphisme $G \to \mathbb{Z}^k$ que nous venons de construire est également injectif. Ainsi, G est isomorphe à l'image de cet homomorphisme.

□

Proposition 14. *Tout sous-groupe de $\mathbb{Z}^k$ est isomorphe à $\mathbb{Z}^r$ pour un certain $r \geq 0$.*

Proof. Nous allons prouver l'énoncé requis par induction sur k. Lorsque $k = 1$, considérons tout sous-groupe $G \subseteq \mathbb{Z}$. Soit $G = 0$, soit G contient un certain élément non nul n. Choisissons le plus petit entier positif $n \in G$. Alors $n\mathbb{Z} \subseteq G$. Si cette inclusion n'était pas une égalité des ensembles, il existerait alors $m \in \mathbb{Z}$ tel que $n \nmid m$. Mais alors le reste de m modulo n serait également dans G, ce qui contredirait la minimalité de n. Nous concluons que $G = n\mathbb{Z} \cong \mathbb{Z}$.

Maintenant, prouvons le pas d'induction : supposons que tout sous-groupe de $\mathbb{Z}^{k-1}$ soit libre, et montrons que c'est également le cas pour tout sous-groupe $G \subseteq \mathbb{Z}^k$. Considérons la suite exacte courte

$$0 \to \mathbb{Z}^{k-1} \xrightarrow{\iota} \mathbb{Z}^k \xrightarrow{\pi} \mathbb{Z} \to 0 \tag{97}$$

où l'homomorphisme π est la projection sur la dernière coordonnée. Définissons alors $K = G \cap \mathbb{Z}^{k-1}$ et $L = \pi(G)$, et nous vous laissons vérifier par vous-même que (97) induit une suite exacte courte

$$0 \to K \xrightarrow{\iota'} G \xrightarrow{\pi'} L \to 0 \tag{98}$$

Cependant, nous avons déjà classé les sous-groupes de $\mathbb{Z}$: si $L = 0$, alors $G \cong K$ est un sous-groupe de $\mathbb{Z}^{k-1}$, que l'hypothèse d'induction montre être libre. Sinon, $L \cong \mathbb{Z}$ et nous pouvons choisir un scindement de la projection π' : il suffit d'envoyer $1 \in L$ sur un élément arbitraire dans $\pi'^{-1}(1)$. Comme nous l'avons vu à la fin du Cours 4, une suite exacte courte scindée de groupes abéliens a la propriété $G \cong K \times L$. Étant donné que K est libre par l'hypothèse d'induction et $L \cong \mathbb{Z}$, nous avons terminé.

□

5.5

Dans le cadre de la preuve de la Proposition 14, nous avons (essentiellement) prouvé la propriété suivante intéressante du groupe abélien $\mathbb{Z}^\ell$, pour tout $\ell \in \mathbb{N}$.

Lemme 11. *Toute suite exacte courte de groupes abéliens*

$$0 \to K \to G \xrightarrow{\pi} \mathbb{Z}^\ell \to 0 \tag{99}$$

est scindée, et en particulier, $G \cong K \times \mathbb{Z}^\ell$.

Proof. Pour chaque $i \in \{1, \ldots, \ell\}$, soit e_i le générateur standard de $\mathbb{Z}^\ell$, à savoir le vecteur

$$(0, \ldots, 1, \ldots, 0)$$

avec un seul 1 à la position i-ème et des 0 partout ailleurs. Puisque l'homomorphisme $\pi : G \to \mathbb{Z}^\ell$ dans la suite exacte courte donnée est surjectif, nous pouvons choisir $g_i \in \pi^{-1}(e_i)$ pour tous i. Alors la fonction

$$\psi : \mathbb{Z}^\ell \to G, \qquad (n_1, \ldots, n_\ell) \mapsto n_1 g_1 + \cdots + n_\ell g_\ell$$

est facilement vue comme un homomorphisme (vérifier cela). De plus, par construction, c'est un scindement au sens où $\pi \circ \psi = \mathrm{Id}_{\mathbb{Z}^\ell}$. Par conséquent, la suite exacte courte (99) est scindée.

□

En corollaire du Lemme 10, du Lemme 11 et de la Proposition 12, nous avons

$$G \cong \mathbb{Z}^r \times \mathrm{Tors}(G) \tag{100}$$

pour tout groupe abélien de type fini G, pour un certain $r \geq 0$. Pour comprendre cela, rappelons que le Lemme 10 donne une suite exacte courte

$$0 \to \mathrm{Tors}(G) \to G \xrightarrow{\pi} L \to 0$$

où L est un groupe abélien sans torsion. Cependant, le fait que G soit de type fini signifie qu'il en est de même pour L (en particulier, un ensemble fini de générateurs de L est donné par les images sous π de certains éléments générateurs de G). La Proposition 12 implique alors que L est isomorphe à $\mathbb{Z}^r$ pour un certain $r \geq 0$, et ensuite le Lemme 11 implique (100).

Cours 6

6.1

La formule (100) réduit le problème de classification des groupes abéliens finiment engendrés G (le théorème recherché 5) à la compréhension de $\mathrm{Tors}(G)$. La première étape est la suivante.

Proposition 15. *Si G est un groupe abélien finiment engendré, alors tout sous-groupe $H \leq G$ est également finiment engendré.*

Remarquons que la proposition 15 ne s'applique pas aux groupes non abéliens (pour lesquels il existe une notion analogue de génération finie).

Proof. La preuve présente beaucoup de similitudes avec celle de la proposition 14. Nous prouverons la proposition 15 par induction sur le nombre de générateurs de G. Lorsque G a un seul générateur (c'est-à-dire qu'il est cyclique), alors $G \cong \mathbb{Z}$ ou $G \cong \mathbb{Z}/n\mathbb{Z}$. Nous avons déjà montré que tous les sous-groupes de $\mathbb{Z}$ sont soit 0, soit $m\mathbb{Z}$, et nous vous laissons comme exercice de montrer que tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $m\mathbb{Z}/n\mathbb{Z}$ pour un certain diviseur $m|n$.

Supposons maintenant que la proposition 15 soit vraie pour tous les groupes abéliens avec moins de n générateurs, et prouvons-la pour un groupe G avec les générateurs $g_1, \ldots, g_n$. Choisissons un sous-groupe arbitraire H, que nous allons prouver être finiment engendré. Soit $G' \subset G$ le sous-groupe engendré par $g_1, \ldots, g_{n-1}$, et considérons la suite exacte courte

$$0 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G/G' \to 0.$$

Si nous posons $K = H \cap G'$ et $L = \pi(H)$, alors nous avons une suite exacte courte

$$0 \to K \xrightarrow{\iota} H \xrightarrow{\pi} L \to 0$$

Puisque K et L sont des sous-groupes de G' et G/G' (qui ont respectivement $n-1$ et 1 générateurs), l'hypothèse d'induction implique que K et L sont tous deux finiment engendrés. Soit $x_1, \ldots, x_k$ les générateurs de K et $y_1, \ldots, y_\ell$ les générateurs de ℓ. Nous affirmons alors que

$$\iota(x_1), \ldots, \iota(x_k), g_1, \ldots, g_\ell \tag{101}$$

sont les générateurs de H, pour tout choix de $\{g_i \in \pi^{-1}(y_i)\}_{i\in\{1,\ldots,\ell\}}$. En effet, pour tout $h \in H$, nous pouvons écrire

$$\pi(h) = b_1 y_1 + \cdots + b_\ell y_\ell$$

pour divers $b_1, \ldots, b_\ell \in \mathbb{Z}$. Cela implique que

$$h - b_1 g_1 - \cdots - b_\ell g_\ell \in \text{Ker } \pi = \text{Im } \iota.$$

Étant donné que ι est injective, son image est isomorphe à K, il doit donc exister $a_1, \ldots, a_k \in \mathbb{Z}$ tels que

$$h - b_1 g_1 - \cdots - b_\ell g_\ell = a_1 \iota(x_1) + \cdots + a_k \iota(x_k).$$

Cela établit l'affirmation que H est engendré par les éléments (101).

□

6.2

En conséquence de la Proposition 15, le sous-groupe de torsion d'un groupe abélien de type fini G est de type fini. Si nous prenons $g_1, \ldots, g_k$ comme une collection de tels générateurs de $\text{Tors}(G)$ (qui doivent avoir des ordres finis $a_1, \ldots, a_k \in \mathbb{N}$, respectivement), alors tout élément de $\text{Tors}(G)$ est de la forme

$$b_1 g_1 + \cdots + b_k g_k$$

où $b_i \in \{0, \ldots, a_i - 1\}$ pour tout $i \in \{1, \ldots, k\}$. Ainsi, nous concluons que

tout groupe abélien de torsion de type fini est fini (102)

(lorsque nous disons "groupe abélien de torsion", nous désignons un groupe abélien dans lequel chaque élément a un ordre fini). Par conséquent, il reste à classifier les groupes abéliens finis. À cette fin, nous devrons étudier la structure des sous-groupes de torsion de manière plus détaillée.

Une généralisation naturelle du produit direct de deux groupes est le produit direct d'une infinité dénombrable de groupes abéliens $G_1, G_2, \ldots$

$$\prod_{i=1}^{\infty} G_i = \Big\{ (g_1, g_2, \ldots) \Big| g_i \in G_i, \ \forall i \in \mathbb{N} \Big\}$$

(avec toutes les opérations définies composante par composante), qui est également un groupe abélien. De plus, la **somme directe** d'une infinité dénombrable de groupes abéliens $G_1, G_2, \ldots$

$$\bigoplus_{i=1}^{\infty} G_i = \Big\{ (g_1, g_2, \ldots) \Big| g_i \in G_i, \ \forall i \in \mathbb{N}, \text{tous sauf un nombre fini des } g_i \text{ sont } 0 \Big\} \tag{103}$$

(avec toutes les opérations encore définies composante par composante) est également un groupe abélien. Si seulement un nombre fini des groupes $G_1, G_2, \ldots$ sont non triviaux, alors le produit direct et la somme directe sont identiques, mais en général, le produit peut être plus grand que la somme directe.

6.3

Considérons maintenant un groupe abélien quelconque G et un nombre premier p. Le sous-groupe de p-torsion (notez la distinction terminologique entre ceci et le "sous-groupe de p-ième torsion" défini dans la sous-section 5.2) est

$$\boxed{A_p(G))} = \bigcup_{n=0}^{\infty} \mathrm{Tors}_{p^n}(G) \tag{104}$$

Tout comme dans la démonstration du Lemme 9, on montre (et je vous conseille de refaire la preuve) que

$$\mathrm{Tors}_{p^0}(G) \subseteq \mathrm{Tors}_{p^1}(G) \subseteq \mathrm{Tors}_{p^2}(G) \subseteq \ldots$$

et que (104) est bien un sous-groupe. De plus, ces sous-groupes de torsion fournissent une décomposition en somme directe du sous-groupe de torsion complet (95), comme indiqué dans le résultat suivant.

Lemme 12. *Pour tout groupe abélien G, nous avons*

$$\mathrm{Tors}(G) \cong \bigoplus_{p \ premier} A_p(G) \tag{105}$$

avec la somme directe des groupes abéliens définie comme dans (103).

Proof. Il existe un homomorphisme naturel du côté droit au côté gauche de (105)

$$\sum_{p \text{ premier}} g_p \leftarrow \Big(g_p \in A_p(G) \Big)_{p \text{ premier}} \tag{106}$$

Le fait que tous sauf un nombre fini des g_p soient égaux à 0 (la caractéristique définissante de la somme directe) signifie que leur somme est bien définie. Il reste à montrer que (106) est

- *injectif*: supposons que nous ayons une collection d'éléments $g_1, \dots, g_k \in G$ tels que

$$p_1^{d_1} g_1 = \cdots = p_k^{d_k} g_k = 0,$$

où $p_1, \dots, p_k$ sont des nombres premiers distincts et $d_1, \dots, d_k$ sont des nombres naturels. Si la collection de ces g_i est dans le noyau de (106), c'est-à-dire si

$$g_1 + g_2 + \cdots + g_k = 0$$

alors nous pouvons multiplier la formule ci-dessus par $p_2^{d_2} \dots p_k^{d_k}$. Si nous le faisons, nous avons

$$p_2^{d_2} \dots p_k^{d_k} g_1 + \underbrace{p_2^{d_2} \dots p_k^{d_k} g_2}_{=0} + \cdots + \underbrace{p_2^{d_2} \dots p_k^{d_k} g_k}_{=0} = 0 \quad \Rightarrow \quad p_2^{d_2} \dots p_k^{d_k} g_1 = 0$$

Cependant, nous avons aussi $p_1^{d_1} g_1 = 0$. Comme $p_1^{d_1}$ et $p_2^{d_2} \dots p_k^{d_k}$ sont premiers entre eux, alors (96) implique que $g_1 = 0$. Un argument analogue montre que $g_2 = \cdots = g_k = 0$, ce qui implique que le noyau de (106) est trivial.

- *surjective* : supposons que nous avons un élément $g \in \mathrm{Tors}_n(G) \subset \mathrm{Tors}(G)$ et considérons la décomposition en facteurs premiers

$$n = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$$

où $p_1, \dots, p_k$ sont des premiers distincts, et $d_1, \dots, d_k \in \mathbb{N}$. Alors l'élément

$$g_i = p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} g$$

a un ordre divisant $p_i^{d_i}$, et donc appartient à $A_{p_i}(G)$. Cependant, les entiers naturels

$$\left\{ p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} \right\}_{i \in \{1,\dots,k\}}$$

ont un plus grand commun diviseur égal à 1. Par un raisonnement similaire à l'existence des entiers a, b tels que (59) est vérifiée, il existe des entiers $a_1, \dots, a_k$ tels que

$$\sum_{i=1}^{k} a_i p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} = 1.$$

Par conséquent, nous avons

$$a_1 g_1 + \cdots + a_k g_k = \left(\sum_{i=1}^{k} a_i p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} \right) g = g$$

ce qui implique que g appartient à l'image de l'homomorphisme (106).

□

6.4

La notion suivante est très importante. Fixons un nombre premier p.

Définition 19. *Nous appelons un groupe G un p-**groupe** si l'ordre de chaque élément de G est une puissance de p.*

Bien que la notion ci-dessus ait du sens pour tous les groupes (et nous allons la voir appliquée comme telle dans quelques leçons), pour le moment, nous la considérerons dans le contexte des groupes abéliens. Par définition, $A_p(G)$ défini dans (104) est un p-groupe pour tout groupe abélien G.

Proposition 16. *Un groupe abélien fini G est un p-groupe si et seulement si $|G|$ est une puissance de p.*

L'énoncé "si" est une conséquence immédiate du théorème de Lagrange, puisque l'ordre de tout élément divise l'ordre du groupe. L'énoncé "seulement si" est une corollaire immédiate du fait suivant.

Proposition 17. *Si un premier p divise l'ordre d'un groupe abélien fini G, alors G a un élément d'ordre p.*

Proof. Nous allons prouver l'énoncé par induction sur l'ordre de G. Si G est cyclique, alors le résultat est facile à prouver, alors veuillez le faire vous-mêmes. Sinon, nous pouvons considérer un élément $h \in G$ qui ne génère pas tout G, et supposons dans le but de contradiction que $a = \mathrm{ord}_G(h)$ est premier avec p (en effet, si $p|a$, alors nous pouvons facilement trouver une puissance de h dont l'ordre est exactement p). Ensuite, nous laissons H être le sous-groupe généré par h et considérons le quotient

$$G/H.$$

Parce que l'ordre de H est premier avec p, alors p divise l'ordre de G/H. Par l'hypothèse d'induction, il existe un élément $g \in G$ tel que $[g]$ a ordre p dans G/H. Cela implique que

$$pg \in H \quad \Rightarrow \quad apg = 0$$

dans G. Cela implique que ag a soit l'ordre p (dans quel cas nous avons terminé) soit que $ag = 0$. Cependant, puisque $\gcd(a, p) = 1$, alors $pg \in H$ et $ag = 0 \in H$ impliquerait que $g \in H$, ce qui contredirait le fait que $[g]$ a ordre p dans G/H.

□

6.5

Si G est un groupe abélien fini, alors il est égal à son sous-groupe de torsion. Dans ce cas, seuls un nombre fini de $A_p(G)$ peuvent être non triviaux, sinon le côté droit de (105) serait un ensemble infini. Par conséquent, tout groupe abélien fini G a la propriété que

$$G \cong A_{p_1}(G) \times \cdots \times A_{p_k}(G) \tag{107}$$

pour des premiers distincts $p_1, \ldots, p_k$, où chaque $A_{p_i}(G)$ est un p_i-groupe abélien fini.

Proposition 18. *Tout p-groupe abélien fini est isomorphe à*

$$\mathbb{Z}/p^{d_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z} \tag{108}$$

pour divers entiers positifs $d_1, \ldots, d_k$.

Proof. Nous allons prouver la proposition par induction sur $|G|$, avec la base d'induction correspondant au groupe trivial. Considérons un élément de G d'ordre maximal possible : appelons-le h et supposons que son ordre est p^{d_1}. Soit $H \cong \mathbb{Z}/p^{d_1}\mathbb{Z}$ le sous-groupe de G généré par h. Le groupe quotient

$$G/H$$

est un p-groupe, en raison de la proposition 16 (si un groupe a un ordre égal à une puissance de p, alors tous ses sous-groupes, et donc tous ses quotients, ont aussi cet ordre). Par l'hypothèse d'induction, il existe des entiers positifs $d_2, \ldots, d_k$ tels que $G/H \cong \mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z}$. Tout élément de G/H a un ordre inférieur (à tout préimage du même élément) dans G, donc le fait que p^{d_1} soit l'ordre maximal implique que $d_1 \geq d_2, \ldots, d_k$. Nous concluons qu'il existe une suite exacte courte

$$0 \to \mathbb{Z}/p^{d_1}\mathbb{Z} \to G \xrightarrow{\pi} \mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z} \to 0.$$

Pour conclure la preuve de la proposition 18, il suffit de construire un inverse à droite de l'homomorphisme π ci-dessus. Pour ce faire, pour chaque $i \in \{2, \ldots, k\}$, nous définissons g_i comme un élément arbitraire de G dont l'image sous π est

$$(0, \ldots, 1, \ldots, 0) \in \mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_i}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z}.$$

Nous avons

$$p^{d_i}[g_i] = 0 \in G/H \quad \Rightarrow p^{d_i} g_i = a_i h, \quad \forall i \in \{2, \ldots, k\}$$

pour certains $a_i \in \mathbb{Z}$. Écrivons $a_i = p^{s_i} t_i$ où t_i est premier avec p. Alors la formule ci-dessus s'écrit

$$p^{d_i} g_i = p^{s_i} t_i h \tag{109}$$

Comme tous les éléments de G ont un ordre qui est par hypothèse $\leq p^{d_1}$, nous avons

$$0 = p^{d_1} g_i = p^{d_1 - d_i + s_i} t_i h$$

Puisque t_i est premier avec p, l'ordre de h est le même que l'ordre de th (trouvez un argument pour cela, en utilisant le fait que G est un p-groupe) et donc la formule ci-dessus implique que $d_1 - d_i + s_i \geq d_1 \Rightarrow s_i \geq d_i$ pour tout $i \in \{2, \ldots, k\}$. Mais alors nous pouvons réécrire (109) comme

$$p^{d_i}(\underbrace{g_i - p^{s_i - d_i} t_i h}_{\text{appelons cela } g_i'}) = 0$$

La formule ci-dessus garantit que l'application

$$\mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z} \xrightarrow{\psi} G, \qquad (x_2, \ldots, x_k) \mapsto x_2 g_2' + \cdots + x_k g_k'$$

est un homomorphisme bien défini. Il est également clair que $\pi \circ \psi = \mathrm{Id}$ par construction, et nous avons terminé.

□

Proof. de Théorème 5 (sans l'énoncé selon lequel la décomposition (91) *est unique à permutation des facteurs, ce que nous choisissons de ne pas faire) :* Par (100), tout groupe abélien de type fini est de la forme $\mathbb{Z}^r$ fois son sous-groupe de torsion. Par la Proposition 15 et l'équation (102), ce dernier est fini. Cela implique que le sous-groupe de torsion en question est un produit de facteurs comme dans (107), et la Proposition 18 assure que tous ces facteurs sont des produits de la forme $\mathbb{Z}/p^d\mathbb{Z}$ pour divers premiers p et divers $d \in \mathbb{N}$.

□

Cours 7

7.1

On pense généralement que les groupes abéliens sont simples, mais cette terminologie appartient en réalité à une autre famille de groupes.

Définition 20. *Un groupe G est appelé* ***simple*** *s'il a exactement deux sous-groupes normaux :* 1 *et G (ainsi, le groupe trivial n'est pas considéré comme simple, tout comme le nombre 1 n'est pas considéré comme premier).*

Autrement, un groupe est simple si et seulement si ses seuls quotients sont lui-même et le groupe trivial. En particulier, toute action d'un groupe simple doit soit être triviale (c'est-à-dire que chaque élément du groupe agit par l'identité), soit fidèle. Puisque tout sous-groupe d'un groupe abélien est normal, les seuls groupes abéliens simples sont $\mathbb{Z}/p\mathbb{Z}$ pour un nombre premier p. Mais parmi les groupes non abéliens, nous avons beaucoup plus d'exemples ; le suivant est particulièrement important.

Théorème 6. *Bien que le groupe symétrique S_n ne soit pas simple, son sous-groupe normal d'indice deux*

$$A_n = \operatorname{Ker}\left(S_n \xrightarrow{\text{sgn}} \mathbb{Z}/2\mathbb{Z}\right)$$

est simple, pour tout $n \geq 5$ (rappelons que sgn *envoie tout cycle de longueur $k+1$ vers k mod 2).*

Proof. Soit $H \trianglelefteq A_n$ un sous-groupe normal non trivial de A_n, et soit $h \in H$ un élément qui n'est pas l'identité. Comme nous le savons du cours de Math 113, la permutation h peut être écrite comme un produit de cycles disjoints. De plus, puisque H est normal, nous pouvons conjuguer h par n'importe quelle permutation et obtenir un élément de H. Comme nous l'avons vu dans la preuve de la Proposition 5, conjuguer une permutation a pour effet de changer les entrées de ses cycles constituants. Donc si

$$h = \ldots (i_1\ i_2\ \ldots\ i_k) \ldots \tag{110}$$

alors

$$h' = \ldots (j_1\ j_2\ \ldots\ j_k) \ldots \tag{111}$$

se trouve aussi dans H, où $\{j_1, \ldots, j_k\}$ est n'importe quelle permutation de $\{i_1, \ldots, i_k\}$. En particulier, nous pouvons choisir $j_1 = i_k$, $j_2 = i_{k-1}$, $\ldots$, $j_k = i_1$, et alors le cycle dans (111) sera l'inverse du cycle dans (110). Ou si nous choisissons $j_1 = i_k$, $j_2 = i_{k-1}$, $\ldots$, $j_{k-3} = i_4$, $j_{k-2} = i_2$, $j_{k-1} = i_3$, $j_k = i_1$, alors le produit du cycle dans (111) avec le cycle dans (110) sera le cycle de longueur 3 $(i_1\ i_3\ i_2)$. Ainsi, en choisissant de manière appropriée (111) par rapport à (110), nous pouvons nous assurer que H contient un cycle de longueur 3. En conjuguant convenablement le cycle de longueur 3 susmentionné, nous concluons que H contient tous les cycles de longueur 3. Cependant, tout produit de deux transpositions (c'est-à-dire des cycles de longueur 2) peut être écrit comme un produit de cycles de longueur 3, en raison des identités suivantes pour tous les nombres distincts a, b, c, d

$$\begin{aligned}
(a\ b)(a\ b) &= e \\
(a\ b)(a\ c) &= (c\ b\ a) \\
(a\ b)(c\ d) &= (c\ a\ d)(b\ c\ a)
\end{aligned}$$

Puisque toute permutation est un produit de transpositions, il en résulte que tout élément de A_n est un produit d'un nombre pair de transpositions, d'où il s'ensuit que tout élément de A_n est un produit de cycles de longueur 3. Ainsi, $A_n = H$, ce qui implique que A_n est simple.

□

7.2

On peut utiliser des groupes simples comme les blocs de construction pour des groupes plus généraux, comme suit.

Définition 21. *Une **série sous-normale** d'un groupe G est une collection de sous-groupes*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G \tag{112}$$

telle que G_{i-1} soit un sous-groupe normal de G_i, pour tout $i \in \{1, \ldots, k\}$. Si de plus tous les quotients $G_1/G_0, \ldots, G_k/G_{k-1}$ sont des groupes simples, alors on appelle (112) *une **série de composition** de G.*

Tous les groupes ne possèdent pas de série de composition, par exemple $\mathbb{Z}$ n'en a pas. En effet, chacun de ses sous-groupes non triviaux est isomorphe à $\mathbb{Z}$ lui-même, donc toute série comme (112) est vouée à durer indéfiniment. Cependant, tous les groupes finis ont des séries de composition, selon le résultat suivant.

Proposition 19. *Tout groupe fini possède une série de composition.*

Proof. Par induction sur l'ordre de G. Prenons un sous-groupe normal maximal $H \triangleleft G$, qui existe car G est un ensemble fini. Ensuite, considérons l'homomorphisme

$$\pi : G \to G/H.$$

Si le groupe G/H n'était pas simple, alors par le Théorème 4

$$\pi^{-1}(\text{un sous-groupe normal propre de } G/H)$$

serait un sous-groupe normal de G strictement compris entre H et G. Cela n'est pas permis, en raison de l'hypothèse que H est maximal, donc nous concluons que G/H est simple. Par l'hypothèse d'induction, H a une série de composition ; en ajoutant G à sa droite, nous obtenons la série de composition requise de G.

□

Pour un groupe abélien fini, les séries de composition peuvent être écrites très explicitement. Par exemple

$$0 < \mathbb{Z}/p\mathbb{Z} < \mathbb{Z}/p^2\mathbb{Z} < \cdots < \mathbb{Z}/p^k\mathbb{Z}$$

est une série de composition, où $\mathbb{Z}/p^{i-1}\mathbb{Z} = p\mathbb{Z}/p^i\mathbb{Z}$ est interprété comme un sous-groupe de $\mathbb{Z}/p^i\mathbb{Z}$.

7.3

Les sous-groupes normaux et les groupes quotients héritent des séries de composition de leur groupe parent, comme nous le montrerons dans les propositions ci-dessous.

Proposition 20. *Si un groupe G a une série de composition* (112)*, alors pour tout sous-groupe normal $H \trianglelefteq G$, nous pouvons former*

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{k-1} \trianglelefteq H_k = H \tag{113}$$

où $H_i = H \cap G_i$. En supprimant les redondances dans la série ci-dessus (c'est-à-dire si $H_{i-1} = H_i$ pour un certain i, alors nous supprimons H_i de la série), alors (113) *donne une série de composition pour H.*

Proof. Montrons que pour tout i, le sous-groupe H_{i-1} est normal dans H_i. À cette fin, prenons n'importe quel $g \in H_i$ et $h \in H_{i-1}$. L'élément ghg^{-1} est

- dans G_{i-1}, car G_{i-1} est normal dans G_i, et
- dans H, car H est un sous-groupe.

Ainsi $ghg^{-1} \in H_{i-1}$, ce qui implique que H_{i-1} est normal dans H_i. Cela étant dit, nous remarquons que les inclusions $G_{i-1} \hookrightarrow G_i$ induisent un homomorphisme injectif

$$H_i/H_{i-1} \overset{\varphi}{\hookrightarrow} G_i/G_{i-1} \tag{114}$$

Montrons maintenant que Im φ est normal dans G_i/G_{i-1}. Prenons n'importe quels $[g], [h] \in G_i/G_{i-1}$ représentés par certains $g \in G_i$ et $h \in H_i$. Alors l'élément ghg^{-1} est

- dans G_i, car G_i est un sous-groupe, et
- dans H, car H est normal dans G

Ainsi $ghg^{-1} \in H_i$, donc $[g][h][g]^{-1} \in$ Im φ. Puisque G_i/G_{i-1} est simple, alors Im φ est soit le sous-groupe trivial, soit l'ensemble entier G_i/G_{i-1}. Dans le premier cas, nous avons $H_i = H_{i-1}$ et dans le second cas, nous avons $H_i/H_{i-1} \cong G_i/G_{i-1}$. Cela implique la conclusion requise.

□

Remarque. *Les sous-groupes non normaux n'héritent pas nécessairement des séries de composition. Par exemple, de nombreux groupes simples G contiennent des éléments d'ordre infini (donc ils contiennent $\mathbb{Z}$ comme sous-groupe) mais nous avons déjà vu que $\mathbb{Z}$ n'a pas de série de composition.*

7.4

Tout comme les sous-groupes normaux héritent des séries de composition (comme nous l'avons montré dans la sous-section précédente), nous allons maintenant montrer que les groupes quotients les héritent également.

Proposition 21. *Si un groupe G a une série de composition* (112)*, alors pour tout sous-groupe normal $H \trianglelefteq G$ avec le groupe quotient correspondant $\bar{G} = G/H$, nous pouvons former*

$$1 = \bar{G}_0 \trianglelefteq \bar{G}_1 \trianglelefteq \cdots \trianglelefteq \bar{G}_{k-1} \trianglelefteq \bar{G}_k = \bar{G} \tag{115}$$

où $\bar{G}_i = HG_i/H$. En supprimant les redondances dans la série ci-dessus (c'est-à-dire si $\bar{G}_{i-1} = \bar{G}_i$ pour un certain i, alors nous supprimons $\bar{G}_i$ de la série), alors (115) *donne une série de composition pour $\bar{G}$.*

Proof. Nous montrons d'abord que le fait que G_{i-1} soit normal dans G_i implique que HG_{i-1} est normal dans HG_i. Pour voir cela, prenons n'importe quel $hg \in HG_i$ et n'importe quel $h'g' \in HG_{i-1}$ (avec $h, h' \in H$, $g \in G_i$ et $g' \in G_{i-1}$). Alors

$$(hg)(h'g')(hg)^{-1} = hgh'g'g^{-1}h^{-1} \in hgHg'g^{-1}h^{-1} = hH \underbrace{gg'g^{-1}}_{\text{un certain } g'' \in G_{i-1}} h^{-1} \subseteq Hg''H = Hg''$$

(le fait que H soit normal implique que $gH = Hg$ pour tout $g \in G$). Maintenant que nous avons montré que HG_{i-1} est un sous-groupe normal de HG_i, le Théorème 4 implique que $\bar{G}_{i-1}$ est un sous-groupe normal de $\bar{G}_i$.

Par le deuxième théorème d'isomorphisme, nous avons $\bar{G}_i \cong G_i/H \cap G_i$ pour tout i. L'inclusion $G_{i-1} \hookrightarrow G_i$ induit un homomorphisme injectif

$$\bar{G}_{i-1} \cong G_{i-1}/H \cap G_{i-1} \hookrightarrow G_i/H \cap G_i \cong \bar{G}_i$$

Le quotient $\bar{G}_i/\bar{G}_{i-1}$ est isomorphe à G_i/K, où K est le sous-groupe de G_i engendré par G_{i-1} et $H \cap G_i$. Puisque G_{i-1} et $H \cap G_i$ sont tous deux des sous-groupes normaux de G_i, la deuxième remarque de la Proposition 7 implique que K est également normal dans G_i. Cependant, par le théorème de correspondance, la simplicité de G_i/G_{i-1} implique qu'il n'y a pas de sous-groupes normaux strictement contenus entre G_{i-1} et G_i. Par conséquent, G_i/K est soit le groupe trivial, soit un groupe simple, donc (115) est (après avoir supprimé les redondances) une série de composition. □

7.5

Nous allons maintenant étudier comment les séries de composition de groupes plus petits se relèvent à des groupes plus grands.

Proposition 22. *Supposons que nous ayons une suite exacte courte de groupes*

$$1 \to K \to G \xrightarrow{\pi} L \to 1$$

et que K et L aient des séries de composition

$$1 = K_0 \triangleleft K_1 \triangleleft \cdots \triangleleft K_{m-1} \triangleleft K_m = K$$

$$1 = L_0 \triangleleft L_1 \triangleleft \cdots \triangleleft L_{n-1} \triangleleft L_n = L$$

Alors il existe une série de composition

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{m+n-1} \triangleleft G_{m+n} = G \tag{116}$$

avec $G_i \cong K_i$ pour $i \leq m$ et $G_i \cong \pi^{-1}(L_{i-m})$ pour $i > m$.

Proof. Tout d'abord, il est clair que les m premières inclusions dans (116) sont des sous-groupes normaux, avec des quotients isomorphes à ceux dans la série de composition de K (ainsi les quotients sont simples). Quant aux m inclusions suivantes, le Théorème de correspondance 4 indique qu'il existe une correspondance bijective

$$\Big\{\text{sous-groupes } K \leq H \leq G\Big\} \leftrightarrow \Big\{\text{sous-groupes } \bar{H} \leq L\Big\}$$

donnée explicitement par $H = \pi^{-1}(\bar{H})$. La propriété 2 dudit théorème indique que les sous-groupes $\bar{H} \trianglelefteq \bar{H}'$ du côté droit correspondent aux sous-groupes $H \trianglelefteq H'$ du côté gauche, de telle sorte que

$$H'/H \cong \bar{H}'/\bar{H}$$

Cela montre que les n dernières inclusions dans (116) sont également des sous-groupes normaux, avec des quotients isomorphes à ceux dans la série de composition de L (ainsi les quotients sont simples).

□

7.6

Si un groupe possède une série de composition, il est probable qu'il en a plusieurs. Cependant, deux séries de composition quelconques sont liées par le résultat suivant, appelé le théorème de Jordan-Hölder.

Théorème 7. *Pour tout groupe G, deux séries de composition quelconques*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G = G'_\ell \triangleright G'_{\ell-1} \triangleright \cdots \triangleright G'_1 \triangleright G'_0 = 1 \tag{117}$$

sont ***équivalentes****, c'est-à-dire que les suites de quotients*

$$\Big\{G_1/G_0, \ldots, G_k/G_{k-1}\Big\} \quad \textit{et} \quad \Big\{G'_1/G'_0, \ldots, G'_\ell/G'_{\ell-1}\Big\} \tag{118}$$

sont identiques à une permutation et à un isomorphisme près. En particulier, $k = \ell$. Les (classes d'isomorphisme des) groupes (118) *sont appelés les* ***facteurs de composition*** *de G.*

Remarquons que l'équivalence des séries de composition est une relation d'équivalence. Avant de passer à la démonstration du théorème, donnons un exemple illustratif. Il existe deux séries de composition de longueur 2 pour $\mathbb{Z}/6\mathbb{Z}$, l'une impliquant le sous-groupe $\{0, 3\} \cong \mathbb{Z}/2\mathbb{Z}$ et l'autre impliquant le sous-groupe $\{0, 2, 4\} \cong \mathbb{Z}/3\mathbb{Z}$. Les facteurs de composition pour ces deux séries de composition sont $(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$ et $(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

Proof. Nous allons procéder par induction sur le nombre $\min(k, \ell)$ (et ensuite par $k + \ell$ pour départager les égalités). Le cas où ce nombre est égal à 1 est trivial, car un groupe simple ne peut pas avoir de série de composition de longueur ≥ 2, du fait qu'il n'a pas de sous-groupes normaux non triviaux. Supposons maintenant que $\min(k, \ell) \geq 2$, et prouvons l'étape d'induction. Nous pouvons supposer que $G_{k-1} \neq G'_{\ell-1}$ (sinon nous appliquons simplement l'hypothèse d'induction à $G_{k-1} = G'_{\ell-1}$ au lieu de G). Puisque G_{k-1} et $G'_{\ell-1}$ sont tous deux normaux dans G, leur produit

$$P = G_{k-1}G'_{\ell-1}$$

et leur intersection

$$H = G_{k-1} \cap G'_{\ell-1}$$

sont normaux dans G (voir la Proposition 7). Ensuite, le second théorème d'isomorphisme 3 implique que

$$G_{k-1}/H \cong P/G'_{\ell-1} \quad \text{et} \quad G'_{\ell-1}/H \cong P/G_{k-1}$$

Cependant, d'après le théorème de correspondance, $P/G'_{\ell-1}$ est un sous-groupe normal de $G/G'_{\ell-1}$. Comme ce dernier groupe est simple, il doit en découler que $P = G$, et nous obtenons ainsi les isomorphismes suivants de groupes simples

$$G_{k-1}/H \cong G/G'_{\ell-1} \quad \text{et} \quad G'_{\ell-1}/H \cong G/G_{k-1} \tag{119}$$

La Proposition 20 garantit que H possède une série de composition (dont la longueur m doit être inférieure ou égale à celles des séries de composition de G_{k-1} ou de $G'_{\ell-1}$, qui sont respectivement $\leq k-1$ et $\leq \ell-1$), que nous pouvons prolonger en séries de composition

$$1 \lhd H_1 \lhd \cdots \lhd H_{m-1} \lhd H \lhd G_{k-1} \lhd G \tag{120}$$

et

$$1 \lhd H_1 \lhd \cdots \lhd H_{m-1} \lhd H \lhd G'_{\ell-1} \lhd G \tag{121}$$

D'après l'hypothèse d'induction, (120) et (121) sont équivalentes aux séries de composition à gauche et à droite de (117), respectivement. Comme (120) et (121) sont équivalentes via (119), nous avons terminé.

□

Cours 8

8.1

Nous avons déjà rencontré des groupes qui possèdent des séries de composition (112). La notion suivante est alors liée.

Définition 22. *Un groupe G est appelé* ***résoluble*** *s'il possède une série sous-normale*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G \tag{122}$$

telle que G_{i-1} soit un sous-groupe normal propre de G_i et que G_i/G_{i-1} soit abélien, pour tout $i \in \{1, \ldots, k\}$.

La terminologie provient de la théorie de Galois, en particulier de la théorie des équations polynomiales qui admettent des solutions par radicaux, dans laquelle les groupes résolubles jouent un rôle clé. Plus précisément, si vous suivez un cours de théorie de Galois, vous rencontrerez certainement le résultat suivant.

Proposition 23. *Le groupe symétrique S_n n'est pas résoluble pour $n \geq 5$.*

Proof. Supposons que $G = S_n$ admette une série sous-normale (122) avec des quotients abéliens, et nous considérons une telle série de longueur maximale k. Comme S_n est fini, cela implique que les groupes quotient abéliens G_i/G_{i-1} sont finis pour tout $i \in \{1, \ldots, k\}$. Si l'un de ces groupes quotient abéliens G_i/G_{i-1} n'était pas isomorphe à $\mathbb{Z}/p\mathbb{Z}$, alors on pourrait trouver un sous-groupe propre $1 \subsetneq \bar{H} \subsetneq G_i/G_{i-1}$ (montrez ceci, c'est assez facile). Par le théorème de correspondance 4, cela signifierait l'existence d'un sous-groupe

$$G_{i-1} \triangleleft H \triangleleft G_i$$

ce qui contredit la maximalité du nombre k. Cependant, $\mathbb{Z}/p\mathbb{Z}$ est également un groupe simple, donc nous concluons que S_n admet une série de composition dont tous les facteurs sont $\mathbb{Z}/p\mathbb{Z}$. Cependant, cela contredit le théorème de Jordan-Hölder 7 et le fait que S_n admette la série de composition

$$1 \triangleleft A_n \triangleleft S_n$$

(rappelons d'après le théorème 6 que A_n est simple pour $n \geq 5$).

□

8.2

Les groupes résolubles possèdent des propriétés similaires aux groupes ayant des séries de composition, en particulier les analogues suivants des propositions 20, 21 et 22.

Proposition 24. *Tout sous-groupe d'un groupe résoluble est résoluble.*

Proof. La preuve suit celle de la proposition 20 de près, sauf qu'elle s'applique aux sous-groupes arbitraires et non seulement aux sous-groupes normaux. Ainsi, prenons un groupe résoluble G avec une série sous-normale

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G$$

avec chaque G_i/G_{i-1} abélien. Alors, pour tout sous-groupe $H \leq G$, considérons la série

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{k-1} \triangleleft H_k = H \tag{123}$$

avec $H_i = H \cap G_i$. On montre que H_{i-1} est un sous-groupe de H_i comme dans la preuve de la proposition 20, et de plus nous avons un analogue de l'homomorphisme injectif

$$H_i/H_{i-1} \overset{\varphi}{\hookrightarrow} G_i/G_{i-1}$$

de (114). Comme tout sous-groupe d'un groupe abélien est abélien, le fait que G_i/G_{i-1} soit abélien implique que H_i/H_{i-1} est abélien. Par conséquent, l'existence de la série (123) implique que H est résoluble.

□

Les résultats suivants se démontrent de la même manière que les propositions 21 et 22, donc nous ne répéterons pas les preuves.

Proposition 25. *Tout quotient d'un groupe résoluble est résoluble.*

Proposition 26. *Supposons que nous ayons une suite exacte courte de groupes*

$$1 \to K \to G \overset{\pi}{\to} L \to 1$$

avec K et L résolubles. Alors G est résoluble.

La Proposition 26 fournit une riche classe d'exemples de groupes résolubles : tout groupe qui peut être obtenu par un nombre fini d'étapes d'extensions (telles que les produits semi-directs) de groupes abéliens. Tous les groupes diédraux sont résolubles, de même que le groupe alterné A_4.

8.3

Nous allons maintenant donner une description alternative des groupes résolubles. Rappelons ce qui suit de Math 113.

Définition 23. *Étant donné un sous-ensemble X d'un groupe G, le plus petit sous-groupe $H \leq G$ qui contient X est appelé le sous-groupe **engendré** par X. Explicitement, H consiste en des produits arbitraires d'éléments de X et de leurs inverses.*

Définition 24. *Étant donnés des sous-ensembles $X, Y \subseteq G$, soit $[X, Y] \leq G$ le sous-groupe de G engendré par*

$$\left\{ xyx^{-1}y^{-1} \middle| x \in X, y \in Y \right\}$$

*Le **sous-groupe dérivé** (ou **sous-groupe des commutateurs**) de G est défini par*

$$\boxed{[G, G]} \tag{124}$$

Proposition 27. *Pour tout groupe G, le sous-groupe dérivé $[G,G]$ est un sous-groupe normal de G et*

$$G/[G,G]$$

est abélien. De plus, si $H \trianglelefteq G$ a la propriété que G/H est abélien, alors $[G,G] \subseteq H$.

Proof. Pour montrer qu'un sous-groupe est normal, il faut montrer qu'il est préservé par conjugaison avec un $h \in G$ quelconque. Cependant, la conjugaison de tout commutateur par g est un autre commutateur, car

$$gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$$

Ainsi, la conjugaison par g d'un produit quelconque de commutateurs est un produit de commutateurs, donc $[G,G]$ est un sous-groupe normal de G. Le quotient $G/[G,G]$ est clairement abélien puisque

$$[a][b][a^{-1}][b^{-1}] = [aba^{-1}b^{-1}] = e \in G/[G,G] \quad \Rightarrow \quad [a][b] = [b][a]$$

Plus généralement, pour tout sous-groupe normal $H \trianglelefteq G$ tel que le quotient G/H soit abélien, nous avons

$$[a][b][a^{-1}][b^{-1}] = [aba^{-1}b^{-1}] = e \text{ dans } G/H \quad \Rightarrow \quad aba^{-1}b^{-1} \in H$$

pour tous $a, b \in G$. Par conséquent, $[G,G] \subseteq H$.

□

8.4

Le sous-groupe dérivé d'un groupe est trivial si et seulement si le groupe est abélien. Mais le sous-groupe dérivé n'a pas besoin d'être abélien lui-même, donc on peut prendre le sous-groupe dérivé du sous-groupe dérivé, et ainsi de suite. Cela mène à la notion de **série dérivée** d'un groupe G, qui est définie comme

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G \tag{125}$$

où $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ est le sous-groupe dérivé de $G^{(i-1)}$ pour tout i.

Proposition 28. *Un groupe G est résoluble si et seulement si sa série dérivée devient éventuellement triviale, c'est-à-dire s'il existe un certain $k \in \mathbb{N}$ tel que $G^{(k)} = 1$.*

Proof. L'implication "si" est triviale, car si la série dérivée est finie, alors la Proposition 27 garantit qu'elle fournit précisément le type de série sous-normale avec quotients abéliens, qui caractérise les groupes résolubles. Pour prouver l'implication "seulement si", considérons un groupe résoluble G avec la série (122). La dernière phrase de la Proposition 27 garantit que

$$G^{(1)} \subseteq G_{k-1}$$

Prendre les sous-groupes dérivés dans l'inclusion ci-dessus implique

$$G^{(2)} \subseteq [G_{k-1}, G_{k-1}] \subseteq G_{k-2}$$

où la seconde inclusion découle également du fait que le quotient G_{k-1}/G_{k-2} est abélien (en invoquant la dernière phrase de la Proposition 27). Répéter cet argument $k-2$ fois de plus implique finalement $G^{(k)} \subseteq G_0 = 1$, ce qui signifie que la série dérivée devient éventuellement triviale.

□

8.5

Dans la Proposition 28, nous avons considéré la série des sous-groupes de commutateurs en partant de G, et montré qu'elle se termine si et seulement si G est résoluble. Une notion plus forte est la suivante.

Définition 25. *Un groupe G est appelé **nilpotent** si la suite de sous-groupes définie par $G^{\{0\}} = G$ et*

$$G^{\{i\}} = [G^{\{i-1\}}, G]$$

devient le groupe trivial 1 après un nombre fini d'étapes.

Pour un groupe abélien, on a $G^{\{1\}} = 1$, donc les groupes nilpotents peuvent être interprétés comme des généralisations des groupes abéliens. Pour un groupe nilpotent G, la suite de sous-groupes

$$\cdots \trianglelefteq G^{\{2\}} \trianglelefteq G^{\{1\}} \trianglelefteq G^{\{0\}} = G \tag{126}$$

est en fait une série normale, dans le sens où chaque $G^{\{i\}}$ est un sous-groupe normal de G. On peut le prouver par récurrence sur i : si l'on suppose que $G^{\{i-1\}}$ est normal dans G, alors tout commutateur

$$a \underbrace{ba^{-1}b^{-1}}_{\in G^{\{i-1\}}}, \quad \forall a \in G^{\{i-1\}}, b \in G \tag{127}$$

appartient à $G^{\{i-1\}}$, et donc $G^{\{i\}}$ est un sous-groupe de $G^{\{i-1\}}$. Le fait que $G^{\{i\}}$ soit normal dans G découle du fait que la conjugaison d'un élément de la forme (127) par un élément quelconque de G produit encore un élément de la forme (127), ce que nous vous laissons comme exercice.

Proposition 29. *Tout groupe nilpotent est résoluble.*

Proof. Soit G un groupe nilpotent. On peut prouver par récurrence sur i que $G^{(i)} \subseteq G^{\{i\}}$ pour tout i, ce qui est immédiat, mais important, donc nous vous laissons le soin de le vérifier. Par conséquent, le fait que la suite (126) se termine implique que (125) se termine, donc G est également résoluble. □

Cours 9

9.1

Dans le cours 6, nous avons étudié les p-groupes abéliens finis pour un certain nombre premier p, voir la définition 19. Nous allons maintenant abandonner l'hypothèse d'abelianité et étudier les p-groupes finis, c'est-à-dire les groupes dans lesquels l'ordre de chaque élément est une puissance de p (nous écrirons cela comme "a un ordre dans $p^{\mathbb{N}}$" désormais).

Lemme 13. *Un groupe fini est un p-groupe si et seulement s'il a un ordre p^n pour un certain $n \in \mathbb{N}$.*

L'implication " si " est une conséquence immédiate du théorème de Lagrange, car l'ordre de tout élément divise l'ordre du groupe. L'implication " seulement si " est une conséquence immédiate du résultat suivant, souvent appelé **premier théorème de Sylow**.

Théorème 8. *Soit G un groupe fini d'ordre*

$$|G| = p^n r$$

pour un certain nombre premier p, un certain $n \geq 0$ et un certain r premier avec p. Alors G possède un sous-groupe d'ordre p^n.

En effet, une fois que nous avons le théorème 8, l'énoncé " seulement si " du lemme 13 est assez immédiat. Si $|G|$ n'était pas une puissance de p, alors prenons un autre nombre premier $q \neq p$ qui divise $|G|$. Le théorème 8 garantit que $|G|$ a un sous-groupe d'ordre dans $q^{\mathbb{N}}$, et tout élément de ce sous-groupe aura un ordre dans $q^{\mathbb{N}}$. Cela contredit le fait que G est un p-groupe, c'est-à-dire que chaque élément a un ordre dans $p^{\mathbb{N}}$.

9.2

Il est clair que le cas $n = 0$ du théorème 8 est trivial, donc on suppose généralement $n > 0$.

Proof. du théorème 8 : Nous ferons une induction sur $|G|$ (le cas de base est $|G| = p$, qui est trivial, car le seul groupe d'ordre premier p est $\mathbb{Z}/p\mathbb{Z}$). S'il existe un sous-groupe propre $H < G$ tel que

$$[G : H] \text{ divise } r \tag{128}$$

alors $|H| = p^n r'$ pour un certain $r' < r$ premier avec p. L'hypothèse d'induction implique alors qu'il existe un sous-groupe de H d'ordre p^n, qui sera aussi le sous-groupe recherché de G d'ordre p^n. Il nous reste donc l'opposé logique de (128) : pour tous les sous-groupes propres $H < G$, nous avons

$$p \text{ divise } [G : H] \tag{129}$$

(en effet, puisque $[G : H] > 1$ est un diviseur de $|G| = p^n r$, alors (128) et (129) sont des énoncés logiquement opposés). Appliquons ensuite l'équation des classes (50)–(52)

$$|G| = \sum_{\text{classes de conjugaison } \widetilde{g}} .$$

Le côté gauche est un multiple de p. D'après (129), il en est de même pour tout terme de la somme du côté droit pour lequel $C_G(\widetilde{g}) \neq G$. Par conséquent, nous concluons que

$$\text{le nombre de classes de conjugaison pour lesquelles } \Big(C_G(\widetilde{g}) = G\Big) \text{ est un multiple de } p.$$

Cependant, un élément $g \in G$ a la propriété que $C_G(g) = G$ si et seulement si $g \in Z(G)$, le centre de G. Puisque chaque élément $g \in Z(G)$ appartient à sa propre classe de conjugaison, la formule ci-dessus se lit

$$p \text{ divise } |Z(G)|.$$

Comme $Z(G)$ est abélien, la proposition 17 implique qu'il existe un $g \in Z(G)$ d'ordre p. Par conséquent, le sous-groupe H engendré par g est d'ordre p et est normal car $g \in Z(G)$. Le groupe quotient

$$\bar{G} = G/H$$

est d'ordre $p^{n-1}r$. Par l'hypothèse d'induction, $\bar{G}$ possède un sous-groupe $\bar{K}$ d'ordre p^{n-1}. D'après le théorème de correspondance 4, ce sous-groupe correspond à un sous-groupe $K \leq G$ d'ordre p^n, comme requis.

□

9.3

Un sous-groupe d'ordre p^n comme dans le Théorème 8 est appelé un **sous-groupe de Sylow p-sous-groupe** de G. Il est d'usage de noter un tel sous-groupe par P. Les résultats suivants fournissent des informations supplémentaires sur ces sous-groupes. Nous commençons par le **deuxième théorème de Sylow**.

Théorème 9. *Tous les sous-groupes de Sylow p d'un groupe G sont conjugués les uns aux autres.*

En d'autres termes, si nous avons un sous-groupe de Sylow p $P \leq G$, alors tous les autres sous-groupes de Sylow p de G sont de la forme gPg^{-1} pour divers $g \in G$.

Proof. Considérons deux sous-groupes de Sylow p P et P', et considérons l'action à gauche de P sur l'ensemble des classes à gauche de P'

$$P \curvearrowright G/P'.$$

L'application de la formule (37) à cette action donne

$$r = |G/P'| = \sum_{\text{orbites } P\cdot x} \frac{|P|}{|\text{Stab}_P(x)|}.$$

Comme l'ordre de P est une puissance de p, toutes les orbites dans le membre de droite pour lesquelles $\text{Stab}_P(x) \neq P$ contribueront un multiple de p. Cependant, r est premier avec p, donc cela signifie qu'il doit y avoir au moins une orbite dont le stabilisateur est tout entier P. Cette orbite correspond précisément à une classe à gauche gP' qui est fixée par P, ce qui signifie que

$$hgP' = gP', \quad \forall h \in P \quad \Leftrightarrow \quad g^{-1}hg \in P', \quad \forall h \in P \quad \Leftrightarrow \quad P \subseteq gP'g^{-1}. \tag{130}$$

Cependant, le fait que $|P| = |P'|$ implique que nous devons avoir $P = gP'g^{-1}$, comme requis.

□

9.4

La réciproque du Théorème 9 est une déclaration évidente : tout conjugué d'un sous-groupe de Sylow p est un sous-groupe de Sylow p. Ainsi, si pour une raison quelconque il existe un unique sous-groupe de Sylow p, il doit être préservé par conjugaison, et serait donc normal. Dans cet esprit, il devient très important de calculer le nombre de sous-groupes de Sylow p, qui est le sujet du **troisième théorème de Sylow**.

Théorème 10. *Le nombre n_p de sous-groupes de Sylow p d'un groupe G possède les propriétés suivantes :*

- $n_p = [G : N_G(P)]$, *où P est un sous-groupe de Sylow p fixé, et n_p divise r*
- $n_p \equiv 1$ *modulo p*

Proof. Par le deuxième théorème de Sylow, la conjugaison induit une action transitive

$$G \curvearrowright \Big\{\text{sous-groupes de Sylow } p \text{ de } G\Big\} \tag{131}$$

et donc n_p est la cardinalité de l'unique orbite. Le stabilisateur de tout sous-groupe de Sylow p donné P n'est autre que le normalisateur $N_G(P)$. Par conséquent, le théorème de l'orbite-stabilisateur (36) implique que la cardinalité de l'unique orbite est

$$\frac{|G|}{|N_G(P)|} = [G : N_G(P)].$$

Puisque $P \leq N_G(P)$, nous avons que $n_p = [G : N_G(P)]$ divise $[G : P] = r$. Fixons maintenant un sous-groupe de Sylow p P et considérons la restriction de l'action de conjugaison (131) à

$$P \curvearrowright \Big\{\text{sous-groupes de Sylow } p \text{ de } G\Big\}.$$

L'application de (37) à cette action implique que

$$n_p = \sum_{\text{orbites } P\cdot P'} \frac{|P|}{|\mathrm{Stab}_P(P')|}.$$

Puisque $|P| = p^n$, chaque terme de la somme dans le membre de droite est un multiple de p, sauf pour les sous-groupes de Sylow p P' qui sont fixés par la conjugaison par tout élément de P. Si nous montrons que le seul sous-groupe de Sylow p P' ayant cette propriété est P lui-même, alors nous concluons que $n_p \equiv 1$ modulo p et nous avons terminé. Cependant, P' étant fixé par la conjugaison avec tout élément de P implique que

$$P \leq N_G(P')$$

Comme $|N_G(P')|$ divise $|G| = p^n r$, alors P est un sous-groupe de Sylow p de $N_G(P')$. D'autre part, P' est un sous-groupe normal de $N_G(P')$ (par la définition même du normalisateur), donc le deuxième théorème de Sylow (avec G remplacé par $N_G(P')$) implique que $P = P'$, comme désiré.

□

9.5

Exemplifions maintenant les théorèmes de Sylow pour le groupe diédral D_{2n}. Le lemme suivant sera utile.

Lemme 14. *Considérons un sous-groupe normal $H \trianglelefteq G$ d'un groupe fini G. Alors pour tout nombre premier p, l'intersection d'un p-sous-groupe de Sylow de G avec H sera un p-sous-groupe de Sylow de H.*

Proof. Soit P un p-sous-groupe de Sylow de G. Comme le groupe $H \cap P$ a un ordre en $p^{\mathbb{N}}$, nous devons montrer que $[H : H \cap P]$ est premier avec p afin de garantir que l'ordre de $H \cap P$ est la puissance maximale de p qui divise $|H|$. Le deuxième théorème d'isomorphisme 3 implique que HP est un groupe d'ordre

$$|HP| = \frac{|H||P|}{|H \cap P|}$$

Ainsi,

$$[HP : P] = [H : H \cap P]$$

Comme HP est un sous-groupe de G, le nombre à gauche de l'affichage ci-dessus divise $[G : P]$, qui est premier avec p par définition d'un p-sous-groupe de Sylow. Par conséquent, le nombre à droite de l'affichage ci-dessus sera également premier avec p, ce qui implique que $H \cap P$ est un p-sous-groupe de Sylow de H.

□

Appliquons le lemme ci-dessus pour $G = D_{2n}$ et $H \cong \mathbb{Z}/n\mathbb{Z}$ étant le sous-groupe normal des rotations, où $n = 2^k r$ pour un r impair. Comme $\mathbb{Z}/n\mathbb{Z}$ est abélien, il possède un unique 2-sous-groupe de Sylow, à savoir

$$P = \{0, r, 2r, \ldots, (2^k - 1)r\} \subseteq \{0, 1, 2, \ldots, 2^k r - 1\} = \mathbb{Z}/n\mathbb{Z}$$

Tout 2-sous-groupe de Sylow de $G = D_{2n}$ a un ordre 2^{k+1} et contient le sous-groupe d'ordre 2^k P par le lemme 14. Par conséquent, si nous prenons une réflexion quelconque $\tau \in G - H$, alors tout 2-sous-groupe de Sylow doit être de la forme

$$P_\tau = P \sqcup P\tau \tag{132}$$

Cependant, tout ensemble P_τ est un sous-groupe de G (essayez de le prouver), de sorte qu'il y a autant de 2-sous-groupes de Sylow que de réflexions τ modulo la multiplication à gauche par P. Comme il y a n réflexions au total et $|P| = 2^k$, il existe alors r 2-sous-groupes de Sylow distincts P_τ, ce qui soutient le troisième théorème de Sylow 10. Par le même théorème, le fait que $n_2 = r$ implique que $N_G(P_\tau) = P_\tau$, ce que vous pouvez également essayer de prouver vous-même. Enfin, comme toutes les réflexions sont conjuguées les unes aux autres, il est clair que tous les 2-sous-groupes de Sylow (132) sont également conjugués entre eux, ce qui soutient le deuxième théorème de Sylow 9.

Cours 10

10.1

Nous allons maintenant utiliser les théorèmes de Sylow pour tirer des conclusions sur les groupes finis dont les ordres ont peu de facteurs premiers. Tout d'abord, rappelons le fait fondamental que tout groupe G d'ordre p est isomorphe à

$$\mathbb{Z}/p\mathbb{Z}.$$

Pour le voir, prenons un élément $g \in G$ non égal à l'identité. Comme l'ordre de g divise $|G| = p$, l'ordre de g doit être égal à p, et donc G est égal au groupe cyclique engendré par g.

Proposition 30. *Si p et q sont des nombres premiers distincts tels que $p \nmid q-1$ et $q \nmid p-1$, tout groupe d'ordre pq est isomorphe à*

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{133}$$

Notez qu'un tel groupe est également cyclique, en raison de (90).

Proof. Supposons que $|G| = pq$. D'après le troisième théorème de Sylow, le nombre n_p de p-sous-groupes de Sylow divise q et est congru à 1 modulo p, donc la seule option est que $n_p = 1$. De manière similaire, nous devons avoir $n_q = 1$. Ainsi, nous avons un seul p-sous-groupe de Sylow P et un seul q-sous-groupe Q, et ils doivent être des sous-groupes normaux de G. Notez que $P \cap Q = \{e\}$, car tout élément dans l'intersection de P et Q aurait un ordre divisant à la fois les nombres premiers distincts p et q. Mais alors, nous avons un isomorphisme

$$PQ \cong P \times Q \tag{134}$$

(vous avez prouvé cela en Math 113, rappelons l'argument : la fonction $P \times Q \to PQ, (x, y) \mapsto xy$ est injective car $P \cap Q = \{e\}$. Elle est surjective par définition, et le fait qu'elle soit un homomorphisme découle de $xy = yx$ pour tous $x \in P, y \in Q$, ce qui à son tour est dû au fait que le commutateur $xyx^{-1}y^{-1}$ appartient à $P \cap Q = \{e\}$. La dernière affirmation utilise le fait que P et Q sont tous deux normaux). Puisque $|P| = p$ et $|Q| = q$, alors $P \cong \mathbb{Z}/p\mathbb{Z}$ et $Q \cong \mathbb{Z}/q\mathbb{Z}$, tandis que $|PQ| = pq \Rightarrow PQ = G$. Ainsi (134) $\Rightarrow$ (133).

□

Notez que la Proposition 30 échoue si $p|q-1$. Par exemple, $D_6 \cong S_3$ est un groupe non abélien d'ordre 6.

10.2

Bien qu'il n'utilise pas les théorèmes de Sylow, le résultat de classification suivant est également très important.

Proposition 31. *Si p est un nombre premier, alors tout groupe d'ordre p^2 est isomorphe soit à*

$$\mathbb{Z}/p^2\mathbb{Z} \quad \textit{ou} \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}. \tag{135}$$

L'un des éléments clés dans la preuve de la Proposition 31 est le suivant.

Lemme 15. *Si G est un p-groupe fini non trivial pour un certain nombre premier p, alors $Z(G)$ est non trivial.*

Proof. L'équation des classes (50) donne

$$|G| = |Z(G)| + \sum_{\text{classes de conjugaison } \widetilde{g} \text{ de cardinalité } >1} |\widetilde{g}|.$$

Cependant, comme $|G| = p^n$ avec $n > 0$ et que la cardinalité de toute classe de conjugaison divise $|G|$ (grâce à la formule (52)), nous concluons que $|Z(G)|$ est un multiple de p. Par conséquent, $Z(G)$ doit être non trivial.

□

Proof. de la Proposition 31 : Soit G un groupe d'ordre p^2. Comme son centre $Z(G)$ est non trivial d'après le Lemme 15, le centre doit avoir un ordre égal à p^2 ou p. Dans le premier cas, G doit être abélien, donc la Proposition 18 implique que G doit être isomorphe à l'une des deux options dans (135). Dans le second cas, considérons un élément $g \in G - Z(G)$ et posons $H = C_G(g)$. Nous affirmons que

$$Z(G) \subsetneq H \subsetneq G$$

ce qui est une contradiction car le nombre $|H|$ devrait être simultanément un multiple propre de $p = |Z(G)|$ et un diviseur propre de $p^2 = |G|$. La première inclusion stricte $\subsetneq$ ci-dessus est due au fait que $g \in H - Z(G)$, tandis que la seconde inclusion stricte $\subsetneq$ est due au fait que $H = G$ impliquerait $g \in Z(G)$.

□

10.3

La combinaison des idées des Propositions 30 et 31 nous donne le résultat suivant.

Proposition 32. *Si p et q sont des nombres premiers distincts tels que $p \nmid q - 1$ et $q \nmid p^2 - 1$, tout groupe d'ordre p^2q est isomorphe soit à*

$$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \quad ou \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Proof. Comme dans la preuve de la Proposition 30, il existe un unique p-sous-groupe de Sylow P et un unique q-sous-groupe de Sylow Q. Ces sous-groupes doivent être normaux par le troisième théorème de Sylow et les hypothèses $p \nmid q - 1$ et $q \nmid p^2 - 1$, et leur intersection est triviale. Par conséquent, (134) est vérifiée pour la même raison que dans la preuve de la Proposition 30, et la preuve est complétée par la classification des groupes d'ordre p^2 dans la Proposition 31.

□

Cependant, même lorsque les hypothèses de non-divisibilité des Propositions 30 et 32 ne sont pas satisfaites, nous pouvons toujours utiliser les théorèmes de Sylow pour déduire des informations importantes sur les groupes. Par exemple, vous avez démontré le résultat suivant par des moyens élémentaires dans le cours Math 113, mais utiliser les théorèmes de Sylow est beaucoup plus rapide.

Proposition 33. *Tout groupe d'ordre 12 est isomorphe soit à*

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad ou \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad ou \quad A_4 \quad ou \quad D_{12} \tag{136}$$

ou au ***groupe dicyclique*** *que nous définirons au cours de la preuve.*

Proof. Supposons $|G| = 12$ et considérons le nombre n_3 de 3-sous-groupes de Sylow. Par le troisième théorème de Sylow 10, nous avons $n_3|4$ et $n_3 \equiv 1 \bmod 3$. Ainsi, n_3 peut être égal soit à 1, soit à 4. Dans le cas $n_3 = 4$, nous avons quatre 3-sous-groupes de Sylow, que nous noterons P_1, P_2, P_3, P_4. Comme ils sont d'ordre 3, ces sous-groupes ne peuvent s'intersecter que dans l'élément neutre, ce qui signifie que notre groupe contient au moins $2 \times 4 = 8$ éléments d'ordre 3. Considérons l'action

$$G \curvearrowright \Big\{P_1, P_2, P_3, P_4\Big\}, \qquad g \cdot P_i = gP_ig^{-1}$$

ce qui induit un homomorphisme $f : G \to S_4$. Le troisième théorème de Sylow 10 implique que $4 = n_3 = [G : N_G(P_i)]$, donc $|N_G(P_i)| = P_i$ pour tout i. Ainsi, le noyau de f doit être contenu dans P_i pour tout i. Comme nous l'avons expliqué dans le paragraphe précédent, $P_i \cap P_j = \{e\}$ pour tout $i \neq j$, donc le noyau de f est trivial. Par conséquent, G est isomorphe à un sous-groupe de S_4. Cependant, rappelez-vous que G contient au moins 8 éléments d'ordre 3. Dans le groupe symétrique S_4, les seuls éléments d'ordre 3 sont les cycles de longueur 3, qui sont tous contenus dans le groupe alterné A_4. Par conséquent, le sous-groupe $|\text{Im } f \cap A_4|$ de A_4 a un ordre d'au moins 8. Cependant, comme l'ordre de ce sous-groupe doit diviser $12 = |A_4|$, la seule option est $\text{Im } f = A_4$, ce qui implique que $G \cong A_4$.

Considérons maintenant le cas $n_3 = 1$, c'est-à-dire qu'il existe un unique 3-sous-groupe de Sylow de G, et ce sous-groupe doit donc être normal par le deuxième théorème de Sylow 9. Nous obtenons ainsi une suite exacte courte

$$0 \to \mathbb{Z}/3\mathbb{Z} \to G \xrightarrow{\pi} L \to 0$$

où L est un groupe d'ordre 4. Cependant, soit P un 2-sous-groupe de Sylow de G. Comme son intersection avec $\mathbb{Z}/3\mathbb{Z}$ se limite à l'élément neutre (sinon P contiendrait un sous-groupe d'ordre 3, ce qui est impossible pour un groupe d'ordre 4), alors π induit un isomorphisme $\pi' : P \cong L$ de groupes d'ordre 4. L'inverse de π' fournit précisément un scindement pour π, et donc la Proposition 10 implique que

$$G \cong \mathbb{Z}/3\mathbb{Z} \rtimes L$$

pour une certaine action $L \curvearrowright \mathbb{Z}/3\mathbb{Z}$ par automorphismes. Si cette action est triviale, alors les deux possibilités $L \cong \mathbb{Z}/4\mathbb{Z}$ et $L \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nous donnent les deux premières options dans (136). D'autre part, nous devons classifier les actions non triviales de L par automorphismes sur $\mathbb{Z}/3\mathbb{Z}$. Comme le seul automorphisme non trivial de $\mathbb{Z}/3\mathbb{Z}$ est $\Phi(k) = (2k \bmod 3)$, alors à isomorphisme près, nous avons deux options :

$$\begin{array}{lll} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{Z}/3\mathbb{Z}, & (a,b) \bmod 2 \text{ agit par } \Phi^a & \Rightarrow \quad G \cong D_{12} \\ \mathbb{Z}/4\mathbb{Z} \curvearrowright \mathbb{Z}/3\mathbb{Z}, & a \bmod 4 \text{ agit par } \Phi^a & \Rightarrow \quad G = \text{Dic}_{12}. \end{array}$$

La dernière égalité est la définition du groupe dicyclique Dic_{12}. Dans la première équation ci-dessus, je prétends que le groupe diédral $\mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est également isomorphe à $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ car l'action du dernier facteur de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$ est triviale. C'est un fait général sur les actions par automorphismes que nous vous laissons vérifier : pour toute action $L \curvearrowright K$ par automorphismes et tout groupe H, il existe un isomorphisme de produits semi-directs $(K \times H) \rtimes L \cong K \rtimes (L \times H)$, où dans le côté gauche l'action sur H est triviale et dans le côté droit l'action de H est triviale.

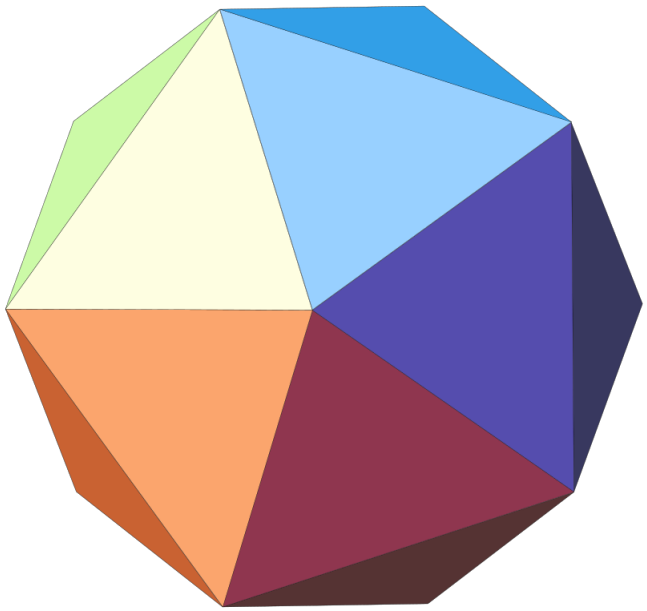
□

10.4

Comme montré dans le Théorème 6, le groupe alterné A_5 est un groupe simple d'ordre $\frac{5!}{2} = 60$. Dans le résultat suivant, nous utiliserons les théorèmes de Sylow pour montrer qu'il s'agit du seul groupe de ce type.

Proposition 34. *Si G est un groupe simple d'ordre 60, alors $G \cong A_5$.*

Une conséquence intéressante de la Proposition 34 est que A_5 est isomorphe au groupe icosaédrique I, c'est-à-dire le groupe des rotations de l'espace tridimensionnel qui préservent un icosaèdre régulier [1].



En effet, décrire géométriquement les rotations en question (ce que nous ne ferons pas) permet de classifier les classes de conjugaison de I. La réponse révèle que l'équation des classes (50) pour I est

$$60 = 1 + 12 + 12 + 15 + 20.$$

Si I avait un sous-groupe normal propre H, alors par normalité, H devrait être une réunion disjointe de classes de conjugaison (ainsi $|H| = 1 +$ un sous-ensemble propre des nombres 12, 12, 15, 20), tandis qu'en tant que sous-groupe, $|H|$ devrait diviser 60. Il est facile de voir que cela est numériquement impossible, donc I est un groupe simple. Mais alors la Proposition 34 implique que $I \cong A_5$.

Proof. de la Proposition 34 : Supposons que G possède un sous-groupe H d'indice $n \in \{2, 3, 4, 5\}$. L'action à gauche

$$G \curvearrowright \Big\{\text{classes à gauche de } H\Big\}$$

[1] Source de l'image : https://commons.wikimedia.org/w/index.php?curid=18278544

est transitive, ce qui induit un homomorphisme non trivial $f : G \to S_n$. Puisque G est simple, il n'a pas de sous-groupes normaux propres, et donc f doit être injectif. Cela est clairement impossible pour $n \in \{2, 3, 4\}$ pour des raisons de cardinalité, tandis que pour $n = 5$, cela implique que G est isomorphe à un sous-groupe d'indice 2 dans S_n. Cependant, tout sous-groupe d'indice 2 est normal, et le seul sous-groupe normal de S_5 est A_5 (sinon nous étendrions le sous-groupe normal en question à une série de composition de S_5 non équivalente à $1 \triangleleft A_5 \triangleleft S_5$, ce qui contredirait le Théorème de Jordan-Hölder 7).

Nous pouvons donc supposer que tous les sous-groupes de G ont un indice ≥ 6, c'est-à-dire ont un ordre ≤ 10. Cependant, considérons le nombre n_2 de 2-sous-groupes de Sylow. Par le troisième Théorème de Sylow 10, ce nombre divise 15 et est égal à l'indice d'un sous-groupe de G, donc la seule option est $n_2 = 15$. Nous avons donc des 2-sous-groupes de Sylow distincts $P_1, \ldots, P_{15}$ d'ordre 4 (donc abéliens), et étudions leurs intersections.

- Si $P_i \cap P_j \supsetneq \{e\}$ pour certains $i \neq j$, alors choisissons un élément $e \neq g \in P_i \cap P_j$. Puisque P_i et P_j sont abéliens, nous avons $P_i, P_j \leq C_G(g)$. Cependant, l'ordre du sous-groupe $C_G(g)$ devrait être ≥ 6 (car il contient $P_i \cup P_j$ comme sous-ensemble), un multiple de 4 (car il contient P_i comme sous-groupe), un diviseur de 60 (car il est un sous-groupe de G) et ≤ 10 (par l'hypothèse au début du paragraphe ci-dessus). Cela est clairement impossible pour des raisons numériques.

- Si $P_i \cap P_j = \{e\}$ pour tous $i \neq j$, alors $P_1 \cup \cdots \cup P_{15}$ contient $1 + 3 \times 15 = 46$ éléments, ayant tous un ordre égal à 1, 2 ou 4. Cependant, par le troisième Théorème de Sylow 10, le nombre n_5 est l'indice d'un sous-groupe de G, et donc $n_5 \geq 6$ par l'hypothèse au début du paragraphe ci-dessus. Nous avons donc au moins 6 5-sous-groupes de Sylow, qui doivent tous être isomorphes à $\mathbb{Z}/5\mathbb{Z}$ et qui ne peuvent pas s'intersecter sauf en l'élément identité (en effet, montrez que dans tout groupe, différents sous-groupes isomorphes à $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p'\mathbb{Z}$ pour des nombres premiers p, p' s'intersectent uniquement en l'élément identité). Ainsi, G contient au moins $4 \times 6 = 24$ éléments d'ordre 5, et comme $46 + 24 > 60$, nous avons compté plus d'éléments que le groupe G ne peut en contenir.

□

Cours 11

11.1

La formule (107) montre que tout groupe abélien fini est un produit direct de p-groupes abéliens. Pour obtenir un résultat similaire dans le cas non abélien, nous devons rappeler la définition des groupes nilpotents donnée dans la Définition 25. Avec cela en tête, le résultat principal de ce cours est le suivant.

Théorème 11. *Un groupe fini G est nilpotent si et seulement s'il peut être écrit comme*

$$G \cong P_1 \times \cdots \times P_k \tag{137}$$

pour des nombres premiers distincts $p_1, \ldots, p_k$, où chaque P_i est un p_i-groupe fini.

Notez que, puisque chaque P_i est normal dans le membre de droite de (137), nous concluons que P_i correspondrait au sous-groupe de Sylow p_i unique de G. En fait, la preuve du Théorème 11 montre qu'un groupe fini est nilpotent si et seulement si tous ses sous-groupes de Sylow sont normaux. Avant d'entamer la preuve du Théorème 11, nous devons donner une caractérisation alternative des groupes nilpotents.

Proposition 35. *Un groupe G est nilpotent si et seulement s'il possède une* ***série centrale***

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G \tag{138}$$

c'est-à-dire une série dans laquelle chaque G_{i-1} est un sous-groupe normal de G (et pas seulement de G_i), et chaque quotient G_i/G_{i-1} est contenu dans le centre de G/G_{i-1}.

Proof. La condition que $G_i/G_{i-1} \leq Z(G/G_{i-1})$ est équivalente à exiger que

$$[G_i, G] \leq G_{i-1}$$

pour tout $i \in \{1, \ldots, k\}$. Si G est nilpotent, une fois que nous supprimons tous les doublons de la série (126), nous obtiendrons la série requise (138). Réciproquement, si nous avons une série centrale (138), il est simple, et laissé comme exercice, de démontrer par récurrence sur i que

$$G^{\{i\}} \leq G_{k-i}$$

Par conséquent, nous aurons $G^{\{k\}} = 1$, ce qui signifie que G est nilpotent.

□

11.2

La caractérisation des groupes nilpotents donnée dans la Proposition 35 est plus robuste que la définition originale. En particulier, elle rend assez simple de prouver les analogues suivants des Propositions 24, 25 et 26.

Proposition 36. *Tout sous-groupe d'un groupe nilpotent est nilpotent.*

Proposition 37. *Tout quotient d'un groupe nilpotent est nilpotent.*

Proposition 38. *Supposons que nous ayons une suite exacte courte de groupes*

$$1 \to K \to G \xrightarrow{\pi} L \to 1$$

avec $K \leq Z(G)$ et L nilpotent. Alors G est nilpotent.

Les preuves des Propositions 36 et 37 sont très similaires aux résultats analogues pour les groupes résolubles, donc nous laissons les détails comme exercice. Nous présenterons les détails de la preuve de la Proposition 38 en raison de l'hypothèse supplémentaire $K \leq Z(G)$, qui n'était pas présente dans le cas des groupes résolubles.

Proof. de la Proposition 38 : Considérons une série centrale

$$1 = L_0 \triangleleft L_1 \triangleleft \cdots \triangleleft L_{k-1} \triangleleft L_k = L$$

dans laquelle chaque quotient L_i/L_{i-1} est contenu dans le centre de L/L_{i-1}. Ensuite, définissons

$$G_{i+1} = \pi^{-1}(L_i)$$

pour tout $i \geq 0$. Notez que $G_1 = K$. Nous affirmons que

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_k \triangleleft G_{k+1} = G$$

est la série centrale requise de G. Le fait que chaque G_{i+1} soit normal dans G découle du théorème de correspondance appliqué au fait que chaque L_i est normal dans L. Par ailleurs, la propriété

$$[G_{i+1}, G] \leq G_i$$

découle immédiatement de $[L_i, L] \leq L_{i-1}$ pour tout $i \geq 1$ (merci de vérifier cela). Enfin, le fait que

$$[G_1, G] = 1$$

résulte du fait que $G_1 = K$ est contenu dans le centre de G.

□

11.3

Montrons que le produit direct de groupes nilpotents est nilpotent en utilisant la définition originale 25. En effet, nous vous laissons démontrer par récurrence sur i que

$$(G \times G')^{\{i\}} \cong G^{\{i\}} \times G'^{\{i\}}.$$

L'isomorphisme ci-dessus, pour i suffisamment grand, montre que

$$\textbf{si } G \textbf{ et } G' \textbf{ sont nilpotents, alors } G \times G' \textbf{ est nilpotent} \tag{139}$$

Proposition 39. *Pour tout nombre premier p, tout p-groupe fini est nilpotent.*

Proof. Nous allons raisonner par récurrence sur l'ordre de G. Comme montré dans le Lemme 15, $|Z(G)| > 1$. Par conséquent, la Proposition 37 implique que $G/Z(G)$ est un p-groupe d'ordre strictement inférieur à celui de G. Par l'hypothèse de récurrence, $G/Z(G)$ est donc nilpotent. Cependant, G est (de manière tautologique) une extension de ce sous-groupe nilpotent par le centre $Z(G)$, donc la Proposition 38 implique que G est nilpotent.

□

Comme nous avons déjà montré que le produit direct de groupes nilpotents est nilpotent, la Proposition 39 établit que tout groupe apparaissant dans le membre de droite de (137) est nilpotent. Par conséquent, pour compléter la preuve du Théorème 11, nous devons montrer que tout groupe nilpotent fini se décompose en produit direct de ses sous-groupes de Sylow p. Cela fera l'objet des sous-sections suivantes.

11.4

La dernière propriété technique des groupes nilpotents concerne le comportement des normalisateurs des sous-groupes.

Proposition 40. *Tout groupe nilpotent G possède la **propriété du normalisateur**, c'est-à-dire que pour tout sous-groupe propre $H < G$, nous avons*

$$H \subsetneq N_G(H) \tag{140}$$

En d'autres termes, "les normalisateurs des sous-groupes croissent strictement".

Proof. Soit G un groupe nilpotent, et considérons un sous-groupe quelconque $H < G$. Considérons la série normale (126), et un entier naturel i tel que

$$G^{\{i\}} \subseteq H$$

(un tel i existe car $G^{\{k\}} = 1$ pour k suffisamment grand). Cependant, nous affirmons que

$$G^{\{i-1\}} \subseteq N_G(H)$$

car pour tout $g \in G^{\{i-1\}}$ et tout $h \in H$, nous avons

$$ghg^{-1}h^{-1} \in G^{\{i\}} \subseteq H \quad \Rightarrow \quad ghg^{-1} \in H.$$

Ainsi, si H ne respectait pas la propriété du normalisateur, c'est-à-dire si $H = N_G(H)$, alors l'argument ci-dessus impliquerait récursivement que $G = G^{\{0\}} \subseteq H$, ce qui contredit le fait que H est un sous-groupe propre.

□

11.5

Pour les groupes finis, la réciproque de la Proposition 40 est également vraie. En effet, tout ce que nous utiliserons dans la preuve suivante du Théorème 11 est que si un groupe fini G satisfait la propriété du normalisateur (140) pour tout sous-groupe propre $H < G$, alors G est le produit direct de ses sous-groupes de Sylow (et donc nilpotent par (139) et Proposition 39).

Proof. du Théorème 11 : L'implication "si" découle de (139) et de la Proposition 39. Pour prouver l'implication "seulement si", considérons un groupe nilpotent fini G et soit $p_1, \ldots, p_k$ les diviseurs premiers distincts de $|G|$. Soient

$$P_1, \ldots, P_k$$

les sous-groupes de Sylow de G correspondant aux nombres premiers $p_1, \ldots, p_k$. Pour chaque $i \in \{1, \ldots, k\}$, posons

$$H_i = N_G(P_i). \tag{141}$$

Si $H_i = G$ pour tout i, alors chaque P_i est normal, et donc le sous-groupe de Sylow p_i unique d'après le Théorème 9. Si cela est vrai, alors nous affirmons que la fonction

$$P_1 \times \cdots \times P_k \xrightarrow{\tau} G, \qquad (g_1, \ldots, g_k) \mapsto g_1 \ldots g_k$$

est un isomorphisme. Cela découle des points ci-dessous :

- τ *est un homomorphisme :* pour tout $i \neq j$, tout $g_i \in P_i$ commute avec tout $g_j \in P_j$. À cette fin, notons que la normalité de P_i et P_j implique que le commutateur $g_i g_j g_i^{-1} g_j^{-1}$ appartient à la fois à P_i et P_j. Cependant, tout élément dans l'intersection $P_i \cap P_j$ aurait un ordre divisant à la fois une puissance de p_i et une puissance de p_j, donc l'ordre devrait être 1.

- τ *est injective :* si $g_1 \ldots g_k = g_1' \ldots g_k'$ pour divers $g_i, g_i' \in P_i$, alors le point précédent implique que

$$(g_1' g_1^{-1}) \ldots (g_k' g_k^{-1}) = e \quad \Rightarrow \quad \underbrace{(g_1' g_1^{-1}) \ldots (g_{k-1}' g_{k-1}^{-1})}_{x} = \underbrace{(g_k' g_k^{-1})^{-1}}_{y}$$

  L'ordre de l'élément noté x ci-dessus divise une puissance de $p_1 \ldots p_{k-1}$, tandis que l'ordre de l'élément noté y divise une puissance de p_k. Puisque $x = y$, la seule possibilité est que ces éléments soient l'identité, donc $g_k' = g_k$. Par analogie, on prouve que $g_{k-1}' = g_{k-1}, \ldots, g_1' = g_1$.

- *Le domaine et l'image de* τ *ont le même ordre :* cela découle du fait que l'ordre d'un sous-groupe de Sylow p est, par définition, la puissance maximale de p qui divise l'ordre du groupe.

Ayant prouvé le Théorème sous l'hypothèse que les sous-groupes H_i de (141) sont tous égaux à G, supposons maintenant par l'absurde que l'un de ces H_i est un sous-groupe propre de G. Si en effet $H_i < G$ pour un $i \in \{1, \ldots, k\}$, alors la propriété du normalisateur (140) implique qu'il existe $g \in N_G(H_i) - H_i$. Nous avons alors

$$gP_i g^{-1} \subseteq gH_i g^{-1} = H_i$$

donc nous concluons que P_i et $gP_i g^{-1}$ sont tous deux des sous-groupes de Sylow p_i de H_i. Par le deuxième Théorème de Sylow 9, il existe un $h \in H_i$ tel que

$$gP_i g^{-1} = hP_i h^{-1} \quad \Rightarrow \quad (h^{-1}g)P_i = P_i(h^{-1}g)$$

ce qui implique que $h^{-1}g \in H_i$. Cela contredit le fait que $g \in N_G(H_i) - H_i$.

□

Cours 12

12.1

Nous allons maintenant développer ce qui est, en un sens, l'une des classes les plus générales (et fondamentales) de groupes existants. Fixons un ensemble S, et définissons un **mot** dans S comme étant toute séquence

$$s_1^{\pm 1} s_2^{\pm 1} \dots s_k^{\pm 1} \tag{142}$$

pour des $s_1, \dots, s_k \in S$ quelconques, où nous écrivons $s^{+1} = s$ et considérons s^{-1} comme un symbole formel, pour tout $s \in S$. Un mot est appelé **réduit** s'il ne contient pas les séquences de longueur 2 ss^{-1} ou $s^{-1}s$, $\forall s \in S$.

Définition 26. *Le **groupe libre** F_S sur S est l'ensemble des mots réduits, muni d'une structure de groupe avec :*

- *l'élément neutre donné par le mot vide ;*
- *l'inverse de* (142) *donné par $s_k^{\mp 1} \dots s_2^{\mp 1} s_1^{\mp 1}$;*
- *le produit de deux mots donné par la concaténation, suivie de la suppression de toutes les séquences ss^{-1} et $s^{-1}s$ (pour divers $s \in S$) afin de rendre le résultat un mot réduit.*

Nous vous laissons montrer que les axiomes de groupe sont satisfaits dans F_S. Toute fonction $f : S \to S'$ induit un homomorphisme (que nous appellerons aussi, par abus) $f : F_S \to F_{S'}$, défini par la formule

$$s_1^{\pm 1} \dots s_k^{\pm 1} \rightsquigarrow f(s_1)^{\pm 1} \dots f(s_k)^{\pm 1}$$

pour tous les mots (142).

Lemme 16. *Pour tout ensemble S et tout groupe G, il existe une correspondance bijective*

$$\Psi_{S,G} : \Big\{ \textit{fonctions } S \to G \Big\} \leftrightarrow \Big\{ \textit{homomorphismes } F_S \to G \Big\} \tag{143}$$

*qui est **fonctorielle** au sens où le diagramme*

$$\begin{array}{ccc} \Big\{ \textit{fonctions } S \to G \Big\} & \xrightarrow{\Psi_{S,G}} & \Big\{ \textit{homomorphismes } F_S \to G \Big\} \\ \downarrow & & \downarrow \\ \Big\{ \textit{fonctions } S' \to G' \Big\} & \xrightarrow{\Psi_{S',G'}} & \Big\{ \textit{homomorphismes } F_{S'} \to G' \Big\} \end{array} \tag{144}$$

commute pour toutes fonctions $f : S' \to S$ et tous homomorphismes $g : G \to G'$ (les flèches verticales sont données par la composition avec f et g, selon le cas).

Proof. Le contenu de (143) est simplement que toute fonction $\alpha : S \to G$ peut être prolongée de manière unique en un homomorphisme $\beta : F_S \to G$. Cependant, cela découle simplement du fait que les axiomes d'un homomorphisme nous obligent à définir

$$\beta\left(s_1^{\pm 1} \dots s_k^{\pm 1}\right) = \alpha(s_1)^{\pm 1} \dots \alpha(s_k)^{\pm 1}$$

pour tous les mots (142). La fonctorialité est vraiment facile à voir, donc réfléchissez-y par vous-même.

□

12.2

Nous avons $F_\emptyset = 1$ et $F_{\{x\}} = \{x^n | n \in \mathbb{Z}\} \cong \mathbb{Z}$. Cependant, dès que l'ensemble S contient au moins deux éléments, le groupe libre F_S est un groupe assez grand et compliqué. De plus, le résultat suivant montre que des ensembles S différents produisent des groupes libres F_S non isomorphes, ce qui rend cette construction très riche.

Théorème 12. *Il existe un isomorphisme $F_S \overset{\cong}{\leftrightarrow} F_T$ si et seulement s'il existe une bijection $S \leftrightarrow T$.*

Avant de démontrer le Théorème ci-dessus, introduisons une notion étroitement liée à celle de groupes libres. Rappelons le sous-groupe dérivé (124). Pour tout ensemble S, le groupe

$$\boxed{F_S^{\text{ab}} = F_S \Big/ [F_S, F_S]}$$

est appelé le **groupe abélien libre** sur S.

Proposition 41. *Pour tout ensemble S, nous avons un isomorphisme*

$$F_S^{\text{ab}} \cong \mathbb{Z}^S = \bigoplus_{s \in S} \mathbb{Z} \cdot s$$

En particulier, si $|S| = r$, alors $F_S^{\text{ab}} \cong \mathbb{Z}^r$.

Proof. Considérons les fonctions

$$\mathbb{Z}^S \to F_S^{\text{ab}}, \qquad \sum_{s \in S} n_s \cdot s \mapsto \prod_{s \in S} s^{n_s} \tag{145}$$

pour toutes les collections $\{n_s \in \mathbb{Z}\}_{s \in S}$, telles que tous sauf un nombre fini des n_s soient nuls (le fait que F_S^{ab} soit abélien implique qu'il n'importe pas dans quel ordre nous prenons le produit dans le membre de droite de (145)) et

$$F_S^{\text{ab}} \to \mathbb{Z}^S, \qquad \text{mot (142)} \mapsto \sum_{i=1}^{k} \pm s_i \tag{146}$$

Il est facile de voir que ces fonctions sont mutuellement inverses. Le fait qu'elles soient des homomorphismes découle directement (ce que nous vous laissons vérifier) du fait que dans F_S^{ab}, le mot (142) est égal à n'importe laquelle de ses permutations. Ainsi, la liberté de déplacer arbitrairement les symboles implique la formule

$$\ldots s^m \ldots s^n \cdots = \ldots s^{m+n} \ldots$$

dans F_S^{ab}, quel que soit le contenu des mots placés à la place des "$\ldots$". □

12.3

Nous sommes maintenant prêts à démontrer le Théorème 12. La preuve que nous allons fournir établira également l'énoncé suivant, étroitement lié :

il existe un isomorphisme $F_S^{\mathrm{ab}} \overset{\cong}{\leftrightarrow} F_T^{\mathrm{ab}}$ si et seulement s'il existe une bijection $S \leftrightarrow T$

Proof. du Théorème 12 : L'assertion "si" est évidente, donc prouvons l'assertion "seulement si". Supposons qu'il existe un isomorphisme $F_S \cong F_T$. Cet isomorphisme induit naturellement un isomorphisme des quotients correspondants :

$$\mathbb{Z}^S \cong F_S/[F_S, F_S] \cong F_T/[F_T, F_T] \cong \mathbb{Z}^T$$

Cependant, l'isomorphisme ci-dessus envoie les multiples de 2 (c'est-à-dire les sommes formelles $\sum_{s\in S} n_s \cdot s$ où tous les n_s sont pairs) sur les multiples de 2. Comme les sous-ensembles des multiples de 2 dans $\mathbb{Z}^S$ et $\mathbb{Z}^T$ sont des sous-groupes, ce que vous pouvez facilement prouver, nous pouvons quotienter par ceux-ci et obtenir un isomorphisme :

$$(\mathbb{Z}/2\mathbb{Z})^S \cong (\mathbb{Z}/2\mathbb{Z})^T \tag{147}$$

Le groupe $(\mathbb{Z}/2\mathbb{Z})^S$ consiste en des sommes formelles $\sum_{s\in S} n_s \cdot s$ où un nombre fini des n_s peut être égal à 1 mod 2, tandis que tous les autres valent 0 mod 2. Ces sommes formelles correspondent bijectivement à des sous-ensembles finis de S (explicitement, à une somme formelle $\sum_{s\in S} n_s \cdot s$, nous associons le sous-ensemble des $s \in S$ tels que $n_s = 1 \bmod 2$). Par conséquent, l'isomorphisme (147) induit une bijection :

$$\left\{\text{sous-ensembles finis de } S\right\} \leftrightarrow \left\{\text{sous-ensembles finis de } T\right\} \tag{148}$$

- Si S et T ont une cardinalité finie m et n (respectivement), alors l'ensemble des sous-ensembles finis de S et T a une cardinalité 2^m et 2^n (respectivement). L'égalité $2^m = 2^n$ implique $m = n$, donc il existe une bijection entre S et T.

- Si l'un des ensembles S et T est fini et l'autre infini, alors (148) ne peut pas tenir.

- Si S et T sont tous deux infinis, alors nous invoquons le fait que tout ensemble infini est en bijection avec son ensemble de sous-ensembles finis (prouver cela n'est pas très difficile, mais cela dépasse le cadre de notre cours). Par conséquent, la bijection (148) implique qu'il existe une bijection entre S et T.

□

12.4

Si G est un groupe et $X \subseteq G$ est un sous-ensemble, vous avez appris dans Math 113 que

$$K = \left\{\text{produits de } x^{\pm 1} \middle| x \in X\right\} \tag{149}$$

est un sous-groupe de G, et que

$$H = \left\{\text{produits de } gx^{\pm 1}g^{-1} \middle| g \in G, x \in X\right\} \tag{150}$$

est un sous-groupe normal de G. Nous écrirons G/X au lieu de G/H.

Définition 27. *Considérons maintenant un ensemble R de mots* (142)*. Le groupe quotient (défini comme ci-dessus)*

$$\boxed{\langle S|R\rangle := F_S \Big/ R} \tag{151}$$

est appelé le groupe avec ***générateurs*** *S et* ***relations*** *R.*

Pour un groupe G, trouver une présentation par générateurs et relations de G signifie trouver un isomorphisme

$$G \cong \langle S|R\rangle$$

pour certains ensembles S et R. Si l'ensemble S est fini, alors G est appelé **finitement engendré**. Si S et R sont tous deux finis, alors G est appelé **finitement présenté**.

Exemple 4. *Pour tout ensemble S, nous avons :*

$$F_S^{\text{ab}} \cong \langle S|aba^{-1}b^{-1}, \forall a, b \in S\rangle$$

12.5

Les groupes cycliques finis admettent la présentation

$$\mathbb{Z}/n\mathbb{Z} \cong \langle x|x^n\rangle$$

Les groupes diédraux admettent la présentation

$$D_{2n} \cong \langle \sigma, \tau|\sigma^n, \tau^2, (\sigma\tau)^2\rangle$$

où σ est une rotation et τ une réflexion. Enfin, les groupes symétriques admettent la présentation

$$S_n \cong \langle \sigma_1, \ldots, \sigma_{n-1}|\sigma_i^2, (\sigma_i\sigma_j)^2, (\sigma_i\sigma_{i+1})^3\rangle$$

où i parcourt tous les indices, et j parcourt tous les indices sauf $i-1, i, i+1$. Le fait que ces trois groupes admettent des présentations par générateurs et relations n'est pas une coïncidence, comme le montre le résultat suivant.

Proposition 42. *Tout groupe G admet une présentation par générateurs et relations.*

Proof. En prenant $S = G$ et l'identité dans le membre de gauche de (143), on obtient un homomorphisme

$$\pi : F_G \to G$$

Comme tout élément de G est l'image du générateur portant le même nom, l'homomorphisme ci-dessus est surjectif. On pose alors H comme le noyau de π, et le premier théorème d'isomorphisme implique que $G \cong F_G/H$. Il reste donc à choisir $X = H$ dans (149) et (150), et avec ces choix, on a

$$\langle G|H\rangle \cong G$$

□

La preuve de la Proposition 42 est très peu économique : nous avons pris chaque élément de G comme un générateur ! Des présentations plus utiles par générateurs et relations d'un groupe ont relativement peu de générateurs et un ensemble "agréable" de relations. De plus, le même groupe admet souvent plusieurs présentations différentes par générateurs et relations, et il est en général difficile de déterminer si $\langle S|R\rangle$ est isomorphe à $\langle S'|R'\rangle$.

12.6

Pour ceux d'entre vous qui aiment les mathématiques plus abstraites, il existe une définition abstraite du groupe $\langle S|R\rangle$. Ce qui suit est une généralisation du Lemme 16.

Lemme 17. *Pour tout ensemble S, tout ensemble R de mots* (142) *et tout groupe G, il existe une correspondance bijective*

$$\Psi_{S|R,G} : \Big\{\textit{fonctions } S \xrightarrow{\alpha} G \textit{ t.q. } \alpha(r) = e, \forall r \in R\Big\} \leftrightarrow \Big\{\textit{homomorphismes } \langle S|R\rangle \to G\Big\} \tag{152}$$

(on écrit $\alpha(s_1^{\pm 1} \dots s_k^{\pm 1}) = \alpha(s_1)^{\pm 1} \dots \alpha(s_k)^{\pm 1}$) qui est ***fonctionnelle*** *au sens où le diagramme*

$$\begin{array}{ccc} \Big\{\textit{fonctions } S \xrightarrow{\alpha} G \textit{ t.q. } \alpha(r) = e, \forall r \in R\Big\} & \xrightarrow{\Psi_{S,R|G}} & \Big\{\textit{homomorphismes } \langle S|R\rangle \to G\Big\} \\ \downarrow & & \downarrow \\ \Big\{\textit{fonctions } S' \xrightarrow{\alpha} G' \textit{ t.q. } \alpha(r) = e, \forall r \in R'\Big\} & \xrightarrow{\Psi_{S',R'|G'}} & \Big\{\textit{homomorphismes } \langle S'|R'\rangle \to G'\Big\} \end{array} \tag{153}$$

commute pour toutes fonctions $f : S' \to S$ qui prennent tout mot de R' comme une concaténation de mots dans R, et tous homomorphismes $g : G \to G'$ (les flèches verticales sont données par composition avec f et g).

Le Lemme 17 est prouvé comme le Lemme 16, donc nous laissons les détails comme exercice. Cependant, nous expliquerons le sens dans lequel il fournit une définition abstraite du groupe $\langle S|R\rangle$, qui en mathématiques est appelée une **propriété universelle**. Pour S et R fixes, supposons qu'il existe un groupe $\langle S|R\rangle$ tel que nous ayons une correspondance bijective fonctionnelle (152), même si nous n'avons pas besoin de savoir qu'il est construit comme dans (151). Cette correspondance détermine alors de manière unique $\langle S|R\rangle$ à isomorphisme près. Pour le voir, supposons qu'il existe deux groupes $\langle S|R\rangle$ et $\langle S|R\rangle'$ tels que nous ayons des correspondances fonctionnelles bijectives :

$$\begin{aligned} &\Big\{\text{fonctions } S \xrightarrow{\alpha} G \text{ t.q. } \alpha(r) = e, \forall r \in R\Big\} \leftrightarrow \Big\{\text{homomorphismes } \langle S|R\rangle \to G\Big\} \\ &\Big\{\text{fonctions } S \xrightarrow{\alpha} G \text{ t.q. } \alpha(r) = e, \forall r \in R\Big\} \leftrightarrow \Big\{\text{homomorphismes } \langle S|R\rangle' \to G\Big\}. \end{aligned}$$

En composant les bijections ci-dessus, nous obtenons une correspondance bijective

$$\Upsilon_G : \Big\{\text{homomorphismes } \langle S|R\rangle \to G\Big\} \leftrightarrow \Big\{\text{homomorphismes } \langle S|R\rangle' \to G\Big\} \tag{154}$$

pour tout groupe G, qui est fonctorielle au sens où le diagramme suivant commute

$$\begin{array}{ccc} \Big\{\text{homomorphismes } \langle S|R\rangle \to G\Big\} & \xrightarrow{\Upsilon_G} & \Big\{\text{homomorphismes } \langle S|R\rangle' \to G\Big\} \\ \downarrow & & \downarrow \\ \Big\{\text{homomorphismes } \langle S|R\rangle \to G'\Big\} & \xrightarrow{\Upsilon_{G'}} & \Big\{\text{homomorphismes } \langle S|R\rangle' \to G'\Big\} \end{array} \tag{155}$$

pour tout homomorphisme $g : G \to G'$ (les flèches verticales sont données par la composition avec g). En prenant $G = \langle S|R\rangle$ dans (154), l'identité dans le membre de gauche donne un homomorphisme

$$\langle S|R\rangle' \xrightarrow{\beta'} \langle S|R\rangle$$

dans le membre de droite, tandis qu'en prenant $G = \langle S|R\rangle'$ dans (154), l'identité dans le membre de droite donne un homomorphisme

$$\langle S|R\rangle \xrightarrow{\beta} \langle S|R\rangle'$$

dans le membre de gauche. Si nous considérons les flèches verticales dans (155) comme la composition avec

$$G = \langle S|R\rangle \xrightarrow{\beta} \langle S|R\rangle' = G',$$

, la commutativité du carré appliquée à la fonction identité $\langle S|R\rangle \to \langle S|R\rangle$ dans le coin supérieur gauche implique la formule $\beta \circ \beta' = \mathrm{Id}$ dans le coin inférieur droit.

De même, si nous considérons les flèches verticales dans (155) comme la composition avec

$$G = \langle S|R\rangle' \xrightarrow{\beta'} \langle S|R\rangle = G',$$

la commutativité du carré appliquée à la fonction identité $\langle S|R\rangle' \to \langle S|R\rangle'$ dans le coin supérieur droit implique la formule $\beta' \circ \beta = \mathrm{Id}$ dans le coin inférieur gauche. Nous avons ainsi montré que β et β' fournissent des fonctions mutuellement inverses $\langle S|R\rangle \leftrightarrow \langle S|R\rangle'$, d'où $\langle S|R\rangle \cong \langle S|R\rangle'$.

Cours 13

13.1

Lorsque nous disons qu'un groupe G agit sur un ensemble X, cela signifie que pour chaque $g \in G$, nous associons une fonction $\Phi_g : X \to X$ ayant diverses propriétés. Lorsque X possède une structure supplémentaire, nous exigeons généralement que les fonctions Φ_g respectent cette structure supplémentaire : par exemple, dans la Définition 13, nous avons vu que si X est un groupe, alors nous exigeons généralement que les fonctions Φ_g soient elles-mêmes des homomorphismes. Le point de départ de la **théorie des représentations** est de traiter le cas où X est un espace vectoriel et les fonctions Φ_g sont des transformations linéaires sur un corps $\mathbb{F}$ fixé.

Définition 28. *Soit V un espace vectoriel sur $\mathbb{F}$. Une* ***représentation***

$$\boxed{G \curvearrowright V}$$

est une assignation

$$\forall g \in G \quad \rightsquigarrow \quad \textit{une transformation linéaire } \Phi_g : V \to V \tag{156}$$

satisfaisant les propriétés (18)*,* (19) *et* (20)*.*

Rappelons-nous de vos cours d'algèbre linéaire que les transformations linéaires sont les fonctions $\Phi : V \to V$ qui respectent l'addition et la multiplication scalaire dans V :

$$\Phi(v + v') = \Phi(v) + \Phi(v') \quad \text{et} \quad \Phi(cv) = c\Phi(v)$$

pour tout $v, v' \in V$ et $c \in \mathbb{F}$. Un exemple de représentation est

$$D_{2n} \curvearrowright \mathbb{R}^2$$

via les rotations et réflexions usuelles, qui sont effectivement des transformations linéaires de $\mathbb{R}^2$.

13.2

Vous vous souvenez probablement de vos cours d'algèbre linéaire que, en choisissant une base, tout espace vectoriel de dimension finie peut être rendu isomorphe à

$$\mathbb{F}^n = \left\{ \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \text{ pour divers } v_1, \ldots, v_n \in \mathbb{F} \right\} \tag{157}$$

Toute transformation linéaire $\Phi : \mathbb{F}^n \to \mathbb{F}^n$ peut être écrite de manière unique sous la forme

$$\Phi(v) = Av$$

pour une certaine matrice $n \times n$ $A = (a_{ij})_{1 \leq i,j \leq n}$, où v représente un vecteur colonne $n \times 1$ comme dans (157). Dans ce cas, une représentation

$$G \curvearrowright \mathbb{F}^n$$

revient à une assignation

$$\forall g \in G \quad \rightsquigarrow \quad \text{une matrice } n \times n \ A_g$$

telle que :

- A_e est la matrice identité $n \times n$
- $A_{g^{-1}} = A_g^{-1}$, pour tout $g \in G$
- $A_{gg'} = A_g A_{g'}$, pour tous $g, g' \in G$

Avec cela à l'esprit, il devient clair que la théorie des représentations est l'étude des matrices $n \times n$ et de la manière dont leurs produits reproduisent diverses structures de groupes. Dans le langage abstrait de la théorie des groupes, une représentation $G \curvearrowright \mathbb{F}^n$ est équivalente à un homomorphisme

$$G \to GL(n, \mathbb{F})$$

où, dans le membre de droite, nous avons le **groupe linéaire général** constitué de matrices $n \times n$ inversibles à coefficients dans $\mathbb{F}$, avec le produit donné par la multiplication matricielle.

13.3

Les notions suivantes devraient maintenant paraître naturelles et prévisibles.

Définition 29. *Étant données les représentations $G \curvearrowright V$ et $G \curvearrowright W$ (déterminées respectivement par les collections $\{\Phi_g : V \to V\}_{g \in G}$ et $\{\Psi_g : W \to W\}_{g \in G}$), un G-**entrelacement** est une transformation linéaire*

$$f : V \longrightarrow W$$

telle que le diagramme suivant commute :

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \Phi_g}\downarrow & & \downarrow{\scriptstyle \Psi_g} \\ V & \xrightarrow{f} & W \end{array}$$

pour tout $g \in G$. Si nous écrivons $\Phi_g(v) = g \cdot v$ et $\Psi_g(w) = g \cdot w$ pour tout $v \in V$ et $w \in W$, alors la propriété d'être un G-entrelacement est équivalente à :

$$f(g \cdot v) = g \cdot f(v)$$

*pour tout $v \in V$ et tout $g \in G$. Si un G-entrelacement est en outre bijectif, alors nous l'appelons un **isomorphisme** (de représentations de G) et nous l'indiquons comme suit :*

$$\boxed{V \cong W}$$

Rappelons qu'une partie d'un espace vectoriel est appelée un sous-espace si et seulement si elle est stable par addition de vecteurs et par multiplication par un scalaire. Si nous avons une représentation $G \curvearrowright V$, alors un sous-espace $W \subseteq V$ est appelé une **sous-représentation** si

$$\Phi_g(W) \subseteq W$$

pour tout $g \in G$. De plus, dans ce cas, il existe une **représentation quotient** induite :

$$\boxed{G \curvearrowright V/W}$$

13.4

L'une des notions les plus fondamentales de la théorie des représentations est la suivante.

Définition 30. *Une représentation $G \curvearrowright V$ est dite* ***irréductible*** *si elle n'a aucune sous-représentation propre (c'est-à-dire aucune sous-représentation autre que 0 ou V).*

L'un des outils principaux de la théorie des représentations est le résultat suivant, connu sous le nom de **Lemme de Schur**.

Lemme 18. *Supposons que nous ayons un G-entrelacement $f : V \to W$, entre deux représentations de G, qui n'est pas identiquement nul. Si V est irréductible, alors f est injectif. Si W est irréductible, alors f est surjectif.*

Proof. Le lemme découle rapidement du fait évident (dont nous vous laissons la démonstration) que pour tout G-entrelacement, $f : V \to W$, le noyau $f^{-1}(0)$ est une sous-représentation de V et l'image de f est une sous-représentation de W. Mais si V est irréductible, cela signifie que le noyau est soit 0 (ce qui implique que f est injectif) soit que le noyau est tout V (ce qui implique que f est identiquement nul). De même, si W est irréductible, alors l'image est soit 0 (ce qui implique que f est identiquement nul) soit que l'image est tout W (ce qui implique que f est surjectif).

□

Comme corollaire immédiat du Lemme 18, tout entrelacement non nul entre deux représentations irréductibles doit être un isomorphisme.

13.5

Nous nous spécialisons désormais à $\mathbb{F} = \mathbb{C}$, c'est-à-dire que nous considérons des représentations qui sont des espaces vectoriels sur le corps des nombres complexes. Dans ce cas, nous pouvons améliorer le Lemme 18 avec le résultat suivant.

Proposition 43. *Pour toute représentation irréductible $G \curvearrowright \mathbb{C}^n$, les seuls entrelacements*

$$f : \mathbb{C}^n \to \mathbb{C}^n$$

(les actions de G dans le domaine et le codomaine de f sont les mêmes) sont des multiples scalaires de l'identité.

Proof. Étant donné que nous travaillons sur les nombres complexes, toute transformation linéaire $f : \mathbb{C}^n \to \mathbb{C}^n$ possède un vecteur propre, c'est-à-dire qu'il existe un $0 \neq v \in \mathbb{C}^n$ et un $c \in \mathbb{C}$ tels que

$$f(v) = cv$$

Alors la fonction $f - c \cdot \mathrm{Id}$ est encore un entrelacement (vérifiez cela) mais elle ne peut plus être injective puisqu'elle a v dans son noyau. Ensuite, le Lemme de Schur 18 implique que $f - c \cdot \mathrm{Id}$ est identiquement nulle.

□

Comme toute représentation n-dimensionnelle V sur le corps des nombres complexes est isomorphe à $\mathbb{C}^n$ (en choisissant simplement une base de V), la Proposition 43 s'applique également aux entrelacements $f : V \to V$. En particulier, cela montre que si deux représentations de G de dimension finie sur les nombres complexes sont isomorphes, alors l'isomorphisme entre elles est unique à un multiple scalaire près. En effet, si nous avons deux isomorphismes

$$f_1 : V \to W \quad \text{et} \quad f_2 : V \to W$$

alors $f_1^{-1} \circ f_2$ est un isomorphisme $V \to V$. Par conséquent, la Proposition 43 implique qu'il existe $c \in \mathbb{C}$ tel que $f_1^{-1} \circ f_2 = c \cdot \mathrm{Id}$, ce qui entraîne $f_2 = c \cdot f_1$.

13.6

Si nous avons deux représentations $G \curvearrowright V$ et $G \curvearrowright W$, nous pouvons former la somme directe

$$V \oplus W = \Big\{ (v, w) \Big| v \in V, w \in W \Big\}$$

et en faire une représentation de G via $g \cdot (v, w) = (g \cdot v, g \cdot w)$. Dans le langage de la Sous-section 13.2, les matrices A_g qui décrivent la représentation $V \oplus W$ sont diagonales par blocs, avec des blocs diagonaux donnés par les matrices qui décrivent les représentations V et W, respectivement. Si vous prenez Math 314, vous apprendrez le résultat très important suivant, connu sous le nom de **théorème de Maschke**.

Théorème 13. *Toute représentation de dimension finie d'un groupe fini G sur le corps des nombres complexes est isomorphe à une somme directe de représentations irréductibles.*

Illustrons le Théorème 13 avec la représentation de permutation $\mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{C}^2$, donnée sous forme matricielle par

$$0 \bmod 2 \mapsto A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad 1 \bmod 2 \mapsto A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Les deux sous-espaces de coordonnées de $\mathbb{C}^2$ ne sont pas des sous-représentations, car ils ne sont pas préservés par la matrice A_1. Cependant, les deux sous-espaces de dimension un

$$V_1 = \Big\{ (c, c) \Big| c \in \mathbb{C} \Big\} \quad \text{et} \quad V_2 = \Big\{ (c, -c) \Big| c \in \mathbb{C} \Big\}$$

sont des sous-représentations. Parce qu'ils sont de dimension un, ils n'ont pas de sous-espaces propres, ils sont donc automatiquement irréductibles. Par conséquent, le théorème de Maschke dans ce cas affirme que

$$\mathbb{C}^2 \cong V_1 \oplus V_2$$

est la décomposition de la représentation $\mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{C}^2$ en représentations irréductibles.

13.7

En conséquence du Théorème 13, toute représentation $G \curvearrowright V$ de dimension finie sur le corps des nombres complexes peut s'écrire comme

$$V \cong V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k} \tag{158}$$

où $V_1, \ldots, V_k$ sont des représentations irréductibles non isomorphes de G, et $n_1, \ldots, n_k$ sont des entiers non négatifs appelés **multiplicités**. Nous affirmons que les multiplicités sont en fait entièrement déterminées par la représentation V. Pour voir cela, considérons un entrelacement

$$f : V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k} \longrightarrow V_1^{\oplus n'_1} \oplus \cdots \oplus V_k^{\oplus n'_k}$$

pour divers $n_1, \ldots, n_k, n'_1, \ldots, n'_k \geq 0$, et demandons-nous quand un tel f peut être un isomorphisme. Le Lemme 18 et la Proposition 43 impliquent que l'entrelacement agit par blocs diagonaux, c'est-à-dire

$$f(\ldots, v_{i1}, \ldots, v_{in_i}, \ldots) = (\ldots, v'_{i1}, \ldots, v'_{in'_i}, \ldots)$$

(ci-dessus, v_{ia} et v'_{ia} désignent des vecteurs généraux dans la a-ième somme directe de V_i et V'_i, respectivement) où pour tout $i \in \{1, \ldots, k\}$ et $b \in \{1, \ldots, n'_i\}$, nous avons

$$v'_{ib} = \sum_{a=1}^{n_i} \gamma_{ab}^{(i)} v_{ia}$$

pour certains nombres complexes $\gamma_{ab}^{(i)}$. Il est alors facile de croire qu'un tel G-entrelacement f peut être un isomorphisme uniquement si $n_i = n'_i$ pour tout $i \in \{1, \ldots, k\}$ (c'est une version légèrement plus sophistiquée de l'énoncé selon lequel une matrice $n' \times n$ peut être inversible uniquement si $n = n'$), ce qui implique que les nombres $n_1, \ldots, n_k$ dans (158) sont entièrement déterminés par V. En Math 314, vous apprendrez à utiliser la théorie des caractères pour calculer efficacement ces multiplicités pour toutes les représentations de dimension finie d'un groupe fini.

Cours 14

14.1

La théorie des catégories fournit un langage unificateur pour de nombreux objets que nous avons abordés ce semestre. Nous allons maintenant donner une brève introduction aux bases de ce langage.

Définition 31. *Une (petite)* ***catégorie*** $\mathcal{C}$ *est constituée des données suivantes :*

- *un ensemble* $\mathrm{Ob}(\mathcal{C})$ *appelé les* ***objets****, et*
- *pour tout* $X, Y \in \mathrm{Ob}(\mathcal{C})$*, un ensemble* $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ *appelé les* ***morphismes****, accompagné d'*
- *une opération appelée* ***composition***

$$\mathrm{Mor}_{\mathcal{C}}(Y, Z) \times \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{C}}(X, Z), \qquad (f, g) \mapsto f \circ g$$

  pour tous $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$*.*

On écrit typiquement $f : X \to Y$ *au lieu de* $f \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$*. La composition des morphismes doit satisfaire deux axiomes : premièrement, il doit exister un morphisme* ***identité***

$$\boxed{\mathrm{Id}_X : X \to X}$$

pour tout $X \in \mathrm{Ob}(\mathcal{C})$*, tel que*

$$\mathrm{Id}_Y \circ f = f \circ \mathrm{Id}_X = f, \quad \forall f : X \to Y$$

Deuxièmement, la composition des morphismes doit être associative, au sens où

$$f \circ (g \circ h) = (f \circ g) \circ h$$

pour tout $h : X \to Y$*,* $g : Y \to Z$*,* $f : Z \to T$*.*

14.2

On représente typiquement une catégorie $\mathcal{C}$ comme un graphe orienté : les sommets sont les éléments de $\mathrm{Ob}(\mathcal{C})$ et les flèches entre le sommet X et le sommet Y correspondent bijectivement aux éléments de l'ensemble $\mathrm{Mor}_{\mathcal{C}}(X, Y)$. Notez qu'il peut y avoir une infinité de sommets et de flèches ! Les exemples de catégories incluent :

- Ens : les objets sont des ensembles et les morphismes sont des fonctions (remarque : ce n'est pas une petite catégorie, donc il faut légèrement modifier le mot "ensemble" dans la Définition 31)
- Grp : les objets sont des groupes et les morphismes sont des homomorphismes (même remarque que pour "ensemble" ci-dessus)
- Rep_G : les objets sont des représentations d'un groupe fixé G et les morphismes sont des G-entrelacements.

Il existe une notion de morphismes inverses dans une catégorie $\mathcal{C}$: on appelle $f : X \to Y$ et $g : Y \to X$ des **inverses** l'un de l'autre (et on note $g = f^{-1}$) si

$$g \circ f = \mathrm{Id}_X \qquad \text{et} \qquad f \circ g = \mathrm{Id}_Y$$

Les morphismes inversibles dans les exemples de catégories ci-dessus sont respectivement les bijections, les isomorphismes (de groupes) et les isomorphismes de représentations de G.

Proposition 44. *Il existe une correspondance bijective entre les groupes d'une part, et les catégories avec un unique objet où tous les morphismes sont inversibles d'autre part.*

Proof. La proposition est presque évidente : si $\bullet$ est l'unique objet de la catégorie considérée, alors $G = \mathrm{Mor}(\bullet, \bullet)$ possède un élément neutre et une opération associative, et l'hypothèse selon laquelle chaque élément de G a un inverse complète précisément les axiomes d'un groupe.

□

14.3

La notion suivante est essentielle en théorie des catégories.

Définition 32. *Un foncteur $F : \mathcal{C} \to \mathcal{D}$ entre catégories consiste en :*

- *une fonction $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$*
- *une application*
$$f : X \to Y \qquad \rightsquigarrow \qquad F(f) : F(X) \to F(Y)$$
pour tous $X, Y \in \mathrm{Ob}(\mathcal{C})$, qui envoie les identités sur les identités et respecte la composition des morphismes.

Si l'on désigne par $\bullet_G$ la catégorie correspondant à un groupe G dans la Proposition 44, alors donner un foncteur $\bullet_G \to \bullet_{G'}$ revient à donner un homomorphisme de groupes $G \to G'$.

Un autre exemple de foncteur entre catégories est

$$\mathrm{Gr} \xrightarrow{\text{oub}} \mathrm{Set}$$

qui associe à un groupe l'ensemble sous-jacent, et à un homomorphisme ϕ entre groupes la fonction ϕ interprétée comme une application entre les ensembles sous-jacents. Ce foncteur est appelé le **foncteur oubli**.

Exemple 5. *La construction du groupe libre dans la Sous-section 12.1 définit un foncteur*

$$\mathrm{Set} \xrightarrow{\text{libre}} \mathrm{Gr}$$

Il associe à un ensemble S le groupe F_S, et à une fonction $s : S \to T$ l'homomorphisme de groupes $F_S \to F_T$ induit en envoyant les générateurs $s^{\pm 1}$ du groupe F_S sur les générateurs $f(s)^{\pm 1}$ du groupe F_T.

Définition 33. *Les foncteurs $F : \mathcal{D} \to \mathcal{C}$ et $G : \mathcal{C} \to \mathcal{D}$ sont dits **adjoints**, s'il existe des bijections*

$$\Psi_{X,Y} : \mathrm{Mor}_{\mathcal{C}}(F(X), Y) \leftrightarrow \mathrm{Mor}_{\mathcal{D}}(X, G(Y))$$

pour tout $X \in \mathrm{Ob}(\mathcal{D})$ et $Y \in \mathrm{Ob}(\mathcal{C})$. Ces bijections doivent être naturelles, c'est-à-dire que

$$\begin{array}{ccc} \mathrm{Mor}_{\mathcal{C}}(F(X), Y) & \xrightarrow{\Psi_{X,Y}} & \mathrm{Mor}_{\mathcal{D}}(X, G(Y)) \\ {\scriptstyle g\circ - \circ F(f)}\downarrow & & \downarrow{\scriptstyle G(g)\circ - \circ f} \\ \mathrm{Mor}_{\mathcal{C}}(F(X'), Y') & \xrightarrow{\Psi_{X',Y'}} & \mathrm{Mor}_{\mathcal{D}}(X', G(Y')) \end{array}$$

doit commuter pour tous les morphismes $f : X' \to X$ dans $\mathcal{D}$ et $g : Y \to Y'$ dans $\mathcal{C}$.

Le Lemme 16 exprime précisément que (F = libre) et (G = oub) forment une paire de foncteurs adjoints.

14.4

Définition 34. *Si $f : X \to Y$ et $f' : X \to Y'$ sont des morphismes dans une catégorie $\mathcal{C}$, alors nous disons que leur **pushout** est un objet Z muni de morphismes*

$$g : Y \to Z \quad et \quad g' : Y' \to Z$$

*tels que $g \circ f = g' \circ f'$, avec la propriété **universelle** suivante. Pour tout objet A et pour tout morphisme*

$$h : Y \to A \quad et \quad h' : Y' \to A$$

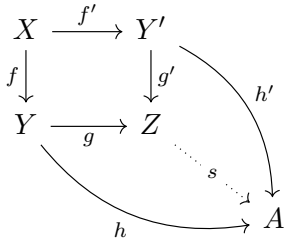
tels que $h \circ f = h' \circ f'$, il existe un morphisme unique

$$s : Z \to A$$

tel que

$$h = s \circ g \qquad et \qquad h' = s \circ g'.$$

De manière plus visuelle, la condition ci-dessus affirme qu'il existe une unique flèche pointillée telle que tous les carrés et triangles dans le diagramme ci-dessous commutent :



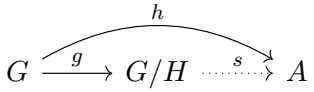
(159)

Lorsque le pushout, il est unique à isomorphisme près (veuillez prouver ceci). Nous allons maintenant fournir deux exemples que nous avons déjà rencontrés dans notre cours.

Exemple 6. *Dans la catégorie* Grp*, soit $f : H \hookrightarrow G$ l'inclusion d'un sous-groupe normal $H \trianglelefteq G$, et $f' : H \to 1$ l'homomorphisme trivial. Dans ce cas, le pushout est simplement le groupe quotient $g : G \to G/H$. La propriété universelle dans ce cas peut être résumée ainsi :*

$$\begin{aligned} &\textit{chaque fois que nous avons un homomorphisme de groupes } h : G \to A \textit{ tel que } h(H) = 1, \\ &\qquad\qquad \textit{il existe un homomorphisme unique } s : G/H \to A \textit{ tel que } h = s \circ g \end{aligned} \tag{160}$$

ou, de manière plus visuelle, qu'il existe une unique flèche pointillée rendant le diagramme ci-dessous commutatif :



Si H n'est pas normal dans G, alors le pushout est G/N, où N est le plus petit sous-groupe normal de G contenant H (également appelé la ***fermeture normale*** *de H). Ainsi, la construction du pushout ne distingue pas tous les sous-groupes (et dans des catégories plus générales, les pushout peuvent même ne pas exister).*

Exemple 7. *Dans la catégorie* Set*, toute relation d'équivalence peut être présentée comme un pushout. Plus précisément, si nous notons $R \subseteq X \times X$ l'ensemble des paires (x, x') telles que $x \sim x'$, alors nous affirmons que le pushout des fonctions $f : R \to X,\ f(x, x') = x$ et $f' : R \to X,\ f'(x, x') = x'$ est l'ensemble des classes d'équivalence $Z = X/\sim$. En effet, pour tout ensemble A comme dans le diagramme* (159)*, accompagné des fonctions*

$$g : X \to A \quad et \quad g' : X \to A$$

telles que $g(x) = g'(x')$ chaque fois que $x \sim x'$, alors premièrement, nous devons avoir $g = g'$ par réflexivité, et deuxièmement, nous pouvons définir

$$s : X/\sim \to A$$

en posant $s([x]) = g(x)$. Puisque $g(x) = g(x')$ chaque fois que $x \sim x'$, cette définition est bien définie.