# Structures algébriques
# (notes pour le cours d'automne de 2020, BA 1, EPFL)

Zsolt Patakfalvi

(avec l'aide de Quentin Posva)

Tuesday 10th November, 2020

# Contents

# Chapter 1

# Preuves et ensembles

## 1.1 Preuves

Une preuve est un argumentaire où chaque ligne est une conséquence logique des lignes précédentes. Grâce au langage de la logique mathématique, il existe une définition stricte d'une preuve mathématique. D'après cette définition, on ne peut utiliser que des signes mathématiques, comme :

(1) il existe : $\exists$,

(2) il existe un unique : $\exists!$,

(3) pour chaque : $\forall$,

(4) et : $\wedge$,

(5) ou : $\vee$,

(6) non : $\neg$,

(7) cela implique : $\Longrightarrow$,

(8) et les autres signes que l'on aura définis.

(9) etc.

Selon la logique mathématique, il faut démontrer toutes nos propositions en partant d'axiomes, et chaque ligne d'une preuve doit être l'une des suivantes :

(1) un axiome,

(2) une proposition déjà démontrée,

(3) une tautologie, comme par exemple $\neg(A \vee B) \Leftrightarrow ((\neg A) \wedge (\neg B))$ (pour démontrer que c'est une tautologie, on peut vérifier que tous les deux côtés sont vrais si est seulement si $A$ est $B$ sont tous les deux faux).

(4) moduls ponens: s'il y a une ligne précédente de la forme $A \Longrightarrow B$, et une autre de la forme $A$, alors on peut écrire $B$.

(5) etc

On appelle les preuve écrite de cette manière les *preuves formelles*. Écrire une preuve formelle est utile pour la vérifier avec un ordinateur. Mais il est quasiment impossible de la lire pour un lecteur humain. En pratique, on essaie d'approximer les preuves formelle par un mélange de

texte et de symboles mathématique. Quand on écrit un preuve, il faut trouver un compromis qui est lisible, et qui contient tous les pas importants de l'argumentaire. Il faut être strict : *tous les pas importants doivent figurer dans la preuve.* Quand on écrit un preuve, il faut se demander après chaque ligne : est-ce logiquement correct ? Il n'est pas possible de donner un algorithme pour l'écriture de preuves, seule la pratique permet de l'apprendre. On pourrait dire que c'est le but principal pour lequel vous êtes ici, et nous verrons beaucoup d'exemples pendant le semestre. Dans tous les cas, si vous n'êtes pas certain de la manière d'écrire une preuve, je suggère que vous vous exerciez beaucoup et que vous discutiez souvent avec les assistants.

Considérons ensemble un exemple de preuve. Elle suit un schéma logique fréquent : l'induction. L'idée de l'induction est que pour montrer une proposition pour chaque entier $n$, il suffit de le montrer pour $n = 0$, puis pour chaque $n > 0$ en supposant que la proposition est établie pour $n - 1$. Avant de donner cet exemple, nous avons besoin de définitions.

**Définition 1.1.1.** Un nombre entier $a$ est *positif* si $a > 0$, et *non-négatif* si $a \geq 0$. En particulier 0 n'est ni positif ni négatif. (Nous suivons ici la terminologie usuelle aujourd'hui dans la pratique internationale de la mathématique.)

**Définition 1.1.2.** Soient $a$ et $q$ deux entiers. On dit que $q \neq 0$ *divise* $a$, ce que l'on dénote $q|a$, s'il existe un entier $r$ tel que $a = rq$.

**Proposition 1.1.3.** (DIVISON AVEC RESTE) *Soient $q$ un entier positif, et $a$ un entier non-négatif. Alors il existe deux uniques entiers non-négatifs $b$ et $r$ tels que $r < q$ et*

$$a = bq + r. \tag{1.3.a}$$

*Preuve.* Supposons d'abord que $b$ et $r$ existent. On démontre qu'ils sont unique. Supposons que $b$, $r$, $b'$ and $r'$ soient des entiers non-négatifs tels que $r, r' < q$, $a = bq + r$ et $a = b'q + r'$. Alors,

$$bq + r = b'q + r' \implies \underbrace{r - r'}_{\uparrow} = \underbrace{q(b' - b)}_{\uparrow} \implies r - r' = 0 \implies r = r' \implies bq = b'q \underset{\uparrow}{\implies} b = b'$$

$0 \leq r, r' < q \implies -q < r - r' < q$

les possibilités sont $\ldots, -2q, -q, 0, q, 2q, \ldots$, parce que $b' - b$ est entier

$q > 0$

Ceci démontre que $b$ et $r$ sont uniques, s'ils existent. Pour conclure la preuve, il faut encore démontrer que $b$ et $r$ existent. On le démontre par induction sur $a$.

Le plus petit entier non-négatif est 0. Commençons alors avec le cas $a = 0$. Dans ce cas, on peut choisir $b = r = 0$.

Il nous reste donc à démontrer le pas d'induction. Supposons démontrée l'existence si l'on remplace $a$ par $a - 1$. On a ainsi $a - 1 = cq + s$, où $c$ et $s$ sont des entiers non-négatifs, et $s < q$. Il y a alors deux cas:

(1) Si $s < q - 1$, on peut choisir $b = c$ et $r = s + 1 < q$, et dans ce cas on a

$$a = 1 + (a - 1) = 1 + cq + s = bq + r.$$

(2) Si $s = q - 1$, on peut choisir $b = c + 1$ et $r = 0 < q$, et dans ce cas on a

$$a = 1 + (a - 1) = 1 + cq + s = 1 + cq + (q - 1) = q + cq = q(c + 1) = qb + 0 = qb + r.$$

Ceci conclut notre preuve.

□

**Exemple 1.1.4.** Si $a = 13$, $q = 3$, alors $b = 4$ et $r = 1$, parce que $13 = 4 \cdot 3 + 1$.

## 1.2 Ensembles

### 1.2.1 Axiomes de théorie des ensembles

La situation avec les ensembles est similaire à celle des preuves. Il y a une définition et une manière extrêmement précises de les manipuler, qui est lisible pour un ordinateur. Mais pour que nous soyons capables de travailler avec les ensembles, il faut l'assouplir un peu. La raison est que tout ce que vous allez rencontrer durant cette année, et qui semble être un ensemble, est presque sûrement un ensemble. Mais il est bien de se rappeler que notre intuition peut être trompeuse dans quelques cas délicats.

Intuitivement, un *ensemble* est un collection des "choses", et une sous-collections de "choses" est un *sous-ensemble*. Le problème avec cette définition est qu'elle nous mène au paradoxe de Russell.

**Paradoxe de Russel.** *La collection:*

$$B := \{\ A \text{ est un ensemble } \mid A \text{ n'est pas un élément de } A\ \}$$

*ne peut pas être pas un ensemble.*

*Preuve.* La définition de $B$ dit que $B$ est contenu dans $B$ si est seulement si $B$ n'est pas contenu dans $B$. Avec les symboles :

$$B \in B \iff B \notin B.$$

C'est un paradoxe. □

*Remarque* 1.2.1.

On peut voir que l'origine de cette paradoxe est qu'on a considéré une collection de "choses" très spéciale. Donc il ne faut pas s'inquiéter, il n'y a pas de problèmes quand on travaille avec des ensembles raisonnables. Dans ce cours, on va travailler la plupart de temps avec des ensembles construits à partir de l'ensemble des entiers, et dans cette situation aucun problème ne peut survenir. Mentionnons quand même comment le paradoxe de Russel fût résolu vers la fin de la XIXe siècle.

Un système d'axiomes fût établi, appelé le système d'axiomes de Zermelo-Fraenkel. Ce système définit ce qui est un ensemble de manière précise ; en particulier la collection considérée dans le paradoxe de Russell n'est pas un ensemble. On donne en-dessous une approximation de ce système d'axiomes. (Il s'agit de culture générale, vous n'avez pas besoin de le retenir) :

(0) $A$ est égal à $B$ si et seulement si ils ont les mêmes éléments.

(1) Il existe un ensemble.

(2) (Axiome du sous-ensemble) Si $A$ est un ensemble, est $E(x)$ est une expression logique applicable aux éléments $x$ de $A$, alors

$$\{\ x \in A \mid E(x) \text{ est vrai } \}$$

est aussi un ensemble.

(3) (Axiome de l'union) L'union d'ensembles, indicé par un ensemble, est aussi un ensemble. Avec des symboles : si $A_i$ sont des ensembles pour chaque $i \in I$, où $I$ est lui-même un ensemble, alors

$$\bigcup_{i \in I} A_i$$

est aussi un ensemble.

(4) (Axiome de la paire) Si $A$ est $B$ sont des ensembles, $\{A, B\}$ est aussi un ensemble.

(5) (Axiome de l'ensemble puissance) Si $A$ est un ensemble, l'ensemble $2^A$ des tous les sous-ensembles de $A$ est aussi un ensemble.

(6) (Axiome du choix) Intuitivement: si $A_i$ sont ensembles (pour $i \in I$), alors on peut choisir $a_i \in A_i$ pour chaque $i \in I$.

(7) etc.

Il n'est pas nécessaire de mémoriser les axiomes au-dessus, mais il est utile de les comprendre, afin de

- connaître les opérations les plus basiques permettant de définir un ensemble (en commençant avec les autres ensembles), et pour
- savoir qu'il y a un système d'axiomes.

Par exemple, en utilisant le système des axiomes de Zermelo-Fraenkel, on peut déduire (mais on ne va pas le faire pas dans ce cours) que les collections suivantes sont des ensembles:

(1) les ensembles finis:

  (i) l'ensemble vide: $\emptyset$
  (ii) l'ensemble à un élément: $\{1\}$
  (iii) l'ensemble à deux éléments: $\{1, 2\}$
  (iv) etc.

(2) l'ensemble des entiers naturels:
$$\mathbb{N} := \{0, 1, 2, \dots\}$$

(3) l'ensemble des entiers:
$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

(4) etc.

Condition (2) du système de Zermelo-Fraenke dit que l'on peut couper des sous-ensembles avec des conditions logiques. Par exemple :

(5) les entiers positifs forment un ensemble:
$$\mathbb{Z}^{>0} := \{x \in \mathbb{Z} | x > 0\}.$$

(6) les entiers naturels pairs forment un ensemble:
$$\{x \in \mathbb{N} \mid x \text{ est pair } \}.$$

(7) Plus généralement, on peut former des compléments: soit $A \subseteq B$ un sous-ensemble (ce qui signifie que chaque élément de $A$ est aussi un élément de $B$, ou avec formules $a \in A \implies a \in B$). Dans ce cas on peut prendre la différence des deux ensembles, aussi appellée le complément de $A$ dans $B$, définit par
$$B \setminus A = \{\ b \in B \mid \underbrace{b \neg \in A}_{\text{notation en logique mathématique}}\ \} = \{\ b \in B \mid \underbrace{b \notin A}_{\text{notation plus commune en mathématique}}\ \}$$

(8) Une application similaire consiste à former des intersections. Plus précisément, si $A$ et $B$ sont des sous-ensembles de $C$, alors l'intersection $A \cap B$ est définie par l'équation suivante, qui nous montre qu'il s'agit aussi un sous-ensemble de $C$ :

$$A \cap B = \{\, c \in C \mid c \in A \wedge c \in B \,\} = \{\, c \in C \mid c \in A, \text{ et } c \in B \,\}$$

notation en logique mathématique — notation plus commune en mathématique

Contrairement aux unions, on ne peut pas prendre l'intersection d'ensembles pris au hasard, mais seulement de sous-ensembles d'un ensemble ambiant fixé.

(9) etc.

La fin du 1. cours, en 15.09.2020.

### 1.2.2 Applications entres ensembles

On peut également déduire du système de Zermelo-Fraenkel (mais on ne va pas le faire pas dans ce cours) que pratiquement toutes les opérations mathématiques produisent des ensembles, entendu que l'on commence avec des ensembles. Un exemple est le produit d'ensembles:

**Définition 1.2.2.** Soient $A$ et $B$ des ensembles, *l'ensemble produit* $A \times B$ est l'ensemble des paires $(a, b)$ avec $a \in A$ et $b \in B$:

$$A \times B = \{\, (a, b) \mid a \in A, b \in B \,\}.$$

Etant donnée une paire $(a, b)$, on appelle $a$ la première cordonnée et $b$ la seconde.

**Exemple 1.2.3.** Soient $A = \{1, 2\}$ et $B = \{5, 6\}$. Dans ce cas on a

$$A \times B = \big\{(1, 5), (1, 6), (2, 5), (2, 6)\big\}.$$

*Remarque* 1.2.4. Soient $A$, $B$ et $C$ des ensembles. On a un isomorphisme naturel

$$(A \times B) \times C \cong A \times (B \times C)$$

$$\big((a, b), c\big) \leftrightarrow \big(a, (b, c)\big)$$

On identifie les deux ensembles grâce à cet isomorphisme, et on les écrira simplement $A \times B \times C$.

**Définition 1.2.5.** Soient $A$ et $B$ des ensembles. Une application $\phi : A \to B$ est un sous-ensemble (appelé le graphe de $\phi$)

$$\Gamma_\phi \subseteq A \times B$$

tel que:

$$\forall a \in A, \exists! b \in B \text{ tel que } (a, b) \in \Gamma_\phi$$

i.e. l'ensemble des paires contenues dans $\Gamma_\phi$ dont la première coordonne est $a$, est réduit à un seul élément. On note la deuxième coordonnée de cette paire $\phi(a)$, et on l'appelle l'image de $a$ par $\phi$.

On appelle $A$ le domaine, et $B$ le codomaine de $\phi$.

**Exemple 1.2.6.** Soit $A, B$ des ensembles. Voici quelques exemples d'applications entre $A$ et $B$ :

(1) $\mathrm{id}_A : A \to A$ est définie par

$$\forall a \in A \ : \ \mathrm{id}_A(a) = a$$

$$\Updownarrow$$

$$\Gamma_{\mathrm{id}_A} = \{\, (a, a) \in A \times A \mid a \in A \,\}$$

(2) $\mathrm{pr}_A : A \times B \to A$ est définie par

$$\forall (a,b) \in A \times B \ : \ \mathrm{pr}_A\big((a,b)\big) = a$$

$$\Updownarrow$$

$$\Gamma_{\mathrm{pr}_A} = \{\ (a,b,a) \in A \times B \times A \mid a \in A, b \in B\ \}$$

**Définition 1.2.7.** Soit $\phi : A \to B$ une application entre ensembles. On dit que

(1) $\phi$ est *injective*, si

$$\phi(a) = \phi(a') \ \Rightarrow \ a = a'$$

(2) $\phi$ est *surjective*, si

$$\forall b \in B, \exists a \in A \ : \ \phi(a) = b$$

(3) $\phi$ est *bijective*, si elle est injective et surjective.

(4) l'image de $\phi$ est

$$\phi(A) = \big\{\ \phi(a) \in B \ \big|\ a \in A\ \big\}$$

Quelquefois une application injective est appelée une *injection*, une application surjective est appelée une *surjection*, et une application bijective est appelée une *bijection*.

**Définition 1.2.8.** Soient $\phi : A \to B$ et $\xi : B \to C$ les applications entre ensembles. La composition $\xi \circ \phi$ est l'application

$$(\xi \circ \phi)(a) = \xi(\phi(a))$$

$$\Updownarrow$$

$$\Gamma_{\xi\circ\phi} = \big\{\ (a,c) \ \big|\ \exists b \in B : (a,b) \in \Gamma_\phi \text{ et } (b,c) \in \Gamma_\xi\ \big\}$$

**Proposition 1.2.9.** *Soient $\phi : A \to B$ et $\xi : B \to C$ les applications entre ensembles, et supposons que $\xi \circ \phi$ est surjective. Alors,*

*(1) $\xi$ est aussi surjective, mais*

*(2) $\phi$ n'est pas nécessairement surjective.*

*Preuve.* (1) Fixons $c \in C$. Il faut montrer qu'il existe au moins un $b \in B$ tel que $\xi(b) = c$. On a supposé que $\xi \circ \phi$ est surjective : il existe donc un $a \in A$ tel que $\xi(\phi(a)) = c$, et donc on peut choisir $b = \phi(a)$.

(2) Voici un contre-exemple :

$$A = \{1\}, \qquad B = \{1,2\} \qquad C = \{1\},$$

$$\phi(1) = 1, \qquad \xi(1) = 1, \qquad \xi(2) = 1.$$

□

**Définition 1.2.10.** Soit $\phi : A \to B$ une bijection entre ensembles. *L'inverse* $\phi^{-1}$ de $\phi$ est l'application $\phi^{-1} : B \to A$ définie par

$$\phi^{-1}(b) = a \iff \phi(a) = b.$$

$$\Updownarrow$$

$$(b,a) \in \Gamma_{\phi^{-1}} \iff (a,b) \in \Gamma_\phi.$$

**Exemple 1.2.11.** Soit $\phi : \{1,2\} \to \{5,6\}$ la bijection définie par $\phi(1) = 6$ et $\phi(2) = 5$. Dans ce cas $\phi^{-1} : \{5,6\} \to \{1,2\}$ est l'application pour laquelle on a $\phi^{-1}(5) = 2$ et $\phi^{-1}(6) = 1$.

### 1.2.3 Relations d'équivalence

**Définition 1.2.12.** Soit $A$ un ensemble. Une relation d'équivalence est un sous-ensemble $R \subseteq A \times A$ tel que

(1) (réflexivité) $\forall a \in A \ : \ (a,a) \in R$,

(2) (symétrie) $(a,b) \in R \ \Rightarrow \ (b,a) \in R$,

(3) (transitivité) $(a,b) \in R, (b,c) \in R \ \Rightarrow \ (a,c) \in R$.

**Proposition 1.2.13.** *Si $a$, $b$ et $m$ sont des entiers tel que $m > 0$, $m|a$ et $m|b$, alors $m|a+b$.*

*Preuve.* Par définition, $m|a$ et $m|b$ signifie qu'il existe des entiers $c$ et $d$ tels que $a = cm$ et $b = dm$. Si on somme les deux dernières égalités, on obtient $a + b = cm + dm = (c+d)m$. Ainsi $m|a+b$. □

**Exemple 1.2.14.** Fixons un entier $m > 0$. On définit une *relation d'équivalence* sur $\mathbb{Z}$ par le sous-ensemble $R \subseteq \mathbb{Z} \times \mathbb{Z}$ défini par la condition suivante :

$$(a,b) \in R \iff m|a-b$$

On vérifie que ce $R$ définit une relation d'équivalence:

(1) (réflexivité) $\forall a \in \mathbb{Z} \ : \ m|a-a \implies (a,a) \in R$,

(2) (symétrie) $(a,b) \in R \implies m|a-b \implies m|b-a \implies (b,a) \in R$,

(3) (transitivité) $(a,b) \in R, (b,c) \in R \implies m|a-b$ et $m|b-c$
$\implies m|(a-b)+(b-c) = a-c \implies (a,c) \in R$.

**Définition 1.2.15.** Soit $R \subseteq A \times A$ une relation d'équivalence. Pour chaque $a \in A$ on définit la *classe d'équivalence* de $a$ par

$$R_a := \{ \ b \in A \ | \ (a,b) \in R \ \}.$$

*Remarque* 1.2.16. On démontre en exercice que $(a,b) \in R \iff R_a = R_b$.

**Définition 1.2.17.** Soit $R \subseteq A \times A$ une relation d'équivalence. L'ensemble quotient $A/R$ est l'ensemble des classes d'équivalences, vu comme un sous-ensemble de l'ensemble puissance de $A$. En d'autres termes :

$$A/R = \{ \ R_a \subseteq A \ | \ a \in A \ \} \subseteq 2^A$$

Le prochain exemple est notre premier exemple de groupe. Nous donnerons la définition de groupe dans quelques semaines.

**Exemple 1.2.18.** Soit $m \in \mathbb{Z}$. On définit $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/R$, ou $R$ est la relation d'équivalence défini dans Exemple 1.2.14.

Autrement dit, si $m\mathbb{Z}$ dénote le sous-ensemble

$$m\mathbb{Z} = \{ \ a \in \mathbb{Z} \ | \ m|a \ \} = \{ \ bm \in \mathbb{Z} \ | \ b \in \mathbb{Z} \ \}$$

de $\mathbb{Z}$, et si $m\mathbb{Z} + x$ dénote le sous-ensemble

$$m\mathbb{Z} + x = \{ \ c + x \in \mathbb{Z} \ | \ c \in \mathbb{Z} \ \}$$

de $\mathbb{Z}$, alors on a

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, m\mathbb{Z}+1, \ldots, m\mathbb{Z}+(m-1)\}.$$

Par exemple,

$$\mathbb{Z}/2\mathbb{Z} = \Big\{ \ \{ \ \ldots, -4, -2, 0, 2, 4, \ldots \ \} \ , \ \{ \ \ldots, -5, -3, -1, 1, 3, 5, \ldots \ \} \ \Big\}.$$

### 1.2.4 Cardinal d'un ensemble

Le dernier sujet important à propos des 'ensembles que l'on aborde dans ce cours est la définition de la taille d'un ensemble. On donne dans la définition suivante la notion d'"avoir le même cardinal", ce qui veut dire que les deux ensemble concernés ont la même grandeur.

**Définition 1.2.19.** Soient $A$ et $B$ des ensembles. On dit que

(1) $A$ et $B$ ont *le même cardinal*, ce que l'on écrit $|A| = |B|$, s'il existe une bijection $\phi : A \to B$,

(2) *le cardinal* de $A$ et *plus petit* que celui de $B$, ce que l'on écrit $|A| \leq |B|$, s'il existe une injection $\phi : A \to B$,

(3) $A$ est *infinie dénombrable*, si $A$ a le même cardinal que $\mathbb{N}$.

(4) $A$ a le *cardinal du continu*, si $A$ a le même cardinal que $\mathbb{R}$.

La relation "avoir le même cardinal" semble être une relation d'équivalence, parce qu'elle satisfait le trois conditions de la Définition 1.2.12: identité (par d'existence des applications d'identité), reflexivité (par d'existence des inverses des bijections), transitivité (par composition des application). Mais il faut faire attention : le paradoxe de Russell nous dit que ce n'est pas vraiment une relation d'équivalence, parce que l'ensemble des tous les ensembles n'existe pas, donc il n'existe pas d'ensemble auquel cette relation s'applique. On peut dire que "avoir le même cardinal" est juste une propriété de deux ensembles, qui satisfait les trois propriétés de Définition 1.2.12, mais qui n'est pas une relation d'équivalence. Une conséquence importante est que l'on ne peut pas prendre les classes d'équivalences de cette relation.

**Théorème 1.2.20** (Théorème de Cantor-Schröder-Bernstein)**.** *Soient $A$ et $B$ des ensembles. Si $|A| \leq |B|$ et $|B| \leq |A|$, alors $|A| = |B|$.*

On doit démontrer un lemme avant de procéder à la preuve du Théorème 1.2.20. Dans ce lemme, on utilisera la notation suivante:

**Définition 1.2.21.** Soient $X$ et $Y$ des sous-ensembles d'un ensemble $A$. Ils sont *disjoints*, si $X \cap Y = \emptyset$, et ils forme une *partition* de $A$, s'ils sont disjoints et satisfont $X \cup Y = A$. Ces deux notions sont définies d'une manière similaire pour une collection de sous-ensembles $\{X_i\}$ de $A$.

**Exemple 1.2.22.** Les classes d'équivalences d'une relation d'équivalence $R \subseteq A \times A$ forment une partition de $A$.

Dans la preuve du lemme suivant, on s'autorise un abus de langage courant en mathématique : on ne change pas la notation d'une application après avoir restreint son codomaine. Par exemple, dans la preuve ci-dessous, $g|_Y$ est a priori une application $Y \to A$, mais on la consièdre vraiment comme une application $Y \to g(Y)$. Avec cette convention, $g|_Y$ devient bijective, et on peut prendre son inverse.

**Lemme 1.2.23.** *Soit $f : A \to B$ et $g : B \to A$ des injections. S'il existe un sous-ensemble $X \subseteq A$ tel que*

$$X = A \setminus g\big(B \setminus f(X)\big), \tag{2.23.a}$$

*alors il existe une bijection $A \to B$.*

*Preuve.* Définissons

$$Y_A := A \setminus X \underset{\uparrow}{=} g(B \setminus f(X)), \qquad Y := B \setminus f(X) \underset{\uparrow}{=} (g|_Y)^{-1}(Y_A), \qquad X_B := f(X)$$

(2.23.a)

$g$ est injective, alors elle induit une bijection $Y \to Y_A = g(Y) \Longrightarrow$ on dénote l'inverse de cette bijection par $g^{-1}$

On obtient directement que $X$ et $Y_A$ forment une partition de $A$, et que $X_B$ et $Y$ forment une partition de $B$. De plus, $f : X \to X_B = f(X)$ et $g^{-1} : Y_A = g(Y) \to Y$ sont des bijections. Le diagramme suivant résume la situation :

$$\begin{array}{ccc} A & & B \\ \| & & \| \\ X & \xrightarrow[f]{\text{bijection}} & X_B \\ \cup & & \cup \\ Y_A & \xrightarrow[\text{bijection}]{g^{-1}} & Y \end{array}$$

Cela implique que l'on peut définir une bijection $\phi : A \to B$ par la formule

$$\phi(a) = \left\{ \begin{array}{ll} f(a) & \text{si } a \in X \\ g^{-1}(a) & \text{si } b \in Y_A \end{array} \right\}$$

□

*Preuve du Théorème 1.2.20.* Pour chaque sous-ensemble $X \subseteq A$ définissons

$$H(X) := A \setminus g\big(B \setminus f(X)\big)$$

Par le Lemme 1.2.23, il suffit de montrer qu'il existe un $X$ pour lequel $X = H(X)$. Premièrement on démontre que $H$ respecte la relation d'inclusion :

$$X \subseteq Z \underset{\uparrow}{\implies} f(X) \subseteq f(Z) \underset{\uparrow}{\implies} B \setminus f(X) \supseteq B \setminus f(Z) \underset{\uparrow}{\implies} g\big(B \setminus f(X)\big) \supseteq g\big(B \setminus f(Z)\big)$$

par définition de l'image dans la Définition 1.2.7 — prendre le complément renverse l'inclusion (ce sera un exercice) — par définition de l'image dans la Définition 1.2.7

$$\underset{\uparrow}{\implies} H(X) = A \setminus g\big(B \setminus f(X)\big) \subseteq A \setminus g\big(B \setminus f(Z)\big) = H(Z) \quad (2.23.b)$$

prendre le complément renverse l'inclusion

Deuxièmement on définit

$$W := \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X, \quad (2.23.c)$$

et on observe que la définition fait sens, puisque $A$ lui-même satisfait $H(A) \subseteq A$. On finit notre preuve en démontrant que $H(W) = W$. On commence par démontrer que $H(W) \subseteq W$:

La fin du 2. cours, en 22.09.2020.

$$W \underset{\uparrow}{\subseteq} \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X \implies \forall X \subseteq A : \text{ si } H(X) \subseteq X, \text{ alors } W \subseteq X$$

(2.23.c)

$$\underset{\uparrow}{\implies} \forall X \subseteq A : \text{ si } H(X) \subseteq X, \text{ alors } H(W) \subseteq (X)$$

(2.23.b)

$$\implies H(W) \subseteq \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} H(X) \underset{\uparrow}{\subseteq} \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X \underset{\uparrow}{=} W$$

$H(X) \subseteq X$ — (2.23.c)

Pour conclure, il suffit maintenant de montrer que $H(W) \supseteq W$. Notons que $H(W) \subseteq W$ et (2.23.b) implique que $H(H(W)) \subseteq H(W)$. Cela veut dire que $H(W)$ fait partie de la collection que $X$ parcourt dans (2.23.c). Ceci implique que $H(W) \supseteq W$, ce qui conclut notre argument. □

Un aspect fascinant de la théorie des ensembles, est la suivante: on peut démontrer en utilisant les axiomes de Zermelo-Fraenkel qu'il existe un cardinal $\omega_1$ minimal entre les cardinals plus grand que $|\mathbb{N}| = \omega_0$. Il y aura une exercise aussi sur la fiche d'exercise qui nous montre que $|\mathbb{R}| = \left|2^{\mathbb{N}}\right| > \omega_0$. Ainsi, c'est natural de demander si $|\mathbb{R}| = \omega_1$. Ce qui est surprenant ce que l'on peut démontrer qu'il n'est pas possible de prouver que $|\omega_1| = |\mathbb{R}|$ ni que $|\omega_1| \neq |\mathbb{R}|$ dans le système d'axiomes de Zermelo-Fraenkel. Cette question est longtemps restée ouverte ; les mathématiciens ont quelquefois supposé que l'égalité était vraie, ce que on appelle l'hypothèse du continu. Cohen a finalement démontré que l'hypothèse du continu est indépendante du système d'axiomes de Zermelo-Fraenkel, en construisant un modèle où elle est vraie, et un autre où elle est fausse. Cohen a d'ailleurs reçu le prix mathématique le plus prestigieux, la Médaille Fields en 1966, pour ce résultat.

# Chapter 2

# Théorie des nombres

## 2.1 Algorithme d'Euclide

**Définition 2.1.1.** Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^{\neq 0}$. Le *plus grand commun diviseur* de $a$ et $b$ et

$$(a,b) := \max \left\{ \; m \in \mathbb{Z}^{>0} \;\middle|\; m|a \text{ et } m|b \; \right\}$$

(On note que l'ensemble ci-dessus est non-vide, parce qu'il contient $m = 1$, et qu' il est majoré par $|b|$. Ainsi le maximum existe.)

On dit que $a$ et $b$ sont *premiers entre eux* ou $a$ est *premier avec* $b$ si $(a,b) = 1$.

**Lemme 2.1.2.** *Si, $a, b \in \mathbb{Z}$ tel que $a \neq 0$ et $r \in \mathbb{Z}$, alors $(a,b) = (a, b+ra)$.*

*Preuve.* Par Définition 2.1.1, il suffit de montrer que pour chaque entier $m \in \mathbb{Z}^{>0}$,

$$m|a \text{ et } m|b \qquad \Longleftrightarrow \qquad m|a \text{ et } m|b+ra$$

On montre chaque direction de cette équivalence ci-dessous:

- $\boxed{\Longrightarrow}$ $m|a \implies m|ra \underset{\uparrow}{\implies} m|b+ra.$

  $\boxed{m|b \text{ et Proposition 1.2.13}}$

- $\boxed{\Longleftarrow}$ $m|a \implies m|-ra \underset{\uparrow}{\implies} m|(b+ra)-ra = b.$

  $\boxed{m|b+ra \text{ et Proposition 1.2.13}}$

□

**Notation 2.1.3.** Algorithme d'Euclide. Soient $a, b \in \mathbb{Z}^{>0}$. On définit l'algorithme récursif suivant, en prenant pour valeurs initiales $i := 2$, $q_1 := \max\{a,b\}$ et $q_2 := \min\{a,b\}$. Le pas de récursion est :

- si $q_i | q_{i-1}$, alors on s'arrête, $q_i$ est le résultat de l'algorithme, et on pose $t := i$ ($t$ encode le temps d'arrêt de l'algorithme) ;
- sinon :
  - ◇ on définit $q_{i+1}$ prenant une division avec reste: $q_{i-1} := s_i q_i + q_{i+1}$ (notons que par le point précédent $q_i \nmid q_{i-1}$, ainsi en utilisant la définition de la division avec reste on a $0 < q_{i+1} < q_i$), et
  - ◇ on augmente $i$ de 1.

On note que cet algorithme s'arrête toujours. En effet, dans le cas $a = b$ il s'arrête au début ; et quand $a \neq b$ on a la suite $q_1 > q_2 > \cdots > q_t > 0$ de nombres entiers, qui ne peut avoir de plus $q_1$ pas, autrement dit $t \leq q_1$.

**Lemme 2.1.4.** *Dans la situation de la Notation 2.1.3, il existe $m, n \in \mathbb{Z}$ tel que $ma + nb = q_t$.*

*Preuve.* On démontre par induction descendante sur $i$ qu'il existe $m_i, n_i \in \mathbb{Z}$ tel que $m_i q_i + n_i q_{i+1} = q_t$ pour chaque entier $1 \leq i \leq t-1$.

Pour $i = t-1$ on peut choisir $m_i = 0$ et $n_i = 1$. Il faut encore montrer le pas d'induction. Fixons $i \leq t-1$, et supposons connue la proposition pour les indices supérieurs ou égaux à $i$. Le calcul suivant démontre la proposition pour $i-1$ :

$$q_t = m_i q_i + n_i q_{i+1} = m_i q_i + n_i(q_{i-1} - s_i q_i) = \underbrace{n_i}_{\boxed{:= m_{i-1}}} q_{i-1} + (\underbrace{m_i - n_i s_i}_{\boxed{:= n_{i-1}}}) q_i$$

□

**Lemme 2.1.5.** *Dans la situation de la Notation 2.1.3, $q_t | q_i$ pour chaque entier $1 \leq i \leq t$.*

*Preuve.* On démontre la proposition par induction descendant par rapport à $i$. Pour $i = t$, on a $q_i = q_t$, auquel cas la proposition est vraie trivialement. Pour $i = t-1$ on a $q_{t-1} | q_t$ par la définition de l'algorithme.

Supposons maintenant que $i < t$, que l'on sait la proposition pour les indices supérieurs ou égaux à $i$, et on démontre la proposition pour $i-1$. C'est une conséquence immédiate de la définition de l'algorithme :

$$q_{i-1} = q_{i+1} + s_i q_i \qquad \underset{\boxed{q_t | q_{i+1} \text{ et } q_t | q_i \text{ par hypothèse d'induction}}}{\Longrightarrow} \qquad q_t | q_{i-1}$$

□

**Théorème 2.1.6.** *Si $a, b \in \mathbb{Z}^{>0}$, l'algorithme d'Euclide nous donne $q_t = (a, b)$.*

*En particulier, on a une relation de Bézout : il existe $m, n \in \mathbb{Z}$ tels que $ma + nb = (a, b)$.*

*Preuve.* $\boxed{q_t = (a,b):}$ C'est impliqué par les deux lemmes précédent:

- Lemme 2.1.4 dit que $(a, b) | q_t$, et
- Lemme 2.1.5 dit que $q_t | a$ et $q_t | b$, alors $q_t | (a, b)$.

$\boxed{\text{Existence de } m \text{ et } n:}$ c'est impliqué par $q_t = (a, b)$ et par le Lemme 2.1.4. □

**Corollaire 2.1.7.** *Supposons que $q, a, b \in \mathbb{Z}^{>0}$, $q | ab$ et que $(q, a) = 1$. Alors $q | b$.*

*Preuve.* Par le Théorème 2.1.6, il existe $m, n \in \mathbb{Z}^{>0}$ tel que $1 = ma + nq$. En multipliant cette équation par $b$ on obtient $b = mab + nqb$. Puisqu'on a supposé que $q | ab$, on obtient que $q | b$. □

## 2.2 THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE

**Définition 2.2.1.** Soit $p \geq 2$ un entier. On dit que :

(1) $p$ est *irréductible*, si pour chaque $a \in \mathbb{Z}^{>0}$ : $a | p \Longrightarrow a = 1$ ou $a = p$.

(2) $p$ est *premier*, si pour chaque $a, b \in \mathbb{Z}^{>0}$ : $p | ab \Longrightarrow p | a$ ou $p | b$.

*Remarque* 2.2.2. Notons bien que $p \geq 2$ dans cette définition. En particulier, le nombre 1 n'est, par convention, ni premier ni irréductible.

**Proposition 2.2.3.** *Si $p \geq 2$ est un entier, alors $p$ est irréductible si est seulement si $p$ est premier.*

*Preuve.* $\boxed{\Longleftarrow:}$ Soit $a \in \mathbb{Z}^{>0}$ un diviseur de $p$. On peut écrire $ab = p$ pour un entier $b \in \mathbb{Z}^{>0}$. En particulier $a, b \leq p$. En utilisant que $p$ est premier on obtient $p|a$ ou $p|b$. Cela implique, en utilisant $a, b \leq p$, que $p = a$ ou $p = b$. Si $p = b$, on obtient que $a = 1$. En somme, on a obtenu que $a = p$ ou $a = 1$, ce qui est exactement la définition d'être irréductible.

$\boxed{\Longrightarrow:}$ Prenons $a, b \in \mathbb{Z}^{>0}$ tels que $p|ab$. Il faut montrer que $p|a$ ou $p|b$. Si $p|a$ on a terminé, donc on peut supposer que $p \nmid a$, autrement dit que $(p, a) \neq p$. Mais $p$ est irréductible, alors il a seulement deux diviseurs (positifs) 1 et $p$. Cela force $(p, a) = 1$. Finalement dans ce cas Corollaire 2.1.7 nous donne que $p|b$. □

**Théorème 2.2.4.** *Pour chaque $n \in \mathbb{Z}^{>1}$ on peut écrire $n = \prod_{i=1}^{r} p_i$ pour un nombre fini de premiers $p_1, \ldots, p_r$. De plus la liste de ces premiers sont uniques modulo leur ordre.*

*Preuve.* $\boxed{\text{Existence:}}$ On démontre qu'on peut écrire $n = \prod_{i=1}^{r} p_i$ par induction sur $n$. Pour $n = 2$ c'est clair, parce que 2 est premier.

Supposons que $n > 2$ et qu'on a déjà démontré la proposition pour chaque entier plus grand que 1 et plus petit que $n$. Si $n$ est premier on a terminé. Sinon, en utilisant Proposition 2.2.3, $n$ n'est pas irréductible, et ainsi il existe $n > a, b \in \mathbb{Z}^{>0}$ tels que $n = ab$. Par l'hypothèse d'induction on peut écrire $a = \prod_{i=1}^{s} p_i$ et $b = \prod_{i=s+1}^{r} p_i$ pour certains nombres premiers $p_i$. Ainsi on obtient

$$n = ab = \left(\prod_{i=1}^{s} p_i\right) \cdot \left(\prod_{i=s+1}^{r} p_i\right) = \prod_{i=1}^{r} p_i$$

$\boxed{\text{Unicité:}}$ Supposons qu'il y ait deux expressions:

$$n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j \tag{2.4.a}$$

où les $p_i$ et $q_j$ sont des nombres premiers. En échangeant si besoin les $p_i$ et les $q_j$, on peut supposer que $r \leq s$.

On démontre par induction sur $s$ que les listes des $p_i$ et des $q_j$ est la même modulo leur ordre. Si $s = 1$, alors $r = 1$, et il n'y a rien à démontrer.

Supposons que $s > 1$. Dans ce cas on a

$$q_1 | n = \prod_{i=1}^{r} p_i.$$

Utilisant $r-1$ fois la contraposée de la définition d'être premier on obtient qu'il existe un indice $l$ tel que $q_1|p_l$. Par la Proposition 2.2.3, $p_l$ est irréductible. En utilisant que $q_1 > 1$, on obtient $q_1 = p_l$. Alors par (2.4.a) on obtient

$$\mathbb{Z} \ni \frac{n}{q_1} = \prod_{1 \leq i \leq r,\ i \neq l} p_i = \prod_{j=2}^{s} q_j$$

En particulier $r > 2$, parce qu'autrement le premier produit dans (2.2) serait vide. Ça veut dire que on peut appliquer l'hypothèse d'induction pour les deux produits dans (2.2). Ceci conclut notre démonstration. □

La fin du 3. cours, en 29.09.2020.

# Chapter 3

# Théorie des groupes

## 3.1 Définition et premiers exemples

**Définition 3.1.1.** Un groupe est une pair $(G, \cdot)$ constituée d'un ensemble $G$, et d'une application

$$\begin{array}{ccc} \cdot : & G \times G & \longrightarrow G \\ & \cup & \cup \\ & (a,b) & \longmapsto a \cdot b \end{array}$$

tels que

(1) (associativité) pour chaque $g, h, f \in G$ : $g \cdot (h \cdot f) = (g \cdot h) \cdot f$.

(2) (élément neutre à gauche) il existe un élément $e \in G$ tel que pour chaque $g \in G$ on a $e \cdot g = g$.

(3) (inverse à gauche) pour chaque $g \in G$ il existe $g^{-1} \in G$ tel que $\left(g^{-1}\right) \cdot g = e$.

Quelques remarques et conventions :

- L'application $(f, g) \mapsto f \cdot g$ est appelée la multiplication du groupe ; l'application $f \mapsto f^{-1}$ est appelée l'opération d'inversion du groupe.
- Au lieu de $a \cdot b$ on écrit parfois simplement $ab$.
- Grâce à l'associativité et au point au-dessus, on peut écrire $gfh$ pour $g \cdot (h \cdot f) = (g \cdot h) \cdot f$.
- On prend la convention d'écriture suivante : l'opération d'inversion a la priorité sur la multiplication. Par exemple on a $g \cdot g^{-1} = g \cdot \left(g^{-1}\right)$, mais en général $g \cdot g^{-1} \neq (g \cdot g)^{-1}$.
- D'habitude on écrit juste $G$ au lieu de $(G, \cdot)$.
- On dit que $G$ est *abélien* si : $\forall g, h \in G$ : $g \cdot h = h \cdot g$. Dans ce cas quelque fois on écrit $+$, $-$ et $0$ au lieu de $\cdot$, $(\_)^{-1}$ et $e$.
- On appelle $|G|$ l'ordre du groupe $G$.

**Proposition 3.1.2.** *Si $G$ est un groupe, alors un inverse à gauche est aussi un inverse à droite. Autrement dit :*

$$\forall g \in G : \; g^{-1} \cdot g = e \implies g \cdot g^{-1} = e$$

*Preuve.* On peut écrire

$$g \cdot g^{-1} \underset{\uparrow}{=} e \cdot g \cdot g^{-1} \underset{\uparrow}{=} \left(g^{-1}\right)^{-1} \cdot g^{-1} \cdot g \cdot g^{-1} \underset{\uparrow}{=} \left(g^{-1}\right)^{-1} \cdot e \cdot g^{-1} \underset{\uparrow}{=} \left(g^{-1}\right)^{-1} \cdot g^{-1} \underset{\uparrow}{=} e$$

$$\boxed{(2)} \qquad \boxed{(3)} \qquad \boxed{(3)} \qquad \boxed{(2)} \qquad \boxed{(3)}$$

où les chiffres réfèrent aux points correspondants de la Définition 3.1.1. □

**Proposition 3.1.3.** *Si $G$ est un groupe, alors $e$ est aussi un élément neutre à droite. Autrement dit :*

$$\forall g \in G : \ g \cdot e = g$$

*Preuve.* On a :

$$g \cdot e \underset{\uparrow}{=} g \cdot g^{-1} \cdot g \underset{\uparrow}{=} e \cdot g \underset{\uparrow}{=} g$$

(3) de Définition 3.1.1 | Proposition 3.1.2 | (2) de Définition 3.1.1

□

**Proposition 3.1.4.** *Si $G$ est un groupe, alors l'élément neutre est unique. En formules, pour chaque $e' \in G$:*

$$\left(\forall g \in G : \ e' \cdot g = e'\right) \implies e' = e$$

*Preuve.* Si $e'$ est comme dans l'énoncé :

$$e' \underset{\uparrow}{=} e' \cdot e \underset{\uparrow}{=} e$$

l'hypothese de la proposition | Proposition 3.1.3

□

**Proposition 3.1.5.** *Si $G$ est un groupe, alors dans les égalités on peut simplifier à droite :*

$$\forall f, g, h \in G : \ f \cdot g = h \cdot g \implies f = h.$$

*ainsi qu'à gauche :*

$$\forall f, g, h \in G : \ g \cdot f = g \cdot h \implies f = h.$$

*En particulier l'inverse $g^{-1}$ d'un élément $g \in G$ est unique.*

*Preuve.*

$$f \cdot g = h \cdot g \implies f \cdot g \cdot g^{-1} = h \cdot g \cdot g^{-1} \underset{\uparrow}{\implies} f \cdot e = g \cdot e \underset{\uparrow}{\implies} f = g$$

Proposition 3.1.2 | Proposition 3.1.3

$$g \cdot f = g \cdot h \implies g^{-1} \cdot g \cdot f = g^{-1} \cdot g \cdot h \underset{\uparrow}{\implies} e \cdot f = e \cdot g \underset{\uparrow}{\implies} f = g$$

(3) de Définition 3.1.1 | (2) de Définition 3.1.1

Ceci montre qu'il est possible de simplifier à droite et à gauche. Pour montrer que les inverses sont uniques, prenons $g \in G$ et supposons que $g^{-1}, h$ sont des inverses de $g$. Alors

$$g \cdot g^{-1} = e = g \cdot h$$

et en simplifiant à gauche on obtient $g^{-1} = h$. □

**Proposition 3.1.6.** *Si $G$ est un groupe et $g, h \in G$, alors $(gh)^{-1} = h^{-1}g^{-1}$.*

*Preuve.* En utilisant la Proposition 3.1.5 et le point (3) de Définition 3.1.1 il suffit de démontrer que $h^{-1}g^{-1}gh = e$. En effet:

$$h^{-1}g^{-1}gh \underset{\uparrow}{=} h^{-1}eh \underset{\uparrow}{=} h^{-1}h \underset{\uparrow}{=} e$$

(3) de Définition 3.1.1 | (2) de Définition 3.1.1 | (3) de Définition 3.1.1

□

**Notation 3.1.7.** Pour un groupe $G$ et un élément $g \in G$ on utilise la notation

$$g^n = \begin{cases} e & \text{si } n = 0 \\ \underbrace{g \cdot g \cdot \ldots \cdot g}_{n-\text{fois}} & \text{si } n > 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{n-\text{fois}} & \text{si } n < 0 \end{cases}$$

On a alors les identités suivantes (exercice : démontrez-les soigneusement) :

$$\forall m, n \in \mathbb{Z} : \ g^m g^n = g^{m+n} \quad \text{et} \quad \forall m, n \in \mathbb{Z} : \ (g^m)^n = g^{mn} \tag{1.7.a}$$

**Exemple 3.1.8.** On donne deux exemples de (1.7.a). La démonstration précise de (1.7.a) est laissée en exercice.

$$g^3 g^{-2} = gggg^{-1}g^{-1} = ggeg^{-1} = ggg^{-1} = ge = g = g^1$$

et

$$\left(g^3\right)^{-2} = (ggg)^{-1}(ggg)^{-1} \underset{\uparrow}{=} g^{-1}g^{-1}g^{-1}g^{-1}g^{-1}g^{-1} = g^{-6}$$

par Proposition 3.1.6 $(ggg)^{-1} = \left(g(gg)\right)^{-1} = (gg)^{-1}g^{-1} = g^{-1}g^{-1}g^{-1}$

**Notation 3.1.9.** Si $G$ est abélien et on dénote la multiplication par $+$, alors on écrit $n \cdot g$ au lieu de $g^n$. Dans ce cas, exploitant la propriété abélien on a la relation suivante pour chaque $g, f \in G$:

$$n \cdot (g + f) = (n \cdot g) + (n \cdot f) \tag{1.9.b}$$

Ici on démontre la propriété (1.9.b) juste dans le cas de $n \geq 0$ (on laisse comme devoir de la démontrer pour $n < 0$):

$$n \cdot (g+f) = \underbrace{(g+f) + \ldots + (g+f)}_{\uparrow} \underset{\uparrow}{=} \underbrace{g + \ldots + g}_{\uparrow} + \underbrace{f + \ldots + f}_{\uparrow} = n \cdot g + n \cdot f.$$

$n$ copies — $G$ est abélien — $n$ copies — $n$ copies

**Définition 3.1.10.** Soit $G$ un groupe et $g \in G$ un élément. L'*ordre* $o(g)$ de $g$ est le plus petit entier positif $n > 0$ que $g^n = e$. Si tel élément n'existe pas, on dit que $o(g) = \infty$.

**Exemple 3.1.11.** (1) Le groupe trivial: $G = \{e\}$.

(2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$. Dans ces trois cas l'élément neutre est 0, et l'ordre de tous les éléments sont $\infty$.

(3) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$. Dans ces deux cas l'élément neutre est 1, est les seules éléments d'ordre finie sont $-1$ et 1. En fait, pour tous les autres éléments $x$ de ces groupes on a $|x| \neq 1$, et alors pour chaque entier $n > 0$ on obtient $|x^n| = |x|^n \neq 1$, et par conséquence $x^n \neq 1$.

(4) Voici un exemple d'un ensemble avec une opération associative et avec l'identité qui n'est pas un groupe : $(\mathbb{Z} \setminus \{0\}, \cdot)$. En effet $-1$ et $1 \in \mathbb{Z} \setminus \{0\}$ sont les seuls éléments qui ont des inverses dans $(\mathbb{Z} \setminus \{0\}, \cdot)$. En particulier on appelle $(\mathbb{Z} \setminus \{0\}, \cdot)$ un demi-groupe (ce qui signifie : on a une opération associative) avec identité, ou simplement un monoïde.

(5) $(\mathrm{Bij}(X), \circ)$, où

$$\mathrm{Bij}(X) = \left\{ \ f : X \to X \ \middle| \ f \text{ est une bijection} \ \right\}$$

et $\circ$ est la composition des applications. L'inverse est donné par l'inverse des applications, et l'élément neutre est donné par $\mathrm{id}_X$.

(6) En particulier si $X = \{1, \dots, n\}$, alors on appelle $\mathrm{Bij}(X)$ *le groupe symétrique de degré* $n$, on le dénote par $S_n$, et on appelle ses éléments les *permutations* de $\{1, \dots, n\}$. Une notation de $\sigma \in S_n$ est:

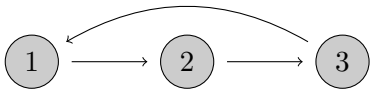
$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Par exemple pour $n = 3$, les éléments de $S_3$ sont

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{\substack{\mathrm{id}_{\{1,2,3\}} \\ \text{l'ordre vaut 1}}} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}_{\substack{\text{permutations avec un point fixe;} \\ \text{l'ordre de ces éléments est 2}}} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}_{\substack{\text{éléments sans points fixes;} \\ \text{l'ordre de ces éléments est 3}}}$$

On peut aussi visualiser les éléments de $S_n$ en utilisant les graphes orientés. De manière générale, un graphe orienté est un diagramme composé des sommets et des arêtes orientées entres les sommets. Quand on veut visualiser un élément de $S_n$, on dessine un sommet pour chaque élément de l'ensemble $\{1, \dots, n\}$, et on dessine une arête de $i$ à $\sigma(i)$ pour chaque $i \in \{1, \dots, n\}$. Par exemple:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} =$$




ou

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} =$$


Finalement, l'exemple suivant nous montre que $S_3$ n'est pas abélien. Soyons prudent parce que multiplication en $S_n$ est écrit en ordre de la composition des application. Ça veut dire que un produit $\tau\sigma \in S_n$ correspond à la composition $\tau \circ \sigma$ des fonctions, et alors on applique premièrement $\sigma$ aux éléments de $\{1, \dots, n\}$ et on applique $\tau$ deuxièmement. Ainsi, la computation démontrant que $S_3$ et non-abélien est:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

En fait, on démontrera plus loin que $S_3$ est le plus petit groupe non-abélien.

Pour notre autres exemples on a besoin de la construction générale suivante:

*Remarque* 3.1.12. Soient $G$ un groupe et $R \subseteq G \times G$ une relation d'équivalence. On se demande sous quelle(s) conditions(s) la structure de groupe de $G$ descend à l'ensemble quotient $G/R$ défini dans la Définition 1.2.17. Ecrivons $[g]$ la classe d'équivalence de l'élément $g \in G$, qui était précédemment notée $R_g$ dans la Définition 1.2.15. En d'autres termes

$$[g] = \{\ h \in G \mid (g, h) \in R\ \}$$

On voudrait définir une structure de groupe sur $G/R$ à partir des opérations de $G$ :

- Pour deux classes $x, y \in G/R$, on peut les écrire comme $x = [g|$ et $z = [f]$ ($g$ et $f$ sont appelé les *représentants* des classes d'équivalence), et on voudrait définir le produit de $x$ avec $y$ par $x \cdot y = [g] \cdot [f] = [gf]$.
- De même, pour définir l'inverse d'une classe $x \in G/R$ on écrit $x = [g]$, et on voudrait poser $x^{-1} := \left[g^{-1}\right]$.

- Finalement, on souhaiterait que l'élément neutre de $G/R$ soit $[e]$.

Le problème avec ces définitions est qu'en général il y a un grand choix de représentants $g \in G$ pour chaque classe d'équivalence $x \in G/R$, et que nos définitions doivent donner les mêmes résultats pour chaque choix de représentants. Autrement dit les opérations envisagées au-dessus doivent être bien définies.

**Proposition 3.1.13.** *Soient $G$ un groupe et $R \subseteq G \times G$ une relation d'équivalence. Les opérations sur $G/R$ envisagées dans la Remarque 3.1.12 sont bien définies si et seulement si les deux conditions suivantes sont satisfaites :*

*(1)* $(x, \tilde{x}) \in R, (y, \tilde{y}) \in R \implies (xy, \tilde{x}\tilde{y}) \in R$

*(2)* $(x, \tilde{x}) \in R \implies \left(x^{-1}, \tilde{x}^{-1}\right) \in R.$

*Dans ce cas $G/R$, avec les opérations et l'élément neutre définis dans la Remarque 3.1.12, est un groupe.*

*Preuve.* La condition (1) est, tautologiquement, la condition nécessaire et suffisante pour que l'application

$$\cdot : G/R \times G/R \to G/R, \quad ([g], [f]) \mapsto [gf]$$

soit bien définie. De la même manière, la condition (2) est vérifiée si et seulement si l'application

$$(\_)^{-1} : G/R \to G/R, \quad [g] \mapsto [g^{-1}]$$

est bien définie. Ainsi il faut seulement vérifier que dans ce cas $G/R$ avec ces opérations est un groupe. La raison est simplement que toutes les équations définissant la structure de groupe de $G/R$ sont vraies au niveau des représentants, puisque $G$ est un groupe. Par exemple pour l'associativité, si on prend des représentants $g, f, h \in G$ des classes $x, y, z \in G/R$, alors en utilisant plusieurs fois la définition de la multiplication de $G/R$ donnée dans Remarque 3.1.12 on obtient

$$(xy)z = ([g][f])[h] = [gf][h] = [(gf)h] \underset{\uparrow}{=} [g(fh)] = [g][fh] = [g]([f][h])$$

$G$ est un groupe, donc la multiplication de $G$ est associative

La vérification des points (2) et (3) de la Définition 3.1.1 est similaire et laissée en exercice. □

**Exemple 3.1.14.** Pour un entier $m > 0$, prenons l'ensemble quotient $\mathbb{Z}/m\mathbb{Z}$ construit dans les Exemple 1.2.14 et Exemple 1.2.18. On rappelle que

$$\mathbb{Z}/m\mathbb{Z} = \{\, m\mathbb{Z}\,,\ m\mathbb{Z}+1\,, \ldots,\ m\mathbb{Z}+(m-1)\,\} = \{\,[0]\,,\ [1]\,, \ldots,\ [m-1]\,\} \quad \text{et} \quad \left|\mathbb{Z}/m\mathbb{Z}\right| = m$$

En utilisant la Proposition 3.1.13, l'opération de groupe $+$ sur $\mathbb{Z}$ nous donne une opération de groupe sur $\mathbb{Z}/m\mathbb{Z}$ si et seulement si les conditions (1) et (2) de la Proposition 3.1.13 sont vérifiées. On les vérifie une par une :

La fin du 4. cours, en 06.10.2020.

- (1) de Proposition 3.1.13 : Prenons $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$ tel que $m|x - \tilde{x}$ et $m|y - \tilde{y}$. Alors $m|(x - \tilde{x}) + (y - \tilde{y})$. Cependant $(x - \tilde{x}) + (y - \tilde{y}) = (x + y) - (\tilde{x} + \tilde{y})$, alors on obtient $m|(x + y) - (\tilde{x} + \tilde{y})$.

- (2) de Proposition 3.1.13: Prenons $x, \tilde{x} \in \mathbb{Z}$ tel que $m|x - \tilde{x}$. Alors $m|\tilde{x} - x$ parce que $\tilde{x} - x = -(x - \tilde{x})$.

Ainsi, on a finit démontrer que $\mathbb{Z}/m\mathbb{Z}$ est un groupe. Par exemple, si on prend $m = 2$, le groupe $\mathbb{Z}/2\mathbb{Z}$ a deux éléments, les classes $[0]$ et $[1]$, et les tableaux d'opérations sont:

| $+$ | $[0]$ | $[1]$ |
|---|---|---|
| $[0]$ | $[0]$ | $[1]$ |
| $[1]$ | $[1]$ | $[0]$ |

| | $[0]$ | $[1]$ |
|---|---|---|
| $-$ | $[0]$ | $[1]$ |

Dans une façon similaire, le groupe $\mathbb{Z}/3\mathbb{Z}$ a trois éléments, les classes $[0]$, $[1]$ et $[2]$, et les tableaux d'opérations sont:

| $+$ | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ |
| $[1]$ | $[1]$ | $[2]$ | $[0]$ |
| $[2]$ | $[2]$ | $[0]$ | $[1]$ |

| | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $-$ | $[0]$ | $[2]$ | $[1]$ |

On a vérifié dans l'Exemple 3.1.14 que l'addition nous donne une structure de groupe sur $\mathbb{Z}/m\mathbb{Z}$. Plus surprenamment, la multiplication sur $\mathbb{Z}$ descend aussi au quotient et donne une structure de groupe à condition de jeter quelques classes d'équivalence. C'est expliqué dans l'Exemple 3.1.16, pour lequel le lemme suivant sera utile.

**Lemme 3.1.15.** *Soient $a \in \mathbb{Z}$ et $m \in \mathbb{Z}^{>0}$. Si $a$ et $m$ sont premiers entre eux, alors: il existe des entiers $x$ et $y$ tels que $xa + ym = 1$.*

*Preuve.* Choisissons un entier $n$ tel que $a + nm > 0$. Le Théorème 2.1.6 nous donne des entiers $x$ et $z$ tels que $x(a+nm)+zm = 1$. En développant la parenthèse on obtient $xa+(z+n)m = 1$, et on peut poser $y := z + n$. □

**Exemple 3.1.16.** Considérons $\mathbb{Z}/m\mathbb{Z}$ pour un entier $m > 0$ fixé. Comme dans le cas de l'addition, la multiplication est bien définie sur les classes d'équivalence de $\mathbb{Z}$ :

$$\forall x, \tilde{x}, y, \tilde{y} \in \mathbb{Z} : \ m|x - \tilde{x}, \ m|y - \tilde{y} \implies m|(x - \tilde{x})\tilde{y} + x(y - \tilde{y}) = xy - \tilde{x}\tilde{y}.$$

Ainsi la version de la Proposition 3.1.13 pour les monoïdes (plus précisément : c'est la même proposition sauf que *groupe* est remplacé par *monoïde* et que le point (2) est supprimé) nous donne que la multiplication induit une structure de monoïde sur $(\mathbb{Z}/m\mathbb{Z}, \cdot)$, avec $[1]$ comme l'élément neutre. Cependant il ne s'agit presque jamais d'un groupe (si $m > 1$, alors $[0]$ n'a pas d'inverse pour la multiplication).

On voudrait trouver un sous-ensemble de $\mathbb{Z}/m\mathbb{Z}$ qui est un groupe avec la multiplication comme opération. Un tel sous-ensemble est contenu dans le sous-ensemble d'éléments inversible de $(\mathbb{Z}/m\mathbb{Z}, \cdot)$. Alors notre mieux chance est d'essayer d'utiliser cet ensemble espérant que ça tournera d'être un groupe.

Pour réaliser ce plan, réfléchissons ce que être inversible en $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ signifie. La classe $[b] \in \mathbb{Z}/m\mathbb{Z}$ est inversible si et seulement si il existe un $[x] \in \mathbb{Z}/m\mathbb{Z}$ tel que $[x][b] = [1]$. De plus on a les équivalences suivantes:

$$[x][b] = [1] \ \Leftrightarrow \ [xb] = [1] \ \Leftrightarrow \ m|1 - xb \ \Leftrightarrow \ \exists y \in \mathbb{Z} : \ ym = 1 - xb \ \Leftrightarrow \ \exists y \in \mathbb{Z} : \ 1 = xb + ym \tag{1.16.c}$$

Un entier $x$ qui satisfait la condition finale de (1.16.c) existe si et seulement si $(b, m) = 1$. En fait $(b, m)|xb + ym$, qui montre une direction de cette proposition, et l'autre direction est exactement la proposition de Lemme 3.1.15. En somme, on a démontré que le sous-ensemble d'éléments inversible de $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ est exactement le sous-ensemble d'éléments de forme $[b]$ tel que $b$ est premier avec $m$.

Premièrement réfléchissons si être premier avec $m$ est bien défini sur les classes d'équivalence qu'on considère. Autrement dit il faut montrer que pour $a, b \in \mathbb{Z}$ tel que $[a] = [b]$ on a

$$(m, a) = 1 \implies (m, b) = 1 \tag{1.16.d}$$

Puisque, $[a] = [b]$ est équivalent à dire $m|a-b$, (1.16.d) est une conséquence directe de Lemme 2.1.2. En conséquent on peut définir $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ comme le sous-ensemble des classes d'équivalence qui sont premier avec $m$. On prétend que la multiplication de $\mathbb{Z}/m\mathbb{Z}$ donne une structure de groupe sur $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$.

Commençons par vérifier que $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ est stable par multiplication. Si $x, y \in \mathbb{Z}$ sont premiers avec $m$, alors $xy$ est aussi premier avec $m$. Donc $[x], [y] \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ implique que $[xy] \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. Il est clair que $[1] \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. Il reste à vérifier que $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ contient les inverses de ses éléments,

Pour le faire, prenons $[b] \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. On a déjà vu que l'inverse de $[b]$ en $\left(\mathbb{Z}/m\mathbb{Z}, \cdot\right)$ est $[x]$ ou $xb + ym = 1$ pour un entier adéquat $y$, et tel $x$ existe par Lemme 3.1.15. Si $x$ n'est pas premier avec $m$, alors $xb + ym = 1$ n'est pas premier avec $m$, ce qui est absurde. Donc $[x] \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ comme souhaité.

**Définition 3.1.17.** On définit la fonction $\phi : \mathbb{Z}^{>0} \to \mathbb{Z}^{>0}$, appelée *fonction phi d'Euler*, par

$$\phi(m) = \left|\left(\mathbb{Z}/m\mathbb{Z}\right)^\times\right| = \left\{\ m \geq b \in \mathbb{Z}^{>0} \ \middle|\ (m, b) = 1\ \right\}.$$

En somme, si nous envisageons les groupes de petit ordre, nous avons construit les exemples suivants :

| ordre | 1 | 2 | 3 | 4 | 5 | 6 | 7 | ... |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Z}/7\mathbb{Z}$ | ... |
| | $\left(\mathbb{Z}/2\mathbb{Z}\right)^\times$ | $\left(\mathbb{Z}/3\mathbb{Z}\right)^\times$<br>$\left(\mathbb{Z}/4\mathbb{Z}\right)^\times$<br>$\left(\mathbb{Z}/6\mathbb{Z}\right)^\times$ | | $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times$<br>$\left(\mathbb{Z}/8\mathbb{Z}\right)^\times$<br>$\left(\mathbb{Z}/10\mathbb{Z}\right)^\times$ | | $S_3$<br>$\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$<br>$\left(\mathbb{Z}/9\mathbb{Z}\right)^\times$<br>$\left(\mathbb{Z}/14\mathbb{Z}\right)^\times$ | | |

La contemplation de ce tableau soulève les questions suivantes :

*Question* 3.1.18. (1) Tous ces groupes sont-ils vraiment différents? Quand peut-on dire que deux groupes sont les mêmes ?

(2) Existent-ils d'autre groupes de petite taille qui ne sont pas dans ce tableau ? En particulier, existe-t-il d'autres manières de construire des groupes ? Par exemple sans utiliser $\mathbb{Z}$ ?

(3) Après avoir trouvé d'autres méthodes de construction et quelques nouveaux groupes, comment s'assurer que l'on a trouvé tous les groupes de petite taille ?

Pour la suite du cours, la Question 3.1.18 servira de guide à nos efforts.

## 3.2 HOMOMORPHISMES DE GROUPES

Commencons avec le point (1) de la Question 3.1.18 : on veut pouvoir définir lorsque deux groupes sont les mêmes. La notion correspondante pour les ensembles était celle de bijection. On ferra de même pour les groupes. On définit d'abord les "applications" entres groupes, puis on dira que deux groupes sont les mêmes s'il existe une "application" bijective entre eux. Un groupe étant un ensemble muni d'une opérations respectant certaines propriétés, il est naturel qu'une "application" entre groupes soit une fonction entre ensembles tenant compte de la structure additionnelle. La notion précise que l'on obtient est celle d'homomorphisme dont la définition est la suivante:

**Définition 3.2.1.** Soient $G$ et $H$ des groupes.

(1) Un *homomorphisme* $\phi : G \to H$ (ou simplement *morphisme*, qui n'est pas vraiment utilisé internationalement) est une application entre ensembles $\phi : G \to H$ telle que

$$\forall g, f \in G : \ \phi(gf) = \phi(g)\phi(f). \tag{2.1.a}$$

(2) Un *endomorphisme* de $G$ et un homomorphisme $G \to G$.

(3) Un *isomorphisme* $G \to H$ et un homomorphisme bijectif.

(4) Un *automorphisme* de $G$ et un endomorphisme qui est un isomorphisme.

(5) Deux groupes $G$ et $H$ sont isomorphes si il existe un isomorphisme entres eux, qui on dénote par $G \cong H$.

**Lemme 3.2.2.** *Si $\phi : G \to H$ est un homomorphisme de groupes, alors pour chaque $g \in G$ et $n \in \mathbb{Z}$:*

$$\phi(g^n) = \big(\phi(g)\big)^n.$$

*En particulier, pour $n = 0$ et pour $n = -1$ on obtient:*

$$\phi(e_G) = e_H \qquad et \qquad \forall g \in G \ : \ \phi\left(g^{-1}\right) = \big(\phi(g)\big)^{-1},$$

*où $e_G$ et $e_H$ sont les éléments neutres des groupes correspondants.*

*Preuve.* Pour chaque $g \in G$ on a

$$e_H \cdot \phi(g) \underset{\uparrow}{=} \phi(g) \underset{\uparrow}{=} \phi(e_G \cdot g) \underset{\uparrow}{=} \phi(e_G) \cdot \phi(g)$$

| $e_H$ est l'élément neutre | $e_G$ est l'élément neutre | $\phi$ est un homomorphisme |
|---|---|---|

En utilisant la simplification à droite (Proposition 3.1.5) on obtient le cas $n = 0$.

Pour $n > 0$ on démontre la proposition dans la computation suivante:

$$\phi\left(g^n\right) = \phi(\underbrace{g \cdot \ldots \cdot g}_{\uparrow\ n\text{-fois}}) \underset{\uparrow\ \text{Définition 3.2.1}}{=} \underbrace{\phi(g) \cdot \ldots \cdot \phi(g)}_{\uparrow\ n\text{-fois}} \underset{\uparrow\ \text{Notation 3.1.7}}{=} \big(\phi(g)\big)^n$$

Finalement, pour $n < 0$ le calcul suivante démontra la proposition, en tenant compte que l'inverse de $\big(\phi(g)\big)^{-n}$ est exactement $\big(\phi(g)\big)^n$ comme on l'a démontré dans Notation 3.1.7:

$$\big(\phi(g)\big)^{-n} \cdot \phi\left(g^n\right) \underset{\uparrow}{=} \phi\left(g^{-n}\right) \cdot \phi\left(g^n\right) \underset{\uparrow}{=} \phi\left(g^{-n} \cdot g^n\right) \underset{\uparrow}{=} \phi(e_G) \underset{\uparrow}{=} e_H$$

| on a déjà démontre le cas $n > 0$ | $\phi$ est un homomorphisme | Notation 3.1.7 | on a déjà démontré le cas $n = 0$ |
|---|---|---|---|

□

**Exemple 3.2.3.** (1) Soit $(G, +)$ un groupe abélien, et soit $n$ un entier. On définit une application entre ensembles $m_n : G \to G$ par

$$G \ni x \longmapsto n \cdot x \in G$$

On vérifie que $m_n$ est un homomorphisme: pour chaque $x, y \in G$ on a vérifié dans la Notation 3.1.9 que

$$m_n(x + y) = n \cdot (x + y) = (n \cdot x) + (n \cdot y) = m_n(x) + m_n(y).$$

On appelle cet homomorphisme "la multiplication par $n$". Un exemple particulier: si $G = \mathbb{Z}$, alors $m_n(d) = dn$.

(2) Soient $G$ un groupe et $g \in G$ un élément. Quels sont les homomorphismes $\phi : \mathbb{Z} \to G$ tels que $\phi(1) = g$ ? Pour un tel homomorphisme il faut forcement avoir

$$\mathbb{Z} \ni \phi(x) = \phi(x \cdot 1) \underset{\uparrow}{=} \big(\phi(1)\big)^x = g^x$$

Pour les groupes abéliens écrits additivement, la multiplication correspond à prendre la puissance adéquate

Lemme 3.2.2

En somme il y a une seule possibilité de définir un homomorphisme $\phi : \mathbb{Z} \to G$ tel que $\phi(1) = g$. S'il existe, alors il est donné par l'application entre ensembles suivante :

$$\mathrm{dexp}_g : \mathbb{Z} \ni x \longmapsto g^x \in G$$

Cette application est en fait un homomorphisme parce qu'on a vérifié dans la Notation 3.1.7 que pour chaque $x, y \in \mathbb{Z}$ on a $g^{x+y} = g^x g^y$. On appelle cet homomorphisme *l'exponentiel discret donné par* $g$.

Notons que pour $m \in \mathbb{Z}$, on a l'égalité $\mathrm{dexp}_n = m_n$. En utilisant la propriété d'unicité de $\mathrm{dexp}_n$ on obtient que les endomorphismes de $\mathbb{Z}$ sont:

$$\{\ m_n = \mathrm{dexp}_n \mid n \in \mathbb{Z}\ \}$$

(3) Considérons $\mathrm{dexp}_{[1]} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. C'est le premier exemple d'homomorphisme quotient, qu'on étudiera avec soin dans la section suivante. Cet homomorphisme peut être décrit de la manière suivante : on envoie un entier $x$ sur la classe d'équivalence $[x]$ de $x$ modulo $n$.

(4) Soient $G$ et $H$ deux groupes formé chacun par un unique élément, et soit $\phi : G \to H$ l'application qui envoie le seul élément $e_G$ de $g$ sur le seul élément $e_H$ de $H$. C'est un homomorphisme parce que $e_G$ et $e_H$ sont forcément les éléments neutres des groupes correspondants, et donc :

$$\phi(e_G e_G) \underset{\uparrow}{=} \phi(e_G) \underset{\uparrow}{=} e_H \underset{\uparrow}{=} e_H e_H$$

$e_G$ est l'élément neutre | définition de $\phi$ | $e_H$ est l'élément neutre

En somme, tous les groupes avec un élément sont isomorphes.

**Lemme 3.2.4.** *Si $\phi : G \to H$ et $\xi : H \to F$ sont homomorphismes de groupes, alors $\xi \circ \phi : G \to F$ est aussi un homomorphisme.*

*Preuve.* Il faut juste vérifier la Définition 3.2.1: pour chaque $g, h \in G$ on a

$$(\xi \circ \phi)(gh) \underset{\uparrow}{=} \xi(\phi(gh)) \underset{\uparrow}{=} \xi(\phi(g)\phi(h)) \underset{\uparrow}{=} \xi(\phi(g))\xi(\phi(h)) = \big((\xi \circ \phi)(g)\big)\big((\xi \circ \phi)(h)\big).$$

Définition 1.2.8 | $\phi$ est un homorphisme | $\xi$ est un homorphisme

□

*Remarque* 3.2.5. Sur la série d'exercices de cette semaine il y aura deux exercices montrant, d'une manière similaire au point (4) de l'Exemple 3.2.3, que tous les groupes avec deux éléments sont isomorphes entre eux, et que tous les groupes avec trois éléments sont isomorphes entre eux.

La fin du 5. cours, en 13.10.2020.

En utilisant le point (4) de l'Exemple 3.2.3 et la Remarque 3.2.5 on peut mettre à jour le tableau des groupes de petite taille (le signe ✓ signifie que l'on connaît tous les groupes de cet ordre, modulo les isomorphismes) :

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 | 6 | 7 | ... |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial<br>~~$(\mathbb{Z}/2\mathbb{Z})^\times$~~ | $\mathbb{Z}/2\mathbb{Z}$<br>~~$(\mathbb{Z}/3\mathbb{Z})^\times$~~<br>~~$(\mathbb{Z}/4\mathbb{Z})^\times$~~<br>~~$(\mathbb{Z}/6\mathbb{Z})^\times$~~ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>$(\mathbb{Z}/5\mathbb{Z})^\times$<br>$(\mathbb{Z}/8\mathbb{Z})^\times$<br>$(\mathbb{Z}/10\mathbb{Z})^\times$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$<br>$(\mathbb{Z}/7\mathbb{Z})^\times$<br>$(\mathbb{Z}/9\mathbb{Z})^\times$<br>$(\mathbb{Z}/14\mathbb{Z})^\times$ | $\mathbb{Z}/7\mathbb{Z}$ | ... |

**Définition 3.2.6.** Le produit $G \times H$ des groupes $G$ et $H$ est une structure de groupe sur l'ensemble produit $G \times H$, où la multiplication donnée par

$$(g, h) \cdot (g', h') = (gg', hh').$$

On vérifie dans le Lemme 3.2.7 que cette définition nous donne bien un groupe.

**Lemme 3.2.7.** *Le groupe définit en Définition 3.2.6 est bien un groupe avec :*

- *l'élément neutre donné par $(e_G, e_H)$, où $e_G$ et $e_H$ sont les éléments neutre des groupes correspondants, et*
- *avec l'inverse donné par $(g, h)^{-1} = \left(g^{-1}, h^{-1}\right)$.*

*Preuve.* Il faut vérifier les trois condition de la Définition 3.1.1. Premièrement on vérifie l'associativité :

$$\begin{aligned}\forall g, g', g'' \in G, \forall h, h', h'' \in H \ : \ \big((g, h) \cdot (g', h')\big) \cdot (g'', h'') &= (gg', hh') \cdot (g'', h'') \\ &= (gg'g'', hh'h'') \\ &= (g, h) \cdot (g'g'', h'h'') \\ &= (g, h) \cdot \big((g', h') \cdot (g'', h'')\big)\end{aligned}$$

Deuxièmement on vérifie que $(e_G, e_H)$ est vraiment l'élément neutre :

$$\forall g \in G, \forall h \in H \ : \ (e_G, e_H) \cdot (g, h) = (e_G g, e_H h) = (g, h)$$

Finalement on vérifie que l'inverse est donné comme dans l'énoncé :

$$\forall g \in G, \forall h \in H \ : \ \left(g^{-1}, h^{-1}\right) \cdot (g, h) = \left(g^{-1} g, h^{-1} h\right) = (e_G, e_H)$$

□

En utilisant la Définition 3.2.6 on peut ajouter les petits produits au tableau des groupes de petite taille:

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 | 6 | 7 | ... |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>$(\mathbb{Z}/5\mathbb{Z})^\times$<br>$(\mathbb{Z}/8\mathbb{Z})^\times$<br>$(\mathbb{Z}/10\mathbb{Z})^\times$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$<br>$(\mathbb{Z}/7\mathbb{Z})^\times$<br>$(\mathbb{Z}/9\mathbb{Z})^\times$<br>$(\mathbb{Z}/14\mathbb{Z})^\times$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/7\mathbb{Z}$ | ... |

Maintenant que les trois premières colonnes sont complètes, intéressons-nous aux quatrième et sixième colonnes. Pour trouver leur forme finale, on commence par déterminer si $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont isomorphes, et si $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont isomorphes. Vous répondrez à la première de ces questions dans une série d'exercices, et on répond de la deuxième ici, dans le texte.

Une manière élégante de répondre est d'utiliser la propriété universelle des produits, que nous expliquons maintenant.

**Notation 3.2.8.** Soient $F$ et $H$ des groupes. On définit les homomorphismes des projections $\mathrm{pr}_F : F \times H \to F$ et $\mathrm{pr}_H : F \times H \to H$ par les formules:

$$\forall (f,h) \in F \times H : \ \mathrm{pr}_F\big((f,h)\big) = f \qquad \text{et} \qquad \mathrm{pr}_H\big((f,h)\big) = h.$$

On vérifie que $\mathrm{pr}_F$ et $\mathrm{pr}_H$ sont des homomorphismes. Par symétrie il suffit de le vérifier pour $\mathrm{pr}_F$ :

$$\forall (f,h),(f',h') \in F\times H : \ \mathrm{pr}_F\big((f,h)\cdot(f',h')\big) \underset{\uparrow}{=} \mathrm{pr}_F\big((ff',hh')\big) \underset{\uparrow}{=} ff' = \mathrm{pr}_F\big((f,h)\big)\cdot\mathrm{pr}_F\big((f',h')\big).$$

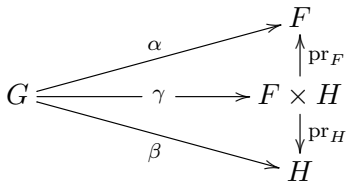
Définition 3.2.6 — définition de $\mathrm{pr}_F$

**Proposition 3.2.9.** PROPRIÉTÉ UNIVERSELLE DES PRODUITS. *Soient $G, F, H$ des groupes. Etant donné des homomorphismes $\alpha : G \to F$ et $\beta : G \to H$, il existe un unique homomorphisme $\gamma : G \to F \times H$ tel que $\mathrm{pr}_F \circ \gamma = \alpha$ et $\mathrm{pr}_H \circ \gamma = \beta$.*

*On note aussi que $\gamma$ est donné par la formule*

$$\gamma(g) = \big(\alpha(g), \beta(g)\big) \tag{2.9.b}$$

*et la situation peut être visualisée dans le diagramme commutatif suivant :*




*Preuve.* Par la définition de $\mathrm{pr}_F$ et $\mathrm{pr}_H$, les égalités $\mathrm{pr}_F \circ \gamma = \alpha$ et $\mathrm{pr}_H \circ \gamma = \beta$ sont équivalentes à (2.9.b). Il suffit donc de démontrer que $\gamma$ avec la définition donné en (2.9.b) est un homomorphisme:

$$\forall g, f \in G : \ \gamma(gf) \underset{\uparrow}{=} \big(\alpha(gf), \beta(gf)\big) \underset{\uparrow}{=} \big(\alpha(g)\alpha(f), \beta(g)\beta(f)\big) \underset{\uparrow}{=} \big(\alpha(g),\beta(g)\big)\cdot\big(\alpha(f),\beta(f)\big) \underset{\uparrow}{=} \gamma(g)\gamma(f)$$

(2.9.b) — $\alpha$ et $\beta$ sont des homomorphismes — définition de la multiplication pour les produits dans Définition 3.2.6 — (2.9.b)

□

En appliquant la Proposition 3.2.9 aux homomorphismes $\alpha : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ et $\alpha : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ donnés par le point (3) de l'Exemple 3.2.3, on obtient $\gamma : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. D'un autre côté, le point (3) de l'Exemple 3.2.3 nous donne $\delta : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$. Les homomorphismes $\gamma$ et $\delta$ semblent être très similaire. Les deux sont surjectifs, et l'ensemble des éléments qui sont envoyé sur l'élément neutre sont les mêmes : il s'agit dans les deux cas de $6\mathbb{Z}$ (nous laissons au lecteur le soin de prouver ces affirmations). On soupçonne ainsi $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ d'être isomorphes. La théorie permettant de confirmer ce soupçon est développée dans la section suivante.

## 3.3 SOUS-GROUPES: INTRODUCTION

**Définition 3.3.1.** Soit $(G, \cdot)$ un groupe. Un sous-ensemble $H \subseteq G$ est un *sous-groupe* de $H$ si

(1) $\cdot(H \times H) \subseteq H$, ou autrement dit $\forall a, b \in H : a \cdot b \in H$, et en particulier on peut prendre la restriction $\cdot|_{H\times H} : H \times H \to H$, et

(2) $(H, \cdot|_{H\times H})$ et un groupe.

Pour signifier qu'un sous-ensemble $H \subseteq G$ est un sous-groupe, on utilise la notation $H \leq G$.

**Proposition 3.3.2.** *Soit $(G, \cdot)$ un groupe. Un sous-ensemble $H \subseteq G$ est un* sous-groupe *si est seulement si*

*(1)* $H \neq \emptyset$,

*(2)* $a, b \in H \implies ab \in H$, *et*

*(3)* $a \in H \implies a^{-1} \in H$.

*De plus l'identité de $H$ et de $G$ sont les mêmes, et l'inverse d'un élément $h \in H$ pris dans $H$ est le même que dans $G$.*

*Preuve.* $\boxed{\implies:}$ Supposons que $H \subseteq G$ est un sous-groupe. En utilisant la Définition 3.3.1, $H$ muni de la restriction de $\cdot$ à $H$ est un groupe. Ainsi $H$ contient un élément neutre $e_H$, et alors on obtient la condition (1). La condition (2) s'obtient encore plus facilement, parce qu'elle est supposée dans la Définition 3.3.1.

Fixons $h \in H$. Il a un inverse dans $H$ que l'on dénote par $h_H^{-1}$. Pour établir la condition (3) il suffit de démontrer que c'est aussi l'inverse de $h$ en $G$. L'unicité de l'inverse (Proposition 3.1.5) nous donne exactement cela, une fois établi que l'élément neutre $e_H$ de $H$ est aussi un élément neutre de $G$. Ainsi il nous reste à démontrer cette dernière affirmation, ce qui est fait dans le calcul suivant, où $e_G$ est l'élément neutre de $G$:

$$e_H e_H = e_H = e_H \cdot e_G \underset{\uparrow}{\implies} e_H = e_G$$

$\boxed{\text{simplification à gauche (Proposition 3.1.5}}$

$\boxed{\impliedby:}$ Pour cette direction on suppose que les conditions (1), (2) et (3) de l'énoncé sont satisfaites ; il faut démontrer que $H$ est un sous-groupe. Mais la condition (2) est la même que la condition (1) de la Définition 3.3.1. Ainsi il suffit de démontrer la condition (2) de la Définition 3.3.1 pour conclure que $(H, \cdot|_{H\times H})$ est un groupe. Pour cela, il suffit de démontrer que l'élément neutre $e_G$ de $G$ est contenu dans $H$, parce que dans ce cas $e_G$ nous donne un élément neutre pour $H$ et l'existence de l'inverse en $H$ est donné par la condition (3) de la présente proposition.

Pour démontrer que $e_G \in H$ prenons un élément quelconque $h$ de $H$, qui existe par la condition (1) de la présente proposition. Les implications suivantes concluent notre démonstration :

$$\underset{\uparrow}{\implies} h^{-1} \in H \underset{\uparrow}{\implies} H \in h^{-1} \cdot h = e_G.$$

$\boxed{(3)}$ $\boxed{(2)}$

□

**Exemple 3.3.3.** On peut vérifier que les exemples suivants sont les sous-groupes en utilisant la Proposition 3.3.2 :

(1) Pour un groupe quelconque $G$, le sous-ensemble $\{e\} \subseteq G$ est un sous-groupe. Ce sous-groupe, ainsi que $G$, sont appelés les *sous-groupes triviaux* de $G$. Les autre sous-groupes sont appelé les *sous-groupes propres*.

(2) Le sous-ensemble $\{1, -1\} \subseteq (\mathbb{Q}, \cdot)$ est un sous-groupe. Puisqu'il a deux éléments, en utilisant l'exercice correspondant de la série on obtient que $\{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$.

(3) Pour un entier $m > 0$, le sous-ensemble

$$m\mathbb{Z} = \{\ ma \mid a \in \mathbb{Z}\ \} = \{\ b \in \mathbb{Z} \mid m|b\ \} \subseteq \mathbb{Z}$$

est un sous-groupe de $(\mathbb{Z}, +)$. Pour vérifier cela, comme indiqué au début de l'exemple, il faut vérifier les conditions de la Proposition 3.3.2. On note que cela ressemble à la vérification que "mod m" nous donne une relation d'équivalence, qui est faite dans l'Exemple 1.2.14. Plus précisément, la vérification de la symétrie ressemble à la vérification que $m\mathbb{Z}$ est stable pour l'inversion, et la vérification de la transitivité ressemble à la vérification que $m\mathbb{Z}$ est stable pour l'addition. Ce n'est en fait pas une coïncidence. On verra dans la Section 3.5 que chaque sous-groupe définit une relation d'équivalence, et pour $m\mathbb{Z} \subseteq \mathbb{Z}$ cette relation d'équivalence est exactement la relation d'équivalence de l'Exemple 1.2.14.

(4) Fixons deux entiers positifs $m, n$ tels que $m|n$. Être divisible par $m$ est bien défini sur les classe d'équivalence qui forment $\mathbb{Z}/n\mathbb{Z}$. Cela siginifie que si $[x] = [y] \in \mathbb{Z}/n\mathbb{Z}$, alors $m|x \iff m|y$, ce qui est démontré dans le calcul suivant :

$$\begin{array}{ccccccc} [x] = [y] & \iff & n|x-y & \implies & m|x-y & \implies & m|x \text{ si et seulement si } m|y \\ \uparrow & & \uparrow & & \uparrow & & \\ \boxed{\text{en } \mathbb{Z}/n\mathbb{Z}} & & \boxed{\text{Exemple 1.2.14}} & & \boxed{m|n} & & \end{array}$$

Ainsi il est sensé de dire qu'un élément de $\mathbb{Z}/n\mathbb{Z}$ est divisible par $m$ ou qu'il n'est pas divisible par $m$. Si $m$ divise $[x] \in \mathbb{Z}/n\mathbb{Z}$, alors on écrit $m|[x]$. En particulier on peut définir le sous-ensemble:

$$H := \left\{\ [x] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; m|[x]\ \right\} \subseteq \mathbb{Z}/n\mathbb{Z}$$

On laisse comme exercice (extrêmement facile) de démontrer en utilisant la Proposition 3.3.2 que $H$ est un sous-groupe (en fait c'est pratiquement la même vérification que dans le point précédent).

Par exemple pour $\mathbb{Z}/6\mathbb{Z}$ on obtient deux sous-groupes propres :

- pour $m = 3$, on a $H = \{[0], [3]\}$, qui a deux élément et par conséquent est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (en utilisant l'exercice correspondant sur l'une des séries d'exercices) ;
- pour $m = 2$, on a $H = \{[0], [2], [4]\}$, qui a trois élément et par conséquent est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ (en utilisant l'exercice correspondant sur l'une des séries d'exercices).

Une question naturelle est s'il existe d'autres sous-groupes propres de $\mathbb{Z}/6\mathbb{Z}$ ; on y répondra dans les sections suivantes.

(5) Soit $1 < n \in \mathbb{N}$. On prétend que le sous-ensemble

$$H = \left\{\ \sigma \in S_n \;\middle|\; \sigma(1) = 1\ \right\} \subseteq S_n$$

est un sous-groupe. En fait $\mathrm{id} \in H$ et alors $H \neq \emptyset$, et il est clair que la composition et l'inverse des permutations qui fixent l'élément 1, fixent aussi l'élément 1. On peut se

convaincre de cette affirmation en réalisant que la réprésentation via son graphe d'une permutation avec cette propriété est


Par conséquent on a obtenu en utilisant la Proposition 3.3.2 que $H$ est un sous-groupe de $S_n$.

Pour un exemple spécifique, on peut prendre $n = 3$. Dans ce cas on obtient le sous-groupe

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \subseteq S_3$$

(6) Similairement au point précédent, si $X \subseteq \{1, \ldots, n\}$ on peut prendre

$$H = \left\{ \sigma \in S_n \;\middle|\; \forall x \in X : \; \sigma(x) = x \right\} \subseteq S_n$$

et on peut démontrer dans la même façon que $H$ un sous-groupe. En jetant les élément de $X$ et en réétiquetant les éléments qui nous restent on peut identifier $H$ avec $S_{n-|X|}$. Autrement dit, $S_n$ contient plusieurs copies des $S_j$, pour $j < n$.

(7) Le centre $Z(G)$ d'un groupe $G$ est défini par

$$Z(G) = \left\{ g \in G \;\middle|\; \forall f \in G : \; fg = gf \right\} \subseteq G$$

On démontre que $Z(G)$ est un sous-groupe de $G$ en vérifiant les trois conditions de la Proposition 3.3.2:

(i) Par la Définition 3.1.1 et par la Proposition 3.1.3, on a $eg = g = ge$. Ainsi $e \, in Z(G)$, et alors $Z(G) \neq \emptyset$.

(ii) Si $f, h \in Z(G)$, alors pour chaque $g \in G$ on a

$$\begin{array}{ccccc} fhg & = & fgh & = & gfh \\ & & \uparrow & & \uparrow \\ & & \boxed{h \in Z(G)} & & \boxed{f \in Z(G)} \end{array}$$

Par conséquent $fh \in Z(G)$.

(iii) Si $f \in Z(G)$, alors pour chaque $g \in G$ les deux éléments$f^{-1}g$ et $gf^{-1}$ sont des inverse de $fg^{-1}$:

$$\begin{array}{ccccc} f^{-1}gfg^{-1} & = & f^{-1}fgg^{-1} = e & \quad \text{et} \quad & gf^{-1}fg^{-1} = gg^{-1} = e \\ & \uparrow & & & \\ & \boxed{f \in Z(G)} & & & \end{array}$$

En utilisant l'unicité de l'inverse on obtient que $f^{-1}g = gf^{-1}$, et par conséquent $f^{-1} \in Z(G)$.

**Définition 3.3.4.** Soit $\phi : G \to H$ un homomorphisme de groupes. Le *noyau* de $\phi$ est défini par

$$\ker \phi = \left\{ g \in G \;\middle|\; \phi(g) = e \right\}$$

et l'*image* de $\phi$ et définie par

$$\operatorname{im} \phi = \left\{ \phi(g) \in H \;\middle|\; g \in G \right\}$$

Ces sont des sous-groupes par la Proposition 3.3.5.

**Proposition 3.3.5.** *Si $\phi : G \to H$ est un homomorphisme de groupes, alors* $\operatorname{im}\phi$ *et* $\ker\phi$ *sont des sous-groupes de $H$ et de $G$ respectivement.*

*Preuve.* Dans les deux cas il faut vérifier les trois conditions de la Proposition 3.3.2. On le fait séparément pour $\ker\phi$ et pour $\operatorname{im}\phi$ :

$\ker\phi$ est un sous-groupe de $G$:

(1) Par le Lemme 3.2.2, $\phi(e) = e$, alors $e \in \ker\phi$.

(2) Si $g, f \in \ker\phi$, alors le calcul suivant nous montre que $g, f \in \ker\phi$:

$$\phi(gf) \underset{\uparrow}{=} \phi(g)\phi(f) \underset{\uparrow}{=} ee \underset{\uparrow}{=} e$$

Définition 3.2.1 — $g, f \in \ker\phi$ — Définition 3.2.1

(3) Si $g \in \ker\phi$, alors le calcul suivant nous montre que $g^{-1} \in \ker\phi$:

$$\phi\left(g^{-1}\right) \underset{\uparrow}{=} \left(\phi(g)\right)^{-1} \underset{\uparrow}{=} e^{-1} \underset{\uparrow}{=} e$$

Lemme 3.2.2 — $g \in \ker\phi$ — un exercise d'une série

$\operatorname{im}\phi$ est un sous-groupe de $H$:

(1) Par Lemme 3.2.2, $\phi(e) = e$, alors $e \in \operatorname{im}\phi$.

(2) Si $\phi(g), \phi(f) \in \operatorname{im}\phi$, alors

$$\phi(g)\phi(f) \underset{\uparrow}{=} \phi(gf) \in \operatorname{im}\phi.$$

Définition 3.2.1

(3) Si $\phi(g) \in \operatorname{im}\phi$, alors $\left(\phi(g)\right)^{-1} = \phi\left(g^{-1}\right) \in \operatorname{im}\phi$ par Lemme 3.2.2.

□

**Exemple 3.3.6.** Calculons les noyaux et les images des homomorphismes de l'Exemple 3.2.3.

(1) Pour un groupe abélien $(G, +)$, considérons $m_n : G \to G$ défini au point (1) de l'Exemple 3.2.3.

$$\ker m_n = \underbrace{G[n] \overset{\text{Def}}{=} \left\{ g \in G \;\middle|\; n \cdot g = 0 \right\}}_{\uparrow}$$

élément de $G$ de $n$-torsion

$$\operatorname{im} m_n = n \cdot G \overset{\text{Def}}{=} \left\{ n \cdot g \;\middle|\; g \in G \right\}$$

(2) Pour un groupe $G$ et un élément $g \in G$, considérons $\operatorname{dexp}_g : \mathbb{Z} \to G$ défini en point (2) de l'Exemple 3.2.3.

$$\ker \operatorname{dexp}_g = \begin{cases} \{e\} & \text{si } o(g) = \infty \\ o(g) \cdot \mathbb{Z} & \text{si } o(g) \neq \infty \end{cases}$$

$$\operatorname{im} \operatorname{dexp}_g = \underbrace{\left\{ g^n \;\middle|\; n \in \mathbb{Z} \right\} \overset{\text{Def}}{=} \langle g \rangle_G = \langle g \rangle}_{\uparrow}$$

le sous-groupe de $G$ engendré par $g$, le sous-indice $G$ est généralement ommis

On donne aussi plus spécifique exemples des sous-groupes engendrés par un élément $g$ de $S_3$:

La fin du 6. cours, en 20.10.2020.

- si on prend $g = (1\ 2)$, alors $o(g) = 2$, qui implique que $\langle g \rangle = \{\mathrm{id}, g\}$, et
- si on prend $g = (1\ 2\ 3)$, alors $o(g) = 3$, qui implique que $\langle g \rangle = \{\mathrm{id}, g, g^2\}$.

(3) Considérons $\mathrm{dexp}_{[1]} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

$$\ker \mathrm{dexp}_{[1]} = n \cdot \mathbb{Z}$$

$$\mathrm{im}\, \mathrm{dexp}_{[1]} = \mathbb{Z}/n\mathbb{Z}$$

(4) Pour un homomorphisme quelconque $\phi : G \to H$, on a

$$\phi \text{ et un isomorphisme } \Leftrightarrow \ \phi \text{ et injectif et } \ \mathrm{im}\, \phi = H$$

(5) Considérons l'homomorphisme $m_2 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ et $m_3 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$. Les noyaux et images de ces homomorphismes sont exactement les sous-groupes considérés dans le point (4) de l'Exemple 3.3.3. Plus précisément :

$$\ker m_2 = 3 \cdot \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{im}\, m_2 = 2 \cdot \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$$

$$\ker m_3 = 2 \cdot \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \qquad \mathrm{im}\, m_3 = 3 \cdot \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$$

**Lemme 3.3.7.** *Soit $\phi : G \to H$ un homomorphisme de groupes. On a $\ker \phi = \{e\}$ si et seulement si $\phi$ est injective.*

*Preuve.* Si $\phi$ et injective, alors $\ker \phi = \{e\}$ par définition. En conséquence il suffit de montrer que si $\ker \phi = \{e\}$, alors $\phi$ est injective. Supposons donc que $\ker \phi = \{e\}$ et considérons $g, h \in G$ tels que $\phi(g) = \phi(h)$. On a

$$\phi\left(gh^{-1}\right) \underset{\uparrow}{=} \phi(g)\phi\left(h^{-1}\right) \underset{\uparrow}{=} \phi(g)\phi(h)^{-1} \underset{\uparrow}{=} e \underset{\uparrow}{\Longrightarrow} gh^{-1} = e \implies g = h$$

Définition 3.2.1 | Lemme 3.2.2 | $\phi(g) = \phi(h)$ | $\ker \phi = \{e\}$

□

**Proposition 3.3.8.** *On a $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

*Preuve.* Considérons les homomorphismes $\alpha = m_3 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ et $\beta = m_2 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ définis dans le point (4) de l'Exemple 3.3.3. En utilisant la propriété universelle du produit on obtient un homomorphisme $\gamma : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ tel que $\gamma(x) = (\alpha(x), \beta(x))$.

En utilisant la formule $\gamma(x) = (\alpha(x), \beta(x))$, on a $\ker \gamma = \ker \alpha \cap \ker \beta$. Le calcul suivant nous démontre que $\ker \gamma = \{e\}$ :

$$\ker \alpha \cap \ker \beta \underset{\uparrow}{=} \left(3 \cdot \mathbb{Z}/6\mathbb{Z}\right) \cap \left(2 \cdot \mathbb{Z}/6\mathbb{Z}\right) \underset{\uparrow}{=} \left\{ [x] \in \mathbb{Z}/6\mathbb{Z} \;\middle|\; x \in \mathbb{Z},\ 2|x,\ 3|x \right\}$$

(4) de l'Exemple 3.3.3

les éléments de $\mathbb{Z}/6\mathbb{Z}$ peuvent être répresentés par des entiers dans la classe d'équivalence correspondante

$$= \left\{ [x] \in \mathbb{Z}/6\mathbb{Z} \;\middle|\; x \in \mathbb{Z},\ 6|x \right\} = \{e\}.$$

En utilisant le Lemme 3.3.7 on obtient que $\gamma$ est injective. Puisque les deux groupes entrant en jeu dans la définition de $\gamma$ ont chacun 6 éléments, on obtient qu'en fait $\gamma$ est bijective, et ainsi $\gamma$ est un isomorphisme. □

**Proposition 3.3.9.** *Soient $n_1, \ldots, n_t$ des entiers positifs qui deux-à-deux premiers entre eux, et définissons $n = \prod_{i=1}^{t} n_i$. On a $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z}$.*

*Preuve.* Ce sera un exercice. Comme méthode, on faut généraliser Proposition 3.3.8. □

En utilisant la Proposition 3.3.8, et l'un des exercices vus en séries, on peut mettre à jour le tableau des groupes de petite taille :

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 | 6 | 7 | ... |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>$(\mathbb{Z}/5\mathbb{Z})^\times$<br>~~$(\mathbb{Z}/8\mathbb{Z})^\times$~~<br>$(\mathbb{Z}/10\mathbb{Z})^\times$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$<br>$(\mathbb{Z}/7\mathbb{Z})^\times$<br>$(\mathbb{Z}/9\mathbb{Z})^\times$<br>$(\mathbb{Z}/14\mathbb{Z})^\times$<br>~~$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$~~ | $\mathbb{Z}/7\mathbb{Z}$ | ... |

couleur bleu: groupes non-abéliens

Dans la suite (en Section 3.5), on réduira encore les colonnes d'ordre 4 et 6, et on démontrera que les colonnes d'ordre 5 et 7 sont complètes (plus généralement, nous serons capables de lister complètement les colonnes correspondants aux nombres premiers).

## 3.4 L'HOMOMORPHISME sgn

Dans cette section on étudie en détail un premier exemple d'homomorphisme d'un groupe non-abélien. On appelle cet homomorphisme la signature, et on le dénote par sgn. La source de cet homomorphisme et $S_n$ et la cible est $\mathbb{Z}/2\mathbb{Z} \cong \{1, -1\} \subseteq (\mathbb{Z}, \cdot)$. Autrement dit, c'est un homomorphisme sgn : $S_n \to \mathbb{Z}/2\mathbb{Z} \cong \{1, -1\}$.

On rappelle premièrement quelques définitions et résultats vus en série d'exercice :

**Définition 3.4.1.** Un *cycle* est un élément $\sigma \in S_n$ de forme suivante:

$$\begin{aligned} \sigma(a_i) &= a_{i+1} && \text{pour } 1 \leq i < r \\ \sigma(a_r) &= a_1 && \\ \sigma(i) &= i && \text{pour } i \notin \{a_1, \ldots, a_r\} \end{aligned}$$

où $a_1, \ldots, a_r \in \{1, \ldots, n\}$ sont éléments deux-à-deux distincts. On appelle un tel $\sigma$ un $r$-cycle, et on dit que $r$ est la *longueur* de $\sigma$. On dénote le cycle au-dessus par $(a_1 a_2 \ldots a_n)$.

On appelle l'ensemble $\{a_1, \ldots, a_r\}$ le *support* de $\sigma$, qui est bien défini par Remarque 3.4.3, et qui on dénote par $\operatorname{Supp} \sigma$.

On appelle un 2-cycle une *transposition*.

**Exemple 3.4.2.** Le cycle suivant est un 4-cycle :

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

*Remarque* 3.4.3. Notons que

(1) Les $a_i$ de Définition 3.4.1 sont unique modulo leurs rotations. Autrement dit, si des $a'_i$ définissent aussi le même $\sigma \in S_n$, alors il existe un entier $0 \leq l \leq r-1$ tel que

$$a'_i = \begin{cases} a_{i+l} & \text{si } 1 \leq i \leq r-l \\ a_{i-(r-l)} & \text{si } r-l+1 \leq i \leq r \end{cases}$$

(2) On dit que deux cycles $\sigma$ et $\tau \in S_n$ sont disjoints si $(\operatorname{Supp} \sigma) \cap (\operatorname{Supp} \tau) = \emptyset$.

(3) Si $\sigma$ est un cycle de longueur $r$, alors $\sigma^r = \mathrm{id}$.

**Proposition 3.4.4.** *Chaque $\sigma \in S_n$ peut être écrit comme un produit (vide si $\sigma = id$) de cycles disjoints de longueur au moins 2. Ce produit est unique modulo permutation des facteurs.*

*Preuve.* C'était une exercice de série. On en rappelle seulement l'idée : considérons le graphe associé à une permutation $\sigma \in S_n$. Pour chaque sommet de ce graphe il y a exactement une arête qui arrive sur ce sommet, et une arête qui part de ce sommet. Par conséquent, le graphe est constitué de cycles disjoints. □

**Exemple 3.4.5.**

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

**Proposition 3.4.6.** *Chaque $\sigma \in S_n$ est un produit des transpositions.*

*Preuve.* En utilisant la Proposition 3.4.4 il suffit de démontrer le résultat pour $\sigma$ un cycle $(a_1\ a_2 \dots a_r)$. On le démontre par induction sur $r$. Si $r = 1$ alors $\sigma$ est un produit de zéro transpositions, et si $r = 2$ alors $\sigma$ est une transposition. Ainsi on peut supposer que $r > 2$ et que l'on connaît la proposition pour les valeurs plus petites de $r$. Dans ce cas, notons que

$$(a_1\ a_r)(a_1\ a_2 \dots a_r) = (a_1 \dots a_{r-1}).$$

qui nous donne en multipliant par $(a_1\ a_r)$ à gauche

$$(a_1\ a_2 \dots a_r) = (a_1\ a_r)(a_1 \dots a_{r-1}).$$

Par induction on peut écrire $(a_1 \dots a_{r-1})$ comme un produit de transpositions, ce qui conclut notre démonstration. □

**Exemple 3.4.7.** La décomposition de la Proposition 3.4.6 n'est pas unique. Par exemple:

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 3).$$

**Définition 3.4.8.** Fixons un entier $n$. On définit une application $\operatorname{sgn} : S_n \to \{-1, 1\}$ donnée par

$$\operatorname{sgn}(\sigma) = \text{-1}^{\left|\left\{ (i,j)\in\mathbb{N}^2 \;\middle|\; 1\le i<j\le n, \text{ et } \sigma(i)>\sigma(j) \right\}\right|} = \prod_{1\le i<j\le n} \underset{\uparrow}{\operatorname{signe}}\big(\sigma(j) - \sigma(i)\big)$$

la fonction signe vaut -1 si l'arugment est positif et 1 si l'arugment est négatif ; c'est dénoté d'habitude aussi par sgn, mais ici on veux éviter de la confondre avec l'homomorphisme ce que l'on définit)

Autrement dit : la puissance dénombre les paires d'entiers $i < j$ telles que $\sigma$ inverse l'ordre de $i$ et $j$. Dans ce cas on dit que les nombres $i$ et $j$ sont *en inversion* pour $\sigma$.

**Exemple 3.4.9.** On compte les paires en inversion pour

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

La liste de telles paires est

$$(1,3),\ (1,4),\ (1,6),\ (2,3),\ (2,4),\ (2,5),\ (2,6),\ (4,6),\ (5,6).$$

On compte 9 paires en inversion, ce qui implique que $\operatorname{sgn}(\sigma) = -1$.

Notre prochain but est de démontrer que sgn est en fait un homomorphisme. Pour cela on a besoin premièrement d'un lemme :

**Lemme 3.4.10.** *Pour des entiers $1 \le r < s \le n$ et pour $\sigma \in S_n$ considérons $\tau = \sigma \cdot (r\ s)$. Dans ce cas on a l'égalité $\operatorname{sgn}\tau = -\operatorname{sgn}\sigma$.*

*Preuve.* La définition de $\tau$ nous donne

$$\sigma(r) = \tau(s) \qquad \text{et} \qquad \sigma(s) = \tau(r) \tag{4.10.a}$$

Passons en revue les paires d'entiers pour trouver celles qui sont en inversion pour $\tau$ :

(1) *Si $i, j \notin \{r, s\}$, alors $i$ et $j$ sont en inversion pour $\tau$ si et seulement si ils sont en inversion pour $\sigma$:* la raison est simplement que dans ce cas $\sigma(i) = \tau(i)$ et $\sigma(j) = \tau(j)$.

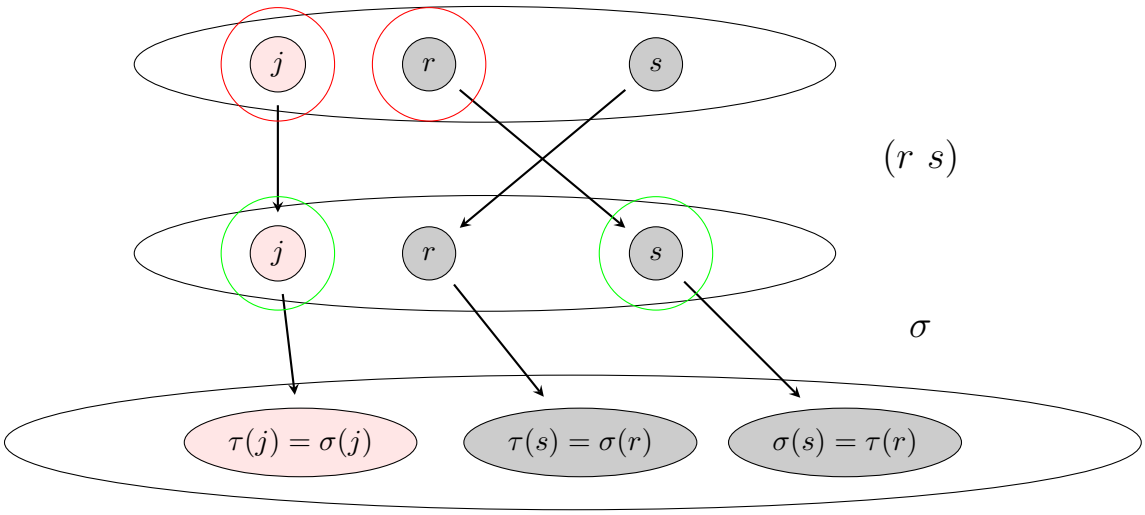
(2) *Si $j < r$ ou $j > s$, alors $r$ et $j$ sont en inversion pour $\tau$ si et seulement si $s$ et $j$ sont en inversion pour $\sigma$. Dans la même façon $s$ et $j$ sont en inversion pour $\tau$ si et seulement si $r$ et $j$ sont en inversion pour $\sigma$:* par (4.10.a) et parce que $j \neq r, s$, on a

$$\text{signe}\big(\tau(r) - \tau(j)\big) = \text{signe}\big(\sigma(s) - \sigma(j)\big) \quad \text{et} \quad \text{signe}\big(\tau(s) - \tau(j)\big) = \text{signe}\big(\sigma(r) - \sigma(j)\big), \tag{4.10.b}$$

et par le choix de $j$ on a

$$j < r \iff j < s \qquad \text{et} \qquad s < j \iff r < j$$

Ce cas est représenté par le dessin ci-dessous. Remarquez que les $\tau$-images des éléments entourés en rouge sont les mêmes que les $\sigma$-images des éléments entourés en vert, et de plus l'ordre de la paire rouge ne change pas en appliquant $(r\ s)$ (opération qui nous donne la paire verte).

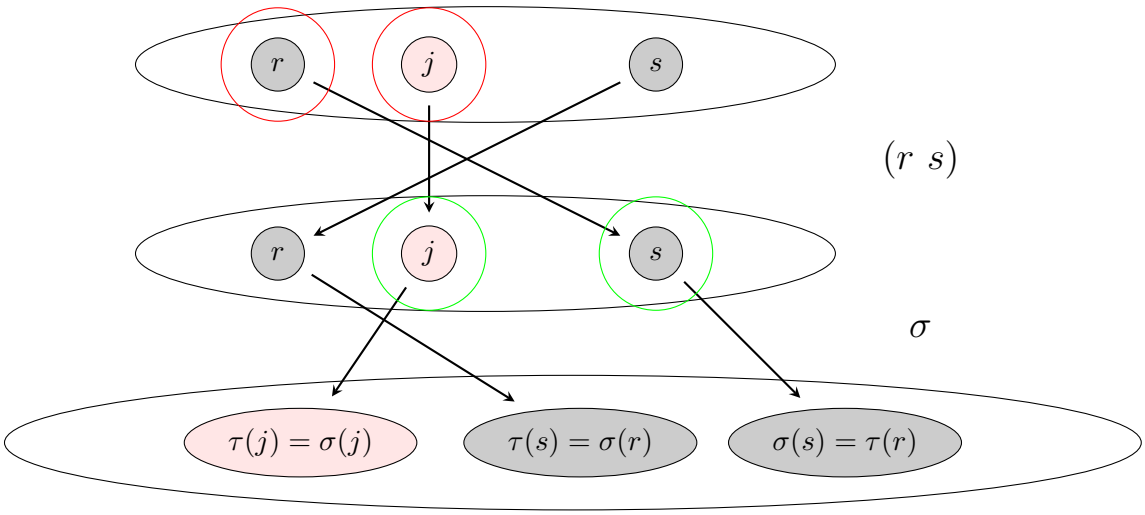



Ce dessin traite le cas $j < r$, et le cas $j > s$ peut être visualisé de la même façon.

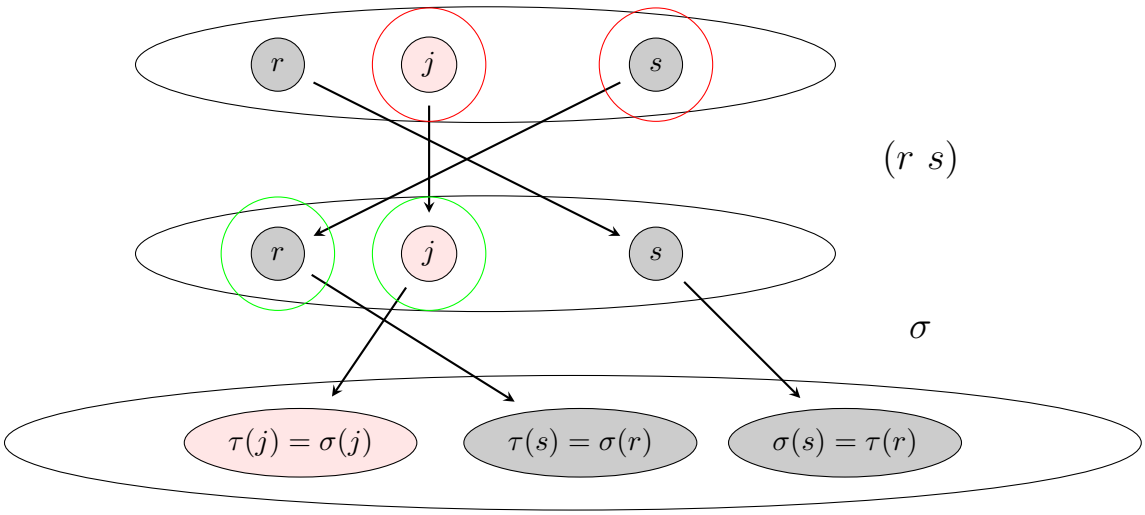
(3) *Si $r < j < s$ est un entier, alors $r$ et $j$ sont en inversion pour $\tau$ si et seulement si $s$ et $j$ ne sont pas en inversion pour $\sigma$. De la même façon $s$ et $j$ sont en inversion pour $\tau$ si et seulement si $r$ et $j$ ne sont pas en inversion pour $\sigma$.* L'équation (4.10.b) nous le donne immédiatement.

Ce cas est aussi représenté dans le dessin suivant. Ce qui change en comparaison du cas

précédent est que l'ordre de la paire rouge change en appliquant $(r\ s)$:




et l'ordre de l'autre paire considérée ici change aussi en appliquant $(r\ s)$:




(4) *Les entiers $r$ et $s$ sont en inversion pour $\tau$ si et seulement si $r$ et $s$ ne sont pas en inversion pour $\sigma$:* c'est impliqué directement par (4.10.a).

On a fait la liste de tous les cas de paires des deux entiers différents entre 1 et $n$. Ainsi on peut compter la différence entre le nombre des paires qui sont en inversion pour $\tau$ et le nombre des paires qui sont en inversion pour $\sigma$.

On obtient que les cas (1) et (2) ne contribuent pas à cette différence. Le cas (3) nous donne un changement de 2, 0 ou $-2$ pour chaque $j$. De toute façon, on obtient une contribution pair pour ce cas. Finalement, le cas (4) nous donne un changement $\pm 1$. On obtient donc que la différence est impair, autrement dit on a $\operatorname{sgn}\tau = -\operatorname{sgn}\sigma$.

Si l'explication finale n'était pas claire, on peut la formaliser dans le forme d'un calcul ou on divise le produit de la Définition 3.4.8 à multiple produits correspondant aux points (1),

(2), (3) et (4):

$$\operatorname{sgn}(\sigma) \underset{\boxed{\text{Définition 3.4.8}}}{\uparrow} \prod_{1\le i<j\le n} \operatorname{signe}\big(\sigma(j)-\sigma(i)\big)$$

$$= \prod_{\substack{1\le i<j\le n,\\ i,j\notin\{r,s\}}} \operatorname{signe}\big(\sigma(j)-\sigma(i)\big) \cdot \prod_{1\le j<r} \operatorname{signe}\big(\sigma(r)-\sigma(j)\big) \operatorname{signe}\big(\sigma(s)-\sigma(j)\big)$$

$$\big(\sigma(j)-\sigma(i)\big) \uparrow \boxed{=\tau(j)-\tau(i)} \qquad \big(\sigma(r)-\sigma(j)\big) \uparrow \boxed{=\tau(s)-\tau(j)} \qquad \big(\sigma(s)-\sigma(j)\big) \uparrow \boxed{=\tau(r)-\tau(j)}$$

$$\cdot \prod_{s<j\le n} \operatorname{signe}\big(\sigma(j)-\sigma(r)\big) \operatorname{signe}\big(\sigma(j)-\sigma(s)\big)$$

$$\big(\sigma(j)-\sigma(r)\big) \uparrow \boxed{=\tau(j)-\tau(s)} \qquad \big(\sigma(j)-\sigma(s)\big) \uparrow \boxed{=\tau(j)-\tau(r)}$$

$$\cdot \prod_{r<j<s} \operatorname{signe}\big(\sigma(j)-\sigma(r)\big) \operatorname{signe}\big(\sigma(s)-\sigma(j)\big)$$

$$\big(\sigma(j)-\sigma(r)\big) \uparrow \boxed{=-\big(\tau(s)-\tau(j)\big)} \qquad \big(\sigma(s)-\sigma(j)\big) \uparrow \boxed{=-\big(\tau(j)-\tau(r)\big)}$$

$$\cdot \operatorname{signe}\big(\sigma(s)-\sigma(r)\big)$$

$$\big(\sigma(s)-\sigma(r)\big) \uparrow \boxed{=-\big(\tau(r)-\tau(s)\big)}$$

$$= - \prod_{1\le i<j\le n} \operatorname{signe}\big(\tau(j)-\tau(i)\big) = -\operatorname{sgn}(\tau)$$

□

**Corollaire 3.4.11.** *Si $\sigma \in S_n$ est un produit de $r$ transpositions, alors* $\operatorname{sgn}(\sigma) = (-1)^r$.
*En particulier, la parité de $r$ est déterminé uniquement par $\sigma$.*

*Preuve.* Pour obtenir la première proposition du corollaire on applique Lemme 3.4.10 par induction sur $r$. Pour la deuxième proposition on remarque que sgn est défini d'une manière indépendente de la représentation de $\sigma$ sous forme de produit de transpositions. Ainsi la seconde assertion découle de la première. □

**Proposition 3.4.12.** $\operatorname{sgn} : S_n \to \{1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$ *est un homomorphisme.*

*Preuve.* Prenons $\sigma, \tau \in S_n$, et écrivons-les sous forme de produits de $r$ et de $s$ transpositions, respectivement. Ainsi on peut écrire $\sigma\tau$ comme un produit de $r+s$ transpositions. Le calcul suivant montre que sgn et un homomorphisme

$$\operatorname{sgn}(\sigma\tau) \underset{\boxed{\text{Corollaire 3.4.11}}}{\uparrow} (-1)^{r+s} = (-1)^r(-1)^s \underset{\boxed{\text{Corollaire 3.4.11}}}{\uparrow} \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

□

**Définition 3.4.13.** On définit le *groupe alterné* $A_n := \ker\big(\operatorname{sgn} : S_n \to \mathbb{Z}/2\mathbb{Z}\big)$.

La fin du 7. cours, en 27.10.2020.

**Exemple 3.4.14.** On trouve les éléments de $A_4$ dans cet exemple. Considérons $\mathrm{id} \neq \sigma \in S_4$. Alors $\sigma$ peut s'écrire comme un produit de cycles disjoints de longueur au moins 2. Il y a 4 cas, et puisque la démonstration de Proposition 3.4.6 donne que la parité d'un cycle est égale à sa longueur moins 1, on obtient :

(1) un cycle de longueur 2 $\rightsquigarrow$ sgn $= -1$,

(2) un cycle de longueur 3 $\rightsquigarrow$ sgn $= 1$,

(3) un cycle de longueur 4 $\rightsquigarrow$ sgn $= -1$,

(4) deux cycles de longueur 2 $\rightsquigarrow$ sgn $= 1$,

On obtient que les éléments de $A_4$, écrit comme des produits de cycles disjoints, sont :

$$\mathrm{id}, \underbrace{(1\ 2\ 3), (1\ 3\ 2)}_{\text{3-cycles fixant 4}}, \underbrace{(1\ 2\ 4), (1\ 4\ 2)}_{\text{3-cycles fixant 3}}, \underbrace{(1\ 3\ 4), (1\ 4\ 3)}_{\text{3-cycles fixant 2}}, \underbrace{(2\ 3\ 4), (2\ 4\ 3)}_{\text{3-cycles fixant 1}}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

En particulier $|A_4| = 12$. On voit aussi que $A_4$ n'est pas abélien:

$$(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4) \neq (1\ 4)(2\ 3) = (1\ 2\ 4)(1\ 2\ 3).$$

On peut mettre à jour notre tableau des petits groupes, en utilisant les remarques suivantes :

- On garde à l'esprit la Proposition 3.3.9 en remplissant le tableau. Par exemple on ne met pas $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ dans le tableau parce que ce groupe est isomorphe à $\mathbb{Z}/10\mathbb{Z}$.
- On utilise également les identités $G \times H \cong H \times G$ et $(G \times H) \times F \cong G \times (H \times F)$, qui ont été démontrées en exercice. Par exemple on ne met pas $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ séparément, mais on met seulement $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ (qui représente les ceux deux produits, à isomorphisme près).
- Plus généralement, $(\mathbb{Z}/n\mathbb{Z})^{\oplus r}$ signifie $\underbrace{\mathbb{Z}/n\mathbb{Z} \times \ldots \times \mathbb{Z}/n\mathbb{Z}}_{r\text{-fois}}$.

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>$(\mathbb{Z}/5\mathbb{Z})^\times$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$<br>$(\mathbb{Z}/7\mathbb{Z})^\times$<br>$(\mathbb{Z}/9\mathbb{Z})^\times$<br>$(\mathbb{Z}/14\mathbb{Z})^\times$ | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Z}/8\mathbb{Z}$<br>$(\mathbb{Z}/16\mathbb{Z})^\times$<br>$(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$<br>$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^\times$ |

| 9 | 10 | 11 | 12 | 13 | 14 | ... |
|---|---|---|---|---|---|---|
| $\mathbb{Z}/9\mathbb{Z}$ | $\mathbb{Z}/10\mathbb{Z}$ | $\mathbb{Z}/11\mathbb{Z}$ | $\mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Z}/13\mathbb{Z}$ | $\mathbb{Z}/14\mathbb{Z}$ | ... |
| $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $(\mathbb{Z}/11\mathbb{Z})^\times$ | | $A_4$ | | | |
| | $(\mathbb{Z}/22\mathbb{Z})^\times$ | | $\mathbb{Z}/2\mathbb{Z} \times S_3$ | | | |
| | | | $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ | | | |
| | | | $(\mathbb{Z}/13\mathbb{Z})^\times$ | | | |
| | | | $(\mathbb{Z}/26\mathbb{Z})^\times$ | | | |
| | | | $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z})^\times$ | | | |
| | | | $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/9\mathbb{Z})^\times$ | | | |
| | | | $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/14\mathbb{Z})^\times$ | | | |
| | | | $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^\times$ | | | |

couleur bleu: groupes non-abéliens

## 3.5 Théorème de Lagrange et théorème d'homomorphisme

Le premier but de cette section est la démonstration du Théorème de Lagrange (Théorème 3.5.6), qui est le premier "grand" théorème de la théorie des groupes.

**Définition 3.5.1.** Soit $H \leq G$ un sous-groupe. Une *classe à gauche (resp. à droite) de $H$ dans $G$* est un sous-ensemble de forme

$$gH := \{\, gh \mid h \in H \,\} \subseteq G \qquad \left( \text{resp. } Hg := \{\, hg \mid h \in H \,\} \subseteq G \right)$$

où $g$ est un élément quelconque de $G$.

**Exemple 3.5.2.** On calcule les classes à gauche de $H := \langle (1\ 2) \rangle = \{\ \mathrm{id},\ (1\ 2)\ \} \leq S_3 = G$. On a déjà rencontré ce sous-groupe dans le point (2) de l'Exemple 3.3.6. On obtient juste trois classes à gauche, chacune étant déterminée par deux choix de $g \in G$:

- Si $g = \mathrm{id}$ ou $(1\ 2)$, alors $gH = \{\ \mathrm{id},\ (1\ 2)\ \}$.
- Si $g = (1\ 3)$ ou $(1\ 2\ 3)$, alors $gH = \{\ (1\ 3),\ (1\ 2\ 3)\ \}$.
- Si $g = (2\ 3)$ ou $(1\ 3\ 2)$, alors $gH = \{\ (2\ 3),\ (1\ 3\ 2)\ \}$.

Dans l'Exemple 3.5.2, les classes à gauches ont toutes le même cardinal. Ce n'est pas une coïncidence :

**Lemme 3.5.3.** *Si $H \leq G$ est un sous-groupe et $g \in G$, alors $|gH| = |H|$.*

*Preuve.* Considérons les applications entre ensembles suivants :

$$\begin{array}{rccc} \alpha & : & H & \longrightarrow & gH \\ & & \cup & & \cup \\ & & h & \longmapsto & gh \end{array} \qquad \begin{array}{rccc} \beta & : & gH & \longrightarrow & H \\ & & \cup & & \cup \\ & & h & \longmapsto & g^{-1}h \end{array}$$

où la définition de $\beta$ fait sens, car si $gh \in gH$, alors $g^{-1}(gh) = h \in H$. On vérifie aisément que $\alpha \circ \beta = \mathrm{id}_H = \beta \circ \alpha$, donc $\alpha$ est une bijection et le résultat s'ensuit. □

Après l'Exemple 3.5.2 et le Lemme 3.5.3, on soupçonne que les classes à gauche d'un sous-groupe sont les classes d'équivalence d'une relation d'équivalence. C'est démontré dans la proposition suivante :

**Proposition 3.5.4.** *Soit $H \leq G$ un sous-groupe, et considérons le sous-ensemble*

$$R_H := \{\ (g,f) \in G \times G \mid g^{-1}f \in H\ \} \subseteq G \times G.$$

*Dans ce cas :*

*(1) $R_H$ est un relation d'équivalence,*

*(2) les classes d'équivalences de $R_H$ sont exactement les classes à gauche de $H$.*

*La proposition reste vrai si on remplace "gauche" par "droite" et $g^{-1}f$ par $fg^{-1}$.*

*Preuve.* La démonstration de la version avec les classes à droite est exactement la même que la version avec les classes à gauche, il suffit d'inverser l'ordre de toutes les multiplications. Ainsi on démontre seulement la version avec les classes à gauche.

(1) Il faut vérifier les trois condition dans la définition des relations d'équivalences (Définition 1.2.12):

- Reflexivité: pour $g \in G$ on a $g^{-1}g = e_G \in H$.
  ($e_G \in H$ : Proposition 3.3.2)
- Symétrie: pour $g, f \in G$, si $g^{-1}f \in H$, alors $f^{-1}g = \left(g^{-1}f\right)^{-1} \in H$
  ($f^{-1}g = \left(g^{-1}f\right)^{-1}$ : Proposition 3.1.6; $\left(g^{-1}f\right)^{-1} \in H$ : $g^{-1}f \in H$ et Proposition 3.1.6)
- Transitivité: pour $g, f, h \in G$, si $g^{-1}f$ et $f^{-1}h \in H$, alors $g^{-1}h = g^{-1}ff^{-1}h \in H$
  ($g^{-1}h \in H$ : $g^{-1}f,\ f^{-1}h \in H$ et Proposition 3.1.6)

(2) Choisissons un $g \in G$. La classe d'équivalence de $g$ est par définition (voir la Définition 1.2.15) :

$$(R_H)_g = \{\ h \in G \mid (g,h) \in H\ \} = \{\ h \in G \mid g^{-1}h \in H\ \} = \{\ h \in G \mid \exists x \in H :\ h = gx\ \} = gH$$

($\{\ h \in G \mid g^{-1}h \in H\ \} = \{\ h \in G \mid \exists x \in H :\ h = gx\ \}$ : $x = g^{-1}h \iff gx = h$)

□

La remarque suivante est le dernier élément nécessaire pour aboutir au Théorème de Lagrange.

*Remarque* 3.5.5. Considérons une relation d'équivalence $R$ sur un ensemble $A$, et soient $R_a$ et $R_b$ deux classes d'équivalences qui contiennent le même élément $c \in A$. Par la définition d'une classe d'équivalence (Définition 1.2.15) cela veut dire que $(b,c) \in R$ et $(a,c) \in R$, ce qui implique en utilisant la Remarque 1.2.16 que $R_a = R_c = R_b$.

En somme on a démontré que les classes d'équivalences forme une *partition* de $A$, ce qui signifie par définition que chaque élément de $A$ est contenu dans exactement une classe d'équivalence. En particulier, si $A$ est fini, on a

$$|A| = \sum_{\substack{X \subseteq A \text{ est une} \\ \text{classe d'équivalence}}} |X|$$

**Théorème 3.5.6.** THÉORÈME DE LAGRANGE. *Si $H \leq G$ est un sous-groupe d'un groupe fini $G$, alors $|H|$ divise $|G|$.*

*Plus précisément, $\frac{|G|}{|H|}$ est égal au nombre de classes à gauche de $H$.*

*Preuve.* Soient $H_1, \dots, H_r$ les classes à gauche de $H$ distinctes deux-à-deux. En utilisant le Lemme 3.5.3 on obtient que $|H_i| = |H|$ pour chaque entier $1 \leq i \leq r$. En utilisant la Proposition 3.5.4 et la Remarque 3.5.5 on obtient :

$$|G| = \sum_i |H_i| = r|H|$$

ce qui conclut. □

**Définition 3.5.7.** Le nombre $\frac{|G|}{|H|}$ du Théorème 3.5.6 est appelé *l'indice de $H$ dans $G$* et est dénoté par $[G : H]$.

**Lemme 3.5.8.** *Si $g \in G$ est un élément d'un groupe, alors $|\langle g \rangle| = o(g)$.*

*Preuve.* Premièrement, prenons des entiers $0 \leq i < j < o(g)$. On a :

$$j - i < o(g) \implies g^{j-i} \neq e \implies g^j = g^i g^{j-i} \neq g^i \tag{5.8.a}$$

Dans le cas $o(g) = \infty$, (5.8.a) implique déjà que $|\langle g \rangle| = \infty$. Par conséquent on peut supposer que $o(g) < \infty$. Dans ce cas :

$$|\langle g \rangle| \underset{\uparrow}{=} \{\ g^n \mid n \in \mathbb{Z}\ \} \underset{\uparrow}{=} \{\ g^n \mid n \in \mathbb{Z},\ 0 \leq n < o(g)\ \}$$

point (2) de l'Exemple 3.3.6

si $n = so(g) + r$ est une division avec reste, alors $g^n = \left(g^{o(g)}\right)^s g^r = g^r$

En utilisant (5.8.a) on voit que $e = g^0, \dots, g^{n-1}$ sont tous différents deux à deux, alors on obtient que $|\langle g \rangle| = o(g)$ dans le cas $o(g) < \infty$. □

**Corollaire 3.5.9.** *Si $g \in G$ est un élément d'un groupe fini, alors $o(g) \big| |G|$.*

*Preuve.* On applique le Théorème 3.5.6 à $H = \langle g \rangle$ et on utilise le Lemme 3.5.8. □

**Définition 3.5.10.** Un groupe $G$ est *cyclique* s'il existe un élément $g \in G$ tel que $\langle g \rangle = G$.

**Exemple 3.5.11.** On donne les exemples des groupes cycliques:

(1) $G = \mathbb{Z}$ est cyclique parce que $\mathbb{Z} = \langle 1 \rangle$, et

(2) $G = \mathbb{Z}/n\mathbb{Z}$ est cyclique parce que $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$,

**Corollaire 3.5.12.** *Si $G$ est un groupe d'ordre premier, alors $G$ est cyclique.*

*Preuve.* Choisissons $g \in G \setminus \{e\}$. Parce que $g \neq e$ on a $o(g) > 1$. D'un autre coté $o(g) \big| |G|$ par le Corollaire 3.5.9. Parce que $|G|$ est premier on obtient que $o(g) = |G|$. En utilisant le Lemme 3.5.8 on obtient que $\langle g \rangle = G$. □

La relation d'équivalence "modulo m" utilisée dans la construction de $\mathbb{Z}/m\mathbb{Z}$ (dans l'Exemple 1.2.18) est souvent notée par ? $\equiv$? $(m)$. Cela veut dire que $a \equiv b\ (m)$ est équivalent à dire $m|a - b$. En utilisant cette notation :

**Théorème 3.5.13.** PETIT THÉORÈME DE FERMAT. *Si $a$ est un entier premier avec un entier positif $m > 0$, alors*

$$a^{\phi(m)} \equiv 1\ (m)$$

*Preuve.* C'est une conséquence directe du Corollaire 3.5.9 et de la définition de $\phi(m)$ (voir la Définition 3.1.17). □

Après avoir récolté les fruits de notre travail sous la forme du Théorème 3.5.6, du Corollaire 3.5.9 et du Théorème 3.5.13, on essaie de mettre une structure de groupe sur $G/R$ où $R$ est une relation d'équivalence obtenue à partir d'un sous-groupe $H$, comme dans la Proposition 3.5.4. Voyons d'abord si une condition spécifique sur le sous-groupe $H$ est nécessaire. Supposons que $G/R$ est un groupe avec les opérations définies dans la Remarque 3.1.12. Notons que la structure du groupe sur $G/R$ est définie de telle manière que l'application quotient

$$\begin{array}{ccc} G & \longrightarrow & G/R \\ \cup & & \cup \\ g & \longmapsto & R_g \end{array}$$

est un homomorphisme. Le noyau de cet homomorphisme est exactement $R_e = H$. Ainsi une condition nécessaire sur $H$ pour que $G/R$ soit un groupe, est que $H$ soit le noyau d'un homomorphisme. Comme on va le voir, cela implique que $H$ possède une propriété particulière.

**Définition 3.5.14.** Un sous-groupe $H \subseteq G$ est *normal*, si pour chaque $g \in G$ et $h \in H$ on a $g^{-1}hg \in H$. On utilise la notation $H \trianglelefteq G$ pour les sous-groupes normaux.

Un groupe $G$ est *simple* si tous les sous-groupes non-triviaux de $G$ ne sont pas normaux.

**Notation 3.5.15.** L'élément $g^{-1}hg$ dans la Définition 3.5.14 est appelé *le conjugué* de $h$ par $g$.

*Remarque* 3.5.16. Par définition un sous-groupe $H \leq G$ est normal si et seulement si les classes à gauche et à droite sont les mêmes, ce qui veut dire que pour chaque $g \in G$ on a $gH = Hg$.

*Remarque* 3.5.17. Si $G$ est abélien, alors il découle immédiatement de la définition que tous les sous-groupes $H \leq G$ sont normaux.

**Exemple 3.5.18.** Les sous-groupe $H = \langle (1\ 2) \rangle$ n'est pas normal. En fait si on prend $g = (1\ 3)$ et $h = (1\ 2)$, alors

$$g^{-1}hg = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H.$$

**Proposition 3.5.19.** *Si $\phi : G \to H$ est un homomorphisme de groupes, alors $\ker \phi \leq G$ est un sous-groupe normal.*

*Preuve.* Par la Proposition 3.3.5, on sait que $\ker \phi$ est un sous-groupe. Fixons $g \in G$ et $h \in \ker \phi$. On démontre que $g^{-1}hg \in \ker \phi$:

$$\begin{array}{ccccc} \phi\left(g^{-1}hg\right) & = & \phi\left(g^{-1}\right)\phi(h)\phi(g) & = & \phi\left(g^{-1}\right)\phi(g) = e_H \\ \uparrow & & \uparrow & & \uparrow \\ \boxed{\phi \text{ est un homomorphisme}} & & \boxed{h \in \ker \phi} & & \boxed{\text{Lemme 3.2.2}} \end{array}$$

et $\ker \phi$ est bien un sous-groupe normal. □

**Exemple 3.5.20.** En utilisant la Proposition 3.4.12, la Proposition 3.5.19 et la définition $A_n = \ker\left(\operatorname{sgn}\colon S_2 \to \mathbb{Z}/2\mathbb{Z}\right)$, on obtient que $A_n$ est un sous-groupe normal de $S_n$.

En reprenant la discussion précédente sur le quotient $G/R$ obtenu à partir d'un sous-groupe $H \leq G$, on voit que $G/R$ est un groupe seulement si $H \leq G$ est normal. Le théorème suivant dit que la normalité de $H \leq G$ n'est pas seulement une condition nécessaire, mais aussi une condition suffisante.

**Théorème 3.5.21.** *Soit $H \trianglelefteq G$ un sous-groupe normal, et soit $R_H$ la relation d'équivalence définie à partir de $H$ comme dans la Proposition 3.5.4. Dans ce cas $G/R_H$ est un groupe en utilisant les opérations définies dans la Remarque 3.1.12, et l'application suivante en un homomorphisme*

$$\begin{array}{rccc} \xi_H & : & G & \longrightarrow & G/R_H \\ & & \cup & & \cup \\ & & g & \longmapsto & (R_H)_g = gH \end{array}$$

La fin du 8. cours, en 03.11.2020.

*Preuve.* On note premièrement que par la Remarque 3.5.16 on a $gH = Hg$ pour chaque $g \in G$. On a déjà mentionné que la structure de groupe donnée dans la Remarque 3.1.12 est définie de telle manière que $\xi_H$ est un homomorphisme dès le moment où $G/R_H$ est un groupe. Par conséquent il suffit de montrer que $G/R_H$ est un groupe. Par la Proposition 3.1.13, il suffit de vérifier que la multiplication et l'inverse sont bien définis.

- La multiplication est bien définie : pour $g, g', h, h' \in G$ tels que $g^{-1}g' \in H$ et $h^{-1}h' \in H$ on a
$$(gh)^{-1}(g'h') = h^{-1}g^{-1}g'h'\text{`} = h^{-1}h'\underbrace{(h')^{-1}g^{-1}g'h'}_{\in H, \text{ parce que } g^{-1}g' \in H \text{ et } H \subseteq G \text{ est un sous-groupe normal}} \in H$$
$h^{-1}h' \in H$
- L'inverse est bien défini : pour $g, g' \in G$ tels que $g^{-1}g' \in H$
$$(g^{-1})^{-1}(g')^{-1} = g(g')^{-1} = \underbrace{g(g')^{-1}gg^{(-1)}}_{\in H, \text{ parce que } (g')^{-1}g = (g^{-1}g')^{-1} \in H \text{ et } H \subseteq G \text{ est un sous-groupe normal}}$$

□

**Définition 3.5.22.** Pour $H \trianglelefteq G$ on appelle le groupe $G/R_H$ de Théorème 3.5.21 *le quotient* de $G$ par $H$ et on le dénote par $G/H$. On appelle l'homomorphisme $\xi_H : G \to G/H$ l'homomorphisme quotient.

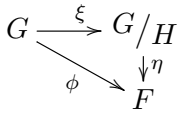
**Exemple 3.5.23.** (1) Par la Remarque 3.5.17, le sous-groupe $n\mathbb{Z} \leq \mathbb{Z}$ est normal, et le quotient $\mathbb{Z}/n\mathbb{Z}$ est exactement le $\mathbb{Z}/n\mathbb{Z}$ qu'on a déjà introduit.

(2) Par le Théorème 3.5.6 on a $\left|G/H\right| = \frac{|G|}{|H|}$. Par exemple, si on prend
$$H = \mathbb{Z}/2\mathbb{Z} \cong 2 \cdot \mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} = G,$$
alors $\left|G/H\right| = 2$, et parce que les groupes d'ordre 2 sont unique modulo isomorphisme, on déduit que $G/H \cong \mathbb{Z}/2\mathbb{Z}$.

(3) De la même façon, si on prend
$$H = \langle(1,0)\rangle \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = G,$$
on obtient $G/H \cong \mathbb{Z}/2\mathbb{Z}$. On sait déjà que $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, alors on voit que même si pour des sous-groupes normaux $H \trianglelefteq G$ et $H' \trianglelefteq G'$ on a $H \cong H'$ et $G/H \cong G'/H'$, il peut arriver que $G \ncong G'$.

**Théorème 3.5.24.** *Soit $H \trianglelefteq G$ un sous-groupe normal, $\xi : G \to G/H$ l'homomorphisme quotient et soit $\phi : G \to F$ un homomorphisme tel que $H \subseteq \ker\phi$.*

*(1) Il existe un unique homomorphisme $\eta : H \to F$ tel que le diagramme suivant commute (ce qui signifie $\eta \circ \xi = \phi$) :*



*(2)* Premier théorème d'isomorphisme. *Si $H = \ker\phi$, alors $\eta$ est une injection. En particulier dans ce cas $\eta$ induit un isomorphisme ${}^{G}\!/_{H} \xrightarrow{\cong} \operatorname{im}\phi$.*

*Preuve.* Premièrement on rappelle que $\xi$ est défini par $\xi(g) = gH$. Deuxièmement, notons que la condition $\eta \circ \xi = \phi$ nous force à écrire

$$\eta(gH) = \eta(\xi(g)) = \phi(g). \tag{5.24.b}$$

Autrement dit il y a juste un choix pour définir $\eta$, même comme une application d'ensembles. Pour démontrer le point (1) il faut vérifier que le $\eta$ définit en (5.24.b) est bien définit est que il est un homomorphisme. Pour montrer que $\eta$ est bien définit sur $G/H$ il suffit de démontrer que $\eta(gH) = \eta(g'H)$ quand $g^{-1}g' \in H$, ou autrement dit que $\big(\eta(gH)\big)^{-1}\eta(g'H) = e_F$. C'est montré dans le calcul suivant:

$$\big(\eta(gH)\big)^{-1}\eta(g'H) \underset{\uparrow}{=} \big(\phi(g)\big)^{-1}\phi(g') \underset{\uparrow}{=} \phi\big(g^{-1}\big)\phi(g') \underset{\uparrow}{=} \phi\big(g^{-1}g'\big) \underset{\uparrow}{=} e_H$$

(5.24.b) — Lemme 3.2.2 — $\phi$ est un homomorphisme — $g^{-1}g' \in H \subseteq \ker\phi$

Deuxièmement on vérifie que $\eta$ est un homomorphisme :

$$\eta\left(gH \cdot g'H\right) \underset{\uparrow}{=} \eta(gg'H) \underset{\uparrow}{=} \phi(gg') \underset{\uparrow}{=} \phi(g)\phi(g') \underset{\uparrow}{=} \eta(gH)\eta(g'H).$$

$gH \cdot g'H$ est la class à gauche qui contient $gg'$ par définition de quotient d'un groupe en Remarque 3.1.12 — (5.24.b) — $\phi$ est un homomorphisme — (5.24.b)

Ce calcul conclut le point (1).

Il nous reste à démontrer le point (2), donc on suppose à partir de maintenant que $H = \ker\xi$. Pour démontrer que $\eta$ est injective, par Lemme 3.3.7 il suffit de démontrer que $\ker\eta = \{e\}$ :

$$gH \in \ker\eta \iff \eta(gH) = e \underset{\uparrow}{\iff} \phi(g) = e \iff g \in \ker\phi \underset{\uparrow}{\iff} g \in H \iff \underbrace{gH = e}_{\uparrow}$$

(5.24.b) — $H = \ker\phi$ — comme élément de ${}^{G}\!/_{H}$

On a démontré que $\eta$ est injective. En conséquent $\eta$ induit un isomorphisme ${}^{G}\!/_{H} \xrightarrow{\cong} \operatorname{im}\eta$. Pour conclure la preuve on montre que $\operatorname{im}\eta = \operatorname{im}\phi$ :

$$\operatorname{im}\phi \underset{\uparrow}{=} \operatorname{im}(\eta\circ\xi) = \{\ \eta(\xi(x)) \mid x \in G\ \} \underset{\uparrow}{=} \left\{\ \eta(y) \;\middle|\; y \in {}^{G}\!/_{H}\ \right\} = \operatorname{im}\eta.$$

$\phi = \eta \circ \xi$ — $\xi$ est surjective

□

**Corollaire 3.5.25.** *Si $\phi : G \to H$ est un homomorphisme surjectif entre groupes finis, alors $|G| = |\ker\phi| \cdot |H|$.*

*Preuve.* Par le point (2) du Théorème 3.5.24 et par la surjectivité de $\phi$ on a ${}^{G}\!/_{\ker\phi} \cong \operatorname{im}\phi = H$. Alors le Théorème 3.5.6 conclut notre argument. □

**Exemple 3.5.26.** En appliquant le Corollaire 3.5.25 à sgn : $S_n \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ On obtient que $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

**Corollaire 3.5.27.** *Soit $n$ et $m$ deux nombres entiers positifs premiers entre eux. Si $\phi : G \to H$ est un homomorphisme tel que $|G| = n$ et $|H| = m$, alors $\phi \equiv e$ (ce qui veut dire que $\phi$ est l'application constante de valeur $e$).*

*Preuve.* En utilisant le Théorème 3.5.6 on obtient que $|\ker\phi|\big|n$ et $|\operatorname{im}\phi|\big|m$. En particulier $\frac{|G|}{|\ker\phi|}$ divise aussi $n$. C'est en contradiction avec Corollaire 3.5.25, à moins que $\frac{|G|}{|\ker\phi|} = 1$ et que $|\operatorname{im}\phi| = 1$. Ces égalités impliquent que $\ker\phi = G$ et que $\operatorname{im}\phi = \{e_H\}$, ce qui implique que $\phi \equiv e$. □

**Exemple 3.5.28.** Un exemple particulier du Corollaire 3.5.27 est qu'il n'existe que l'homomorphisme constant entre $\mathbb{Z}/16\mathbb{Z}$ et $\mathbb{Z}/25\mathbb{Z}$.

**Corollaire 3.5.29.** *Si $g \in G$ est un élément d'ordre fini, alors $\langle g\rangle \cong \mathbb{Z}/o(g)\mathbb{Z}$.*

*Preuve.* Il suffit d'utiliser le point (2) du Théorème 3.5.24 et le point (2) de l'Exemple 3.2.3. □

**Corollaire 3.5.30.** *Si $G$ est un groupe d'ordre $p$ pour un nombre premier $p > 0$, alors $G \cong \mathbb{Z}/p\mathbb{Z}$.*

*Preuve.* Par Corollaire 3.5.12 on sait que $G$ est cyclique. Corollaire 3.5.29 conclut donc notre argument. □

On peut mettre à jour notre tableau des petits groupes. On fait les modifications suivantes dans le tableau :

(1) Par le Corollaire 3.5.30 on sait que, modulo isomorphisme, il n'existe qu'un groupe d'ordre premier. Cela veut dire qu'on peut mettre une coche aux colonnes d'ordre premier.

(2) On peut aussi démontrer que beaucoup des groupes de forme $(\mathbb{Z}/p\mathbb{Z})^\times$ sont cycliques, où $p$ est un entier premier. À cette fin, en utilisant le Corollaire 3.5.30, il suffit de trouver un élément d'ordre $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right|$ dans ces groupes. Pour les groupes cycliques de tel type on donne au-dessous ces éléments. C'est une bonne idée de vérifier par vous-mêmes que les ordre de ces éléments sont effectivement $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right|$ :

- $[2] \in (\mathbb{Z}/5\mathbb{Z})^\times$
- $[3] \in (\mathbb{Z}/7\mathbb{Z})^\times$
- $[2] \in (\mathbb{Z}/9\mathbb{Z})^\times$
- $[2] \in (\mathbb{Z}/11\mathbb{Z})^\times$
- $[2] \in (\mathbb{Z}/13\mathbb{Z})^\times$

(3) On démontre en série d'exercices que si $n$ est un entier impair, alors $(\mathbb{Z}/2n\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Cela nous permet aussi d'éliminer plusieurs entrées.

(4) On démontre en série d'exercices que $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 ✓ | 6 | 7 ✓ | 8 |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>~~$(\mathbb{Z}/5\mathbb{Z})^\times$~~<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$<br>~~$(\mathbb{Z}/7\mathbb{Z})^\times$~~<br>~~$(\mathbb{Z}/9\mathbb{Z})^\times$~~<br>~~$(\mathbb{Z}/14\mathbb{Z})^\times$~~ | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Z}/8\mathbb{Z}$<br>~~$(\mathbb{Z}/16\mathbb{Z})^\times$~~<br>$(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$<br>~~$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^\times$~~ |

| 9 | 10 | 11 ✓ | 12 | 13 ✓ | 14 | ... |
|---|---|---|---|---|---|---|
| $\mathbb{Z}/9\mathbb{Z}$ | $\mathbb{Z}/10\mathbb{Z}$ | $\mathbb{Z}/11\mathbb{Z}$ | $\mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Z}/13\mathbb{Z}$ | $\mathbb{Z}/14\mathbb{Z}$ | ... |
| $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | ~~$(\mathbb{Z}/11\mathbb{Z})^\times$~~ | | $A_4$ | | | |
| | ~~$(\mathbb{Z}/22\mathbb{Z})^\times$~~ | | $\mathbb{Z}/2\mathbb{Z} \times S_3$ | | | |
| | | | $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ | | | |
| | | | ~~$(\mathbb{Z}/13\mathbb{Z})^\times$~~ | | | |
| | | | ~~$(\mathbb{Z}/26\mathbb{Z})^\times$~~ | | | |
| | | | ~~$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z})^\times$~~ | | | |
| | | | ~~$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/9\mathbb{Z})^\times$~~ | | | |
| | | | ~~$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/14\mathbb{Z})^\times$~~ | | | |
| | | | ~~$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^\times$~~ | | | |

couleur bleu: groupes non-abéliens

## 3.6 GROUPES DIÉDRAUX

Notre tableau des petits groupes est dominé jusqu'ici par des groupes abélien. En fait, le nombre de groupes non-abéliens d'ordre $n$ est typiquement plus grand que le nombre de groupes abéliens du même ordre lorsque, dans la décomposition de $n$ en produit de nombres premiers, apparaissent des premiers à de grandes puissances. Nous ne préciserons pas cette assertion, mais nous construirons dans cette section de nouveaux groupes non-abéliens : les groupes diédraux. Ce sont des cas spéciaux de groupes d'automorphismes de graphes simples non-orientés. Nous avons déjà discuté rapidement des graphes orientés pour visualiser les permutations. Les graphes simples non-orientés forment une autre classe de graphes ; on les définit ci-dessous :

**Définition 3.6.1.** Un *graphe $G$ simple non-orienté* est une paire $G = (V, E)$ où $V$ est un ensemble et

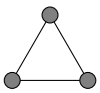
$$E \subseteq \left\{ S \in 2^V \;\middle|\; |S| = 2 \right\} = \left\{ S \subseteq V \;\middle|\; |S| = 2 \right\}$$

On dit que :

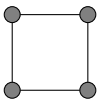
- $V$ est l'ensemble des sommets de $G$.
- $E$ est l'ensemble des arêtes de $G$.
- Pour $e = \{v_1, v_2\} \in E$ on appelle $v_1$ est $v_2$ les *extrémités* de $e$. Le graphe $G$ est appelé non-orienté parce qu'on ne fixe pas d'ordre entre $v_1$ et $v_2$, ou encore que $e$ n'a pas de direction.
- On appelle $G$ simple, parce que, comme on peut le voir dans la définition, les deux extrémités d'une arête sont différentes, et il peut exister au plus une arête entre deux sommets.

**Exemple 3.6.2.** On visualise les graphes simples non-orientés d'une façon similaire à ce qu'on a fait pour les graphes orientés. On dessine un point pour chaque sommet, et on dessine une ligne ou une ligne courbée entre les extrémités de chaque arête.

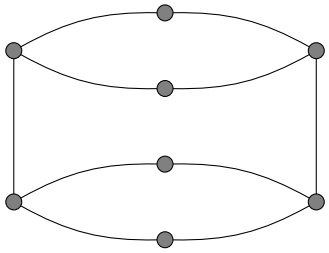
(1) $V = \{1,\ 2,\ 3\}$, $E = \{\ \{1,\ 2\},\ \{2,\ 3\},\ \{1,\ 3\}\ \}$



(2) $V = \{1,\ 2,\ 3,\ 4\}$, $E = \{\ \{1,\ 2\},\ \{2,\ 3\},\ \{3,\ 4\},\ \{4,\ 1\}\ \}$



(3) $V = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\ \}$,
$E = \{\ \underbrace{\{1,\ 8\},\ \{4,\ 5\}}_{\text{lignes verticales sur le dessin}},\ \underbrace{\{1,\ 2\},\ \{1,\ 3\},\ \{2,\ 4\},\ \{3,\ 4\},\ \{5,\ 6\},\ \{5,\ 7\},\ \{6,\ 8\},\ \{7,\ 8\}}_{\text{lignes courbées sur le dessin}}\ \}$



Dans ces représentations graphiques, nous n'avons pas indiqué le nom des sommets, parce que nous ne voulons pas fixer les éléments de $V$. Nous sommes seulement intéressés par le nombre d'éléments de $V$, et par les connections prévues par $E$ entre ces éléments. Cela veut dire qu'on pense au graphe obtenu à partir de $G = (V, E)$ comme étant invariant par réétiquetage de $V$, ou plus précisément invariant par isomorphisme :

**Définition 3.6.3.** Soient $G = (V, E)$ et $G' = (V', E')$ deux graphes.

(1) Un *isomorphisme* $\phi : G \to G'$ est une bijection $\phi : V \to V'$ tel que

$$\forall v \neq w \in V :\ \{v, w\} \in E \iff \{\phi(v), \phi(w)\} \in E' \tag{6.3.a}$$

(2) $G$ et $G'$ sont *isomorphes*, ce que l'on dénote par $G \cong G'$, s'il existe un isomorphisme $\phi : G \to G'$.

(3) Un *automorphisme* de $G$, est un isomorphisme $\phi : G \to G$. On dénote l'ensemble des automorphismes de $G$ par $\mathrm{Aut}(G)$, qui est un groupe avec la composition pour l'opération (si $\phi : G \to H$ et $\xi : H \to F$ sont isomorphismes, alors on peut voir directement que $\xi \circ \phi$ et $\phi^{-1}$ satisfont aussi (6.3.a), et alors $\xi \circ \phi$ et $\phi^{-1}$ sont aussi des automorphismes de $G$).

*Remarque* 3.6.4. On voit que la Définition 3.6.3 est très similaire à la Définition 3.2.1. Ce n'est en fait pas une coïncidence. Pour une structure quelconque en mathématique, on définit d'habitude un isomorphisme comme une application bijective qui préserve la structure, et on définit le fait d'être isomorphes par l'existence d'un isomorphisme, et finalement on définit un automorphisme comme un isomorphisme d'un objet avec lui-même. En général, l'ensemble des automorphisme d'un objet nous donne alors un groupe. Par exemple, si on applique ce procédé à des espaces vectoriels de dimension $n$ sur un corps $k$, on obtient le groupe linéaire $\mathrm{GL}(n, k)$, qui est par définition le groupe des automorphismes linéaires de $k^n$. Vous verrez beaucoup d'autres exemples de groupes d'automorphismes de structures différentes pendant le programme de mathématique à l'EPFL.

**Exemple 3.6.5.** (1) Considérons le graphe $G' = (V', E')$ donné par

$$V' := \mathbb{Z}/4\mathbb{Z} \qquad E' := \left\{\ (x, x + [1]) \;\middle|\; x \in \mathbb{Z}/4\mathbb{Z}\ \right\}$$

L'application $\phi : V \to V'$ suivante nous donne un isomorphisme $\phi : G \to G'$, ou $G = (V, E)$ est le graphe donné dans le point (2) de l'Exemple 3.6.2:

$$\phi(x) = [x] \qquad (x \in \{0, 1, 2, 3\}).$$

(2) Déterminons $\mathrm{Aut}(G')$, où $G'$ est défini dans le point précédent. Réfléchissons premièrement à quels $\alpha \in \mathrm{Aut}(G')$ existent avec $\alpha([0]) = [i]$ pour un élément fixé $[i] \in \mathbb{Z}/4\mathbb{Z}$. Puisque $G'$ est un cycle, cette structure doit être préservée par $\alpha$. On a donc deux possibilité pour $\alpha$:

(i) $\alpha([j]) = [i] + [j]$ pour chaque $j \in \mathbb{Z}/4\mathbb{Z}$ et
(ii) $\alpha([j]) = [i] - [j]$ pour chaque $j \in \mathbb{Z}/4\mathbb{Z}$.

En fait, parce que la structure de cycle est préservée par ces deux applications, elles sont toutes deux des automorphismes. On dénote la première par $\sigma_i$ et on dénote la deuxième par $\tau_i$. On aussi utilise la notation $\sigma := \sigma_1$ et $\tau := \tau_0$. Notons qu'on a

$$\sigma_i = \sigma^i \qquad \tau_i = \sigma^i\tau \qquad \tau\sigma\tau = \sigma^{-1}$$

On vérifier la dernière equation

$$(\tau\sigma\tau)([j]) = \tau\Big(\sigma\big(\tau([j])\big)\Big) = \tau\big(\sigma([-j])\big) = \tau([1-j]) = [j-1] = \sigma^{-1}([j]). \tag{6.5.b}$$

**Définition 3.6.6.** Pour un entier $n \geq 3$ considérons le graphe $G = (V, E)$ donné par

$$V := \mathbb{Z}/n\mathbb{Z} \qquad E := \Big\{ (x, x + [1]) \;\Big|\; x \in \mathbb{Z}/n\mathbb{Z} \Big\}.$$

On définit le groupe diédral $D_{2n}$ comme étant $\mathrm{Aut}(G)$. On définit $\sigma$ et $\tau \in D_{2n}$ comme dans le point (2) de l'Exemple 3.6.5:

- $\sigma([j]) = [1] + [j]$ pour chaque $j \in \mathbb{Z}/n\mathbb{Z} = V$, et
- $\tau([j]) = [-j]$ pour chaque $j \in \mathbb{Z}/n\mathbb{Z} = V$.

*Remarque* 3.6.7. Comme dans le point (2) de l'Exemple 3.6.5 on voit que $D_{2n}$ contient $2n$ éléments, qui sont les suivants:

$$\big\{ \sigma^i, \sigma^i\tau \;\big|\; 0 \leq i \leq n-1 \text{ est un entier } \big\}$$

Toujours comme dans le point (2) de l'Exemple 3.6.5, on aussi l'identité $\tau\sigma\tau = \sigma^{-1}$. La démonstration de cette identité est la même, elle est donnée par le calcul (6.5.b).

*Remarque* 3.6.8. On peut aussi définir $D_{2n}$ comme le groupe d'isométries du plan qui préservent un polygone régulier d'ordre $n$, où isométrie signifie que c'est une bijection du plan qui préserve la distance entre les points. Cette définition est liée à l'étude des formes bilinéaires, qui ne seront introduites que dans le cours d'Algèbre linéaire II. En conséquent, nous ne développerons pas le point de vue des isométries pour $D_{2n}$ dans notre cours, mais il est important de connaître cette description alternative.

*Remarque* 3.6.9. Considérons la Définition 3.6.3. Comme les éléments de $D_{2n} = \mathrm{Aut}(G)$ permute les éléments de $V = \{[1], \ldots, [n]\}$, on obtient un homomorphisme injectif $D_{2n} \subseteq S_n$. Autrement dit $D_{2n}$ est un sous-groupe de $S_n$ naturellement. Pour $n = 3$ on a $2n = 6 = n!$. Par conséquent on a $D_6 \cong S_3$.

En utilisant les informations de cette section, on peut mettre à jour notre tableau des petits groupes.

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 ✓ | 6 | 7 ✓ | 8 |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$<br>~~$D_6$~~ | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Z}/8\mathbb{Z}$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$<br>$(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$<br>$D_8$ |

| 9 | 10 | 11 ✓ | 12 | 13 ✓ | 14 | 15 | ... |
|---|---|---|---|---|---|---|---|
| $\mathbb{Z}/9\mathbb{Z}$<br>$(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/10\mathbb{Z}$<br>$D_{10}$ | $\mathbb{Z}/11\mathbb{Z}$ | $\mathbb{Z}/12\mathbb{Z}$<br>$A_4$<br>$\mathbb{Z}/2\mathbb{Z} \times S_3$<br>$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$<br>$D_{12}$<br>~~$\mathbb{Z}/2\mathbb{Z} \times D_6$~~ | $\mathbb{Z}/13\mathbb{Z}$ | $\mathbb{Z}/14\mathbb{Z}$<br>$D_{14}$ | $\mathbb{Z}/15\mathbb{Z}$ | ... |

couleur bleu: groupes non-abéliens

## 3.7 SOUS-GROUPES ENGENDRÉS, GROUPES LINÉAIRES ET GROUPE DES QUATERNIONS

**Lemme 3.7.1.** *Si $G$ est un groupe, et $H_i \leq G$ sont sous-groupes pour chaque $i \in I$, alors $\bigcap_{i\in I} H_i \subseteq G$ est aussi un sous-groupe de $G$.*

*Preuve.* En utilisant la Proposition 3.3.2, il suffit de vérifier que $H := \bigcap_{i\in I} H_i$ est non-vide, stable pour la multiplication et stable pour l'inverse.

Premièrement, par la Proposition 3.3.2, $e \in H_i$ pour chaque $i \in I$, ce qui implique que $e \in H$ et par conséquent $H \neq \emptyset$.

Pour les deux autres conditions prenons $g, h \in H$. On a que $g, h \in H_i$ pour chaque $i \in H_i$. En appliquant Proposition 3.3.2 pour $H_i$ on obtient que $gh$ et $g^{-1}$ sont contenus dans $H_i$ pour chaque $i \in I$, ce qui implique que $gh, g^{-1} \in H$. □

**Définition 3.7.2.** Si $G$ est un groupe, et $S \subseteq G$ est un sous-ensemble, alors le *sous-groupe* $\langle S\rangle$ *engendré par* $S$ est le sous-groupe $H$ de $G$ qui est minimal pour la propriété d'inclusion $S \subseteq H$ (en d'autres termes, si $H' \leq G$ et $S \subset H'$, alors $H \subseteq H'$).

On note que $\langle S\rangle$ existe puisqu'il est donné par

$$\langle S\rangle = \bigcap_{S\subseteq H\leq G} H$$

qui est un sous-groupe de $G$ par le Lemme 3.7.1 (notez que l'intersection se fait sur un ensemble non-vide, puisque $S \subseteq G \leq G$).

*Remarque* 3.7.3. Pour $S = \{g\}$ pour un élément $g \in G$, on a

$$\underbrace{\langle g\rangle}_{\uparrow} = \underbrace{\langle\{g\}\rangle}_{\uparrow}$$

défini au point (2) de l'Exemple 3.3.6 | défini dans la Définition 3.7.2

En fait, $\langle g\rangle$ est défini comme l'ensemble des élément $g^n$, $n \in \mathbb{Z}$. Ses éléments doivent être contenu dans $\langle\{g\}\rangle$ par la Proposition 3.3.2. Ça donne $\langle g\rangle \subseteq \langle\{g\}\rangle$. Pour l'autre inclusion on

remarque que $\langle g \rangle$ est un sous-groupe parce qu'il est égal à $\operatorname{im} \exp_g$. Il est alors l'un des $H$ dans l'intersection qui définit $\langle \{g\} \rangle$.

**Notation 3.7.4.** Dans la veine de la Remarque 3.7.3, si $S = \{g_1, \dots, g_r\}$ est un sous-ensemble fini d'un groupe $G$, alors on utilise la notation $\langle g_1, \dots, g_r \rangle$ pour $\langle S \rangle$.

De la même façon, si $H_1, \dots, H_r$ sont des sous-groupes de $G$, on dénote $\langle \bigcup_i H_i \rangle$ par $\langle H_1, \dots, H_r \rangle$.

Si il existe un sous-ensemble $S \subseteq G$ tel que $\langle S \rangle = G$, alors on appelle $S$ une (partie) *génératrice* de $G$. Si $G$ possède une génératrice finie, on l'appelle *de type fini*.

*Remarque* 3.7.5. Si $H_i = \langle g_i \rangle$ pour des éléments $g_i$ d'un groupe $G$, alors $\langle H_1, \dots, H_r \rangle = \langle g_1, \dots, g_r \rangle$. En fait, le coté gauche est défini comme le plus petit sous-groupe qui contient tous les $H_i$ et le coté droit est définit comme le plus petit sous-groupe qui contient tous les $g_i$. Ainsi il suffit de démontrer que chaque sous-groupe qui contient tous les $g_i$ contient aussi tous les $H_i$, ce qui est automatique parce que les $H_i$ sont les sous-groupes engendrés par les $g_i$.

Le problème avec la Définition 3.7.2 est qu'elle ne permet pas, en pratique, d'identifier le sous-groupe $\langle S \rangle$. Par exemple, étant donnés deux élément $g, h \in G$, elle ne nous donne pas une manière de faire la liste des éléments de $\langle g, h \rangle$. La proposition suivante résout ce problème :

**Proposition 3.7.6.** *Si $S \subseteq G$ est un sous-ensemble d'un groupe, alors le sous-groupe engendré par $S$ est exactement l'ensemble des produits des éléments de $S$ et de ses inverses:*

$$\langle S \rangle = \left\{ y_1 y_2 \dots y_r \;\middle|\; \forall 1 \leq i \leq r : \; y_i \text{ ou } y_i^{-1} \in S \right\} \tag{7.6.a}$$

*Preuve.* On procède par double-inclusion.
$\boxed{\supseteq:}$ Par la Proposition 3.3.2 les éléments $y_1 y_2 \dots y_r$ de (7.6.a) doivent être contenus dans le sous-groupe engendré par $S$, parce que c'est un sous-groupe de $G$ qui contient $S$.
$\boxed{\subseteq:}$ En utilisant l'inclusion déjà démontrée, il suffit de prouver que l'ensemble de (7.6.a) est un sous-groupe. Grâce à la Proposition 3.3.2, il suffit de démontrer que l'ensemble de (7.6.a) est stable par la multiplication et par l'inverse.

Prenons deux éléments $g = y_1 \dots y_r$ et $h = y_{r+1} \dots y_s$ comme dans l'équation (7.6.a). En particulier $y_i$ ou $y_i^{-1} \in S$ pour chaque $1 \leq i \leq s$. Dans cette situation $gh = y_1 \dots y_s$ et $g^{-1} = y_r^{-1} \dots y_1^{-1}$ sont aussi des éléments de l'ensemble de (7.6.a), ce qui conclut notre démonstration.

□

**Exemple 3.7.7.** Par la Proposition 3.4.6:

$$S_n = \left\langle \; (i\ j) \;\middle|\; 1 \leq i < j \leq n \; \right\rangle.$$

Autrement dit les transpositions forment une partie génératrice de $S_n$

**Exemple 3.7.8.** Pour $S_3$ on a

$$\left\langle \; (1\ 2),\ (1\ 2\ 3) \; \right\rangle = S_3$$

En utilisant le Théorème 3.5.6, il suffit de démontrer que $\left| \left\langle \; (1\ 2),\ (1\ 2\ 3) \; \right\rangle \right| > 3$. C'est évident, parce que id, $(1\ 2)$, $(1\ 2\ 3)$ et $(1\ 2\ 3)^2 = (1\ 3\ 2)$ sont 4 éléments différents.

De la même façon on a

$$\left\langle \; (1\ 2),\ (2\ 3) \; \right\rangle = S_3$$

parce que $(2\ 3)(1\ 2) = (1\ 3\ 2)$.

En somme, $S_n$ a beaucoup de parties génératrices différentes de celle de l'Exemple 3.7.7. Par exemple, pour $S_3$ on peut enlever $(1\ 3)$ de cette partie génératrice, ou on peut aussi enlever $(2\ 3)$ et ajouter $(1\ 2\ 3)$. Il y a un exercise dans la série de cette semaine qui montre qu'en fait pour chaque $S_n$ les transpositions des éléments adjacents $(i\ i{+}1)$ forment une partie génératrice.

**Exemple 3.7.9.** Il est établi dans un exercice que tous les sous-groupes propres de $A_4$ sont d'ordre au plus 4. Ça implique que $\langle\ (1\ 2)(3\ 4),\ (1\ 2\ 3)\ \rangle = A_4$, parce qu'on peut donner plus que 4 éléments distincts de $\langle\ (1\ 2)(3\ 4),\ (1\ 2\ 3)\ \rangle$:

$$\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 3)(1\ 2)(3\ 4) = (1\ 3\ 4)$$

**Exemple 3.7.10.** La Remarque 3.6.7 nous dit que $\{\sigma, \tau\}$ est une génératrice de $D_{2n}$.

On démontre maintenant qu'il y un cas où le sous-groupe engendré par deux sous-groupes peut être calculé facilement : si l'un des sous-groupes est normal.

**Proposition 3.7.11.** *Si $H \trianglelefteq G$ et $F \leq G$, alors $\langle H, F\rangle = HF = FH$, où l'on écrit*

$$HF = \left\{\ hf \in G \;\middle|\; h \in H,\ f \in F\ \right\}$$

*et*

$$FH = \left\{\ fh \in G \;\middle|\; h \in H,\ f \in F\ \right\}$$

*Preuve.* Par symétrie il suffit de démontrer que $\langle H, F\rangle = HF$. Par la Proposition 3.3.2, on a $HF \subseteq \langle H, F\rangle$ ; de plus $F = eF \subset HF$ et $H = He \subset HF$. Ainsi il suffit de démontrer que $HF$ est déjà un sous-groupe. En utilisant Proposition 3.3.2 encore une fois, il suffit de démontrer que $HF$ est stable pour la multiplication et l'inverse. Pour cela prenons $h, \tilde{h} \in H$ et $f, \tilde{f} \in F$. Les calculs suivants concluent notre démonstration :

$$hf\tilde{h}\tilde{f} = h\underbrace{f\tilde{h}f^{-1}}_{\in H \text{ parce que } H \trianglelefteq G}\underbrace{f\tilde{f}}_{\in F} \in HF \qquad (fh)^{-1} = f^{-1}h^{-1} = \underbrace{f^{-1}h^{-1}f}_{\in H \text{ parce que } H \trianglelefteq G}f^{-1} \in HF$$

□

**Exemple 3.7.12.** Considérons $D_{12}$. Premièrement on prétend que $H = \langle\sigma^3\rangle$ est normal. Pour cela il faut démontrer que $H$ contient les conjugués de tous ses éléments. Pour $e$ c'est immédiate parce que le seul conjugué de $e$ est lui-même. Le sous-groupe $H$ contient un seul autre élément : $\sigma^3$, parce que $\sigma^6 = e$ par la Remarque 3.6.7. Ainsi il suffit de démontrer que chaque conjugué de $\sigma^3$ est aussi lui-même. Pour cela, notons d'abord que chaque élément de $D_{12}$ est de la forme $\sigma^i$ ou $\tau\sigma^i$ (voir la Remarque 3.6.7). Ainsi la vérification est donnée par les calculs suivants :

$$\left(\sigma^i\right)^{-1}\sigma^3\sigma^i = \sigma^3$$

$$\left(\tau\sigma^i\right)^{-1}\sigma^3(\tau\sigma^i) = \underset{\text{Proposition 3.1.6}}{\sigma^{-i}\tau^{-1}\sigma^3\tau\sigma^i} = \underset{\tau^2 = e \text{ par la Remarque 3.6.7}}{\sigma^{-i}\tau\sigma^3\tau\sigma^i} = \underset{\tau^2 = e}{\sigma^{-i}\tau\sigma\tau\tau\sigma\tau\tau\sigma\tau\sigma^i} = \underset{\tau\sigma\tau = \sigma^{-1}}{\sigma^{-i}\sigma^{-1}\sigma^{-1}\sigma^{-1}\sigma^i} = \underset{\sigma^6 = e \text{ par la Remarque 3.6.7}}{\sigma^{-3}} = \sigma^3$$

On a finit démontré que $H \trianglelefteq G$. Prenons $F = \langle\tau\rangle$ qui est un autre sous-groupe d'ordre 2. Dans ce cas

$$\langle\sigma^3, \tau\rangle = \underset{\text{Proposition 3.7.11}}{\langle H, F\rangle} = \{e, \tau, \sigma^3, \tau\sigma^3\}$$

Puisque $\tau$ et $\sigma^3$ sont des éléments distincts et non-égaux à $e$, alors on obtient que $\langle\sigma^3, \tau\rangle \leq 12$ et un sous groupe d'ordre 4. Puisque tous les éléments sont d'ordre 2, on peut voir en utilisant l'un des exercices que $\langle\sigma^3, \tau\rangle \cong \mathbb{Z}^2 \times \mathbb{Z}^2$.

Finalement on note que $\langle\sigma^3, \tau\rangle$ n'est pas un sous-groupe normal de $D_{12}$, parce qu'on a vu dans un des exercices que $\{\tau, \tau\sigma^2, \tau\sigma^4\}$ est une classe de conjugaison.

**Exemple 3.7.13.** On démontre que la Proposition 3.7.11 n'est en général pas vraie si aucun des sous-groupes n'est normal. Par exemple, prenons $H = \langle(1\ 2)\rangle$ et $F = \langle(2\ 3)\rangle$ dans $S_3$. Dans l'Exemple 3.7.8 on a démontré que $\langle H, F\rangle = S_3$. Cependant $HF \neq S_3$ parce qu'il contient au plus 4 éléments. En fait $HF \cup FH \neq S_3$, parce qu'en dehors de id, (1 2) et (2 3), cette union contient seulement les deux éléments suivants :

$$(1\ 2)(2\ 3) = (1\ 2\ 3) \qquad (2\ 3)(1\ 2) = (1\ 3\ 2).$$

Autrement dit, $S_3 \setminus (HF \cup FH) = \{(1\ 3)\}$. Remarquez néanmoins qu'on peut écrire (1 3) comme un produit triple : $(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$, et donc qu'on a $HFH = S_3$.

**Corollaire 3.7.14.** *Si $h, f \in G$ sont éléments d'un groupe abélien (écrit additivement), alors*

$$\langle h, f\rangle = \{\ nh + mf \mid n, m \in \mathbb{Z}\ \}$$

*Si de plus $o(h), o(f) < \infty$, alors*

$$\langle h, f\rangle = \{\ \underset{\uparrow}{nh + mf} \mid n, m \in \mathbb{Z},\ 0 \leq n < o(h),\ 0 \leq m < o(f)\ \}$$

*combinaison linéaire avec coefficients dans $\mathbb{Z}$*

*Preuve.* Soit $H = \langle h\rangle$ et $F = \langle f\rangle$. En tenant compte que $\langle H, F\rangle = \langle h, f\rangle$ on obtient le résultat directement à partir de la Proposition 3.7.11. □

**Exemple 3.7.15.** Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $h, f \in G$ les éléments $h = ([1], [1], [0])$ et $f = ([0], [1], [1])$. Alors $\langle h, f\rangle$ contient 4 éléments: $e$, $h$, $f$ et

$$h + f = ([1], [1], [0]) + ([0], [1], [1]) = ([1], [0], [1]).$$

*Remarque* 3.7.16. En itérantle Corollaire 3.7.14 on obtient que si $a_1, \ldots, a_r \in G$ pour un groupe abélien $G$, alors

$$\langle a_1, \ldots, a_r\rangle = \left\{ \sum_{i=1}^{r} n_i a_i \;\middle|\; n_i \in \mathbb{Z},\ 0 \leq n_i < o(a_i) \right\}$$

On termine cette section en construisant un nouveau groupe non-abélien de petit ordre. C'est un sous-groupe engendré par deux éléments d'un autre groupe, qui apparaît souvent en mathématiques.

**Définition 3.7.17.** Soit $k$ un corps, comme défini en algèbre linéaire (on s'intéresse principalement aux cas $k = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{F}_p$, où $\mathbb{F}_p$ est juste $\mathbb{Z}/p\mathbb{Z}$ pour $p$ premier, avec la multiplication donnée par la structure de monoïde construit dans l'Exemple 3.1.16). On dénote par $\mathrm{GL}(n, k)$ le *groupe linéaire* d'un espace vectoriel de dimension $n$ sur $k$, qui peut être définit à la même fois comme le groupe des matrices $n \times n$ sur $k$ ou comme le groupe des automorphismes $k$-linéaires de $k^n$.

**Exemple 3.7.18.** Une matrice $2\times2$ à coefficients dans $\mathbb{F}_2$ appartient à $\mathrm{GL}(2, \mathbb{F}_2)$ si et seulement si ses colonnes forment une famille libre. Cela veut dire que la première colonne doit être non-zero, et la deuxième doit être un vecteur non-zero qui n'est pas un multiple scalaire de la première colonne. La liste d'éléments de $\mathrm{GL}(2, \mathbb{F}_2)$ est alors :

$$e = \begin{pmatrix}[1] & [0]\\ [0] & [1]\end{pmatrix}, \begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}, \begin{pmatrix}[0] & [1]\\ [1] & [0]\end{pmatrix}, \begin{pmatrix}[0] & [1]\\ [1] & [1]\end{pmatrix}, \begin{pmatrix}[1] & [1]\\ [1] & [0]\end{pmatrix}, \begin{pmatrix}[1] & [0]\\ [1] & [1]\end{pmatrix}$$

Un exemple de multiplication est donné par :

$$\begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix} \cdot \begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix} = \begin{pmatrix}[1][1] + [1][0] & [1][1] + [1][1]\\ [0][1] + [1][0] & [0][1] + [1][1]\end{pmatrix} = \begin{pmatrix}[1] & [0]\\ [0] & [1]\end{pmatrix}$$

**Définition 3.7.19.** Considerons le sous-ensemble $Q_8$ de $\mathrm{GL}(2,\mathbb{C})$ qui contient les éléments suivants :

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ i=\begin{pmatrix}i&0\\0&-i\end{pmatrix},\ j=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\ k=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}$$

ainsi que les éléments suivants

$$-e=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ -i=\begin{pmatrix}-i&0\\0&i\end{pmatrix},\ -j=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ -k=\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

La Proposition 3.7.20 ci-dessous nous dit que $Q_8$ est en fait un sous-groupe de $\mathrm{GL}(2,\mathbb{C})$, que l'on appelle le groupe des *quaternions*.

Notez qu'il faut distinguer le $i\in Q_8$ et le $i\in\mathbb{C}$ utilisé dans les matrices au-dessous. Ce sont deux éléments différents, appartenant à deux ensembles différents ; ce n'est cependant un hasard que les notations soient les mêmes, cela est relié à une autre définition possible du groupe des quaternions.

Remarquons aussi que le groupe $Q_8$ n'est pas abélien (cf la Proposition 3.7.20), donc les notations $-e,-i,-j,-k$ ne se réfèrent pas à la structure de groupe de $Q_8$.

**Proposition 3.7.20.** *Le sous-ensemble $Q_8$ de la Définition 3.7.19 est un sous-groupe de $\mathrm{GL}(2,\mathbb{C})$. De plus on a les égalités :*

$$i^2=j^2=k^2=-e,\ \underbrace{ij=k,\ ji=-k,\ jk=i,\ kj=-i,\ ki=j,\ ik=-j}_{\uparrow}$$

*les produits de deux éléments adjacents dans l'ordre de la rotation $i\to j\to k\to i$ est le troisième élément, et les produits de deux éléments adjacents dans l'ordre opposés est l'opposé du troisième élément*

*Preuve.* On vérifie les conditions de la Proposition 3.3.2. La condition $Q_8\neq\emptyset$ est automatique. Vérifions maintenant que $Q_8$ est stable pour la multiplication et pour l'inverse.

$Q_8$ est stable pour l'inverse : Il est clair que $e^2=(-e)^2=e$. Ainsi on calcule que pour $A\in\{i,j,k\}$ on a $A(-A)=e$ :

$$\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}-i&0\\0&i\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}\begin{pmatrix}0&i\\i&0\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$Q_8$ est stable pour la multiplication : Puisque, pour de quelconques éléments $A,B\in\mathrm{GL}(2,\mathbb{C})$, on a $(-A)B=-AB=A(-B)$ et $(-A)(-B)=AB$, il suffit de vérifier que si $g,f\in\{e,i,j,k\}$ alors $gf\in Q_8$. C'est évident si $e=g$ ou si $e=f$, alors on peut supposer que $g,f\in\{i,j,k\}$. On vérifie ces produits :

$$\underbrace{\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}i&0\\0&-i\end{pmatrix}}_{\uparrow}=\underbrace{\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}}_{\uparrow}=\underbrace{\begin{pmatrix}0&-i\\-i&0\end{pmatrix}\begin{pmatrix}0&-i\\-i&0\end{pmatrix}}_{\uparrow}=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=-e$$

$= i^2$ $= j^2$ $= k^2$

$$ij=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}=k \qquad ji=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}i&0\\0&-i\end{pmatrix}=\begin{pmatrix}0&i\\i&0\end{pmatrix}=-k$$

$$jk=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&-i\\-i&0\end{pmatrix}=\begin{pmatrix}i&0\\0&-i\end{pmatrix}=k \qquad kj=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}-i&0\\0&i\end{pmatrix}=-k$$

$$ki=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}\begin{pmatrix}i&0\\0&-i\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}=j \qquad ik=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}0&-i\\-i&0\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}=-j$$

□

*Remarque* 3.7.21. En utilisant la Proposition 3.7.20, on voit que $Q_8$ est non-abélien, par exemple $ij = k \neq -k = ji$. Cependant, $Q_8$ n'est pas loin d'être abélien, dans le sens suivant : $Q_8$ possède des sous-groupes normaux $H$ abélien tel que $Q_8/H$ est aussi abélien. Par exemple, on peut prendre $H = \langle i \rangle$. C'est un sous-groupe cyclique d'ordre 4. Par le Corollaire 3.5.29 on a $H \cong \mathbb{Z}/4\mathbb{Z}$, et $H \trianglelefteq G$ par le Lemme 3.7.22. Ainsi $G/H$ est un groupe d'ordre $8/4 = 2$. Cela implique que $G/H \cong \mathbb{Z}/2\mathbb{Z}$.

**Lemme 3.7.22.** *Si $G$ est un groupe fini et $H \leq G$ est tel que $[G : H] = 2$, alors $H \trianglelefteq G$.*

*Preuve.* En utilisant la Remarque 3.5.16, il suffit de démontrer que pour chaque $g \in G$ on a $gH = Hg$. Si $g \in H$ c'est automatique, parce que les deux cotés de l'équation sont simplement $H$. Ça veut dire qu'on peut supposer que $g \in G \setminus H$. Dans ce cas, $gH$ est un sous-ensemble de $G$ de la taille $\frac{|G|}{2}$ (Lemme 3.5.3) tel que $gH \cap H = \emptyset$, et la même observation est valable pour $Hg$. Parce que $|G| = 2|H|$, on a forcément $gH = G \setminus H = Hg$. □

On continue en démontrant que $Q_8$ est un sous-groupe de $\mathrm{GL}(2, \mathbb{C})$ engendré par deux éléments :

**Exemple 3.7.23.** On démontre que $Q_8 = \langle i, j \rangle$. On a déjà vérifié que $Q_8$ est un sous-groupe, il suffit donc de démontrer que $Q_8 \subseteq \langle i, j \rangle$. Il est automatique que $i, j, e \in \langle i, j \rangle$. On vérifie que les autres 5 éléments de $Q_8$ sont aussi contenus dans $\langle i, j \rangle$ dans le calcul suivant, où on utilise plusieurs fois les égalités démontrées en Proposition 3.7.20 :

$$-e = i^2; \qquad -i = (-e) \cdot i = i^3; \qquad -j = (-e) \cdot j = j^3; \qquad k = ij; \qquad -k = (-e)ij = i^3 j$$

On peut ajouter $Q_8$ à notre tableau des petits groupes :

| ordre | 1 ✓ | 2 ✓ | 3 ✓ | 4 | 5 ✓ | 6 | 7 ✓ | 8 |
|---|---|---|---|---|---|---|---|---|
| groupes | le groupe trivial | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$<br>$S_3$ | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Z}/8\mathbb{Z}$<br>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$<br>$(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$<br>$D_8$<br>$Q_8$ |

| 9 | 10 | 11 ✓ | 12 | 13 ✓ | 14 | 15 | ... |
|---|---|---|---|---|---|---|---|
| $\mathbb{Z}/9\mathbb{Z}$<br>$(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/10\mathbb{Z}$<br>$D_{10}$ | $\mathbb{Z}/11\mathbb{Z}$ | $\mathbb{Z}/12\mathbb{Z}$<br>$A_4$<br>$\mathbb{Z}/2\mathbb{Z} \times S_3$<br>$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$<br>$D_{12}$ | $\mathbb{Z}/13\mathbb{Z}$ | $\mathbb{Z}/14\mathbb{Z}$<br>$D_{14}$ | $\mathbb{Z}/15\mathbb{Z}$ | ... |

couleur bleu: groupes non-abéliens