Structures algébriques
(notes pour le cours d'automne de 2022, BA 1, EPFL)

Zsolt Patakfalvi

(avec l'aide de Quentin Posva et Jefferson Baudin)

13 septembre 2023

Table des matières

Chapitre 1

Codes couleurs

On utilise les couleurs différentes dans ces notes, ce qui indique la suivante :

Partie mathématiquement non 100% précisément écrite

Partie descriptive du texte, où les mathématiques ne sont pas 100% précise. Autrement dit, une partie ce qui ne contient pas les définitions, théorèmes, propositions, lemmes et exemples numérotés.

Partie ce qui n'est pas demandé dans l'examen

Partie optionnelle, qui n'est pas donc demandée à l'examen. Cependant, il y a une vidéo sur Moodle sur cette partie de la matière, et c'est fortement conseillé de la regarder et de comprendre la matière.

Chapitre 2

Preuves et ensembles

2.1 Logique formelle

Partie mathématiquement non 100% précisément écrite

Ce qui est vrai ou faux en mathématiques est dirigé par la logique formelle. Pour cette raison, on apprend quelque faits basiques de la logique formelle, ce qui est indispensable pour être capable de :

(1) lire des preuves,

(2) décider quand une preuve est correcte, et

(3) construire de nouvelles preuves.

Cependant, ce cours-ci n'est pas un cours de logique formelle, donc cette partie de la matière sera courte, et loin de la profondeur d'un cours ce qui se focalise dessus.

La logique formelle concerne des expressions logiques qui contient des *variables logiques*, des *connecteurs logiques*, des *quantificateurs* et quelques parenthèses. Pour simplifier, dans la Section 2.1, on regarde juste des expressions logiques qui ne contiennent pas de quantificateurs. Par exemple une expression logique de tel type est :

$$\big((A \implies B) \wedge (B \implies C)\big) \implies (A \implies C) \tag{2.1.a}$$

On note aussi que les connecteurs logiques sont modelés sur les expressions quotidiennes :

(1) et : $\wedge$,

(2) ou : $\vee$,

(3) non : $\neg$,

(4) "cela implique", ou "si ..., alors" : $\implies$

(5) si et seulement si : $\iff$.

Une expression logique est une recette pour construire de nouvelles expressions mathématiques, à partir de celles que l'on connait déjà. On fait cette construction en mettant une expression mathématique dans chaque variable logique. On peut même faire ce processus aussi avec des affirmations du monde réel. Si dans l'expression (2.1.a) on met :

$$\begin{aligned} A &= \text{on dort beaucoup} \\ B &= \text{on est reposé} \\ C &= \text{on est heureux} \end{aligned}$$

on obtient que

$$\begin{aligned}\big((\text{on dort beaucoup} &\implies \text{on est reposé})\\ &\wedge (\text{on est reposé} \implies \text{on est heureux})\big)\\ &\implies (\text{on dort beaucoup} \implies \text{on est heureux})\end{aligned} \tag{2.1.b}$$

On peut même traduire (2.1.b) dans la langue quotidienne. Puisque (2.1.b) contient beaucoup de parenthèses, cela n'est pas facile, mais c'est possible, au moins de manière un peu encombrante :

Si les deux affirmations suivantes sont vraies :
(1) Si on dort beaucoup, alors on est reposé.
(2) Si on est reposé, alors on est heureux.
alors il est vrai aussi que si on dort beaucoup, alors on est heureux. (2.1.c)

Le point de l'expression (2.1.a) est qu'elle est toujours vraie, et par conséquent (2.1.b) et (2.1.c) sont aussi vraies. Cela veut dire que (2.1.a) et une *tautologie*. On peut tout d'abord comprendre la raison intuitivement. L'expression (2.1.a) formule l'idée que si quelque si A implique B et B implique C, alors A implique C aussi. En effet, on utilise ce petit pas de logique même dans notre vie quotidienne, et surtout on l'utilise partout dans les arguments en mathématiques.

Cependant, on peut aussi comprendre pourquoi (2.1.a) est une tautologie formellement, autrement dit mathématiquement. Pour cela, il faut comprendre comment on évalue les expressions logiques.

2.1.1 Évaluation des expressions logiques

Partie mathématiquement non 100% précisément écrite

Toute variable logique a deux valeurs éventuelles : *vrai* ce que l'on dénote par V, ou faux de que l'on dénote par F. Les autres signes dans nos expressions logiques sont soit des parenthèses soit des connecteurs logiques (on ne considère pas des quantificateurs dans la Section 2.1). Les parenthèses déterminent, comme d'habitude, l'ordre de l'évaluation pour toute opération mathématique. Cependant le comportement des connecteurs est donné par des *tables de vérité*.

Par exemple, $\wedge$ a deux arguments, disons A et B, et le signe $\wedge$ se traduit "et" dans la langue quotidienne. Autrement dit, $A \wedge B$ est vrai si et seulement si A et B sont vrais. Par conséquent la table de vérité pour $\wedge$ est

A \ B	V	F
V	V	F
F	F	F

$= A \wedge B$

De manière similaire, puisque $\vee$ et le signe pour "ou", sa table de vérité est

A \ B	V	F
V	V	V
F	V	F

$\Big\} = A \vee B$

Le signe $\Longrightarrow$ signifie "implique", donc $A \Longrightarrow B$ est faux si et seulement si A est vrai et B est faux. En particulier la table de vérité est

A \ B	V	F
V	V	F
F	V	V

$\Big\} = A \Longrightarrow B$

Notons que *le faux implique tout*. Autrement dit $A \Longrightarrow B$ est vrai si A est faux, peu importe B. Par exemple la phrase suivante et toujours vraie :

Si tous éléphants sont roses, alors ils sont tous capables de voler.

En utilisant les tables de vérité ci-dessus on peut évaluer les expressions logiques. Par exemple on a (2.1.a) :

A	V	V	V	V	F	F	F	F
B	V	V	F	F	V	V	F	F
C	V	F	V	F	V	F	V	F
$A \Longrightarrow B$	V	V	F	F	V	V	V	V
$B \Longrightarrow C$	V	F	V	V	V	F	V	V
$(A \Longrightarrow B) \wedge (B \Longrightarrow C)$	V	F	F	F	V	F	V	V
$A \Longrightarrow C$	V	F	V	F	V	V	V	V
$\big((A \Longrightarrow B) \wedge (B \Longrightarrow C)\big) \Longrightarrow (A \Longrightarrow C)$	V	V	V	V	V	V	V	V

(2.1.d)

Par conséquent, l'expression (2.1.a) est toujours vraie.

Les autres signes sont $\neg$, qui est le symbole de négation (il se lit "non"), et $\Longleftrightarrow$ qui veut dire "si et seulement si", avec comme tables de vérité :

A	$\neg A$
V	F
F	V

et

A \ B	V	F
V	V	F
F	F	V

$\Big\} = A \Longleftrightarrow B$

Finalement, on note que l'on peut écrire toute table de vérité de la manière de la table de $\neg$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Longrightarrow B$	$A \Longleftrightarrow B$
V	V	V	V	F	V	V
V	F	F	V	F	F	F
F	V	F	V	V	V	F
F	F	F	F	V	V	V

2.1.2 Tautologies

Partie mathématiquement non 100% précisément écrite

Une tautologie est une expression logique ce qui est vraie peu importe la valeur des variables. Par exemple, l'expression (2.1.a) est une tautologie par le calcul de (2.1.d). Une autre tautologie est $(A \implies B) \iff \big((\neg B) \implies (\neg A)\big)$ par le calcul suivant. Cette tautologie nous de que "A implique B" et "l'opposé de B implique l'opposé de A" sont les mêmes affirmations d'un point de vue mathématique. On dit que la deuxième affirmation et la contraposée de la première.

A	V	V	F	F
B	V	F	V	F
$A \implies B$	V	F	V	V
$\neg B$	F	V	F	V
$\neg A$	F	F	V	V
$(\neg B) \implies (\neg A)$	V	F	V	V
$(A \implies B) \iff \big((\neg B) \implies (\neg A)\big)$	V	V	V	V

(2.1.e)

Une autre tautologie est $\neg(A \vee B) \Leftrightarrow ((\neg A) \wedge (\neg B))$:

A	V	V	F	F
B	V	F	V	F
$A \vee B$	V	V	V	F
$\neg(A \vee B)$	F	F	F	V
$\neg B$	F	V	F	V
$\neg A$	F	F	V	V
$(\neg B) \wedge (\neg A)$	F	F	F	V
$\neg(A \vee B) \Leftrightarrow ((\neg A) \wedge (\neg B))$	V	V	V	V

(2.1.f)

On donne aussi un exemple d'une expression logique qui N'EST PAS une tautologie : $(A \implies B) \iff (B \implies A)$. Cela se voit par le fait que la dernière ligne de la table suivante n'est pas remplie seulement de V :

A	V	V	F	F
B	V	F	V	F
$A \implies B$	V	F	V	V
$B \implies A$	V	V	F	V
$(A \implies B) \iff (B \implies A)$	V	F	F	V

(2.1.g)

2.2 Preuves

Partie mathématiquement non 100% précisément écrite

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 de preuve mathématique. D'après cette définition, on ne peut utiliser que des signes mathématiques, comme :

(1) connecteurs logiques mentionné ci-dessus : $\wedge$, $\vee$, $\neg$, $\implies$, $\iff$,

(2) les quantificateurs, comme
   (i) il existe : $\exists$,
   (ii) il existe un unique : $\exists!$,
   (iii) pour tout : $\forall$,
(3) les autres signes que l'on définira (par exemple $\in$ qui veut dire "appartenir à un ensemble"),
(4) 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,
(4) modus ponens : s'il y a une ligne précédente de la forme $A \implies B$, et une autre de la forme A, alors on peut écrire B.
(5) etc...

Preuves formelles et leur approximation : On appelle les preuves écrites de la manière ci-dessus des *preuves formelles*. Écrire une preuve formelle est utile pour la vérifier avec un ordinateur. Mais il est quasiment impossible de la lire pour un humain. En pratique, on essaie d'approximer les preuves formelles par un mélange de texte et de symboles mathématique. Quand on écrit une 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 une 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.

Importance de la logique formelle et des tautologies : Malgré le fait que les preuves formelles doivent être approximées en pratique, il faut se souvenir dans que chaque preuve, ce que l'on écrit doit être traduisible en une preuve formelle. En particulier, il faut se souvenir ce que l'on a appris sur la logique formelle, et en particulier des tautologies. Typiquement, la tautologie $(A \implies B) \iff \big((\neg B) \implies (\neg A)\big)$ de (2.1.e) nous dit que "chaque implication est équivalente à sa contraposée". Pour cette raison, dans les preuves, on remplace souvent la démonstration de $A \implies B$ par celle de $(\neg B) \implies (\neg A)$. Par exemple, au lieu de démontrer que "cet animal n'est pas un rongeur $\implies$ cet animal n'est pas un hamster" il est mieux de démontrer la proposition équivalente, mais plus naturelle "cet animal est un hamster $\implies$ cet animal est un rongeur". Notons que l'ordre a changé. Autrement dit, l'affirmation sur les "hamsters" était à droite dans la première implication, mais à gauche dans la deuxième.

De la même manière, il faut se souvenir de ce qui n'est pas une tautologie. Par example dans (2.1.g) on a montré que $(A \implies B) \iff (B \implies A)$ n'est pas une tautologie. Autrement dit, $A \implies B$ n'est pas la même affirmation que $B \implies A$. Mélanger ces deux affirmations est le plus grand péché mathématique imaginable. Ceux qui le font seront tous brulés dans l'enfer mathématique (pour l'éternité).

TYPE DE PREUVES : En pratique, il y deux types fondamentaux de preuves : les preuves rédigées, et les preuves écrites pour accompagner une explication (quand vous expliquez une preuve à un autre étudiant, ou quand l'enseignant vous explique une preuve). La première est soigneusement rédigée, avec tout les détails présentés, comme tout ce que vous trouverez ici dans ces notes à partir de la Section 2.3.2, et aussi dans la Section 2.2.1. Au même temps, la deuxième est juste une aide pour l'explication verbale, comme les notes manuscrites par le professeur pendant le cours.

2.2.1 Un exemple d'une preuve

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 2.2.1. 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 2.2.2. 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 2.2.3. *(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*

$$a = bq + r. \tag{2.2.a}$$

Démonstration. *Unicité* 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.

Existence : 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 2.2.4. Si $a = 13$, $q = 3$, alors $b = 4$ et $r = 1$, parce que $13 = 4 \cdot 3 + 1$.

2.3 Ensembles

2.3.1 Axiomes de théorie des ensembles

Partie mathématiquement non 100% précisément écrite

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 une collection des "choses", et une sous-collection 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.

Démonstration. 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 2.3.1.

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 $A_i \neq \emptyset$ 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 :

$$\mathbb{Z}^{>0} := \{\ x \in \mathbb{Z} \mid x > 0\ \}.$$

(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 appelée le complément de A dans B, définie par

$$B \setminus A = \{\ b \in B \mid \underset{\uparrow}{\neg}(b \in A)\ \} = \{\ b \in B \mid b \underset{\uparrow}{\notin} A\ \}$$

notation en logique mathématique — 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 :

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

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.

2.3.2 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 2.3.2. 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 2.3.3. Soient $A = \{1, 2\}$ et $B = \{5, 6\}$. Dans ce cas on a

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

Remarque 2.3.4. 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 2.3.5. Soient A et B des ensembles. Une application $\phi : A \to B$ est un sous-ensemble (appelé le graphe de ϕ)

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

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 Γ_ϕ 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 ϕ.

On appelle A le domaine, et B le codomaine de ϕ.

Exemple 2.3.6. Soit A, B des ensembles. Voici quelques exemples d'applications entre A et B :

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

$$\forall a \in A \ : \ \mathrm{id}_A(a) = a$$
$$\Updownarrow$$
$$\Gamma_{\mathrm{id}_A} = \left\{ \ (a,a) \in A \times A \ \middle| \ a \in A \ \right\}$$

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

$$\forall (a,b) \in A \times B \ : \ \mathrm{pr}_A\big((a,b)\big) = a$$
$$\Updownarrow$$
$$\Gamma_{\mathrm{pr}_A} = \left\{ \ (a,b,a) \in A \times B \times A \ \middle| \ a \in A, b \in B \ \right\}$$

Définition 2.3.7. Soit $\phi : A \to B$ une application entre ensembles. On dit que

(1) ϕ est *injective*, si

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

(2) ϕ est *surjective*, si

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

(3) ϕ est *bijective*, si elle est injective et surjective.

(4) l'image de ϕ est

$$\phi(A) = \left\{ \ \phi(a) \in B \ \middle| \ a \in A \ \right\}$$

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

Définition 2.3.8. Soient $\phi : A \to B$ et $\xi : B \to C$ les applications entre ensembles. La composition $\xi \circ \phi$ est l'application

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

Proposition 2.3.9. *Soient $\phi : A \to B$ et $\xi : B \to C$ les applications entre ensembles, et supposons que $\xi \circ \phi$ est surjective. Alors,*

(1) ξ est aussi surjective, mais

(2) ϕ n'est pas nécessairement surjective.

Démonstration. (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 2.3.10. Soit $\phi : A \to B$ une bijection entre ensembles. *L'inverse* ϕ^{-1} de ϕ 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 2.3.11. 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 $\phi^{-1}(6) = 1$.

2.3.3 Relations d'équivalence et partitions

La question générale à laquelle on réfléchit dans cette section est "comment peut-on construire de nouveaux ensembles en décrétant quelques éléments équivalents ?". La notion qui formalise cette idée est appelée une relation d'équivalence.

Définition 2.3.12. Soit A un ensemble. Une *relation d'équivalence* sur A 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) $(a,b) \in R, (b,c) \in R \ \Rightarrow \ (a,c) \in R$.

Remarque 2.3.13. Souvent, on dénote une relation d'équivalence $R \subseteq A \times A$ par $\equiv$. Autrement dit, avec les notations ci-dessus, on écrit $a \equiv b$ si et seulement si $(a,b) \in R$. De ce fait, on peut voir une relation d'équivalence comme une notion qui généralise la notion d'égalité.

Dans certains contextes, l'égalité est une notion trop rigide, et on aimerait dire que certains éléments sont, d'un certain point de vue, les "mêmes", bien qu'ils ne soient pas égaux. Les relations d'équivalences permettent de formaliser cette notion, et les quotients (la Définition 2.3.23) permettent de considérer l'ensemble où les éléments de A qui étaient équivalents deviennent égaux.

En effet, par la Proposition 2.3.19, $R_a = R_b$ si et seulement si $a \equiv b$. Ainsi, supposons que l'on aie a, b tels que $a \equiv b$. Alors ces éléments, vus comme des éléments du quotient par l'application ξ_R, deviennent égaux.

Proposition 2.3.14. *Si a, b et m sont des entiers tel que $m > 0$, $m|a$ et $m|b$, alors $m|a+b$.*

Démonstration. 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 2.3.15. Fixons un entier $m > 0$. On définit une *relation d'équivalence* sur $\mathbb{Z}$ par le sous-ensemble $R \subseteq \mathbb{Z} \times \mathbb{Z}$ définie par la condition suivante :

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

On vérifie que 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 2.3.16. Soit $R \subseteq A \times A$ une relation d'équivalence. Pour tout $a \in A$ on définit la *classe d'équivalence* de a par

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

En français, la classe d'équivalence de a est l'ensemble des éléments de A qui sont équivalents à a.

Exemple 2.3.17. Soit $m \in \mathbb{Z}$, et R la relation d'équivalence définie dans l'Exemple 2.3.15.

Considérons le sous-ensemble suivant de $\mathbb{Z}$:

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

et de plus pour chaque $x \in \mathbb{Z}$ le sous-ensemble suivant de $\mathbb{Z}$:

$$m\mathbb{Z}+x = \{\, c+x \in \mathbb{Z} \mid c \in m\mathbb{Z} \,\} \underset{\uparrow}{=} \{\, y \in \mathbb{Z} \mid m|y-x \,\} \underset{\uparrow}{=} \{\, y \in \mathbb{Z} \mid m|x-y \,\} \underset{\uparrow}{=} R_x. \quad (2.3.a)$$

$y = c+x \iff x = y-c$

puisque $x-y = -(y-x)$, on a $m|y-x \iff m|x-y$

par définition de R, et par la Définition 2.3.16

Par la dernière égalité de (2.3.a) on obtient une description précise des classes d'équivalence de R. Ce sont exactement les sous-ensembles de $\mathbb{Z}$ de forme $m\mathbb{Z}+x$.

Remarque 2.3.18. Dans la Définition 2.3.16, R_a est un sous-ensemble de A, et en particulier c'est un élément de 2^A. Par conséquent, on pourrait considérer l'ensemble des toute classe d'équivalence de R, ce qui est un sous-ensemble de 2^A :

$$\{\, R_a \in 2^A \mid a \in A \,\} = \{\, R_a \subseteq A \mid a \in A \,\} \quad (2.3.b)$$

Le sous-ensemble (2.3.b) peut être regardé de deux manières différentes :

(1) Si on se focalise sur le fait que les éléments de (2.3.b) sont des sous-ensembles de A, on obtient que ces ensembles recouvrent A, de telle sorte que chaque élément de A appartient à un seul de ces sous-ensembles. Cela nous ammène à la notion de partition, formalisé dans la Définition 2.3.20.

(2) Si on oublie les éléments de l'ensemble (2.3.b), et qu'on se focalise sur le fait que c'est lui-même un ensemble, on obtient le quotient par R, formalisé dand la Définition 2.3.23.

Pour comprendre les deux points de vue, il faut mieux comprendre le comportement des classes d'équivalence, ce qui est fait dans la Proposition 2.3.19.

Proposition 2.3.19. *Si R est une relation d'équivalence sur l'ensemble A, alors*

(1) $(a,b) \in R \implies R_a = R_b$.

(2) $(a,b) \notin R \implies R_a \cap R_b = \emptyset$.

(3) $(a,b) \in R \iff R_a = R_b$.

Démonstration. (1) Soit $(a,b) \in R$. On a alors $(b,a) \in R$ par symétrie. Ainsi, pour chaque $c \in A$ on a

$$(a,c) \in R \underset{\uparrow}{\implies} (b,c) \in R$$

$(b,a) \in R$ et par transitivité

et

$$(b,c) \in R \underset{\uparrow}{\implies} (a,c) \in R$$

$(a,b) \in R$ et par transitivité

On obtient que $(b,c) \in R$ si et seulement si $(a,c) \in R$, ce qui, par la Définition 2.3.16, implique que $R_a = R_b$.

(2) On montre la contraposée. Si $R_a \cap R_b \neq \emptyset$, alors prenons $c \in R_a \cap R_b$. Par définition de R_a et R_b on a (a,c) et $(b,c) \in R$. Par symétrie on obtient que $(c,b) \in R$, et donc par transitivité $(a,b) \in R$ aussi.

(3) C'est une conséquence des points (1) et (2) ci-dessus.

□

Définition 2.3.20. Une *partition* d'un ensemble A est un sous-ensemble $\mathcal{X} \subseteq 2^A$ tel que chaque élément de A est contenu dans un unique élément de $\mathcal{X}$. On peut écrire cette dernière condition avec des formules :

$$\forall a \in A,\ \exists! Y \in \mathcal{X} : a \in Y.$$

Remarque 2.3.21. La Proposition 2.3.19 nous dit que pour une relation d'équivalence R sur A, l'ensemble

$$\left\{ R_a \in 2^A \;\middle|\; a \in A \right\}$$

et une partition de A. De plus, la Proposition 2.3.22 nous dit que chaque partition nous donne une relation d'équivalence. On laisse en devoir que ces deux constructions sont inverses l' une de l'autre. On dit que les partitions sont équivalentes aux relations d'équivalences.

Proposition 2.3.22. *Si $\mathcal{X} \subseteq 2^A$ est une partition de l'ensemble A, alors le sous-ensemble suivant de $A \times A$ est une relation d'équivalence.*

$$\left\{ (a,b) \in A \times A \;\middle|\; \exists Y \in \mathcal{X} \colon \{a,b\} \subseteq Y \right\}$$

Démonstration. On démontre les trois propriétés de la Définition 2.3.12.

Réflexivité : Soit $a \in A$. Par la Définition 2.3.20, a est contenu dans exactement un $Y \in \mathcal{X}$. Il suit que l'on a $\{a,a\} = \{a\} \subseteq Y$ et ainsi $(a,a) \in R$.

Symétrie : Soit $(a,b) \in R$, ce qui veut dire par définition que $\{a,b\} \subseteq Y$ pour un $Y \in \mathcal{X}$. Puisque $\{b,a\} = \{a,b\}$, on a $\{b,a\} \subseteq Y$, et par conséquent $(b,a) \in R$.

Transitivité : Soit $(a,b) \in R$ et $(b,c) \in R$. Par définition, on a $Y, Z \in \mathcal{X}$ tels que $\{a,b\} \subseteq Y$ et $\{b,c\} \subseteq Z$. Puisque, par la Définition 2.3.20, b est contenu dans exactement un élément de $\mathcal{X}$, on obtient que $Y = Z$. Cela implique que $\{a,c\} \subseteq Y$ et par conséquent $(a,c) \in R$. □

Définition 2.3.23. 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 :

$$A/R = \left\{ R_a \subseteq A \;\middle|\; a \in A \right\} \subseteq 2^A$$

On appelle l'application $\xi_R : A \ni a \mapsto R_a \in A/R$ l'application quotient de R.

Exemple 2.3.24. Il y un exemple d'une quotient par une relation d'équivalence ce que l'on connait très bien, l'ensemble des nombres rationnels $\mathbb{Q}$. En effet, les nombres rationnels par définition sont des paires $(a,b) \in \mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$, dont on pense comme $\frac{a}{b}$, et où *l'on identifie* (a,b) avec (a',b') si et seulement si $ab' = a'b$. En effet, on peut définir une relation d'équivalence sur $\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$ en demandant que $(a,b) \equiv (a',b')$ si et seulement si $ab' = a'b$. Cette relation est réflexive et symétrique par définition.

Transitivité : Pour vérifier transitivité, prenons éléments $(a,b),(a',b'),(a'',b'') \in \mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$, tels que $(a,b) \equiv (a',b')$ et $(a',b') \equiv (a'',b'')$. On obtient que

$$\begin{array}{ccc} ab'b'' & = & a'bb'' \;=\; ba''b'. \\ \uparrow & & \uparrow \\ \boxed{(a,b) \equiv (a',b') \implies ab' = ba'} & & \boxed{(a',b') \equiv (a'',b'') \implies a'b'' = b'a''} \end{array}$$

En divisant les deux cotés de cet égalité par b' on obtient $ab'' = ba''$, ou autrement dit que $(a,b) \equiv (a'',b'')$.

Conclusion : On a défini une relation d'équivalence sur $\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$. En particulier, on peut prendre $\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big) \Big/ \equiv$, et de plus ce quotient est égal à $\mathbb{Q}$.

Exemple 2.3.25. Considérons l'ensemble $A = \{1,2,3,4,5,6\}$ et la partition

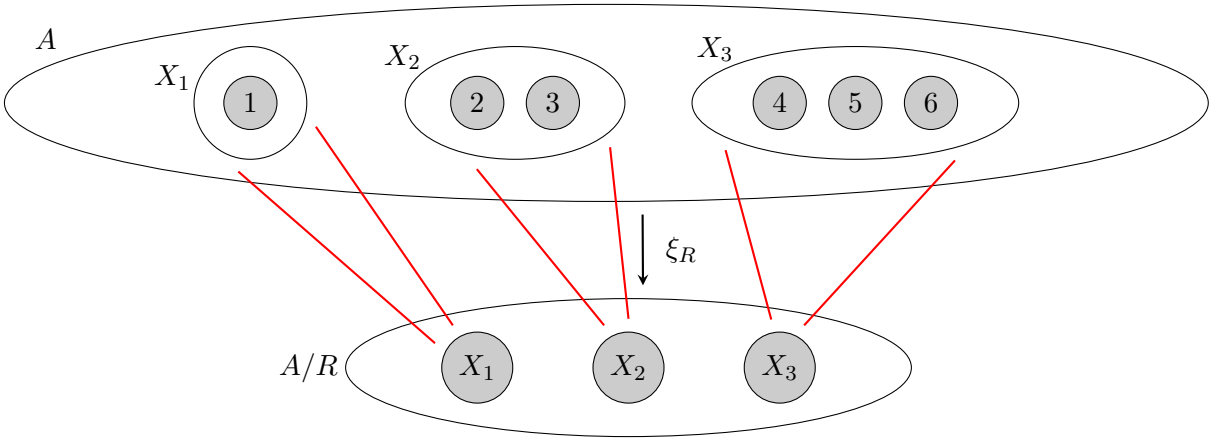
$$\mathcal{X} = \Big\{ X_1 = \{1\} \;,\; X_2 = \{2,3\} \;,\; X_3 = \{4,5,6\} \Big\} \subseteq 2^A.$$

La construction de la Proposition 2.3.22 donne que la relation d'équivalence correspondant à $\mathcal{X}$ est

$$R = \Big\{ \underbrace{(1,1)}_{\uparrow}, \underbrace{(2,2),\ (2,3),\ (3,2),\ (3,3)}_{\uparrow}, \underbrace{(4,4),\ (4,5),\ (4,6),\ (5,4),\ (5,5),\ (5,6),\ (6,4),\ (6,5),\ (6,6)}_{\uparrow} \Big\}$$

correspondant à X_1 | correspondant à X_2 | correspondant à X_3

De plus, on peut visualiser l'application quotient ξ_R dans la manière suivante :



Le problème habituel avec la compréhension du quotient et que les X_i sont à la fois des ensembles et des éléments. Ils sont sous-ensembles de A et éléments de A/R. Il est vraiment important de s'habituer à penser aux deux points de vue au même temps, car en algèbre les quotients sont omniprésents.

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

Exemple 2.3.26. On définit $\mathbb{Z}/_{m\mathbb{Z}} = \mathbb{Z}/R$, où R est la relation d'équivalence définie dans Exemple 2.3.15. Par l'Exemple 2.3.17, on sait que les classes d'équivalences sont les sous-ensembles $m\mathbb{Z} + x \subseteq \mathbb{Z}$. On a par la Définition 2.3.23 :

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

Par exemple,

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

2.3.4 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 2.3.27. 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 *infini 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 2.3.12 : identité (par d'existence des applications d'identité), réflexivité (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 2.3.12, 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 2.3.28 (Théorème de Cantor-Schröder-Bernstein)**.** *Soient A et B des ensembles. Si $|A| \leq |B|$ et $|B| \leq |A|$, alors $|A| = |B|$.*

Partie ce qui n'est pas demandé dans l'examen

On doit démontrer un lemme avant de procéder à la preuve du Théorème 2.3.28. Dans ce lemme, on utilisera la notation suivante :

Définition 2.3.29. 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 2.3.30. 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 considère vraiment comme une application $Y \to g(Y)$. Avec cette convention, $g|_Y$ devient bijective, et on peut prendre son inverse.

Lemme 2.3.31. *Soit $f : A \to B$ et $g : B \to A$ des injections. S'il existe un sous-ensemble $X \subseteq A$ tel que*

$$X = A \setminus g\big(B \setminus f(X)\big), \tag{2.3.c}$$

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

Démonstration. Définissons

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

(2.3.c)

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 2.3.28. Pour chaque sous-ensemble $X \subseteq A$ définissons

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

Par le Lemme 2.3.31, 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 2.3.7

prendre le complément renverse l'inclusion (ce sera un exercice)

par définition de l'image dans la Définition 2.3.7

$$\underset{\uparrow}{\implies} H(X) = A \setminus g\big(B \setminus f(X)\big) \subseteq A \setminus g\big(B \setminus f(Z)\big) = H(Z) \quad (2.3.\text{d})$$

prendre le complément renverse l'inclusion

Deuxièmement on définit

$$W := \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X, \tag{2.3.e}$$

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 $H(W) \subseteq W$:

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

(2.3.e)

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

(2.3.d)

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

$H(X) \subseteq X$ (2.3.e)

Pour conclure, il suffit maintenant de montrer que $H(W) \supseteq W$. Notons que $H(W) \subseteq W$ et (2.3.d) implique que $H(H(W)) \subseteq H(W)$. Cela veut dire que $H(W)$ fait partie de la collection que X parcourt dans (2.3.e). 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 ω_1 minimal parmi les cardinaux plus grands que $|\mathbb{N}| = \omega_0$. Il y aura un exercice aussi sur la fiche d'exercice 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 qu'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.

Chapitre 3

Théorie des nombres

3.1 Algorithme d'Euclide

Définition 3.1.1. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^{\neq 0}$. Le *plus grand commun diviseur* de a et b et

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

(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 $\operatorname{pgcd}(a,b) = 1$.

Lemme 3.1.2. *Si, $a, b \in \mathbb{Z}$ tel que $a \neq 0$ et $r \in \mathbb{Z}$, alors* $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a, b+ra)$.

Démonstration. Par Définition 3.1.1, 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 :

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

$\boxed{m|b \text{ et Proposition 2.3.14}}$

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

$\boxed{m|b+ra \text{ et Proposition 2.3.14}}$

□

Notation 3.1.3. 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 3.1.4. *Relation de Bézout. Dans la situation de la Notation 3.1.3, il existe $m, n \in \mathbb{Z}$ tel que $ma + nb = q_t$.*

Démonstration. 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 $i-1$:

$$q_t = m_i q_i + n_i q_{i+1} = m_i q_i + n_i(q_{i-1} - s_i q_i) = \underbrace{n_i}_{\uparrow}\, q_{i-1} + (\underbrace{m_i - n_i s_i}_{\uparrow})q_i$$

$$\boxed{:= m_{i-1}} \qquad \boxed{:= n_{i-1}}$$

□

Lemme 3.1.5. *Dans la situation de la Notation 3.1.3, $q_t | q_i$ pour chaque entier $1 \leq i \leq t$.*

Démonstration. 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 :

$$q_{i-1} = q_{i+1} + s_i q_i \qquad \underset{\uparrow}{\Longrightarrow} \qquad q_t | q_{i-1}$$

$$\boxed{q_t | q_{i+1} \text{ et } q_t | q_i \text{ par hypothèse d'induction}}$$

□

Théorème 3.1.6. *Si $a, b \in \mathbb{Z}^{>0}$, l'algorithme d'Euclide nous donne $q_t = \mathrm{pgcd}(a, b)$.*

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

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

- Lemme 3.1.5 dit que $q_t | a$ et $q_t | b$, alors q_t est un diviseur commun de a et b, et
- Lemme 3.1.4 dit que $\mathrm{pgcd}(a, b) | q_t$, et par conséquent $q_t \geq \mathrm{pgcd}(a, b)$. On obtient que $\mathrm{pgcd}(a, b) = q_t$.

$\boxed{\textit{Existence de } m \textit{ et } n :}$ c'est impliqué par $q_t = \mathrm{pgcd}(a, b)$ et par le Lemme 3.1.4. □

Corollaire 3.1.7. *Supposons que $q, a, b \in \mathbb{Z}^{>0}$, $q | ab$ et que $(q, a) = 1$. Alors $q | b$.*

Démonstration. Par le Théorème 3.1.6, 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 $q | b$. □

3.2 Théorème fondamental de l'arithmétique

Définition 3.2.1. 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 3.2.2. Notons bien que $p \geq 2$ dans cette définition. En particulier, le nombre 1 n'est, par convention, ni premier ni irréductible.

Proposition 3.2.3. *Si $p \geq 2$ est un entier, alors p est irréductible si est seulement si p est premier.*

Démonstration. $\boxed{\Longleftarrow :}$ 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 $\text{pgcd}(p, a) \neq p$. Mais p est irréductible, alors il a seulement deux diviseurs (positifs) 1 et p. Cela force $\text{pgcd}(p, a) = 1$. Finalement dans ce cas Corollaire 3.1.7 nous donne que $p|b$. □

Théorème 3.2.4. *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.*

Démonstration. $\boxed{\textit{Existence :}}$ 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 3.2.3, 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

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

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

$$n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j \tag{3.2.a}$$

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 3.2.3, p_l est irréductible. En utilisant que $q_1 > 1$, on obtient $q_1 = p_l$. Alors par (3.2.a) on obtient

$$\mathbb{Z} \ni \frac{n}{q_1} = \prod_{1 \leq i \leq r,\ i \neq l} p_i = \prod_{j=2}^{s} q_j \tag{3.2.b}$$

En particulier $r > 2$, parce qu'autrement le premier produit dans (3.2.b) serait vide. Ça veut dire que l'on peut appliquer l'hypothèse d'induction pour les deux produits dans (3.2.b). Ceci conclut notre démonstration. □

Chapitre 4

Théorie des groupes

4.1 Définition et premiers exemples

La notion de groupe donne un cadre abstrait pour comprendre des symétries. Quand on a 3 symétries, on peut les appliquer dans 2 ordres différents naturels (point (1) de la Définition 4.1.1). Quand on travaille avec des symétries, l'identité est d'habitude considérée comme l'une d'eux (point (2) de la Définition 4.1.1). Finalement, quand on a une symétrie, l'inverse est aussi considéré d'habitude comme une symétrie (point (3) de la Définition 4.1.1). Ainsi, la définition suivante de groupe formalise les propriétés des symétries discutées dans ce paragraphe.

Définition 4.1.1. Un groupe est une paire $(G, \cdot)$ constituée d'un ensemble G, et d'une application

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

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

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

Démonstration. On peut écrire

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

(2) (3) (3) (2) (3)

où les chiffres réfèrent aux points correspondants de la Définition 4.1.1. □

Proposition 4.1.3. *Si G est un groupe, alors e est aussi un élément neutre à droite. Autrement dit :*

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

Démonstration. On a :

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

(3) de Définition 4.1.1 | Proposition 4.1.2 | (2) de Définition 4.1.1

□

Proposition 4.1.4. *Si G est un groupe, alors l'élément neutre est unique. En formules, pour chaque $e' \in G$:*

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

Démonstration. Si e' est comme dans l'énoncé :

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

l'hypothese de la proposition | Proposition 4.1.3

□

Proposition 4.1.5. *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.

Démonstration.

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

Proposition 4.1.2 | Proposition 4.1.3

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

(3) de Définition 4.1.1 | (2) de Définition 4.1.1

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

Démonstration. En utilisant la Proposition 4.1.5 et le point (3) de Définition 4.1.1 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 4.1.1 | (2) de Définition 4.1.1 | (3) de Définition 4.1.1

□

Notation 4.1.7. 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) :

$$\forall m, n \in \mathbb{Z} : \ g^m g^n = g^{m+n} \quad \text{et} \quad \forall m, n \in \mathbb{Z} : \ (g^m)^n = g^{mn} \tag{4.1.a}$$

Exemple 4.1.8. On donne deux exemples de (4.1.a). La démonstration précise de (4.1.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 4.1.6 $(ggg)^{-1} = \left(g(gg)\right)^{-1} = (gg)^{-1}g^{-1} = g^{-1}g^{-1}g^{-1}$

Notation 4.1.9. 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 que G est abélien, on a la relation suivante pour chaque $g, f \in G$:

$$n \cdot (g + f) = (n \cdot g) + (n \cdot f) \tag{4.1.b}$$

Ici on démontre la propriété (4.1.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 4.1.10. 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 4.1.11. (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 non nuls est ∞.

(3) $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$. Dans ces deux cas l'élément neutre est 1, est les seuls éléments d'ordre fini 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 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 :

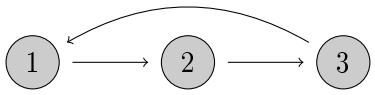
$$\begin{pmatrix}1 & 2 & \dots & n\\ \sigma(1) & \sigma(2) & \dots & \sigma(n)\end{pmatrix}$$

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 σ aux éléments de $\{1,\dots,n\}$ et on applique τ deuxièmement. Ainsi, le calcul 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 4.1.12. 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 2.3.23. Ecrivons $[g]$ la classe d'équivalence de l'élément $g \in G$, qui était précédemment notée R_g dans la Définition 2.3.16. 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 $x^{-1} := [g^{-1}]$.
- 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 4.1.13. *Soient G un groupe et $R \subseteq G \times G$ une relation d'équivalence. Les opérations sur G/R envisagées dans la Remarque 4.1.12 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) $(x,\tilde{x}) \in R \implies (x^{-1}, \tilde{x}^{-1}) \in R$.

Dans ce cas G/R, avec les opérations et l'élément neutre définis dans la Remarque 4.1.12, est un groupe.

Démonstration. 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 4.1.12 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 4.1.1 est similaire et laissée en exercice. □

Exemple 4.1.14. Pour un entier $m > 0$, prenons l'ensemble quotient $\mathbb{Z}/m\mathbb{Z}$ construit dans les Exemple 2.3.15 et Exemple 2.3.26. 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 4.1.13, 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 4.1.13 sont vérifiées. On les vérifie une par une :

— (1) de Proposition 4.1.13 : 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 4.1.13 : 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 fini de 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 4.1.14 que l'addition nous donne une structure de groupe sur $\mathbb{Z}/m\mathbb{Z}$. Plus étonnamment, 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 4.1.16, pour lequel le lemme suivant sera utile.

Lemme 4.1.15. *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 $xa + ym = 1$.*

Démonstration. Choisissons un entier n tel que $a + nm > 0$. Le Théorème 3.1.6 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 4.1.16. 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 4.1.13 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 :

$$[x][b] = [1] \ \Leftrightarrow \ [xb] = [1] \ \Leftrightarrow \ m|1 - xb \ \Leftrightarrow \ \exists y \in \mathbb{Z} : \ ym = 1 - xb \ \Leftrightarrow \ \exists y \in \mathbb{Z} : \ 1 = xb + ym \tag{4.1.c}$$

Un entier x qui satisfait la condition finale de (4.1.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 4.1.15. 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

$$(m, a) = 1 \implies (m, b) = 1 \tag{4.1.d}$$

Puisque, $[a] = [b]$ est équivalent à dire $m|a-b$, (4.1.d) est une conséquence directe de Lemme 3.1.2. Par conséquent on peut définir $(\mathbb{Z}/m\mathbb{Z})^\times$ 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 $(\mathbb{Z}/m\mathbb{Z})^\times$.

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

Pour le faire, prenons $[b] \in (\mathbb{Z}/m\mathbb{Z})^\times$. On a déjà vu que l'inverse de $[b]$ en $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ est $[x]$ ou $xb + ym = 1$ pour un entier adéquat y, et tel x existe par Lemme 4.1.15. Si x n'est pas premier avec m, alors $xb + ym = 1$ n'est pas premier avec m, ce qui est absurde. Donc $[x] \in (\mathbb{Z}/m\mathbb{Z})^\times$ comme souhaité.

Définition 4.1.17. On définit la fonction $\phi : \mathbb{Z}^{>0} \to \mathbb{Z}^{>0}$, appelée *fonction phi d'Euler*, par

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

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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	...
	$(\mathbb{Z}/2\mathbb{Z})^\times$	$(\mathbb{Z}/3\mathbb{Z})^\times$ $(\mathbb{Z}/4\mathbb{Z})^\times$ $(\mathbb{Z}/6\mathbb{Z})^\times$		$(\mathbb{Z}/5\mathbb{Z})^\times$ $(\mathbb{Z}/8\mathbb{Z})^\times$ $(\mathbb{Z}/10\mathbb{Z})^\times$		S_3 $(\mathbb{Z}/7\mathbb{Z})^\times$ $(\mathbb{Z}/9\mathbb{Z})^\times$ $(\mathbb{Z}/14\mathbb{Z})^\times$		

La contemplation de ce tableau soulève les questions suivantes :

Question 4.1.18. (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 4.1.18 servira de guide à nos efforts.

4.2 HOMOMORPHISMES DE GROUPES

Commençons avec le point (1) de la Question 4.1.18 : 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 4.2.1. 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

$$\forall g, f \in G : \ \phi(gf) = \phi(g)\phi(f). \tag{4.2.a}$$

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

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

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

(5) Deux groupes G et H sont isomorphes s'il existe un isomorphisme entres eux, et l'on note alors $G \cong H$.

Lemme 4.2.2. *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.

Démonstration. 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 | ϕ est un homomorphisme

En utilisant la simplification à droite (Proposition 4.1.5) on obtient le cas $n = 0$.

Pour $n > 0$ on démontre la proposition dans le calcul suivant :

$$\phi\left(g^n\right) = \phi(\underbrace{g \cdot \ldots \cdot g}_{\uparrow}) = \underbrace{\phi(g) \cdot \ldots \cdot \phi(g)}_{\uparrow} \underset{\uparrow}{=} \big(\phi(g)\big)^n$$

n-fois | n-fois | Notation 4.1.7 | Définition 4.2.1

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 4.1.7 :

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

on a déjà démontre le cas $n > 0$ | ϕ est un homomorphisme | Notation 4.1.7 | on a déjà démontré le cas $n = 0$

□

Exemple 4.2.3. (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 4.1.9 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

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

Pour les groupes abéliens écrits additivement, la multiplication correspond à prendre la puissance adéquate — Lemme 4.2.2

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 4.1.7 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 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.
En effet, si on regarde la Remarque 4.1.12, on voit que la structure de groupe sur G/R était supposé exactement dans la manière que l'application quotient $G \to G/R$ qui envoie g à sa classe d'équivalence R_g est un homomorphisme de groupe. En particulier, toujours quand on construit une structure de groupe sur G/R en utilisant la Proposition 4.1.13, l'application quotient $G \to G/R$ serait un homomorphisme de groupe.

(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 ϕ — e_H est l'élément neutre

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

Lemme 4.2.4. *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.*

Démonstration. Il faut juste vérifier la Définition 4.2.1 : 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 2.3.8 — ϕ est un homorphisme — ξ est un homorphisme

□

Remarque 4.2.5. Sur la série d'exercices de cette semaine il y aura deux exercices montrant, d'une manière similaire au point (4) de l'Exemple 4.2.3, que tous les groupes avec deux éléments sont isomorphes entre eux, et que tous les groupes avec trois éléments sont isomorphes entre eux.

En utilisant le point (4) de l'Exemple 4.2.3 et la Remarque 4.2.5 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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	...
	~~$(\mathbb{Z}/2\mathbb{Z})^\times$~~	~~$(\mathbb{Z}/3\mathbb{Z})^\times$~~ ~~$(\mathbb{Z}/4\mathbb{Z})^\times$~~ ~~$(\mathbb{Z}/6\mathbb{Z})^\times$~~		$(\mathbb{Z}/5\mathbb{Z})^\times$ $(\mathbb{Z}/8\mathbb{Z})^\times$ $(\mathbb{Z}/10\mathbb{Z})^\times$		S_3 $(\mathbb{Z}/7\mathbb{Z})^\times$ $(\mathbb{Z}/9\mathbb{Z})^\times$ $(\mathbb{Z}/14\mathbb{Z})^\times$		

Définition 4.2.6. 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 4.2.7 que cette définition nous donne bien un groupe.

Lemme 4.2.7. *Le groupe définit en Définition 4.2.6 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 $(g, h)^{-1} = \big(g^{-1}, h^{-1}\big)$.*

Démonstration. Il faut vérifier les trois condition de la Définition 4.1.1. 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 :

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

□

En utilisant la Définition 4.2.6 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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/5\mathbb{Z})^\times$ $(\mathbb{Z}/8\mathbb{Z})^\times$ $(\mathbb{Z}/10\mathbb{Z})^\times$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 $(\mathbb{Z}/7\mathbb{Z})^\times$ $(\mathbb{Z}/9\mathbb{Z})^\times$ $(\mathbb{Z}/14\mathbb{Z})^\times$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	...

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 4.2.8. 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 pr_F et pr_H sont des homomorphismes. Par symétrie il suffit de le vérifier pour pr_F :

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

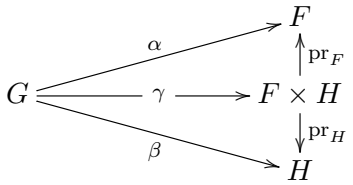
Définition 4.2.6 — définition de pr_F

Proposition 4.2.9. *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 γ est donné par la formule

$$\gamma(g) = \big(\alpha(g), \beta(g)\big) \tag{4.2.b}$$

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



Démonstration. Par la définition de pr_F et pr_H, les égalités $\mathrm{pr}_F \circ \gamma = \alpha$ et $\mathrm{pr}_H \circ \gamma = \beta$ sont équivalentes à (4.2.b). Il suffit donc de démontrer que γ avec la définition donné en (4.2.b) est un homomorphisme :

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

(4.2.b) — α et β sont des homomorphismes — définition de la multiplication pour les produits dans Définition 4.2.6 — (4.2.b)

□

En appliquant la Proposition 4.2.9 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 4.2.3, 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 4.2.3 nous donne $\delta : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$. Les homomorphismes γ et δ 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.

4.3 SOUS-GROUPES : INTRODUCTION

Définition 4.3.1. 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) $(H, \cdot|_{H\times H})$ est un groupe.

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

Proposition 4.3.2. *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.

Démonstration. $\boxed{\implies :}$ Supposons que $H \subseteq G$ est un sous-groupe. En utilisant la Définition 4.3.1, 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 4.3.1.

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 4.1.5) 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 :

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

simplification à gauche (Proposition 4.1.5)

$\boxed{\impliedby :}$ 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 4.3.1. Ainsi il suffit de démontrer la condition (2) de la Définition 4.3.1 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 :

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

(3) (2)

□

Exemple 4.3.3. On peut vérifier que les exemples suivants sont les sous-groupes en utilisant la Proposition 4.3.2 :

(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 4.3.2. On note que cela ressemble à la vérification que "mod m" nous donne une relation d'équivalence, qui est faite dans l'Exemple 2.3.15. 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 4.5 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 2.3.15.

(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 signifie que si $[x] = [y] \in \mathbb{Z}/n\mathbb{Z}$, alors $m|x \iff m|y$, ce qui est démontré dans le calcul suivant :

$$\begin{array}{ccccccc} [x] = [y] & \iff & n|x-y & \implies & m|x-y & \implies & m|x \text{ si et seulement si } m|y \\ \uparrow & & \uparrow & & \uparrow & & \\ \boxed{\text{en } \mathbb{Z}/n\mathbb{Z}} & & \boxed{\text{Exemple 2.3.15}} & & \boxed{m|n} & & \end{array}$$

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 4.3.2 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 représentation via son graphe d'une permutation avec cette propriété est

Par conséquent on a obtenu en utilisant la Proposition 4.3.2 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

$$H = \{ \sigma \in S_n \mid \forall x \in X : \ \sigma(x) = x \} \subseteq S_n$$

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

$$Z(G) = \{ g \in G \mid \forall f \in G : \ fg = gf \} \subseteq G$$

On démontre que $Z(G)$ est un sous-groupe de G en vérifiant les trois conditions de la Proposition 4.3.2 :

(i) Par la Définition 4.1.1 et par la Proposition 4.1.3, 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

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

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} :

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

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

Définition 4.3.4. Soit $\phi : G \to H$ un homomorphisme de groupes. Le *noyau* de ϕ est défini par

$$\ker \phi = \{ g \in G \mid \phi(g) = e \}$$

et l'*image* de ϕ est définie par

$$\operatorname{im} \phi = \{ \phi(g) \in H \mid g \in G \}$$

Ce sont des sous-groupes par la Proposition 4.3.5.

Proposition 4.3.5. *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.*

Démonstration. Dans les deux cas il faut vérifier les trois conditions de la Proposition 4.3.2. On le fait séparément pour $\ker \phi$ et pour $\operatorname{im} \phi$:

$\boxed{\ker \phi \text{ est un sous-groupe de } G :}$

(1) Par le Lemme 4.2.2, $\phi(e) = e$, 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 4.2.1 | $g, f \in \ker \phi$ | Définition 4.2.1

(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 4.2.2 | $g \in \ker \phi$ | un exercice d'une série

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

(1) Par Lemme 4.2.2, $\phi(e) = e$, 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 4.2.1

(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 4.2.2.

□

Exemple 4.3.6. Calculons les noyaux et les images des homomorphismes de l'Exemple 4.2.3.

(1) Pour un groupe abélien $(G, +)$, considérons $m_n : G \to G$ défini au point (1) de l'Exemple 4.2.3.

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

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 4.2.3.

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

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

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

On donne aussi plus d'exemples spécifiques de sous-groupes engendrés par un élément g de S_3 :

— 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 $\operatorname{dexp}_{[1]} : \mathbb{Z} \to {}^{\mathbb{Z}}/_{n\mathbb{Z}}$.

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

$$\operatorname{im} \operatorname{dexp}_{[1]} = {}^{\mathbb{Z}}/_{n\mathbb{Z}}$$

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

$$\phi \text{ est un isomorphisme } \Leftrightarrow \phi \text{ est injectif et } \operatorname{im}\phi = H$$

(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 4.3.3. Plus précisément :

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

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

Lemme 4.3.7. *Soit $\phi : G \to H$ un homomorphisme de groupes. On a $\ker\phi = \{e\}$ si et seulement si ϕ est injective.*

Démonstration. Si ϕ et injective, alors $\ker\phi = \{e\}$ par définition. En conséquence il suffit de montrer que si $\ker\phi = \{e\}$, alors ϕ 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 4.2.1 | Lemme 4.2.2 | $\phi(g) = \phi(h)$ | $\ker\phi = \{e\}$

□

Proposition 4.3.8. *On a $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Démonstration. 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 4.3.3. 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 4.3.3

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 4.3.7 on obtient que γ est injective. Puisque les deux groupes entrant en jeu dans la définition de γ ont chacun 6 éléments, on obtient qu'en fait γ est bijective, et ainsi γ est un isomorphisme. □

Proposition 4.3.9. *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 $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z}$.*

Démonstration. Ce sera un exercice. Comme méthode, on faut généraliser Proposition 4.3.8. □

En utilisant la Proposition 4.3.8, 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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/5\mathbb{Z})^\times$ ~~$(\mathbb{Z}/8\mathbb{Z})^\times$~~ $(\mathbb{Z}/10\mathbb{Z})^\times$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 $(\mathbb{Z}/7\mathbb{Z})^\times$ $(\mathbb{Z}/9\mathbb{Z})^\times$ $(\mathbb{Z}/14\mathbb{Z})^\times$ ~~$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$~~	$\mathbb{Z}/7\mathbb{Z}$	...

couleur bleue : groupes non-abéliens

Dans la suite (en Section 4.5), 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).

4.4 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 $\text{sgn} : S_n \to \mathbb{Z}/2\mathbb{Z} \cong \{1, -1\}$.

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

Définition 4.4.1. Un *cycle* est un élément $\sigma \in S_n$ de forme suivante :

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

où $a_1, \ldots, a_r \in \{1, \ldots, n\}$ sont éléments deux-à-deux distincts. On appelle un tel σ un r-cycle, et on dit que r est la *longueur* de σ. 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 σ, qui est bien défini par Remarque 4.4.3, et qui on dénote par $\operatorname{Supp} \sigma$.

On appelle un 2-cycle une *transposition*.

Exemple 4.4.2. 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 4.4.3. Notons que

(1) Les a_i de Définition 4.4.1 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 σ et $\tau \in S_n$ sont disjoints si $(\operatorname{Supp} \sigma) \cap (\operatorname{Supp} \tau) = \emptyset$.

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

Proposition 4.4.4. *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.*

Démonstration. C'était un 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 4.4.5.

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

Proposition 4.4.6. *Chaque $\sigma \in S_n$ est un produit des transpositions.*

Démonstration. En utilisant la Proposition 4.4.4 il suffit de démontrer le résultat pour σ un cycle $(a_1\ a_2 \dots a_r)$. On le démontre par induction sur r. Si $r = 1$ alors σ est un produit de zéro transpositions, et si $r = 2$ alors σ 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 4.4.7. La décomposition de la Proposition 4.4.6 n'est pas unique. Par exemple :

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

Définition 4.4.8. 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 σ inverse l'ordre de i et j. Dans ce cas on dit que les nombres i et j sont *en inversion* pour σ.

Exemple 4.4.9. 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 4.4.10. *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* $\operatorname{sgn}\tau = -\operatorname{sgn}\sigma$.

Démonstration. La définition de τ nous donne

$$\sigma(r) = \tau(s) \qquad \text{et} \qquad \sigma(s) = \tau(r) \tag{4.4.a}$$

Passons en revue les paires d'entiers pour trouver celles qui sont en inversion pour τ :

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

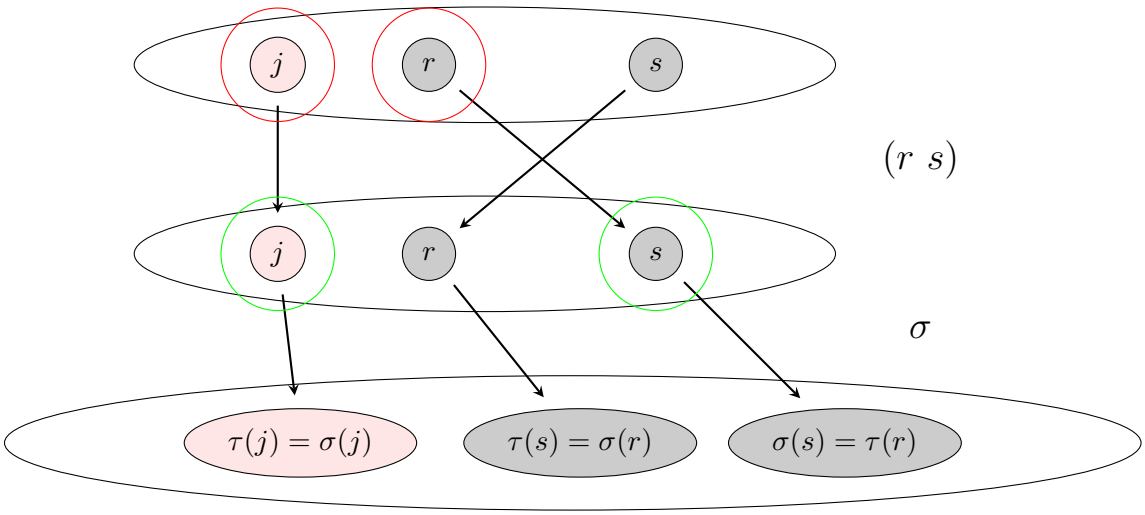
(2) *Si $j < r$ ou $j > s$, alors r et j sont en inversion pour τ si et seulement si s et j sont en inversion pour σ. Dans la même façon s et j sont en inversion pour τ si et seulement si r et j sont en inversion pour σ :* par (4.4.a) et parce que $j \neq r, s$, on a

$$\text{signe}\big(\tau(r) - \tau(j)\big) = \text{signe}\big(\sigma(s) - \sigma(j)\big) \quad \text{et} \quad \text{signe}\big(\tau(s) - \tau(j)\big) = \text{signe}\big(\sigma(r) - \sigma(j)\big), \tag{4.4.b}$$

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 τ-images des éléments entourés en rouge sont les mêmes que les σ-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).

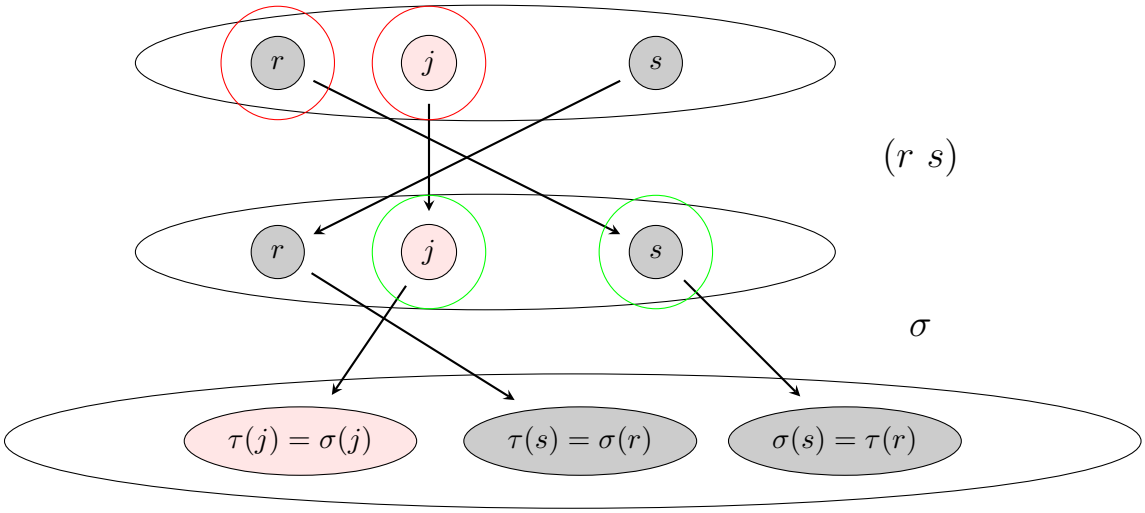


Ce dessin traite le cas $j < r$, et le cas $j > s$ peut être visualisé de la même façon.

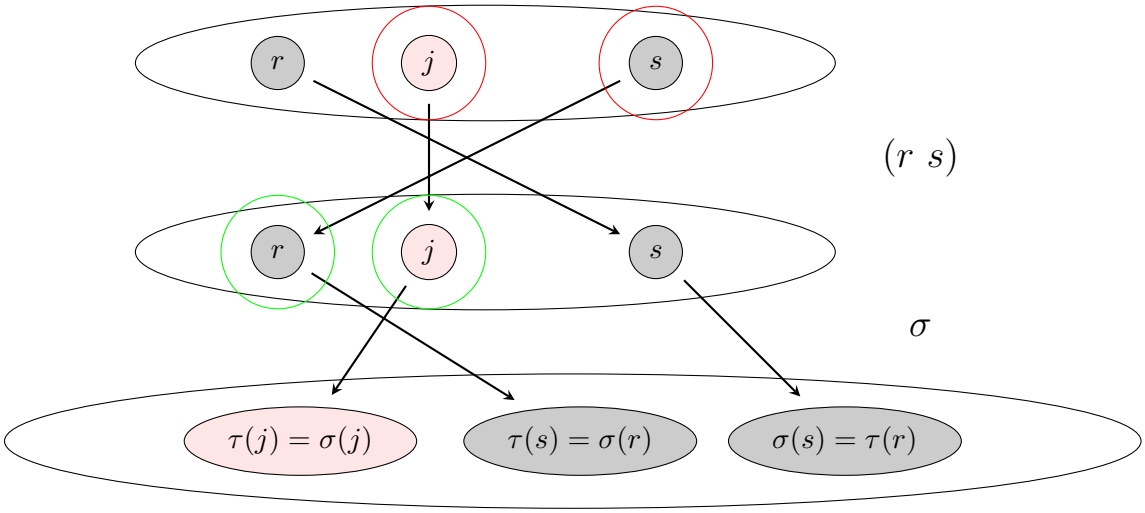
(3) *Si $r < j < s$ est un entier, alors r et j sont en inversion pour τ si et seulement si s et j ne sont pas en inversion pour σ. De la même façon s et j sont en inversion pour τ si et seulement si r et j ne sont pas en inversion pour σ.* L'équation (4.4.b) nous le donne immédiatement.

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 τ si et seulement si r et s ne sont pas en inversion pour σ :* c'est impliqué directement par (4.4.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 τ et le nombre des paires qui sont en inversion pour σ.

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 ± 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 4.4.8 à multiple produits correspondant aux points (1), (2),

(3) et (4) :

$$\operatorname{sgn}(\sigma) \underset{\boxed{\text{Définition 4.4.8}}}{\uparrow} = \prod_{1\le i<j\le n} \operatorname{signe}\big(\sigma(j)-\sigma(i)\big)$$

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

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

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

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

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

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

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

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

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

□

Corollaire 4.4.11. *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 σ.

Démonstration. Pour obtenir la première proposition du corollaire on applique Lemme 4.4.10 par induction sur r. Pour la deuxième proposition on remarque que sgn est défini d'une manière indépendante de la représentation de σ sous forme de produit de transpositions. Ainsi la seconde assertion découle de la première. □

Proposition 4.4.12. $\operatorname{sgn} : S_n \to \{1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$ *est un homomorphisme.*

Démonstration. 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 est un homomorphisme

$$\operatorname{sgn}(\sigma\tau) \underset{\boxed{\text{Corollaire 4.4.11}}}{\uparrow} = (-1)^{r+s} = (-1)^r(-1)^s \underset{\boxed{\text{Corollaire 4.4.11}}}{\uparrow} = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

□

Définition 4.4.13. On définit le *groupe alterné* $A_n := \ker\big(\operatorname{sgn} : S_n \to \mathbb{Z}/2\mathbb{Z}\big)$.

Exemple 4.4.14. On trouve les éléments de A_4 dans cet exemple. Considérons $\mathrm{id} \neq \sigma \in S_4$. Alors σ 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 4.4.6 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 4.3.9 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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/5\mathbb{Z})^\times$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 $(\mathbb{Z}/7\mathbb{Z})^\times$ $(\mathbb{Z}/9\mathbb{Z})^\times$ $(\mathbb{Z}/14\mathbb{Z})^\times$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ $(\mathbb{Z}/16\mathbb{Z})^\times$ $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^\times$

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 bleue : groupes non-abéliens

4.5 Théorème de Lagrange et premier théorème d'isomorphisme

Le premier but de cette section est la démonstration du Théorème de Lagrange (Théorème 4.5.7), qui est le premier "grand" théorème de la théorie des groupes.

Définition 4.5.1. 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 4.5.2. 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 4.3.6. 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 4.5.2, les classes à gauches ont toutes le même cardinal. Ce n'est pas une coïncidence :

Lemme 4.5.3. *Si $H \leq G$ est un sous-groupe et $g \in G$, alors $|gH| = |H|$.*

Démonstration. 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 β 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 α est une bijection et le résultat s'ensuit. □

Après l'Exemple 4.5.2 et le Lemme 4.5.3, 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 4.5.4. *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}.

Démonstration. 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 2.3.12) :

— *Réflexivité :* pour $g \in G$ on a $g^{-1}g = e_G \underset{\uparrow}{\in} H$.
Proposition 4.3.2

— *Symétrie :* pour $g, f \in G$, si $g^{-1}f \in H$, alors $f^{-1}g \underset{\uparrow}{=} \left(g^{-1}f\right)^{-1} \underset{\uparrow}{\in} H$
Proposition 4.1.6 ; $g^{-1}f \in H$ et Proposition 4.1.6

— *Transitivité :* pour $g, f, h \in G$, si $g^{-1}f$ et $f^{-1}h \in H$, alors $g^{-1}h = g^{-1}ff^{-1}h \underset{\uparrow}{\in} H$
$g^{-1}f,\ f^{-1}h \in H$ et Proposition 4.1.6

(2) Choisissons un $g \in G$. La classe d'équivalence de g est par définition (voir la Définition 2.3.16) :

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

□

Exemple 4.5.5. Soit $H = m\mathbb{Z} \subseteq \mathbb{Z} = G$. Alors, la relation d'équivalence R_H définit en Proposition 4.5.4 est la même relation d'équivalence qu'on a utilisé pour construire $\mathbb{Z}/m\mathbb{Z}$ en Exemple 2.3.15. En fait dans ce cas

$$(g,h) \in R_h \iff h - g = g^{-1}h \in H = m\mathbb{Z} \iff m | h - g$$

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

Remarque 4.5.6. 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 2.3.16) cela veut dire que $(b,c) \in R$ et $(a,c) \in R$, ce qui implique en utilisant la Proposition 2.3.19 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

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

Théorème 4.5.7. *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.

Démonstration. Soient $H_1, \dots, H_r$ les classes à gauche de H distinctes deux-à-deux. En utilisant le Lemme 4.5.3 on obtient que $|H_i| = |H|$ pour chaque entier $1 \leq i \leq r$. En utilisant la Proposition 4.5.4 et la Remarque 4.5.6 on obtient :

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

ce qui conclut. □

Définition 4.5.8. Soit G un groupe est $H \leq G$ un sous-groupe. La cardinilaté du quotient G/R_H est appelée *l'indice de H dans G*. En particulier, si le groupe G est fini, par le Théorème 4.5.7 cette cardinalité est finie et est égale à $\frac{|G|}{|H|}$. On note l'indice d'un sous-groupe H par $[G : H]$.

Lemme 4.5.9. *Si $g \in G$ est un élément d'un groupe, alors $|\langle g \rangle| = o(g)$.*

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

$$j - i < o(g) \implies g^{j-i} \neq e \implies g^j = g^i g^{j-i} \neq g^i \tag{4.5.a}$$

Dans le cas $o(g) = \infty$, (4.5.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 4.3.6

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 (4.5.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 4.5.10. *Si $g \in G$ est un élément d'un groupe fini, alors $o(g) \big| |G|$.*

Démonstration. On applique le Théorème 4.5.7 à $H = \langle g \rangle$ et on utilise le Lemme 4.5.9. □

Définition 4.5.11. Un groupe G est *cyclique* s'il existe un élément $g \in G$ tel que $\langle g \rangle = G$.

Exemple 4.5.12. 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 4.5.13. *Si G est un groupe d'ordre premier, alors G est cyclique.*

Démonstration. Choisissons $g \in G \backslash \{e\}$. Parce que $g \neq e$ on a $o(g) > 1$. D'un autre côté $o(g) \big| |G|$ par le Corollaire 4.5.10. Parce que $|G|$ est premier on obtient que $o(g) = |G|$. En utilisant le Lemme 4.5.9 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 2.3.26) 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 4.5.14. *Petit théorème de Fermat. Si a est un entier premier avec un entier positif $m > 0$, alors*

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

Démonstration. C'est une conséquence directe du Corollaire 4.5.10 et de la définition de $\phi(m)$ (voir la Définition 4.1.17). □

Après avoir récolté les fruits de notre travail sous la forme du Théorème 4.5.7, du Corollaire 4.5.10 et du Théorème 4.5.14, 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 4.5.4. 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 4.1.12. 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 4.5.15. Un sous-groupe $H \subseteq G$ est *normal*, si pour chaque $g \in G$ et $h \in H$ on a $ghg^{-1} \in H$. 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 4.5.16. L'élément ghg^{-1} dans la Définition 4.5.15 est appelé *le conjugué* de h par g.

Remarque 4.5.17. Par définition un sous-groupe $H \leq G$ est normal si et seulement si

$$\forall g \in G : \ gHg^{-1} \subseteq H, \tag{4.5.b}$$

où on utilise la notation

$$gHg^{-1} = \{\ ghg^{-1} \in G \mid h \in H\ \}.$$

On prétend que la condition (4.5.b) est équivalente à la condition

$$\forall g \in G : \ gHg^{-1} = H. \tag{4.5.c}$$

Clairement (4.5.c) implique (4.5.b), alors il suffit de démontrer que l'inverse est aussi vrai. Pour ça supposons qu'on connait (4.5.b). Ça implique que (4.5.b) est satisfait aussi quand on remplace g par g^{-1}. Autrement dit, pour chaque $g \in G$ on a

$$\begin{array}{ccc} g^{-1}Hg \subseteq H & \Leftrightarrow & H \subseteq gHg^{-1} \\ & \uparrow & \\ & \boxed{\text{en multipliant à gauche par } g \text{ et à droit par } g^{-1}} & \end{array} \tag{4.5.d}$$

En mettant ensemble le côté droit de (4.5.d) avec (4.5.b) on obtient (4.5.c).

Finalement on note que (4.5.c) est équivalent à dire que pour chaque $g \in G$ on a $gH = Hg$, ou autrement dit que les classes à gauche et à droite de H sont les mêmes.

Remarque 4.5.18. Si G est abélien, alors il découle immédiatement de la définition que tous les sous-groupes $H \leq G$ sont normaux.

Exemple 4.5.19. Le sous-groupe $H = \langle (1\ 2) \rangle \leq S_3$ n'est pas normal. En fait si on prend $g = (1\ 3)$ et $h = (1\ 2)$, alors

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

Proposition 4.5.20. *Si $\phi : G \to H$ est un homomorphisme de groupes, alors* $\ker \phi \leq G$ *est un sous-groupe normal.*

Démonstration. Par la Proposition 4.3.5, on sait que $\ker\phi$ est un sous-groupe. Fixons $g \in G$ et $h \in \ker\phi$. On démontre que $ghg^{-1} \in \ker\phi$:

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

ϕ est un homomorphisme — $h \in \ker\phi$ — Lemme 4.2.2

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

Exemple 4.5.21. En utilisant la Proposition 4.4.12, la Proposition 4.5.20 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 4.5.22. *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 4.5.4. Dans ce cas G/R_H est un groupe en utilisant les opérations définies dans la Remarque 4.1.12, et l'application suivante est un homomorphisme*

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

Démonstration. On note premièrement que par la Remarque 4.5.17 on a $gH = Hg$ pour chaque $g \in G$. On a déjà mentionné que la structure de groupe donnée dans la Remarque 4.1.12 est définie de telle manière que ξ_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 4.1.13, 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

$$(gh)^{-1}(g'h') = h^{-1}g^{-1}g'h' = h^{-1}h'\underbrace{\left(h'\right)^{-1}g^{-1}g'h'}_{\in H,\ \text{parce que } g^{-1}g' \in H \text{ et } H \subseteq G \text{ est un sous-groupe normal}} \in H$$

$h^{-1}h' \in H$

— *L'inverse est bien défini :* pour $g, g' \in G$ tels que $g^{-1}g' \in H$

$$\left(g^{-1}\right)^{-1}\left(g'\right)^{-1} = g\left(g'\right)^{-1} = \underbrace{g\left(g'\right)^{-1}gg^{-1}}_{\in H,\ \text{parce que } (g')^{-1}g = \left(g^{-1}g'\right)^{-1} \in H \text{ et } H \subseteq G \text{ est un sous-groupe normal}}$$

□

Définition 4.5.23. Pour $H \trianglelefteq G$ on appelle le groupe G/R_H de Théorème 4.5.22 *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 4.5.24. (1) Par la Remarque 4.5.18, 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 4.5.7 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 en 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 4.5.25. *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 $\eta : {}^{G}\!/_{H} \to F$ tel que le diagramme suivant commute (ce qui signifie $\eta \circ \xi = \phi$) :
$$\begin{array}{ccc} G & \xrightarrow{\xi} & {}^{G}\!/_{H} \\ & \searrow^{\phi} & \downarrow \eta \\ & & F \end{array}$$

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

Démonstration. Premièrement on rappelle que ξ est défini par $\xi(g) = gH$. Deuxièmement, notons que la condition $\eta \circ \xi = \phi$ nous force à écrire
$$\eta(gH) = \eta(\xi(g)) = \phi(g). \tag{4.5.e}$$
Autrement dit il y a juste un choix pour définir η, même comme une application d'ensembles. Pour démontrer le point (1) il faut vérifier que le η définit en (4.5.e) est bien définit est que il est un homomorphisme. Pour montrer que η 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 :
$$\big(\eta(gH)\big)^{-1}\eta(g'H) \underset{\uparrow}{=} \big(\phi(g)\big)^{-1}\phi(g') \underset{\uparrow}{=} \phi\big(g^{-1}\big)\phi(g') \underset{\uparrow}{=} \phi\big(g^{-1}g'\big) \underset{\uparrow}{=} e_F$$
(4.5.e) — Lemme 4.2.2 — ϕ est un homomorphisme — $g^{-1}g' \in H \subseteq \ker \phi$

Deuxièmement on vérifie que η 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 4.1.12 — (4.5.e) — ϕ est un homomorphisme — (4.5.e)

Ce calcul conclut le point (1).

Il nous reste à démontrer le point (2), donc on suppose à partir de maintenant que $H = \ker \phi$. Pour démontrer que η est injective, par le Lemme 4.3.7 il suffit de démontrer que $\ker \eta = \{e_{G/H}\}$:
$$gH \in \ker \eta \iff \eta(gH) = e_F \underset{\uparrow}{\iff} \phi(g) = e_F \iff g \in \ker \phi \underset{\uparrow}{\iff} g \in H \iff \underbrace{gH = e_{G/H}}_{\uparrow}$$
(4.5.e) — $H = \ker \phi$ — comme élément de ${}^{G}\!/_{H}$

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

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

□

Exemple 4.5.26. En appliquant le Théorème 4.5.25 à l'homomorphisme quotient $\xi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ et à un groupe quelconque G, on obtient la bijection suivante :

$$\begin{array}{ccc} \left\{ \text{ homorphismes } \psi : \mathbb{Z}/n\mathbb{Z} \to G \right\} & \longleftrightarrow & \left\{ \text{ homorphismes } \phi : \mathbb{Z} \to G \;\middle|\; n\mathbb{Z} \subseteq \ker\phi \right\} \\ \cup & & \cup \\ \psi & \longmapsto & \psi\circ\xi \\ \eta \text{ du Théorème 4.5.25} & \longmapsto & \phi \end{array} \tag{4.5.f}$$

De plus, en utilisant point le (2) de l'Exemple 4.2.3 en combinaison avec le point (2) de l'Exemple 4.3.6, on obtient ainsi

$$\begin{array}{ccc} \left\{ \text{ homorphismes } \phi : \mathbb{Z} \to G \;\middle|\; n\mathbb{Z} \subseteq \ker\phi \right\} & \longleftrightarrow & \left\{ g \in G \;\middle|\; o(g) | n \right\} \\ \cup & & \cup \\ \phi & \longmapsto & \phi(1) \\ \operatorname{dexp}_g & \longmapsto & g \end{array} \tag{4.5.g}$$

En combinant (4.5.f) et (4.5.g) on obtient

$$\begin{array}{ccc} \left\{ \text{ homorphismes } \psi : \mathbb{Z}/n\mathbb{Z} \to G \right\} & \longleftrightarrow & \left\{ g \in G \;\middle|\; o(g) | n \right\} \\ \cup & & \cup \\ \psi & \longmapsto & \psi([1]) \\ \eta \text{ du Théorème 4.5.25 donné par } \phi = \operatorname{dexp}_g & \longmapsto & g \end{array}$$

Exemple 4.5.27. On peut utiliser l'Exemple 4.5.26 pour compter les homomorphismes $\mathbb{Z}/n\mathbb{Z} \to G$ pour un groupe G et pour un entier $n \in \mathbb{Z}$ fixés. Prenons par exemple $n = 4$ et $G = S_4$. L'Exemple 4.5.26 nous dit que le nombre des homomorphismes $\mathbb{Z}/4\mathbb{Z} \to S_4$ est le même que le nombre d'éléments g de S_4 dont l'ordre divise 4. Par le Théorème 4.5.7, cela veut dire qu'on peut avoir $o(g) = 1, 2$ ou 4. On considère ces trois cas un par un :

(1) Il existe un seul élément d'ordre 1 : $\mathrm{id} \in S_4$.

(2) En se référant à la décomposition en cycles disjoints, il existe deux types d'éléments d'ordre 2 :
   (i) g est un 2-cycle : on a $\binom{4}{2} = 6$ choix.
   (ii) g est le produit de deux 2-cycles disjoints. Les éléments de ce type sont déterminés par l'élément qui est dans le même 2-cycle que 1. Il y a donc 3 choix possibles.

(3) Selon la décomposition en cycles disjoints, il existe un seul type d'éléments d'ordre 4 : les 4-cycles. Un 4-cycle est uniquement déterminé par l'élément $i \in \{2, 3, 4\}$ qui est l'image de 1, et par l'élément $j \in \{2, 3, 4\} \setminus \{i\}$ qui est l'image de i. On trouve $3 \cdot 2 = 6$ possibilités.

On obtient $1+6+3+6 = 16$ éléments, ce qui implique qu'il existe au total 16 homomorphismes $\mathbb{Z}/4\mathbb{Z} \to S_4$.

Corollaire 4.5.28. *Si $\phi : G \to H$ est un homomorphisme entre groupes finis, alors $|G| = |\ker\phi| \cdot |\operatorname{im}\phi|$.*

Démonstration. Par le point (2) du Théorème 4.5.25 on a ${}^{G}/_{\ker\phi} \cong \operatorname{im}\phi$. Alors le Théorème 4.5.7 conclut notre argument. □

Exemple 4.5.29. En utilisant le Théorème 4.5.25, on va faire la liste des homomorphismes $\phi : S_3 \to G$ où G est tel que $(3, |G|) = 1$ (par exemple, on peut prendre $G = {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$). Premièrement, par le Corollaire 4.5.28 on a $|\operatorname{im}\phi|\big|6$. Parce qu'on a supposé que $(3, |G|) = 1$, cela implique que $|\operatorname{im}\phi| \in \{1, 2\}$ par le Théorème 4.5.7.

On a démontré dans un exercice en série qu'il existe un unique sous-groupe normal non-trivial de S_3, à savoir le sous-groupe $H = \langle(1\ 2\ 3)\rangle$. Ecrivons ξ l'homomorphisme obtenu par la composition suivante :

l'homomorphisme quotient $S_3 \ni \sigma \mapsto \sigma\langle(1\ 2\ 3)\rangle \in {}^{S_3}/_{\langle(1\ 2\ 3)\rangle}$, comme défini dans la Définition 4.5.23 et dans le Théorème 4.5.22

$$\xi : S_3 \xrightarrow[\xi_H]{} {}^{S_3}/_{\langle(1\ 2\ 3)\rangle} \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \tag{4.5.h}$$

en utilisant le seul isomorphisme possible : ${}^{S_3}/_{\langle(1\ 2\ 3)\rangle} \ni (1\ 2)\langle(1\ 2\ 3)\rangle \longleftrightarrow [1] \in {}^{\mathbb{Z}}/_{2\mathbb{Z}}$

En utilisant les descriptions spécifiques de (4.5.h), on voit que pour $g \in S_3$:

$$\xi(g) = \begin{cases} [0] & \text{si } g = \mathrm{id},\ (1\ 2\ 3) \text{ ou } (1\ 3\ 2) \\ [1] & \text{si } g = (1\ 2), (1\ 3) \text{ ou } (2\ 3) \end{cases}$$

Par conséquent, en utilisant l'isomorphisme ${}^{\mathbb{Z}}/_{2\mathbb{Z}} \cong \{1, -1\} \subseteq (\mathbb{Q} \setminus \{0\}, \cdot)$ l'homomorphisme ξ peut être identifié avec la signature $\operatorname{sgn} : S_3 \to \{1, -1\}$. Nous n'utiliserons pas cette identification dans la suite.

Revenons maintenant aux homomorphismes $\phi : S_3 \to G$; on a déjà montré que $|\operatorname{im}\phi| \in \{1, 2\}$. Comme $\langle(1\ 2\ 3)\rangle$ est le seul sous-groupe normal de S_3, on obtient que $\langle(1\ 2\ 3)\rangle \subseteq \ker\phi$. Par conséquent on peut appliquer le point (1) du Théorème 4.5.25 avec $H = \langle(1\ 2\ 3)\rangle$. Dans ce cas on peut identifier ξ avec ξ_H, parce que les deux diffèrent seulement par la post-composition avec un isomorphisme. En utilisant l'Exemple 4.5.26 on obtient les bijections suivantes

$$\left\{ \text{homom. } \psi : S_3 \to G \right\} \longleftrightarrow \left\{ \text{homom. } \eta : {}^{\mathbb{Z}}/_{2\mathbb{Z}} \to G \right\} \longleftrightarrow \left\{ g \in G \;\middle|\; o(g) | 2 \right\}$$
$$\cup \qquad\qquad\qquad\qquad \cup \qquad\qquad\qquad\qquad \cup$$
$$\phi \longmapsto \eta \text{ du Théorème 4.5.25} \longmapsto \eta([1]) = \phi((1\ 2))$$

Exemple 4.5.30. Appliquons l'Exemple 4.5.29 à $G = {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$; il s'agit de compter les éléments de G dont l'ordre divise 2. C'est vrai pour tous les éléments de G, alors on obtient qu'il y a au total 4 homomorphismes $S_3 \to {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$.

Exemple 4.5.31. En appliquant le Corollaire 4.5.28 à $\operatorname{sgn} : S_n \to {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ On obtient que $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Corollaire 4.5.32. *Si $\phi \in G \to G$ est un homomorphisme pour un groupe fini G, alors les conditions suivantes sont équivalentes :*

(1) ϕ est un isomorphisme,

(2) ϕ est injectif, et

(3) ϕ est surjectif.

Démonstration. Par Corollaire 4.5.28 on a $|G| = |\ker\phi||\operatorname{im}\phi|$. Ainsi on voit que

$$|\ker\phi| = 1 \iff |\operatorname{im}\phi| = |G| \text{ et } |\ker\phi| = 1 \iff |\operatorname{im}\phi| = |G|,$$

lesquelles conditions sont équivalents à ϕ être injectif, bijectif ou surjectif. □

Exemple 4.5.33. On utilise aussi le Corollaire 4.5.32 pour démontrer qu'on a l'isomorphisme des groupes suivant, où multiplication dans $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est donné par composition :

$$\begin{array}{ccc} \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) & \xleftrightarrow{\cong} & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \\ \cup & & \cup \\ \phi & \longmapsto & \phi([1]) \\ m_d & \longmapsfrom & [d] \end{array} \tag{4.5.i}$$

La construction de l'application α : On a démontré dans un exercice que

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \left\{ x \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; o(x) = n \right\} \tag{4.5.j}$$

Puisque les automorphismes préserve l'ordre, on obtient que pour $\phi \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ on a

$$o\big(\phi([1])\big) = o([1]) = n.$$

Cela nous donne une application

$$\begin{array}{ccc} \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) & \xrightarrow{\alpha} & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \\ \cup & & \cup \\ \phi & \longmapsto & \phi([1]) \end{array}$$

α est un homomorphisme : On vérifie que α est un homomorphisme dans le calcul suivant où $\phi, \psi \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$:

$$\alpha(\psi \circ \phi) = \psi \circ \phi([1]) = \psi\big(\phi([1])\big) \underset{\uparrow}{=} \psi([d]) = \psi(d \cdot [1]) \underset{\uparrow}{=} d \cdot \psi([1]) = \phi([1])\psi([1]) \underset{\uparrow}{=} \psi([1])\phi([1]).$$

$\boxed{d \in \mathbb{Z} \text{ tel que } [d] = \phi([1])}$ $\boxed{\text{Lemme 4.2.2}}$ $\boxed{\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \text{ est abélien}}$

α est injectif : Pour voir que α est une injection, il faut démontrer en utilisant Lemme 4.3.7 que $\ker\alpha = \left\{\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}\right\}$. Pour cela, prenons $\phi \in \ker\alpha$. Par définition, cela veut dire que $\phi([1]) = [1]$. Alors, c'est démontré dans le calcul suivant que $\phi = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$:

$$\phi([d]) = \phi\big(d \cdot [1]\big) \underset{\uparrow}{=} d \cdot \phi([1]) = d \cdot [1] = [d].$$

$\boxed{\text{Lemme 4.2.2}}$

α est surjectif : Pour voir que α est aussi surjectif il faut juste donner pour chaque $[d] \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ un $\phi \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ tel que $\phi([1]) = [d]$. On prétend que m_d est exactement un tel isomorphisme. Pour cela il faut démontrer que m_d lui-même est bijectif. Par Corollaire 4.5.32 il suffit de démontrer que m_d est injectif. Par définition de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ on a $(d, n) = 1$. Ainsi

$$\ker m_d = \left\{ [r] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; [dr] = [0] \right\} = \left\{ [r] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; n|dr \right\} \underset{\uparrow}{=} \left\{ [r] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; n|r \right\} = \left\{[0]\right\}$$

$\boxed{(d, n) = 1}$

En somme, on a démontré l'isomorphisme de (4.5.i).

Corollaire 4.5.34. *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 ϕ est l'application constante de valeur e).*

Démonstration. En utilisant le Théorème 4.5.7 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 4.5.28, 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 4.5.35. Un exemple particulier du Corollaire 4.5.34 est qu'il n'existe que l'homomorphisme constant entre $\mathbb{Z}/16\mathbb{Z}$ et $\mathbb{Z}/25\mathbb{Z}$.

Corollaire 4.5.36. *Si $g\in G$ est un élément d'ordre fini, alors $\langle g\rangle\cong\mathbb{Z}/o(g)\mathbb{Z}$.*

Démonstration. Il suffit d'utiliser le point (2) du Théorème 4.5.25 et le point (2) de l'Exemple 4.2.3. □

Corollaire 4.5.37. *Si G est un groupe d'ordre p pour un nombre premier $p>0$, alors $G\cong\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Par le Corollaire 4.5.13 on sait que G est cyclique. Le Corollaire 4.5.36 conclut donc notre argument. □

Remarque 4.5.38. On peut mettre à jour notre tableau des petits groupes. On fait les modifications suivantes dans le tableau :

(1) Par le Corollaire 4.5.37 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 4.5.36, 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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ ~~$(\mathbb{Z}/5\mathbb{Z})^\times$~~ $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 ~~$(\mathbb{Z}/7\mathbb{Z})^\times$~~ ~~$(\mathbb{Z}/9\mathbb{Z})^\times$~~ ~~$(\mathbb{Z}/14\mathbb{Z})^\times$~~	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ ~~$(\mathbb{Z}/16\mathbb{Z})^\times$~~ $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ ~~$\mathbb{Z}/2\mathbb{Z}\times(\mathbb{Z}/5\mathbb{Z})^\times$~~

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 bleue : groupes non-abéliens

4.6 GROUPES DIÉDRAUX

Notre tableau des petits groupes est dominé jusqu'ici par des groupes abéliens. Il s'avère qu'en général, 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.

Définition 4.6.1. Pour un entier $n \geq 3$ considérons l'ensemble $V := \mathbb{Z}/n\mathbb{Z}$. On dit que $[i]$ et $[j] \in \mathbb{Z}/n\mathbb{Z}$ sont adjacents, si $[i-j] = [1]$ ou $[-1]$. Le *groupe diédral* D_{2n} est le sous-groupe du groupe symétrique S_V sur l'ensemble V contenant les éléments qui envoient chaque paire d'éléments adjacents de V sur des éléments adjacents.

Remarque 4.6.2. Pour voir que le sous-ensemble de S_V considéré dans la Définition 4.6.1 est en effet un sous-groupe, il faut vérifier les conditions de la Proposition 4.3.2. Cela est une conséquence des faits suivants :

(1) l'identité préserve l'adjacence,

(2) une composition de permutations préservant l'adjacence préserve l'adjacence, et

(3) l'inverse d'une permutation préservant l'adjacence préserve l'adjacence.

En fait, pour une structure quelconque en mathématiques, les bijections préservant cette structures forment usuellement un groupe. Par exemple, si on prend les bijections préservant la structure linéaire d'un espaces vectoriel de dimension n sur un corps k, on obtient le groupe linéaire $\mathrm{GL}(n,k)$.

Exemple 4.6.3. Considérons D_8 qui est définit en utilisant $V = \mathbb{Z}/4\mathbb{Z}$. Réfléchissons tout d'abord à quels $\alpha \in D_8$ existent avec $\alpha([0]) = [i]$ pour un élément fixé $[i] \in \mathbb{Z}/4\mathbb{Z}$. Puisque l'adjacence doit être préservée par α, on a deux possibilités :

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

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

En fait, vu que l'adjacence est préservée par ces deux applications, elles sont les deux des éléments de D_8. On dénote la première par σ_i et la deuxième par τ_i. On utilise aussi 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 vérifie la dernière equation

$$(\tau\sigma\tau)([j]) = \tau\Big(\sigma\big(\tau([j])\big)\Big) = \tau\big(\sigma([-j])\big) = \tau([1-j]) = [j-1] = \sigma^{-1}([j]). \tag{4.6.a}$$

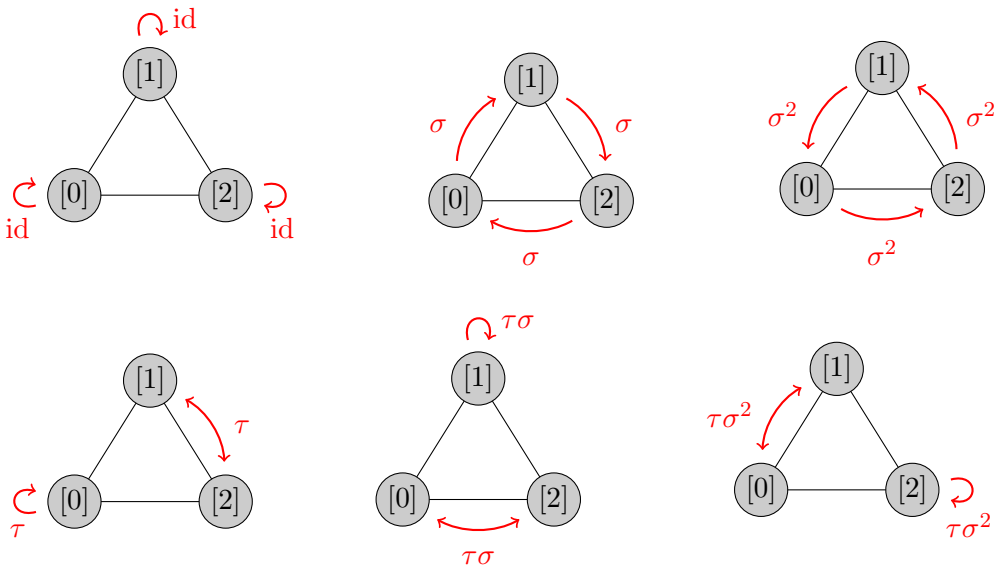
Définition 4.6.4. Pour un entier $n \geq 3$, on définit σ et $\tau \in D_{2n}$ comme dans l'Exemple 4.6.3 :
— $\sigma([j]) = [1] + [j]$ pour chaque $j \in \mathbb{Z}/n\mathbb{Z} = V$, et
— $\tau([j]) = [-j]$ pour chaque $j \in \mathbb{Z}/n\mathbb{Z} = V$.

Remarque 4.6.5. Comme dans l'Exemple 4.6.3, on voit que D_{2n} contient $2n$ éléments, qui sont les suivants :

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

Toujours comme dans l'Exemple 4.6.3, on a aussi les identités $\sigma^n = e$, $\tau^2 = e$ et $\tau\sigma\tau = \sigma^{-1}$. La démonstration de cette identité est la même, et est donc donnée par le calcul (4.6.a).

Exemple 4.6.6. On visualise les éléments de D_6 dans le diagramme au-dessous :



En particulier on voit que $D_6 = S_3$.

Remarque 4.6.7. On peut aussi définir D_{2n} comme le groupe des 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. Par 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.

En utilisant les résultats 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	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 ~~D_6~~	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ D_8

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

couleur bleue : groupes non-abéliens

4.7 SOUS-GROUPES ENGENDRÉS, GROUPES LINÉAIRES ET GROUPE DES QUATERNIONS

Lemme 4.7.1. *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.*

Démonstration. En utilisant la Proposition 4.3.2, 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 4.3.2, $e \in H_i$ 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 4.3.2 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 4.7.2. 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, pour chaque $H' \leq G$ tel que $S \subset H'$ on a $H \subseteq H'$).

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 4.7.1 (notez que l'intersection se fait sur un ensemble non-vide, puisque $S \subseteq G \leq G$).

Remarque 4.7.3. 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 4.3.6 | défini dans la Définition 4.7.2

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 4.3.2. 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 4.7.4. Dans la veine de la Remarque 4.7.3, si $S = \{g_1, \ldots, g_r\}$ est un sous-ensemble fini d'un groupe G, alors on utilise la notation $\langle g_1, \ldots, g_r\rangle$ pour $\langle S\rangle$.

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

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 4.7.5. Si $H_i = \langle g_i\rangle$ pour des éléments g_i d'un groupe G, alors $\langle H_1, \ldots, H_r\rangle = \langle g_1, \ldots, g_r\rangle$. En fait, le côté gauche est défini comme le plus petit sous-groupe qui contient tous les H_i et le côté droit est défini 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 4.7.2 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 4.7.6. *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 :*

$$\langle S \rangle = \left\{ y_1 y_2 \dots y_r \;\middle|\; \forall 1 \leq i \leq r : \; y_i \text{ ou } y_i^{-1} \in S \right\} \tag{4.7.a}$$

Démonstration. On procède par double-inclusion.
$\boxed{\supseteq :}$ Par la Proposition 4.3.2 les éléments $y_1 y_2 \dots y_r$ de (4.7.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 (4.7.a) est un sous-groupe. Grâce à la Proposition 4.3.2, il suffit de démontrer que l'ensemble de (4.7.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 (4.7.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 (4.7.a), ce qui conclut notre démonstration. □

Exemple 4.7.7. Par la Proposition 4.4.6 :

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

Autrement dit les transpositions forment une partie génératrice de S_n

Exemple 4.7.8. Pour S_3 on a

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

En utilisant le Théorème 4.5.7, 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 4.7.7. 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 exercice 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 4.7.9. Il est établi dans un exercice que tous les sous-groupes propres de A_4 sont d'ordre au plus 4. Ça implique que $\left\langle (1\ 2)(3\ 4),\ (1\ 2\ 3) \right\rangle = A_4$, parce qu'on peut donner plus que 4 éléments distincts de $\left\langle (1\ 2)(3\ 4),\ (1\ 2\ 3) \right\rangle$:

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

Exemple 4.7.10. La Remarque 4.6.5 nous dit que $\{\sigma, \tau\}$ est une génératrice de D_{2n}.

Les exemples précédents étaient sur les groupes non-abéliens. En fait, pour les groupes abéliens la situation est même plus facile, ça ressemble beaucoup à ce qu'on a vu pour les espace vectoriels. Ça veut dire que les éléments du sous-groupe engendré sont des combinaisons linéaires de la partie génératrice, mais avec coefficients en $\mathbb{Z}$ au lieu d'un corps :

Proposition 4.7.11. *Si $h, f \in G$ sont des 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 $\mathbb{Z}$

Démonstration. Il suffit de démontrer que pour $S = \{h, f\}$ on peut écrire l'expression $g = y_1 y_2 \dots y_r$ en (4.7.a) dans le forme $nh + mf$ pour $n, m \in \mathbb{Z}$. En fait, en utilisant le fait que G est abélien on peut bouger tous les y_i qui sont égaux à h ou à h^{-1} à côté gauche, et tous les y_i qui sont égaux à f ou à f^{-1} à côté droit. Après ce regroupement il faut juste noter que le produit des facteurs de premier type est égal à nh pour un $n \in \mathbb{Z}$ (écrit additivement), et le produit de deuxième type est égal à mf pour un $m \in \mathbb{Z}$. □

Exemple 4.7.12. 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 4.7.13. En itérant le Proposition 4.7.11 on obtient que si $a_1, \dots, a_r \in G$ sont éléments d'ordre finis d'un groupe abélien G, alors

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

Corollaire 4.7.14. *Si $\phi : G \to H$ est un homomorphisme et $S \subseteq G$ est un sous-ensemble, alors*

$$\phi\left(\langle S \rangle_G\right) = \langle \phi(S) \rangle_H$$

Démonstration. C'est un corollaire direct de la Proposition 4.7.6, parce que

$$g = \phi(y_1 y_2 \dots y_r) \text{ pour } y_i \text{ ou } y_i^{-1} \in S$$

$$\Updownarrow$$

$$g = \phi(y_1)\phi(y_2)\dots\phi(y_r) \text{ pour } y_i \text{ ou } y_i^{-1} \in S$$

$$\Updownarrow$$

$$g = z_1 z_2 \dots z_r \text{ pour } z_i \text{ ou } z_i^{-1} \in \phi(S)$$

□

On démontre maintenant qu'il y a un cas où le sous-groupe engendré par deux sous-groupes peut être calculé facilement. Ce cas contient la situation où l'un des sous-groupes est normal, mais on peut l'inscrire dans une situation plus générale, pour laquelle on fait la définition suivante :

Définition 4.7.15. Pour $H \leq G$ le *normalisateur* est l'ensemble de $g \in G$ tel que conjugaison par g stabilise H. Avec les formules :

$$N_G(H) = \{ \ g \in G \mid gHg^{-1} = H \ \},$$

où

$$gHg^{-1} = \{ \ ghg^{-1} \mid h \in H \ \}.$$

C'est un sous-groupe de G en utilisant le Lemme 4.7.18.

Remarque 4.7.16. Si G est fini, alors une manière équivalente de formuler la Définition 4.7.15 est :

$$N_G(H) = \left\{ g \in G \;\middle|\; \forall h \in H : \; ghg^{-1} \in H \right\} \tag{4.7.b}$$

En fait la condition de (4.7.b) est équivalente à $gHg^{-1} \subseteq H$, qui à son tour en multipliant par g à droite est équivalente à $gH \subseteq Hg$. Finalement par le Lemme 4.5.3 $gH \subseteq Hg$ est équivalent à $gH = Hg$ quand G est fini.

En revanche si G est infini, il existe des exemples qui montrent qu'on ne peut pas définir $N_G(H)$ en utilisant (4.7.b). On donnera un tel exemple dans les exercices dans quelques semaines.

Remarque 4.7.17. Considérons $H \trianglelefteq G$, qui par définition signifie que $gHg^{-1} \subseteq H$ pour chaque $g \in G$ (Définition 4.5.15). Contrairement à la situation générale expliqué dans la Remarque 4.7.16, dans ce cas on peut démontrer que en fait $gHg^{-1} = H$. La raison est la suivante : puisque H est un sous-groupe normal, conjugaison par g et par g^{-1} nous donne des automorphismes α et β, respectivement, de H. Dans ce cas ce n'est pas important que α et β sont homomorphismes. Il suffit de les traiter juste comme des applications d'ensembles $H \to H$, et ainsi on ne vérifie pas qu'ils sont des homomorphismes. Ce qui est important est que α et β sont inverses l'un de l'autre, qui nous donne qu'en fait ils sont bijectifs, et par conséquent $gHg^{-1} = H$. Cette propriété d'inverse est vérifié dans les calculs suivants :

$$\forall h \in H : \; \beta(\alpha(x)) = g^{-1}gxg^{-1}g = x \qquad \text{et} \qquad \alpha(\beta(x)) = gg^{-1}xgg^{-1} = x$$

Lemme 4.7.18. *Si $H \leq G$, alors $N_G(H)$ est un sous-groupe de G.*

Démonstration. Il faut vérifier les trois conditions du Proposition 4.3.2 :

(1) $N_G(H) \neq \emptyset$ parce que $eHe^{-1} = H$.

(2) Si $g, f \in N_G(H)$, alors $gf \in N_G(H)$ parce que :

$$gfH(gf)^{-1} = gfHf^{-1}g^{-1} \underset{\uparrow}{=} gHg^{-1} \underset{\uparrow}{=} H$$

$\boxed{f \in N_G(H)}$ $\boxed{g \in N_G(H)}$

(3) Si $g \in N_G(H)$, alors $g^{-1} \in N_G(H)$ parce que :

$$g^{-1}H\left(g^{-1}\right)^{-1} = g^{-1}Hg \underset{\uparrow}{=} g^{-1}gHg^{-1}g = H$$

$\boxed{g \in N_G(H)}$

□

Exemple 4.7.19. Considérons $g = (1\ 2\ 3\ 4) \in S_4 = G$ et $H = \langle g \rangle \leq G$. On a

$$(1\ 3)g(1\ 3) = (1\ 3)(1\ 2\ 3\ 4)(1\ 3) = (1\ 4\ 3\ 2) = g^3. \tag{4.7.c}$$

On a démontré dans un exercice que $\alpha : g \mapsto (1\ 3)g(1\ 3)$ est un automorphisme de G. Le calcul suivant nous démontre que H est stable par α :

$$\alpha(H) = \alpha(\langle g \rangle) \underset{\uparrow}{=} \langle \alpha(g) \rangle \underset{\uparrow}{=} \langle g^3 \rangle \underset{\uparrow}{=} H$$

$\boxed{\text{Corollaire 4.7.14}}$ $\boxed{(4.7.c)}$ $\boxed{g^3 \text{ est aussi une générateur de } H \text{ parce que } o(g) = 4}$

Autrement dit, on obtient que $(1\ 3) \in N_G(H)$. Pour calculer $N_G(H)$ précisément on a besoin de la Proposition 4.7.20.

Après qu'on a défini le normalisateur on peut formuler la description plus facile du sous-groupe engendré dans un cas particulier :

Proposition 4.7.20. *Si $H \leq G$ et $F \leq G$ tel que $F \subseteq N_G(H)$, 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

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

On note aussi que la condition $F \subseteq N_G(H)$ est satisfaite si $H \trianglelefteq G$.

Démonstration. Par symétrie il suffit de démontrer que $\langle H, F\rangle = HF$. Par la Proposition 4.7.6, on a $HF \subseteq \langle H, F\rangle$. Ainsi il suffit de démontrer que HF est déjà un sous-groupe. En utilisant la Proposition 4.3.2 il suffit de démontrer que $HF \neq \emptyset$, et que HF est stable pour la multiplication et l'inverse. La première de ces conditions est automatique, parce que $e = e \cdot e \in HF$.

Ainsi 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 :

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

□

Exemple 4.7.21. On continue l'Exemple 4.7.19. Grâce à l'Exemple 4.7.19 on sait que $\langle(13)\rangle \subseteq N_G(H)$. En utilisant Proposition 4.7.20 on obtient que $\langle(13)\rangle H$ est un sous-groupe de G qui est contenue dans $N_G(H)$. Parce que $\langle(13)\rangle H$ est l'union des deux classes à gauche de H il contient 8 éléments. Alors, $N_G(H)$ contient un sous-groupe d'ordre 8 est il est contenu dans G dont l'ordre est 24. En utilisant Théorème 4.5.7 on obtient que soit $N_G(H) = S_4$ ou $N_G(H) = \langle(13)\rangle H$. Cependant on peut exclure la première possibilité par le calcul suivant qui conclut la démonstration de l'égalité $N_G(H) = \langle(13)\rangle H$:

$$(1\ 2\ 3)(1\ 2\ 3\ 4)(1\ 3\ 2) = (1\ 4\ 2\ 3) \notin H$$

On a vu dans l'Exemple 4.7.21 une application de la Proposition 4.7.20 pour laquelle $F \subseteq N_G(H)$ mais $H \not\trianglelefteq G$. On donne aussi des applications pour lesquelles même $H \trianglelefteq G$ est satisfait :

Exemple 4.7.22. 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 automatique parce que le seul conjugué de e est lui-même. Le sous-groupe H contient un seul autre élément : σ^3, parce que $\sigma^6 = e$ par la Remarque 4.6.5. Ainsi il suffit de démontrer que chaque conjugué de σ^3 est aussi lui-même. Pour cela, notons d'abord que chaque élément de D_{12} est de la forme σ^i ou $\tau\sigma^i$, aussi par Remarque 4.6.5. Ainsi la vérification est donnée par les calculs suivants :

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

$$\left(\tau\sigma^i\right)^{-1}\sigma^3(\tau\sigma^i) \underset{\text{Proposition 4.1.6}}{=} \sigma^{-i}\tau^{-1}\sigma^3\tau\sigma^i \underset{\tau^2 = e \text{ par la Remarque 4.6.5}}{=} \sigma^{-i}\tau\sigma^3\tau\sigma^i \underset{\tau^2 = e}{=} \sigma^{-i}\tau\sigma\tau\tau\sigma\tau\tau\sigma\tau\sigma^i \underset{\tau\sigma\tau = \sigma^{-1}}{=} \sigma^{-i}\sigma^{-1}\sigma^{-1}\sigma^{-1}\sigma^i = \sigma^{-3} \underset{\sigma^6 = e \text{ par la Remarque 4.6.5}}{=} \sigma^3$$

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

$$\langle\sigma^3, \tau\rangle \underset{\text{Remarque 4.7.5}}{=} \langle H, F\rangle \underset{\text{Proposition 4.7.20}}{=} \{e, \tau, \sigma^3, \tau\sigma^3\}$$

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

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 4.7.23. On démontre que la Proposition 4.7.20 n'est en général pas vraie si aucun des deux sous-groupes n'est inclus dans le normalisateur de l'autre. Par exemple, prenons $H = \langle (1\ 2) \rangle$ et $F = \langle (2\ 3) \rangle$ dans S_3. Dans l'Exemple 4.7.8 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 $HFH = S_3$.

Prochainement on construit 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 4.7.24. 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 4.1.16). On dénote par $\mathrm{GL}(n, k)$ le *groupe linéaire* d'un espace vectoriel de dimension n sur k, qui peut être défini 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. La multiplication est la multiplication des matrices dans le premier cas et la composition des automorphismes dans le deuxième cas.

Exemple 4.7.25. Une matrice 2×2 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 la 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 4.7.26. Considérons 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 4.7.27 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 4.7.27), donc les notations $-e, -i, -j, -k$ ne se réfèrent pas à la structure de groupe de Q_8, mais il réfèrent à prendre la matrice $-A$ associé aux matrices $A = e$,i, j, ou k.

Proposition 4.7.27. *Le sous-ensemble Q_8 de la Définition 4.7.26 est un sous-groupe de $\mathrm{GL}(2,\mathbb{C})$. De plus on a les égalités :*

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

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

Démonstration. On vérifie les conditions de la Proposition 4.3.2. 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 4.7.28. En utilisant la Proposition 4.7.27, 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 4.5.36 on a $H \cong \mathbb{Z}/4\mathbb{Z}$, et $H \trianglelefteq G$ par le Lemme 4.7.29. Ainsi G/H est un groupe d'ordre $8/4 = 2$. Cela implique que $G/H \cong \mathbb{Z}/2\mathbb{Z}$.

Lemme 4.7.29. *Si G est un groupe fini et $H \leq G$ est tel que $[G : H] = 2$, alors $H \trianglelefteq G$.*

Démonstration. En utilisant la Remarque 4.5.17, 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 côtés 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 4.5.3) 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 4.7.30. 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 4.7.27 :

$$-e = i^2; \qquad -i = (-e) \cdot i = i^3; \qquad -j = (-e) \cdot j = j^3; \qquad k = ij; \qquad -k = (-e)ij = i^3 j$$

Exemple 4.7.31. Le groupe $G = \mathrm{GL}(n, k)$ contient beaucoup de sous-groupes intéressants. Nus donnons ici quelques exemples :

(1) $Z(G) = \{\, a \cdot I \mid a \in k \setminus \{0\} \,\}$, où I est la matrice identité (c'est-à-dire, la matrice dont les coefficients diagonaux valent 1, et dont les autres coefficients valent 0). Nous détaillons ici le cas $n = 2$, le cas général étant similaire mais plus laborieux à détailler. Considérons

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Les inverses des S et T sont les matrices suivantes, ce qu'on peut vérifier en calculant les identités $SS^{-1} = TT^{-1} = I$:

$$S = S^{-1} \text{ et } T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

Calculons le conjugué d'une matrice générale

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

par S :

$$SAS^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{22} & a_{21} \\ a_{12} & a_{11} \end{pmatrix} \tag{4.7.d}$$

et par T :

$$\begin{aligned} TAT^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a_{11} + a_{21} & a_{12} + a_{22} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_{11} + a_{21} & a_{12} + a_{22} - a_{11} - a_{21} \\ a_{21} & a_{22} - a_{21} \end{pmatrix} \end{aligned} \tag{4.7.e}$$

En utilisant (4.7.d) on obtient que si $A \in Z(G)$, alors :

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{22} & a_{21} \\ a_{12} & a_{11} \end{pmatrix} \implies a_{11} = a_{22} \text{ et } a_{12} = a_{21}$$

Si on utilise la notation $b = a_{11}$ et $c = a_{12}$, ça veut dire qu'on a

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} b & c \\ c & b \end{pmatrix}$$

En utilisant cette fois (4.7.e), on voit que si $A \in Z(G)$ alors

$$\begin{pmatrix} b & c \\ c & b \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22}-a_{11}-a_{21} \\ a_{21} & a_{22}-a_{21} \end{pmatrix}$$
$$= \begin{pmatrix} b+c & c+b-b-c \\ c & b-c \end{pmatrix} = \begin{pmatrix} b+c & 0 \\ c & b-c \end{pmatrix}$$

On obtient que $c = 0$. En conséquence on obtient que si $A \in Z(G)$ alors A est de la forme

$$A = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = b \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = bI$$

Inversement, supposons que $A = bI$. Alors A commute avec toutes les matrices : si $X \in G$,

$$XAX^{-1} = XbIX^{-1} = bXIX^{-1} = bXX^{-1} = bI = A.$$

En somme on a trouvé que $Z(G) = \left\{ bI \;\middle|\; b \in \backslash\{0\} \right\}$. Si $k = \mathbb{F}_p$, ceci implique que $|Z(G)| = p - 1$.

Nous laissons en exercice la généralisation de ce raisonnement à un entier $n > 0$ arbitraire On prétend que $Z(G)$ est beaucoup plus petit que G. Dans une autre exercice vous calculerez que

$$|\operatorname{GL}(n, \mathbb{F}_p)| = \prod_{i=0}^{n-1} \left(p^n - p^i\right)$$

Comparons l'ordre de $\operatorname{GL}(n, \mathbb{F}_p)$ et de $Z(\operatorname{GL}(n, \mathbb{F}_p))$ pour les petites valeurs de n et p dans le tableau suivant :

n	2	2	3	2
p	2	3	2	5
$\lvert\operatorname{GL}(n, \mathbb{F}_p)\rvert$	6	48	168	480
$\lvert Z(\operatorname{GL}(n, \mathbb{F}_p))\rvert$	1	2	1	4

On voit ainsi que le centre de $\operatorname{GL}(n, \mathbb{F}_p)$ est beaucoup plus petit que $\operatorname{GL}(n, \mathbb{F}_p)$ lui-même, ce qui indique que $\operatorname{GL}(n, \mathbb{F}_p)$ est très loin d'être commutatif. On précisera cette proposition dans le point final de cet exemple.

(2) On définit le *groupe projectif linéaire* $\operatorname{PGL}(n, k) := \operatorname{GL}(n, k) \Big/ Z(\operatorname{GL}(n, k))$. Notons que le centre d'un groupe et toujours un sous-groupe normal, ce qui implique que le quotient $\operatorname{GL}(n, k) \Big/ Z(\operatorname{GL}(n, k))$ est bien un groupe.

Par exemple si $k = \mathbb{F}_3$ alors dans $\operatorname{PGL}(n, \mathbb{F}_3)$ on a

$$\left[\begin{pmatrix} [2] & 0 \\ 0 & [1] \end{pmatrix}\right] = \left[\begin{pmatrix} [2] & 0 \\ 0 & [1] \end{pmatrix} \begin{pmatrix} [2] & 0 \\ 0 & [2] \end{pmatrix}\right] = \left[\begin{pmatrix} [1] & 0 \\ 0 & [2] \end{pmatrix}\right]$$

Les crochets autour des coefficients désignent les classes d'équivalence obtenues par passage au quotient $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, et les crochets autour des matrices désignent les classes d'équivalences obtenues par passage au quotient $\operatorname{GL}(n, \mathbb{F}_3) \to \operatorname{PGL}(n, \mathbb{F}_3)$.

(3) Le *tore maximal standard* $T(n, k)$ est le sous-groupe de $\operatorname{GL}(n, k)$ qui contient les matrices diagonales, c'est-à-dire les matrices de la forme

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

pour $d_i \in k \setminus \{0\}$. On démontre que $T(n,k)$ est un sous-groupe en vérifiant les conditions de la Proposition 4.3.2. Premièrement $T(n,k) \neq \emptyset$ parce que $I \in T(n,k)$. Deuxièmement $T(n,k)$ est stable par la multiplications parce que

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix} \begin{pmatrix} d'_1 & 0 & \dots & 0 \\ 0 & d'_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d'_n \end{pmatrix} = \begin{pmatrix} d_1 d'_1 & 0 & \dots & 0 \\ 0 & d_2 d'_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n d'_n \end{pmatrix}$$

Finalement $T(n,k)$ est stable par l'inversion parce que

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix} \begin{pmatrix} d_1^{-1} & 0 & \dots & 0 \\ 0 & d_2^{-1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} = I.$$

En fait, on vérifie immédiatement que pour chaque $1 \leq i \leq n$ on a un homomorphisme

$$k^\times = \big(k \setminus \{0\}, \cdot\big) \ni d \mapsto \begin{pmatrix} 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & d & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$\uparrow$$

$$\boxed{i\text{-ième colonne}}$$

et dans la même façon l'application suivante est un homomorphisme :

$$\big(k^\times\big)^{\oplus n} \ni (d_1, \dots, d_n) \mapsto \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix} \in T(n,k) \tag{4.7.f}$$

L'application décrite en (4.7.f) est clairement une bijection. On obtient que

$$\big(k^\times\big)^{\oplus n} \cong T(n,k)$$

En particulier, pour $k = \mathbb{F}_p$ on obtient que

$$\Big(\big(\mathbb{Z}/p\mathbb{Z}\big)^\times\Big)^{\oplus n} \cong T(n, \mathbb{F}_p)$$

(4) Le *sous-groupe standard de Borel* $B(n,k)$ contient les matrice de forme

$$\begin{pmatrix} * & * & \dots & * & * \\ 0 & * & \dots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & * & * \\ 0 & 0 & \dots & 0 & * \end{pmatrix} \tag{4.7.g}$$

où le symbole $*$ dénote un élément quelconque de k en-dehors de la diagonale, et un élément quelconque de $k \setminus \{0\}$ sur la diagonale – en effet, puisque $B(n,k) \subset \mathrm{GL}(n,k)$ et

que le déterminant d'un élément de la forme donnée en (4.7.g) est égal au produit des coefficients diagonaux, on voit qu'aucun coefficient diagonal ne peut être égal à 0. Comme d'habitude on va démontrer que $B(n,k)$ est un sous-groupe en montrant qu'il est stable pour la multiplication et l'inverse.

Stabilité par la multiplication : Pour montrer que le produit de deux matrices de $B(n,k)$ appartient encore à $B(n,k)$, il faut démontrer que le coefficient (i,j) d'un tel produit vaut 0 quand $i > j$, où i est le numéro de la ligne et j est le numéro de la colonne. Pour calculer un tel coefficient, il faut faire une produit d'un vecteur horizontal et d'un vecteur vertical de forme suivante :

$$\underset{\substack{\uparrow \\ \text{les entrée dans les positions} \\ \{1,\dots,i-1\} \text{ sont } 0}}{\begin{pmatrix} 0 & \dots & 0 & * & \dots & * \end{pmatrix}} \underset{\substack{\uparrow \\ \text{les entrée dans les positions} \\ \{j+1,\dots,n\} \text{ sont } 0}}{\begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix}} \tag{4.7.h}$$

On voit qu'en calculant le produit de (4.7.h) dans chaque position il y a 0 au moins dans un des vecteurs. On obtient que le produit de (4.7.h) vaut 0 si $i > j$, et est de la forme $ab \neq 0$ si $i = j$.

Stabilité par l'inversion : Il faut démontrer que l'inverse d'une matrice A telle qu'en (4.7.g) est aussi de cette forme. Pour cela, il est utile de savoir qu'on peut calculer l'inverse en utilisant l'élimination de Gauss sur les deux matrices A et I parallèlement. Comme A est déjà une matrice triangulaire supérieure, le premier pas consiste à soustraire un multiple adéquat de la dernière ligne aux autres lignes :

$$\left(\begin{array}{ccccc|ccccc} a_{11} & \dots & a_{1\ n-2} & a_{1\ n-1} & a_{1n} & 1 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & a_{n-2\ n-2} & a_{n-2\ n-1} & a_{n-2\ n} & 0 & \dots & 1 & 0 & 0 \\ 0 & \dots & 0 & a_{n-1\ n-1} & a_{n-1\ n} & 0 & \dots & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & a_{nn} & 0 & \dots & 0 & 0 & 1 \end{array}\right)$$

$$\downarrow$$

$$\left(\begin{array}{ccccc|ccccc} a_{11} & \dots & a_{1\ n-2} & a_{1\ n-1} & 0 & 1 & \dots & 0 & 0 & -\frac{a_{1\ n}}{a_{nn}} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & a_{n-2\ n-2} & a_{n-2\ n-1} & 0 & 0 & \dots & 1 & 0 & -\frac{a_{n-2\ n}}{a_{nn}} \\ 0 & \dots & 0 & a_{n-1\ n-1} & 0 & 0 & \dots & 0 & 1 & -\frac{a_{n-1\ n}}{a_{nn}} \\ 0 & \dots & 0 & 0 & 1 & 0 & \dots & 0 & 0 & \frac{1}{a_{nn}} \end{array}\right)$$

Remarquez que la même opération sur la matrice I produit une matrice du type

$$\begin{pmatrix} 1 & \dots & 0 & 0 & * \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & * \\ 0 & \dots & 0 & 1 & * \\ 0 & \dots & 0 & 0 & * \end{pmatrix}$$

On recommence ensuite le processus avec l'avant-dernière ligne et les lignes supérieures. Après avoir éliminé la $n-1$-ième colonne, la matrice de droite devient

$$\begin{pmatrix} 1 & \dots & 0 & * & * \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & * & * \\ 0 & \dots & 0 & * & * \\ 0 & \dots & 0 & 0 & * \end{pmatrix},$$

On poursuit le processus ligne après ligne, jusqu'à obtenir à gauche la matrice identité. On obtient à droite la matrice A^{-1}, qui est diagonale supérieure, et ses coefficients diagonaux sont non-nuls, puisqu'égaux à a_{ii}^{-1}. Donc l'inverse de A appartient à $B(n,k)$.

Exemples spécifiques : Voici un exemple explicite : $B(2,\mathbb{F}_2)$ contient seulement deux éléments, à savoir

$$I = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix} \qquad \text{et} \qquad I = \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}.$$

Par conséquent $B(2,\mathbb{F}_2) \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. C'est une exception : en général $B(n,\mathbb{F}_p)$ n'est pas abélien. Par exemple dans $B(2,\mathbb{F}_3)$ on a déjà des éléments qui ne commutent pas :

$$\begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}\begin{pmatrix} [2] & [0] \\ [0] & [1] \end{pmatrix} = \begin{pmatrix} [2] & [1] \\ [0] & [1] \end{pmatrix} \neq \begin{pmatrix} [2] & [2] \\ [0] & [1] \end{pmatrix} = \begin{pmatrix} [2] & [0] \\ [0] & [1] \end{pmatrix}\begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}$$

(5) Le *sous-groupe unipotent standard* $U(n,k)$ est constitué des matrices de la forme

$$\begin{pmatrix} 1 & * & \dots & * & * \\ 0 & 1 & \dots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & * \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

La démonstration que $U(n,k)$ est un sous-groupe de $\mathrm{GL}(n,k)$ est similaire au cas de $B(n,k)$ et nous la laissons en exercice.

On note que $U(n,k)$ est abélien dans davantage de cas que $B(n,k)$. Par exemple on a toujours $U(2,k) \cong (k,+)$, puisque l'application

$$k \ni a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in U(2,k)$$

est un isomorphisme, ce que l'on peut voir en utilisant l'identité suivante :

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

(6) On montre que pour $k = \mathbb{F}_p$ tel que $p \neq 2$, on a :

$$N_{\mathrm{GL}(2,k)}(T(2,k)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \in \mathrm{GL}(2,k) \;\middle|\; a,b \in k \setminus \{0\} \right\} \tag{4.7.i}$$

En utilisant la Remarque 4.7.16, il suffit de vérifier que les matrices comme dans (4.7.i) sont exactement celles avec la propriété suivante : lorsqu'on les utilise pour conjuguer une matrices quelconque diagonale inversible, on retrouve une matrices diagonale inversible. Comme $p \neq 2$ on peut prendre $c \neq d \in \mathbb{F}_p \setminus \{0\}$. Considérons la matrice diagonale inversible

$$A = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$$

et soit $\phi : k^2 \to k^2$ l'application k-linéaire associée à A. Cela signifie qu'on a $\phi(v) = Av$, lorsqu'on l'on muni l'espace de départ et d'arrivée de ϕ des bases canoniques. On prétend que les matrices en (4.7.i) sont les seules matrices qui conjuguent A à une matrice diagonale. En fait, on a appris en Algèbre linéaire que la conjugaison de A par une matrice S correspond à trouver la matrice de ϕ dans la base donné par les colonnes de S. Ainsi il suffit de démontrer que les seules bases $\{v, w\}$ de k^2 pour lesquelles la matrice de ϕ est diagonale, sont de la forme

$$\left\{\begin{pmatrix}a\\0\end{pmatrix}, \begin{pmatrix}0\\b\end{pmatrix}\right\} \qquad \text{et} \qquad \left\{\begin{pmatrix}0\\b\end{pmatrix}, \begin{pmatrix}a\\0\end{pmatrix}\right\}$$

pour quelconque $a, b \in k \setminus \{0\}$.
Pour établir cela, il suffit de démontrer que les vecteurs non-zéro $0 \neq v \in k^2$ pour lesquelles on a $\phi(v) = \lambda v$, pour quelconque $\lambda \in k$, sont les vecteurs de la forme

$$\begin{pmatrix}a\\0\end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix}0\\b\end{pmatrix}$$

Si $v = \begin{pmatrix}a\\b\end{pmatrix}$, alors l'égalité $\phi(v) = \lambda v$ nous donne

$$\begin{pmatrix}\lambda a\\ \lambda b\end{pmatrix} = \lambda v = \phi v = \begin{pmatrix}ca\\db\end{pmatrix} \underset{\boxed{0 \neq c \neq d \neq 0}}{\overset{\Longrightarrow}{\uparrow}} \lambda = c \text{ et } b = 0, \text{, ou } \lambda = d \text{ et } a = 0$$

(7) Vous avez appris (ou vous apprendrez bientôt) en Algèbre linéaire I qu'il existe une application $\det : \mathrm{GL}(n,k) \to k^\times = k \setminus \{0\}$, appelée de déterminant, telle que $\det(A)\det(B) = \det(AB)$. En particulier $\det$ est un homomorphisme. On définit le *groupe spécial linéaire* $\mathrm{SL}(n,k) := \ker \det$. Par exemple dans $\mathrm{GL}(2,\mathbb{F}_3)$ on a

$$A = \begin{pmatrix}[2] & [1]\\ [0] & [1]\end{pmatrix} \Rightarrow \det A = [2] \Rightarrow A \notin SL(2,\mathbb{F}_3)$$

et

$$B = \begin{pmatrix}[2] & [1]\\ [0] & [2]\end{pmatrix} \Rightarrow \det A = [2][2] = [1] \Rightarrow A \in SL(2,\mathbb{F}_3).$$

(8) En utilisant le Lemme 4.7.32 et le fait que $Z(\mathrm{GL}(n,k)) \trianglelefteq \mathrm{GL}(n,k)$, on obtient que $Z(\mathrm{GL}(n,k)) \cap \mathrm{SL}(n,k) \trianglelefteq \mathrm{SL}(n,k)$. On définit alors le *groupe spécial projectif linéaire*

$$\mathrm{PSL}(n,k) = \mathrm{SL}(n,k) \Big/ Z(\mathrm{GL}(n,k)) \cap \mathrm{SL}(n,k)$$

En utilisant $\mathrm{PSL}(n,\mathbb{F}_q)$ on peut préciser de quelle manière $\mathrm{GL}(n,\mathbb{F}_q)$ est très loin d'être non-abélien : en effet, $\mathrm{PSL}(n,\mathbb{F}_q)$ est simple pour $n \geq 2$ sauf deux cas : $n = 2$ et $q = 2$ ou $q = 3$. Nous ne démontrerons pas ce théorème dans ce cours.

Remarquons finalement que les groupes définis dans l'exemple précédent ont tous une structure de *groupe algébrique*. Cela signifie qu'ils sont des variétés algébriques et que leurs opérations de groupe sont des morphismes de variétés algébriques. Ce sont des notions de Géométrie Algébrique, que vous aborderez dans vos 3e et 4e années d'étude à l'EPFL. Nous nous contenterons pour l'instant d'une explication intuitive : être un groupe algébrique signifie être l'ensemble de solutions de certains polynômes, et que les opérations (multiplication et inversion) sont elles aussi définies par des polynômes. Ces propriétés donnent beaucoup de structures additionnelles sur ces groupes, et l'on peut utiliser ses structures pour mieux étudier et appliquer ces groupes.

Lemme 4.7.32. *Si $H \trianglelefteq G$ et $F \leq G$, alors $F \cap H \trianglelefteq F$.*

Démonstration. Il faut montrer que pour tout $f \in F$ et pour tout $h \in F \cap H$ on a $f^{-1}hf \in F \cap H$. En utilisant la Proposition 4.3.2 et que tous les éléments concernés sont contenus dans F, on obtient que $f^{-1}hf \in F$. Ainsi il suffit de démontrer que $f^{-1}hf \in H$, ce que l'on obtient en utilisant que H est normal dans G. □

On peut ajouter Q_8 et quelques sous-groupes de $\mathrm{GL}(n, \mathbb{F}_p)$ à notre tableau des petits groupes. Pour y mettre les sous-groupes de $\mathrm{GL}(n, \mathbb{F}_p)$ il faut utiliser les expressions des ordres de ces groupes démontré dans un exercice :

(1) $|\mathrm{GL}(n, \mathbb{F}_p)| = \prod_{i=0}^{n-1} (p^n - p^i)$

(2) $|\mathrm{SL}(n, \mathbb{F}_p)| = \frac{\prod_{i=0}^{n-1}(p^n - p^i)}{p-1}$

(3) $|\mathrm{PGL}(n, \mathbb{F}_p)| = \frac{\prod_{i=0}^{n-1}(p^n - p^i)}{p-1}$

(4) $B(n, \mathbb{F}_p) = (p-1)^n p^{\binom{n}{2}}$

(5) $U(n, \mathbb{F}_p) = p^{\binom{n}{2}}$

(6) $|\mathrm{PSL}(n, \mathbb{F}_p)| = \left(\prod_{i=0}^{n-1} (p^n - p^i) \right) \Big/ \left((p-1) \cdot \left| (\mathbb{Z}/p\mathbb{Z})^\times : \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^n \right| \right)$, où

$$\left((\mathbb{Z}/p\mathbb{Z})^\times\right)^n = \left\{ x^n \in (\mathbb{Z}/p\mathbb{Z})^\times \;\middle|\; x \in (\mathbb{Z}/p\mathbb{Z})^\times \right\} = n \cdot (\mathbb{Z}/p\mathbb{Z})^\times$$

Vous démontrerez ce point juste après apprenant le deuxième théorème d'isomorphisme (Proposition 4.8.1) dans Section 4.8.

ordre	1 ✓	2 ✓	3 ✓	4	5 ✓	6	7 ✓	8
groupes	le groupe trivial	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 $\mathrm{GL}(2, \mathbb{F}_2)$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ D_8 Q_8 $U(3, \mathbb{F}_2)$

9	10	11 ✓	12	13 ✓	14	15	...
$\mathbb{Z}/9\mathbb{Z}$ $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$	$\mathbb{Z}/10\mathbb{Z}$ D_{10}	$\mathbb{Z}/11\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$ A_4 $\mathbb{Z}/2\mathbb{Z} \times S_3$ $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ D_{12} $B(2, \mathbb{F}_3)$ $\mathrm{PSL}(2, \mathbb{F}_3)$	$\mathbb{Z}/13\mathbb{Z}$	$\mathbb{Z}/14\mathbb{Z}$ D_{14}	$\mathbb{Z}/15\mathbb{Z}$	...

couleur bleue : groupes non-abéliens

4.8 Deuxième théorème d'isomorphisme et les produits semi-directs

On a vu dans la Proposition 4.7.20 que si $H, F \leq G$ et $F \leq N_G(H)$, alors $\langle H, F\rangle = FH$. A la suite de cette proposition, il est naturel de se demander si on peut déterminer précisément la structure de FH, modulo isomorphisme. La réponse est oui quand $H \cap F = \{e\}$, et constitue le but principal de cette section.

L'étape principale sera de démontrer, dans la Proposition 4.8.1, que si $H \cap F = \{e\}$, alors les éléments de F sont en bijection avec les classes à gauche de H, via la fonction $f \mapsto fH$. Cela nous donnera, dans le Corollaire 4.8.2, que l'ensemble $F \times H$ est en bijection avec FH, via la fonction $(f, h) \mapsto fh$. Même si cette dernière fonction n'est en général pas un homomorphisme de groupes, cette information nous permettra de comprendre aisément la structure de groupe de FH.

Pour montrer la bijection entre F est les classes à gauche de H, l'outil principal est le deuxième théorème d'isomorphisme, énoncé dans la Proposition 4.8.1 (le premier théorème d'isomorphisme était le point (2) du Théorème 4.5.25). Pour comprendre cette proposition, il est utile de noter qu'en utilisant le Lemme 4.7.32 on peut former le quotient $F/F \cap H$.

Proposition 4.8.1. *Deuxième théorème d'isomorphisme* *Soit G un groupe. Si $H, F \leq G$ et $F \leq N_G(H)$, alors l'application*

$$\begin{array}{ccc} F/F\cap H & \longrightarrow & FH/H = HF/H \\ \cup & & \cup \\ f(F\cap H) & \longmapsto & fH = Hf \\ & & \uparrow \\ & & \boxed{F \subseteq N_G(H)} \end{array}$$

est un isomorphisme.

Démonstration. Notons premièrement que par la Proposition 4.7.20, on a $HF = FH = \langle H, F\rangle$. Par conséquent, puisque $N_G(H)$ est un sous-groupe de G (Lemme 4.7.18), on obtient que $FH \subseteq N_G(H)$, ce qui implique que $H \trianglelefteq FH$.

Considérons maintenant l'homomorphisme quotient $\phi : FH \to FH/H$, et restreignons-le à F. Cela donne l'homomorphisme $\phi|_F : F \to FH/H$ qui envoie f sur la classe $fH \in FH/H$. On obtient l'isomorphisme de notre proposition en appliquant le point (2) du Théorème 4.5.25 à $\phi|_F$, après avoir démontré que $\ker(\phi|_F) = F \cap H$ et que $\phi|_F$ est surjectif :

$\boxed{\ker(\phi|_F) = F \cap H :}$ Par définition de l'homomorphisme quotient $\ker\phi = H$, et ainsi :

$$\ker(\phi|_F) = \{\ f \in F \mid \phi(f) = e\ \} = (\ker\phi) \cap F = H \cap F.$$

$\boxed{\phi|_F \text{ est surjectif :}}$ Par définition FH est recouvert par les classes à gauche de H de la forme fH, où $f \in F$. On obtient que

$$FH/H = \{\ fH \mid f \in F\ \}.$$

Puisque $\phi(f) = fH$ on voit que $\phi|_F$ est surjectif. □

Corollaire 4.8.2. *Si $H, F \leq G$ et $F \leq N_G(H)$ tel que $F \cap H = \{e\}$, alors l'application suivante entre ensembles est bijective :*

$$\begin{array}{rccc} \xi : & H \times F & \longrightarrow & HF \\ & \cup & & \cup \\ & (h, f) & \longmapsto & hf \end{array}$$

Démonstration. Par la Proposition 4.8.1 on voit que $\eta : f \mapsto Hf$ induit une bijection entre les éléments de F et les classes à droite de H dans HF. Choisissons $g \in HF$. Par la Proposition 4.5.4, il existe une unique classe à gauche Hf telle que $g \in Hf$, et puisque η est bijective, ce $f \in F$ est unique. Cela implique qu'on peut écrire $g = hf$ pour $f \in F$ et $h \in H$, et en plus f est uniquement déterminé. Cependant dans l'expression $g = hf$, l'élément h est aussi uniquement déterminé, parce qu'on a $h = gf^{-1}$. Puisque c'est vrai pour chaque $g \in HF$, on obtient que ξ est bijective. □

On note que la fonction ξ dans le Corollaire 4.8.2 n'est pas un isomorphisme de groupes si on munit $H \times F$ de la structure de groupe habituelle. En effet :

$$(hf)(\tilde{h}\tilde{f}) = \underbrace{hf\tilde{h}f^{-1}}_{\in H \text{ parce que } H \trianglelefteq HF} f\tilde{f} \tag{4.8.a}$$

et donc

$$\xi\big((h,f)\cdot(\tilde{h},\tilde{f})\big) = \xi\big((hf\tilde{h}f^{-1}, f\tilde{f})\big)$$

et si ξ était un homomorphisme pour la structure de produit sur $H \times F$, alors par injectivité on obtiendrait $(h,f)\cdot(\tilde{h},\tilde{f}) = (hf\tilde{h}f^{-1}, f\tilde{f})$, ce qui n'est pas vrai en général.

Il est cependant possible de changer la structure de groupe sur $H \times F$ afin que cette fonction ξ devienne un isomorphisme de groupes. Pour cela, il est important de mieux comprendre comment la conjugaison $f\tilde{h}f^{-1}$ dépend de f :

Définition 4.8.3. Soit $H \leq G$ et $g \in N_G(H)$. On définit Ad_g^H l'application

$$\begin{array}{rccc} \mathrm{Ad}_g^H : & H & \longrightarrow & H \\ & \cup & & \cup \\ & h & \longmapsto & ghg^{-1} \end{array}$$

On va démontrer, dans le Lemme 4.8.4 ci-dessous, que $\mathrm{Ad}^H(g)$ est un isomorphisme, donc on peut écrire $\mathrm{Ad}_g^H \in \mathrm{Aut}(H)$.

Soit $F \leq N_G(H)$. On va également démontrer dans le Lemme 4.8.4 que l'application

$$\begin{array}{rccc} \mathrm{Ad}_F^H : & F & \longrightarrow & \mathrm{Aut}(H) \\ & \cup & & \cup \\ & f & \longmapsto & \mathrm{Ad}_f^H \end{array}$$

est un homomorphisme, qui on appelle la *représentation adjointe de F sur H*.

Notons que le point (1) a été démontré en série d'exercices dans le cas $H = G$. La démonstration est la même, mais par souci d'exhaustivité on la répète ici.

Lemme 4.8.4. *Si $H, F \leq G$, $g \in N_G(H)$ et $F \leq N_G(H)$, alors*

(1) $\mathrm{Ad}_g^H \in \mathrm{Aut}(H)$

(2) Ad_F^H *est un homomorphisme* $F \to \mathrm{Aut}(H)$.

Démonstration. (1) On vérifie premièrement que Ad_g^H est un homomorphisme. C'est démontré dans le calcul suivant pour $h, h' \in H$:

$$\Big(\mathrm{Ad}_g^H(hh')\Big) = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = \Big(\mathrm{Ad}_g^H(h)\Big)\Big(\mathrm{Ad}_g^H(h')\Big)$$

Par Lemme 4.7.18, $N_G(H)$ est un sous-groupe de G. Par conséquent, $g^{-1} \in N_G(H)$ et alors $\mathrm{Ad}_{g^{-1}}^H \in \mathrm{End}(H)$ aussi. Le calcul suivant démontre que $\mathrm{Ad}_{g^{-1}}^H$ est en fait l'inverse de

Ad_g^H, ce qui implique que Ad_g^H n'est pas simplement un homomorphisme, mais aussi un isomorphisme :

$$\mathrm{Ad}_{g^{-1}}^H\left(\mathrm{Ad}_g^H(h)\right) = g^{-1}(ghg^{-1})g = h,$$

et

$$\mathrm{Ad}_g^H\left(\mathrm{Ad}_{g^{-1}}^H(h)\right) = g(g^{-1}hg)g^{-1} = h.$$

(2) Pour vérifier que Ad_F^H est un homomorphisme, il faut montrer que pour chaque $f, \tilde{f} \in F$ on a

$$\mathrm{Ad}_f^H \circ \mathrm{Ad}_{\tilde{f}}^H = \mathrm{Ad}_{f\tilde{f}}^H \tag{4.8.b}$$

Parce que les tous les deux côtés de l'équation désiré (4.8.b) sont des application, pour vérifier (4.8.b) il faut démontrer que, pour un élément quelconque $h \in H$, ces deux applications envoient h vers la même image. On le fait dans le calcul suivant, qui conclut notre démonstration :

$$\left(\mathrm{Ad}_f^H \circ \mathrm{Ad}_{\tilde{f}}^H\right)(h) = \mathrm{Ad}_f^H\left(\tilde{f}h\tilde{f}^{-1}\right) = f\tilde{f}h\tilde{f}^{-1}f^{-1} = f\tilde{f}h\left(f\tilde{f}\right)^{-1} = \mathrm{Ad}_{f\tilde{f}}^H(h).$$

□

Exemple 4.8.5. Si G est abélien, alors la conjugaison par tout élément est triviale, et alors Ad_F^H est l'homomorphisme trivial pour tous les sous-groupes $H, F \leq G$.

Exemple 4.8.6. Considérons $H = \langle\sigma^2\rangle$ et $F = \langle\tau\rangle$ dans D_{12}. Puisque $o(\sigma) = 6$, on a $H = \{\mathrm{id}, \sigma^2, \sigma^4\}$. On a vu dans un exercice que $\{\sigma^2, \sigma^4\}$ est une classe de conjugaison de D_{12}. En utilisant que $\{e\}$ est toujours une classe de conjugaison, on obtient que $H \trianglelefteq G$, et en particulier $F \subseteq N_G(H)$. On peut alors regarder Ad_F^H. Par définition $\mathrm{Ad}_F^H(\tau) \in \mathrm{Aut}(H)$ est tel que

$$\left(\mathrm{Ad}_F^H(\tau)\right)(\sigma^{2i}) = \tau\sigma^{2i}\tau^{-1} \underset{\boxed{o(\tau)=2}}{\uparrow} = \tau\sigma^{2i}\tau \underset{\boxed{\sigma\tau = \tau\sigma^{-1} \text{ par la Remarque 4.6.5}}}{\uparrow} = \tau\tau\sigma^{-2i} = \sigma^{-2i}$$

Plus explicitement :

$$\left(\mathrm{Ad}_F^H(\tau)\right)(\sigma^2) = \sigma^4 \qquad \left(\mathrm{Ad}_F^H(\tau)\right)(\sigma^4) = \sigma^2$$

Notons que :

— Puisque $|H| = 3$, on a $H \cong \mathbb{Z}/3\mathbb{Z}$.

— Puisqu'exactement deux éléments de $\mathbb{Z}/3\mathbb{Z}$ sont des générateurs, il existe un seul automorphisme différent de l'identité, lequel échange ces deux générateurs (Exemple 4.5.33). On obtient que $\mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z}$, et que $\mathrm{Ad}_F^H(\tau) \in \mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z}$ est le seul élément non-neutre.

En particulier, en utilisant (4.8.a) on obtient que

$$(\sigma^2\tau)(\sigma^2\tau) = \sigma^2\left(\left(\mathrm{Ad}_F^H(\tau)\right)(\sigma^2)\right)\tau\tau = \sigma^2\sigma^4\tau\tau = \mathrm{id} \neq \sigma^4 = \sigma^2\sigma^2\tau\tau.$$

Cela nous donne un exemple explicite, où la bijection ξ du Corollaire 4.8.2 ne donne pas une isomorphisme entre les groupes $H \times F$ et HF.

Exemple 4.8.7. Prenons $G = S_4$ et $H = A_4$. Dans ce cas on a vu que $H \trianglelefteq G$ dans l'Exemple 4.5.21, ou autrement dit $N_G(H) = G$. Cela veut dire qu'on peut calculer Ad_F^H pour $F = \langle (1\ 2) \rangle$. C'est un homomorphisme

$$\begin{array}{ccccc} \mathrm{Ad}_F^H : & \mathbb{Z}/2\mathbb{Z} & \cong & F & \to \mathrm{Aut}(H) \leq \mathrm{Bij}_H = S_H \\ & \uparrow & & & \\ & \boxed{[1] \longleftrightarrow (1\ 2)} & & & \end{array}$$

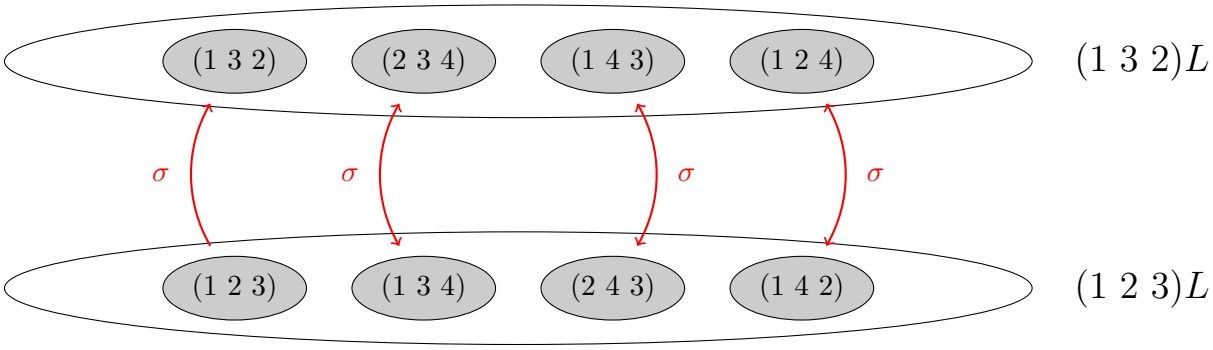
Par conséquent, cette fonction est déterminée par $\sigma = \mathrm{Ad}_F^H\big((1\ 2)\big) \in S_H$. En d'autres termes : la conjugaison par $(1\ 2)$ induit une permutation σ des éléments de H, et Ad_F^H et déterminé par cette permutation. Cette permutation est calculable à la main. On calcule en-dessous les images de quelques éléments par σ :

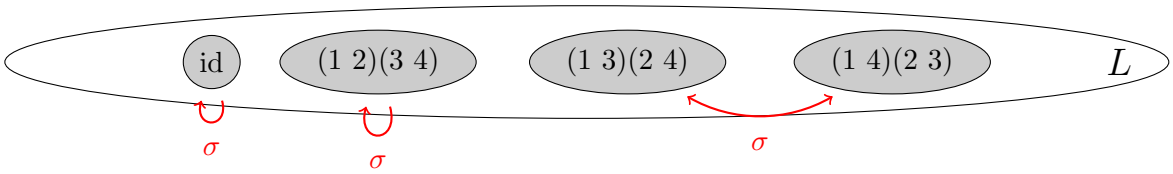
$$\sigma\Big((1\ 2)(3\ 4)\Big) = (1\ 2)\Big((1\ 2)(3\ 4)\Big)(1\ 2) = (1\ 2)(3\ 4)$$

$$\sigma\Big((1\ 3)(2\ 4)\Big) = (1\ 2)\Big((1\ 3)(2\ 4)\Big)(1\ 2) = (1\ 4)(2\ 3)$$

$$\sigma\big((1\ 2\ 3)\big) = (1\ 2)\big((1\ 2\ 3)\big)(1\ 2) = (1\ 3\ 2)$$

Avoir calculé les images des quelques éléments par σ, on visualise les autres images, et on vous laisse de vérifier cette représentation en faisant les calculs (L dénote le seul sous-groupe normal de A_4) :





La structure de groupe alternative qu'on a promis sur l'ensemble $H \times F$ est la suivante :

Définition 4.8.8. Soient H, F deux groupes et $\phi : F \to \mathrm{Aut}(H)$ un homomorphisme. On écrit $\phi_f = \phi(f)$ pour simplifier la notation.

Le *produit semi-direct* $H \rtimes_\phi F$ de H et F par rapport à ϕ est le groupe sur l'ensemble $H \times F$ pour lequel la multiplication est donnée par la formule suivante, pour tous les éléments (h, f) et $\big(\tilde{h}, \tilde{f}\big)$ de l'ensemble $H \times F$:

$$(h, f) \cdot \big(\tilde{h}, \tilde{f}\big) = \Big(h \cdot \phi_f\big(\tilde{h}\big), f \cdot \tilde{f}\Big) \tag{4.8.c}$$

Il est démontré dans la Proposition 4.8.10 que cette règle de multiplication donne bien un groupe.

Remarque 4.8.9. Notons que si ϕ est trivial dans Définition 4.8.8, alors $H \rtimes_\phi F = H \times F$, parce que dans ce cas-là $\phi_f(\tilde{h}) = \tilde{h}$ dans (4.8.c).

Proposition 4.8.10. *Dans la situation de la Définition 4.8.8, $H \rtimes_\phi F$ est un groupe.*
De plus :

(1) l'élément neutre est (e_H, e_F),

(2) $(h,f)^{-1} = \Big(\big(\phi_{f^{-1}}(h)\big)^{-1}, f^{-1}\Big)$,

(3) le sous-ensemble $H' = H \times \{e_F\}$ est un sous-groupe normal,

(4) le sous-ensemble $F' = \{e_h\} \times F$ est un sous-groupe,

(5) les applications

$$\iota_H : H \ni h \ \mapsto \ (h, e_F) \in H \rtimes_\phi F$$

et

$$\iota_F : F \ni f \ \mapsto \ (e_h, f) \in H \rtimes_\phi F$$

nous donnent des isomorphismes $H \cong H'$ et $F \cong F'$, respectivement, et

(6) en utilisant les isomorphismes du point précédent, $\mathrm{Ad}^{H'}_{F'}$ s'identifie avec ϕ, ce qui signifie que pour $f \in F$ et $h \in H$ on a

$$\mathrm{Ad}^{H'}_{\iota_F(f)}\big(\iota_H(h)\big) = \iota_H\big(\phi(h)\big).$$

Démonstration. Par la Définition 4.1.1, il faut vérifier que la multiplication est associative, et que les formules dans l'énoncé nous donnent un élément neutre ainsi que des inverses. Dans le calcul suivant $g, g', g'' \in G$ et $h, h', h'' \in H$. On commence avec l'existence de l'élément neutre :

$$(e_H, e_F)(h,f) = \Big(e_H \cdot \phi_{e_F}(h),\ e_F \cdot f\Big) \underset{\uparrow}{=} \big(e_H \cdot h,\ e_F \cdot f\big) = (h,f)$$

$\boxed{\phi_{e_F} = \mathrm{id}_H \text{ parce que } \phi : F \to \mathrm{Aut}(H) \text{ est un homomorphisme}}$

Deuxièmement on vérifie l'inverse :

$$\Big(\big(\phi_{f^{-1}}(h)\big)^{-1},\ f^{-1}\Big)(h,f) = \Big(\big(\phi_{f^{-1}}(h)\big)^{-1} \cdot \phi_{f^{-1}}(h),\ f^{-1} \cdot f\Big) = (e_H, e_F)$$

Finalement on vérifie l'associativité :

$$\Big((h,f)(h',f')\Big)(h'',f'') = \Big(h \cdot \phi_f(h'),\ f \cdot f'\Big)(h'',f'') = \Big(h \cdot \phi_f(h') \cdot \phi_{f\cdot f'}(h''),\ f \cdot f' \cdot f''\Big)$$
$$\underset{\uparrow}{=} \Big(h \cdot \phi_f(h') \cdot \phi_f\big(\phi_{f'}(h'')\big),\ f \cdot f' \cdot f''\Big) \underset{\uparrow}{=} \Big(h \cdot \phi_f\big(h' \cdot \phi_{f'}(h'')\big),\ f \cdot f' \cdot f''\Big)$$

$\boxed{\phi : F \to \mathrm{Aut}(H) \text{ est un homomorphisme}}$ $\boxed{\phi_f \in \mathrm{Aut}(H)}$

$$= (h,f)\Big(h' \cdot \phi_{f'}(h''),\ f' \cdot f''\Big) = (h,f)\Big((h',f')(h'',f'')\Big)$$

On ainsi démontré que $H \rtimes_\phi F$ est un groupe et en passant les points (1) et (2).

Pour prouver que H' et F' sont des sous-groupes il suffit de démontrer le point (5). En effet par définition $H' = \mathrm{im}\,\iota_H$ et $F' = \mathrm{im}\,\iota_F$, et alors on obtient que H' et F' sont des sous-groupes en utilisant la Proposition 4.3.5. Ainsi on fait les calculs pour démontrer que ι_H et ι_F sont des homomorphismes, où $h, h' \in H$ et $f, f' \in f$:

$$\iota_H(h)\iota_H(h') = (h, e_F)(h', e_F) = \big(h \cdot \phi_{e_f}(h'), e_F \cdot e_F\big) \underset{\uparrow}{=} (hh', e_F) = \iota_H(hh')$$

puisque ϕ est un homomorphisme, l'image de l'élément neutre est l'élément neutre (Lemme 4.2.2), ou autrement dit $\phi_{e_F} = e_{\mathrm{Aut}(H)} = \mathrm{Id}_H$

$$\iota_F(f)\iota_F(f') = (e_H, f)(e_H, f') = \big(e_H \cdot e_H, f \cdot f'\big) = \iota_F(ff')$$

Ces calculs concluent le point (5), et par conséquent aussi le point (4) comme expliqué au-dessus.

Pour montrer le point (3) il nous reste à vérifier que H' est en fait un sous-groupe normal :

$$\begin{aligned}(h, f)(h', e_F)(h, f)^{-1} &= (h, f)(h', e_F)\left(\left(\phi_{f^{-1}}(h)\right)^{-1}, f^{-1}\right)\\ &= \left(h \cdot \phi_f(h'), f\right)\left(\left(\phi_{f^{-1}}(h)\right)^{-1}, f^{-1}\right) = \left(h \cdot \phi_f(h') \cdot \phi_f\left(\left(\phi_{f^{-1}}(h)\right)^{-1}\right), e_f\right) \in H'\end{aligned}$$

Avec ce calcul on a démontré le point (3).

Il nous reste de démontrer le point (6). C'est fait dans le calcul suivant, où $f \in F$ et $h \in H$ sont arbitraires :

$$\begin{aligned}\mathrm{Ad}^{H'}_{\iota_F(f)}\big(\iota_H(h)\big) = \mathrm{Ad}^{H'}_{(e_H,f)}\big((h, e_F)\big) &= (e_H, f)(h, e_F)(e_H, f)^{-1}\\ &\overset{\uparrow}{=} (e_H \cdot \phi_f(h), f \cdot e_F)\left(\left(\phi_{f^{-1}}(e_H)\right)^{-1}, f^{-1}\right) \overset{\uparrow}{=} (\phi_f(h), f)(e_H, f^{-1})\end{aligned}$$

par la définition de la multiplication dans $H \rtimes_\phi F$, et par le point (2) du thorème actuel, qu'on a déjà démontré

$\phi_{f^{-1}} \in \mathrm{Aut}(H)$, donc $\phi_{f^{-1}}(e_H) = e_H$

$$= \big(\phi_f(h) \cdot \phi_f(e_H), ff^{-1}\big) \overset{\uparrow}{=} \big(\phi_f(h) \cdot e_H, e_F\big) = \big(\phi_f(h), e_F\big) = \iota_H\big(\phi(h)\big).$$

$\phi_f \in \mathrm{Aut}(H)$, alors $\phi_f(e_H) = e_H$

□

Remarque 4.8.11. On a implicitement démontré dans la Proposition 4.8.10 que $H \rtimes_\phi F$ est abélien si et seulement si H et F sont abéliens et que ϕ est trivial. On explique les deux directions de cette affirmation ci-dessous :

$\Longleftarrow$: Si ϕ et trivial, qui veut dire que $\phi \equiv \mathrm{id}_H$, alors $H \rtimes_\phi F \cong H \times F$ par la Remarque 4.8.9, et $H \times F$ est abélien si (et seulement si) H et F sont tous deux abéliens.

$\Longrightarrow$: Si $H \rtimes_\phi F$ est abélien, alors tous ses sous-groupes sont abéliens et toutes les représentations adjointes sont triviales par Exemple 4.8.5. On obtient par les points (5) et (6) de la Proposition 4.8.10 qui H et F sont abéliens et que ϕ est trivial.

Exemple 4.8.12. Si $H \cong \mathbb{Z}/n\mathbb{Z}$, alors par l'Exemple 4.5.33 on a

$$\begin{array}{ccc}\mathrm{Aut}(H) & \xrightarrow{\cong} & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times\\ \cup & & \cup\\ \alpha & \longmapsto & \alpha([1])\end{array}$$

On considère quelques exemple spécifiques de $H \rtimes_\phi F$ lorsque $F = \mathbb{Z}/m\mathbb{Z}$.

(1) Prenons $n = 7$ et $m = 5$: nous considérons donc $\mathbb{Z}/7\mathbb{Z} \rtimes_\phi \mathbb{Z}/5\mathbb{Z}$. La première question est de comprendre les possibilités pour

$$\phi : \mathbb{Z}/5\mathbb{Z} = F \to \mathrm{Aut}(H) = \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right) = \left(\mathbb{Z}/7\mathbb{Z}\right)^\times$$

Pour cela on utilisera que $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times \cong \mathbb{Z}/6\mathbb{Z}$, ce que l'on a montré dans le point (2) de la Remarque 4.5.38. Ainsi on peut regarder ϕ comme un homomorphisme $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$. Par le Corollaire 4.5.34 on obtient que ϕ est forcément trivial, ce qui veut dire que $\phi \equiv e$. En utilisant la Remarque 4.8.9 on obtient que $\mathbb{Z}/7\mathbb{Z} \rtimes_\phi \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ dans tous les cas. Autrement dit, on n'obtient pas de nouveau groupe non-abélien dans ce cas.

(2) On peut généraliser le point précédent pour n et m arbitraires tel que n est premier et $(m, n-1) = 1$, en utilisant que $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = n-1$. En fait dans ce cas, on obtient par le Corollaire 4.5.34 qu'il n'existe que l'homomorphisme trivial de $\mathbb{Z}/m\mathbb{Z}$ à $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. On obtient alors que $\mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(3) Une conséquence du point précédent est qu'il faut prendre un cas où $(m, n-1) \neq 1$ pour espérer obtenir de nouveaux groupes. Le plus petit cas où cette condition est satisfaite est $m = 2, n = 3$. Dans ce cas, il existe un seul homomorphisme non-trivial

$$\phi = \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}} : F = \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \cong \left(\mathbb{Z}/3\mathbb{Z}\right)^\times \cong \mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) = \mathrm{Aut}(H)$$

Si on prend ce ϕ, le groupe $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ est un groupe non-commutatif qui possède 6 éléments, un sous-groupe normal d'ordre 3 et d'indice 2, et un autre sous-groupe d'ordre 2 et d'indice 3. Ce produit semi-direct ressemble beaucoup à S_3. En fait, en utilisant la proposition suivante on va démontrer qu'il est isomorphe à S_3.

Théorème 4.8.13. *Si $H, F \leq G$ sont tels que $F \leq N_G(H)$ et $H \cap F = \{e\}$, alors la fonction ξ du Corollaire 4.8.2 induit un isomorphisme $H \rtimes_{\mathrm{Ad}_F^H} F \cong HF$.*

De plus :

(1) Si G est fini et tel que $|G| = |F| \cdot |H|$, alors $G = HF \cong H \rtimes_{\mathrm{Ad}_F^H} F$.

(2) Si $H \subseteq N_G(F)$ est aussi satisfait, alors Ad_F^H est l'homomorphisme trivial. En particulier dans ce cas $HF \cong H \times F$.

Démonstration. On démontre d'abord l'assertion principale :

$$\xi(h,f)\xi\left(\tilde{h},\tilde{f}\right) = (hf)\left(\tilde{h}\tilde{f}\right) \underset{\boxed{(4.8.a)}}{\uparrow} = hf\tilde{h}f^{-1}f\tilde{f} \underset{\boxed{\text{Définition 4.8.3}}}{\uparrow} = h\Big(\mathrm{Ad}_f^H\left(\tilde{h}\right)\Big)f\tilde{f}$$

$$= \xi\Big(h\Big(\mathrm{Ad}_f^H\left(\tilde{h}\right)\Big),\ f\tilde{f}\Big) = \xi\Big((h,f)\cdot\left(\tilde{h},\tilde{f}\right)\Big)$$

Donc ξ devient un homomorphisme de groupes si on munit le produit cartésien de H par F de la structure de produit semi-direct induite par Ad_F^H. Comme ξ est une bijection, c'est un isomorphisme.

On continue en démontrant les assertions additionnelles :

(1) Dans ce cas, en utilisant le Corollaire 4.8.2 on voit que $HF = G$, ce qui conclut ce point.

(2) Il faut démontrer que pour chaque $f \in F$ et $h \in H$ on a $fhf^{-1} = h$, ou autrement dit que $fhf^{-1}h^{-1} = e$. Puisque $H \cap F = \{e\}$, c'est équivalent à démontrer que $fhf^{-1}h^{-1} \in H$ et $fhf^{-1}h^{-1} \in F$, ce que l'on fait dans le calcul suivant :

$$\underbrace{fhf^{-1}}_{\boxed{\in H \text{ parce que } F \subseteq N_G(H)}}h^{-1} \in H \qquad f\underbrace{hf^{-1}h^{-1}}_{\boxed{\in F \text{ parce que } H \subseteq N_G(F)}} \in F$$

□

Exemple 4.8.14. (1) Considérons S_3, et soient $H = \langle(1\ 2\ 3)\rangle$ et $F = \langle(1\ 2)\rangle$. Le sous-groupe H de S_3 est normal par le Lemme 4.7.29, et $\mathrm{Ad}_F^H : F \cong \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\, H \cong \mathbb{Z}/2\mathbb{Z}$ est égal au seul homomorphisme non-trivial $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$, parce que

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

et donc Ad_F^H ne peut pas être trivial. Par le Théorème 4.8.13 on obtient que $S_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$, ce qui confirme notre soupçon avoué au point (3) de l'Exemple 4.8.12.

(2) Considérons $HF \leq D_{12}$ comme dans l'Exemple 4.8.6. En utilisant le Théorème 4.8.13 et le calcul de Ad_F^H dans l'Exemple 4.8.6 on obtient que $HF \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$, où $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z}$ est le seul homomorphisme non-trivial.
Si on combine cela avec le point précédent, on obtient que $HF \leq D_{12}$ de l'Exemple 4.8.6 est isomorphe à S_3.

(3) Considérons les sous-groupes $H = \langle\sigma\rangle$ et $F = \langle\tau\rangle$ de $G = D_{2n}$. Puisque $[G : H] = 2$ on obtient que $H \trianglelefteq G$ par le Lemme 4.7.29. Par la Remarque 4.6.5 on voit que

$$\underset{\boxed{\sigma \longleftrightarrow [1]}}{H \underset{\uparrow}{\cong} \mathbb{Z}/n\mathbb{Z}} \qquad \underset{\boxed{\tau \longleftrightarrow [1]}}{F \underset{\uparrow}{\cong} \mathbb{Z}/2\mathbb{Z}} \qquad H \cap F = \{e\} \qquad \mathrm{Ad}_\tau^H(\sigma) = \tau\sigma\tau^{-1} = \sigma^{-1}.$$

Ainsi, en utilisant les identifications au-dessus, $\mathrm{Ad}_F^H : F \to \mathrm{Aut}(F)$ s'identifie avec $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ donné par

$$\underset{\boxed{\in \mathbb{Z}/2\mathbb{Z}}}{\left(\phi\underbrace{\left([1]\right)}_{\uparrow}\right)}\underset{\boxed{\in \mathbb{Z}/n\mathbb{Z}}}{\underbrace{\left([1]\right)}_{\uparrow}} \underset{\uparrow}{=} [-1]$$
$$\boxed{\mathrm{Ad}_\tau^H(\sigma) = \sigma^{-1}}$$

En utilisant le Théorème 4.8.13 on obtient que $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$.

En utilisant la théorie que l'on a développée dans cette section, on peut montrer que plusieurs nouvelles colonnes de notre tableau de petits groupes sont complètes, à isomorphismes près. On commence par la colonne des groupes d'ordre 4.

Proposition 4.8.15. *Il existe que deux groupes d'ordre 4 modulo d'isomorphisme : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Démonstration. Soit G un groupe d'ordre 4. Si G contient un élément d'ordre 4, alors $G = \langle g\rangle \cong \mathbb{Z}/4\mathbb{Z}$ par le Corollaire 4.5.36.

Ainsi on peut supposer que G ne contient aucun élément d'ordre 4. Par le Théorème 4.5.7 l'ordre de tous les éléments non-triviaux de G est 2. Choisissons deux éléments $h, f \in G \setminus \{e\}$ distincts. En utilisant le Lemme 4.5.9, si on définit $H = \langle h\rangle$ et $F = \langle f\rangle$, alors ces deux sous-groupes contiennent chacun exactement 2 éléments : $H = \{e, h\}$ et $F = \{e, f\}$. En particulier $H \cap F = \{e\}$ parce que nous avons choisi $h \neq f$. De plus H et F sont sous-groupes normaux de G par Lemme 4.7.29. Cela implique qu'on peut appliquer le point (2) du Théorème 4.8.13 pour obtenir que $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

En particulier on obtient que S_3 est le plus petit groupe non-abélien.

On passe aux colonnes des groupes d'ordre $2p$ où p est un entier premier. Pour cela on a besoin du lemme suivant :

Lemme 4.8.16. *Si tous les éléments non-triviaux d'un groupe G sont d'ordre 2, alors G est abélien.*

Démonstration. Prenons $a, b \in G$. Tous les éléments de G sont d'ordre 1 ou 2, donc $abab = e$. Cela implique :

$$\underset{\boxed{abab = e}}{ab \underset{\uparrow}{=}} a(abab)b = (aa)ba(bb) \underset{\boxed{o(a)|2 \text{ et } o(b)|2}}{\underset{\uparrow}{=}} ba$$

□

Théorème 4.8.17. *Si G est un groupe d'ordre $2p$, où $p > 2$ est un nombre premier, alors :*

(1) G contient un élément h d'ordre p,

(2) G contient un élément f d'ordre 2,

(3) Si $H = \langle h \rangle$ et $F = \langle f \rangle$, alors $G = HF$, $H \cap F = \{e\}$ et $H \trianglelefteq G$. En particulier $G \cong H \rtimes_{\mathrm{Ad}_F^H} F \cong \mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ pour un certain $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$.

Démonstration. Si G est cyclique alors, $G \cong \mathbb{Z}/2p\mathbb{Z}$ par le Corollaire 4.5.36. Dans ce cas G est abélien et par conséquent tous les sous-groupes sont normaux et toutes les représentations adjointes sont triviales (Exemple 4.8.5). On peut alors prendre $h = [2]$, $f = [p]$ et $\phi \equiv \mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$.

On suppose pour le reste de la preuve que G n'est pas cyclique. Par le Théorème de Lagrange (Théorème 4.5.7) on obtient que pour chaque élément $g \in G \setminus \{e\}$ on a $o(g) = 2$ ou $o(g) = p$.

(1) Pour prouver que G contient un élément d'ordre p, on argumente par contradiction. Ainsi on suppose que $G \setminus \{e\}$ contient uniquement des éléments d'ordre 2. Choisissons des éléments distincts $a, b \in G \setminus \{e\}$. Par le Lemme 4.8.16, G est abélien. Alors $H = \langle a \rangle = \{e, a\}$ et $F = \langle b \rangle = \{e, b\}$ sont des sous-groupe normaux de G, et de plus $H \cap F = \{e\}$. En utilisant le Théorème 4.8.13 on obtient que HF est un sous-groupe d'ordre 4 de G, ce qui contredit Théorème 4.5.7 puisque 4 ne divise pas $2p$.

(2) Pour prouver que G contient un élément d'ordre 2, on argumente aussi par contradiction. Ainsi on suppose que $G \setminus \{e\}$ contient uniquement des éléments d'ordre p. Choisissons alors $a \in G \setminus \{e\}$ et écrivons $H = \langle a \rangle$, qui est un sous-groupe d'ordre p de G. Ainsi $G \setminus H \neq \emptyset$, et on peut choisir $b \in G \setminus H$. Dénotons $F = \langle b \rangle$ qui est aussi un sous-groupe d'ordre p de G, mais $H \neq F$ par le choix de b. On obtient que $H \cap F$ est un sous-groupe de H et F qui n'est égal à aucun de deux. En utilisant que $|H| = |F| = p$ ainsi que le Théorème de Lagrange (Théorème 4.5.7), on obtient que $|H \cap F| = 1$, ou autrement dit $H \cap F = \{e\}$. Puisque c'est vrai pour chaque choix de $a \in G \setminus \{e\}$ et $b \in G \setminus \langle a \rangle$ on obtient que G est couvert par des sous-groupes G_i $(i = 1, \ldots, s)$ d'ordre p dont les intersections deux-à-deux se réduisent à l'élément neutre. On obtient que

$$2p = |G| = \underset{\substack{\uparrow \\ \text{pour l'élément neutre}}}{1} + \sum_{i=1}^{s} |G_i \setminus \{e\}| = 1 + s(p-1)$$

Autrement dit, $2p \equiv 1 \ (p-1)$. C'est une contradiction, parce que $p \equiv 1 \ (p-1)$, et alors $2p \equiv 2 \ (p-1)$.

(3) On introduit la notation $H = \langle h \rangle$ et $F = \langle f \rangle$. Le sous-groupe $H \cap F$ est contenu dans H et dans F. Par le Théorème de Lagrange (Théorème 4.5.7) on obtient que $|H \cap F|$ divise à la fois 2 et p. Cela implique que $|H \cap F| = 1$, et alors $H \cap F = \{e\}$. De plus, par le Lemme 4.7.29 on obtient que $H \trianglelefteq G$. Ainsi on peut appliquer le Théorème 4.8.13, ce qui conclut notre démonstration.

□

Corollaire 4.8.18. *Pour un nombre premier $p > 2$, il n'existe que 2 groupes d'ordre $2p$ à isomorphisme près : $\mathbb{Z}/2p\mathbb{Z}$ et D_{2p}.*

Démonstration. On a démontré dans le Théorème 4.8.17 que $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ pour un certain $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$. Comme on a vu dans l'Exemple 4.2.3, tels homomorphismes ϕ correspondent bijectivement aux éléments de 2-torsion de $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$.

On postule que *il y a exactement 2 éléments distinctes de 2-torsion dans* $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$. Pour démontrer cette affirmation nous devons utiliser la structure de corps sur $\mathbb{Z}/n\mathbb{Z}$. Autrement

dit, on travaille dans le corps $\mathbb{F}_p$, et on utilise que $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \mathbb{F}_p \setminus \{0\}$. Prenons un éléments $x \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$. Alors, on a l'égalité $x^2 = 1$, ce qui est aussi un égalité dans $\mathbb{F}_p$. Ainsi, dans $\mathbb{F}_p$ on a

$$0 = x^2 - 1 = (x-1)(x+1) \implies 0 = x-1, \text{ ou } 0 = x+1 \implies x = 1, \text{ ou } x = -1.$$

Notons que $1 \neq -1 \in \mathbb{F}_p$, parce que $p > 2$. Cela conclut la démonstration de notre affirmation sur les éléments de 2-torsion.

Du coup, on obtient ainsi qu'il existe deux homomorphismes

$$\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times,$$

à savoir l'homomorphisme trivial ϕ_1 et l'homomorphisme ϕ_{-1} pour lequel $\phi([1]) = [-1]$. Par conséquent il existe au plus deux groupes d'ordre $2p$ modulo isomorphisme :

$$\mathbb{Z}/p\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/2\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/p\mathbb{Z} \rtimes_{\phi_{-1}} \mathbb{Z}/2\mathbb{Z}$$

Par la Remarque 4.8.11, le premier est abélien, et le second est non-abélien. De plus, dans le point (3) de l'Exemple 4.8.14 on a démontré que le second est isomorphe à D_{2p}. □

On finit en montrant plus d'exemples d'utilisation du Théorème 4.8.13.

Exemple 4.8.19. (1) $\boxed{\mathrm{GL}(2,\mathbb{F}_2) \cong S_3 :}$ En utilisant le point (1) de l'Exemple 4.8.14 et le point (3) de l'Exemple 4.8.12 il suffit de démontrer que $\mathrm{GL}(2,\mathbb{F}_2)$ contient un sous-groupe H d'indice 2 d'ordre 3 et un autre sous-groupe F d'indice 3 et d'ordre 2 tel que $\mathrm{Ad}_F^H \not\equiv \mathrm{id}_H$. Les choix de H et F suivants satisfont ces conditions :

$$H = \left\langle \underbrace{\begin{pmatrix}[0] & [1]\\ [1] & [1]\end{pmatrix}}_{\uparrow} \right\rangle \qquad F = \left\langle \underbrace{\begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}}_{\uparrow} \right\rangle$$

Devoir : vérifiez que la troisième puissance est l'identité

Devoir : vérifiez que la deuxième puissance est l'identité

parce que $\mathrm{Ad}_f^H \neq \mathrm{id}_H$ pour $f = \begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}$, qui est montré dans le calcul suivant :

$$\begin{aligned}\mathrm{Ad}_f^H\left(\begin{pmatrix}[0] & [1]\\ [1] & [1]\end{pmatrix}\right) &= \begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}\begin{pmatrix}[0] & [1]\\ [1] & [1]\end{pmatrix}\begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}^{-1} = \begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}\begin{pmatrix}[0] & [1]\\ [1] & [1]\end{pmatrix}\begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix}\\ &= \begin{pmatrix}[1] & [0]\\ [1] & [1]\end{pmatrix}\begin{pmatrix}[1] & [1]\\ [0] & [1]\end{pmatrix} = \begin{pmatrix}[1] & [1]\\ [1] & [0]\end{pmatrix} = \begin{pmatrix}[0] & [1]\\ [1] & [1]\end{pmatrix}^2\end{aligned}$$

(2) On démontre dans un exercice que tous les automorphismes de $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\oplus s}$ sont linéaires. Autrement dit, l'inclusion naturelle $\mathrm{GL}(n,\mathbb{F}_p) \subseteq \mathrm{Aut}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\oplus s}\right)$ est une égalité.

Par conséquent, pour $F = \mathbb{Z}/2\mathbb{Z}$ et $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ il y a plusieurs choix de $\phi : F \to \mathrm{Aut}(H) = \mathrm{GL}(2,\mathbb{F}_2)$ non-triviaux quand on considère $H \rtimes_\phi F$. Par Exemple 4.2.3, un ϕ de cette forme est uniquement déterminé par $\phi([1])$, qui est forcément un élément d'ordre 2. On a vu dans le point précédent du même exemple que $\mathrm{GL}(2,\mathbb{F}_2) \cong S_3$, et alors tous les éléments d'ordre 2 dans ce groupe sont conjugués. Il y aura un autre exercice dans la fiche de cette semaine qui nous dit que changer ϕ par conjugaison nous donne un produit semi-direct isomorphe. Ainsi on voit que toutes les possibilités non-triviales pour ϕ nous donnent des produit semi-directs isomorphes. On appelle cette classe d'isomorphisme de groupes **le** produit semi-direct non-trivial $G = H \rtimes_\phi F$.

(3) On démontre que le produit semi-direct non-trivial $G' = \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ est isomorphe à D_8. Utilisons la notation suivante dans ce point (en particulier H et F dénotent des groupes différents du point précédent) :

$$F = \langle \sigma\tau \rangle \qquad H = \langle \tau, \sigma^2 \rangle$$

Puisque $\sigma^2 \in Z(D_8)$, on obtient que $\tau \in N_{D_8}\left(\langle \sigma^2 \rangle\right)$. Par conséquent on déduit

$$H = \langle \tau, \sigma^2 \rangle \underset{\uparrow}{=} \left\langle \langle \tau \rangle, \langle \sigma^2 \rangle \right\rangle \underset{\uparrow}{=} \langle \tau \rangle \cdot \langle \sigma^2 \rangle \underset{\uparrow}{\cong} \langle \sigma^2 \rangle \rtimes_\psi \langle \tau \rangle \underset{\uparrow}{\cong} \langle \sigma^2 \rangle \times \langle \tau \rangle \underset{\uparrow}{\cong} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Remarque 4.7.5 — Proposition 4.7.20 et le fait que $\tau \in N_{D_8}\left(\langle \sigma^2 \rangle\right)$ — en appliquant Théorème 4.8.13 pour $\psi = \mathrm{Ad}^{\langle \sigma^2 \rangle}_{\langle \tau \rangle}$ — $\langle \sigma^2 \rangle \leq Z(D_8) \Rightarrow \mathrm{Ad}^{\langle \sigma^2 \rangle}_{\langle \tau \rangle} \equiv \mathrm{id}_{\langle \sigma^2 \rangle}$ — $o(\tau) = o(\sigma^2) = 2$

(4.8.d)

Puisque $o(\sigma\tau) = 2$ on sait aussi que

$$F \cong \mathbb{Z}/2\mathbb{Z} \tag{4.8.e}$$

De plus $H \trianglelefteq D_8$, parce que $[D_8 : H] = 2$ (Lemme 4.7.29). Ça veut dire qu'on peut appliquer le Théorème 4.8.13 pour obtenir que

$$D_8 \cong H \rtimes_\xi F \underset{\uparrow}{\cong} \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$$

(4.8.d) et (4.8.e)

De plus ϕ doit être non-trivial en utilisant Remarque 4.8.11, parce que D_8 n'est pas abélien.

Finalement on met à jour le tableau des petits groupes en utilisant les autres isomorphismes qui sont démontrés dans la fiche d'exercices :

(1) pour un ϕ quelconque non-trivial on a

$$\mathbb{Z}/2\mathbb{Z} \times S_3 \cong D_{12} \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \cong B(2, \mathbb{F}_3)$$

(2) pour un ϕ quelconque non-trivial on a

$$\mathrm{PSL}(2, \mathbb{F}_3) \cong \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes_\phi \mathbb{Z}/3\mathbb{Z} \cong A_4$$

(3) pour un ϕ quelconque non-trivial on a

$$U(3, \mathbb{F}_2) \cong \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_8$$

ordre	1 ✓	2 ✓	3 ✓	4 ✓	5 ✓	6 ✓	7 ✓	8
groupes	le groupe trivial	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$ S_3 ~~$\mathrm{GL}(2, \mathbb{F}_2)$~~	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ D_8 Q_8 ~~$U(3, \mathbb{F}_2)$~~

9	10 ✓	11 ✓	12	13 ✓	14 ✓	15	...
$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/10\mathbb{Z}$	$\mathbb{Z}/11\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$	$\mathbb{Z}/13\mathbb{Z}$	$\mathbb{Z}/14\mathbb{Z}$	$\mathbb{Z}/15\mathbb{Z}$	...
$(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$	D_{10}		$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$		D_{14}		
			A_4				
			D_{12}				
			~~$\mathbb{Z}/2\mathbb{Z} \times S_3$~~				
			~~$B(2, \mathbb{F}_3)$~~				
			~~$\mathrm{PSL}(2, \mathbb{F}_3)$~~				
			$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$				

couleur bleue : groupes non-abéliens

Si nous avions encore quelques semaines, nous pourrions finir de démontrer que les groupes listés dans les colonnes d'ordre 8, 9, 12 et 15 sont les seules possibilités à isomorphisme près. Nous aurions besoin des concepts et résultats suivants :

— actions de groupes,

— les théorèmes de Sylow,

— groupes libres et présentations de groupes.

Ces sujets seront présentés dans le cours "Théorie des groupes" au troisième semestre.

Mentionnons aussi que la classification à la main des groupes se complique considérablement pour des ordres plus grands. Pour $|G| = 16$ il existe déjà 14 classes d'isomorphisme, pour $|G| = 32$ il en existe 51, et pour $|G| = 64$ il en existe 267. D'un autre côté, lorsque les premiers divisant $|G|$ apparaissent avec de petites puissances, il n'est pas si difficile de comprendre les structures possibles de G en utilisant les théorèmes de Sylow.