Théorie des groupes

UQàM MAT2250

Christophe Reutenauer
Laboratoire de combinatoire et d'informatique mathématique,
Université du Québec à Montréal

9 décembre 2025

Table des matières

Remerciements : J'ai grandement bénéficié des notes de cours de François Bergeron [1], de Christophe Hohlweg [2], ainsi que des notes de cours de Jacques Labelle et moi-même [3].

Pour la chasse aux coquilles, merci à Félix Racine.

1 Introduction

2 Monoïdes et groupes

Définition 2.1. *Soit E un ensemble. Une* loi de composition interne *sur E est une fonction $E \times E \to E$. On dit aussi une* loi de composition*, ou simplement* loi*, ou encore* opération binaire *sur E.*

Exemple 2.2. *1. Avec $E = \mathbb{N}$, on prend comme loi la fonction $(a, b) \mapsto a + b$. Même chose pour $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{Q}_+ = \{x \in \mathbb{Q} | x \geq 0\}$, $\mathbb{R}_+$, $\mathbb{Z}_-, \mathbb{Q}_-, \mathbb{R}_-$, $\mathbb{N}^* = \{x \in \mathbb{N} | x \neq 0\}$, $\mathbb{R}_+^*, \mathbb{Q}_+^*, \mathbb{Q}_-^*, \mathbb{R}_-^*$. On vérifie en effet que si a, b sont dans un de ces ensembles, $a + b$ l'est aussi.*

2. Toujours avec $E = \mathbb{N}$, on prend comme loi $(a, b) \mapsto ab$ (produit de a par b). Ici aussi, on peut remplacer $\mathbb{N}$ par $\mathbb{N}^*$, $\mathbb{Z}, \mathbb{Z}^*, \mathbb{Q}, \mathbb{Q}^*, \mathbb{R}, \mathbb{R}^*, \mathbb{Q}_+^*, \mathbb{R}_+^*$ (mais pas par $\mathbb{Z}_-, \mathbb{Q}_-, \mathbb{R}_-$: pourquoi ?).

3. Sur $\mathbb{N}$, prenons la loi $(a, b) \mapsto a + b + ab$. Ici aussi, on peut remplacer $\mathbb{N}$ par $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{Q}_+, \mathbb{R}_+$.

4. Sur N, on considère la loi $(a, b) \mapsto 1 + ab$.

5. Soit X un ensemble et $E = \mathcal{P}(X)$ (l'ensemble des parties de X). On définit la loi $(A, B) \mapsto A \cup B$. Une autre loi sur E est $(A, B) \mapsto A \cap B$.

L'addition et la multiplication des nombres ont certaines propriétés bien connues. Lorsqu'on les considère dans l'abstrait, on trouve la notion de monoïde, la notion de groupe, celle d'anneau, de corps, etc...

Définition 2.3. *Soit M un ensemble muni d'une loi $(a, b) \mapsto \ell(a, b)$. On dit que M est un* monoïde *si les deux propriétés suivantes sont réalisées.*

(i) Pour tous a, b, c dans M, on a

$$\ell(\ell(a, b), c) = \ell(a, \ell(b, c)).$$

On dit que la loi est associative.

(ii) Il existe un élément e dans M tel que pour tout a dans M, on a

$$\ell(a, e) = a = \ell(e, a).$$

On dit que e est un élément neutre *de M.*

Exemple 2.4. *1. Soit* $E = \mathbb{N}$, $\ell(a,b) = a+b$. *Alors* $\ell(\ell(a,b),c) = \ell(a+b,c) = (a+b)+c = a+(b+c) = \ell(a,b+c) = \ell(a,\ell(b,c))$. *De plus on a,* $\ell(a,0) = a+0 = a = 0+a = \ell(0,a)$. *Donc* $\mathbb{N}$ *avec la loi* ℓ *est un monoïde.*

2. Sur $\mathbb{N}$, *la loi* $\ell(a,b) = ab+1$ *n'est pas associative. En effet* $\ell(\ell(a,b),c) = \ell(ab+1,c) = (ab+1)c+1 = abc+c+1$, *et* $\ell(a,\ell(b,c)) = \ell(a,bc+1) = a(bc+1)+1 = abc+a+1$ *; donc* $\ell(\ell(a,b),c) \neq \ell(a,\ell(b,c))$ *dès que* $a \neq c$.

Définition 2.5. *Un monoïde est dit* commutatif, *ou* abélien, *si sa loi est* commutative, *c'est-à-dire*

$$(iii)\ \ \forall a,b \in M, \ell(a,b) = \ell(b,a).$$

Toutes les lois considérées dans les exemples précédents sont commutatives.

Le plus souvent, la notation pour une loi dans un monoïde est $a \cdot b$, ou ab, au lieu de $\ell(a,b)$ comme ci-dessus ; c'est ce qu'on appelle la *notation multiplicative* ; la loi est alors appelée *multiplication*. Avec cette notation, les formules dans (i), (ii), (iii) se réécrivent comme suit :

(i) $(ab)c = a(bc)$ (associativité) ;

(ii) $ea = ae = a$ (élément neutre) ;

(iii) $ab = ba$ (commutativité).

Lorsque le monoïde est commutatif, on adopte souvent la *notation additive* $a+b$ au lieu de $\ell(a,b)$. En notation multiplicative, on note souvent 1 (le *un* ou l'*unité* du monoïde) au lieu de e, et en notation additive, on note souvent 0 (le *zéro*). Dans la suite, on adoptera le plus souvent la notation multiplicative.

Dans un monoïde multiplicatif, $(ab)c$ et $a(bc)$ sont égaux, et l'on écrira simplement abc (voir l'exercice 20 pour une généralisation). Dans le cas additif, c'est $a+b+c$ qu'on écrit.

Proposition 2.6. *Un monoïde a un seul élément neutre.*

Nous dirons donc : *l'*élément neutre d'un monoïde M, plutôt qu'*un* élément neutre de M.

Démonstration. Comme dans beaucoup de preuves d'unicité ("un seul") en mathématiques, on suppose que l'objet dont on veut démontrer l'unicité existe en deux exemplaires, et on montre que ces deux n'en forment en fait qu'un. Supposons donc que notre monoïde M ait deux éléments neutres e_1 et e_2, et montrons que $e_1 = e_2$. Utilisons la notation multiplicative. Nous avons $e_1 = e_1e_2$, car e_2 est élément neutre. Mais aussi $e_1e_2 = e_2$, car e_1 est élément neutre. Donc $e_1 = e_2$, ce qu'il fallait démontrer. □

Définition 2.7. *Soit M un monoïde. Un* sous-monoïde *de M est un sous-ensemble P de M qui contient l'élément neutre de M et tel que*

$$\forall a, b \in P, ab \in P.$$

Remarquons que si on note ℓ la loi de M, alors on aura

$$\forall a, b \in P, \ell(a, b) \in P.$$

Ce genre de définition est très courant en mathématiques : on a un ensemble M avec une ou plusieurs lois, ou des opérations plus générales ; appelons ça un "machin". Un "sous-machin" de M est alors un sous-ensemble P de M qui est "fermé" ou "clos" pour toutes ces lois, c'est-à-dire si on prend des éléments de P et qu'on leur applique les lois, le résultat est encore dans P. Dans tous les cas, la définition de "sous-machin" sera ajustée de telle manière que l'analogue de l'énoncé suivant sera vrai. Nous y réutilisons la notation ℓ pour la loi, qui rend mieux compte de ce qui se passe.

Proposition 2.8. *Soit M un monoïde, de loi ℓ, et P un sous-monoïde. On définit sur P la loi $k : P \times P \to \mathbb{P}$ par :*

$$\forall a, b \in P, k(a, b) = \ell(a, b).$$

Avec la loi k, P est un monoïde.

Démonstration. Remarquons d'abord que k est bien une loi sur P, c'est-à-dire une fonction $P \times P \to P$. En effet, P est un sous-monoïde, donc $\forall a, b \in P$, $\ell(a, b) \in P$, donc $k(a, b) \in P$.

Maintenant, l'associativité de la loi k résulte de celle de ℓ : $\forall a, b, c \in P$, on a par définition de k : $k(k(a, b), c) = \ell(\ell(a, b), c)$ et $k(a, k(b, c)) = \ell(a, \ell(b, c))$. On conclut donc par l'associativité de ℓ.

De plus, M a un élément neutre e. Celui-ci est dans P, car P est un sous-monoïde. On a alors : $\forall a \in P$, $k(a, e) = \ell(a, e) = a$ et $k(e, a) = \ell(e, a) = a$, ce qui montre que P est bien un monoïde. □

Exemple 2.9. *1. $\mathbb{N}$ avec l'addition est un monoïde. Alors $P = \{0\} \cup \{n \in \mathbb{N} | n \geq 7\}$ est un sous- monoïde. En effet, l'élément neutre pour l'addition, qui est 0, est dans P. De plus, si $a, b \in P$ avec $a \neq 0$, alors $a + b \in P$, puisque $a + b \in \mathbb{N}$, et que $a + b \geq a \geq 7$.*

2. $\mathbb{Z}$ avec l'addition est un monoïde et $\mathbb{N}$ en est un sous-monoïde.

3. Si X est un ensemble, $E = \mathcal{P}(X)$ est un monoïde avec la loi $(A, B) \mapsto A \cup B$, d'élément neutre $\emptyset$. Soit A_0 un sous-ensemble fixé de X et $P = \{A \subset X | A = \emptyset \text{ ou } A_0 \subset A\}$. Alors P est un sous-monoïde de E.

4. Si M est un monoïde, M et $\{e\}$ sont des sous-monoïdes de M.

Définition 2.10. *Soit M un monoïde noté multiplicativement. On dit que M est un groupe si tout élément a de M a un* inverse *(on dit aussi que a est* inversible *dans M), c'est-à-dire : $\forall a \in M$, $\exists b \in M$ tel que $ab = ba = e$, où e est l'élément neutre de M.*

Exemple 2.11. *1. $\mathbb{Z}$ avec l'addition est un groupe, car pour tout a dans $\mathbb{Z}$, il existe b dans $\mathbb{Z}$ tel que $a + b = b + a = 0$. Il suffit en effet de prendre $b = -a$.*

2. $\mathbb{N}$ avec l'addition n'est pas un groupe, car par exemple pour $a = 1$, on ne peut trouver b dans $\mathbb{N}$ tel que $1 + b = 0$.

3. $\mathbb{Q}^*$ avec la multiplication est un groupe : pour tout $a = r/s \in \mathbb{Q}^*$, son inverse est $a^{-1} = s/r$ (l'élément neutre ici est 1).

4. $\mathcal{P}(X)$ avec la loi "union" n'est pas un groupe, si X a au moins un élément. En effet, on ne peut en général pas trouver $A \in \mathcal{P}(X)$ tel que $A \cup X = \emptyset$.

Proposition 2.12. *Dans un groupe, l'inverse de chaque élément est unique.*

Démonstration. Soit G ce groupe, e son élément neutre, $a \in G$ et b_1, b_2 des inverses de a. On a donc $b_1 = b_1 e$ (car e est élément neutre) $= b_1(ab_2)$ (car b_2 est inverse de a) $= (b_1 a)b_2$ (par associativité) $= eb_2$ (car b_1 est inverse de a) $= b_2$ (car e est élément neutre). D'où $b_1 = b_2$. □

On parlera donc de *l'*inverse d'un élément dans un groupe, plutôt que d'*un* inverse. Dans un groupe additif, on dit plutôt *opposé*. La notation est a^{-1} pour l'inverse de a dans un groupe multiplicatif, et $-a$ pour l'opposé de a dans un groupe additif.

On remarquera que la proposition ci-dessus implique que l'inverse de l'inverse de a est a lui-même.

Définition 2.13. *Soit G un groupe multiplicatif d'élément neutre 1. Un* sous-groupe *de G est un sous-ensemble H de G tel que :*

(i) $1 \in H$;

(ii) $\forall a, b \in H, ab \in H$;

(iii) $\forall a \in H, a^{-1} \in H$.

Donc un sous-groupe de G est un sous-monoïde de G qui contient l'inverse de chacun de ses éléments.

On laissera au lecteur le soin d'énoncer cette définition dans le cas additif.

Exemple 2.14. *1. $\mathbb{Z}$ avec l'addition est un groupe, admettant comme sous-groupe, par exemple, l'ensemble des nombres pairs.*

2. $\mathbb{Q}$ *avec l'addition admet comme sous-groupe le sous-ensemble* $\{a/2^n | a \in \mathbb{Z}, n \in \mathbb{N}\}$.

3. $\mathbb{R}^*$ *avec la multiplication contient* $\mathbb{Q}^*$, $\{1, -1\}$, *et* $\mathbb{R}_+^*$, *comme sous-groupes.*

Théorème 2.15. *Pour tout sous-groupe* H *de* $\mathbb{Z}$, *il existe un entier naturel* b *tel que* $H = \{bn \mid n \in \mathbb{Z}\}$.

La notation pour le dernier ensemble est $b\mathbb{Z}$; c'est l'ensemble des entiers relatifs qui sont multiples de b.

Démonstration. Si $H = \{0\}$, nous prenons $b = 0$ et c'est gagné. Si $H \neq \{0\}$, H contient sûrement un entier > 0 : en effet, H contient un entier $n \neq 0$, et il contient aussi son opposé $-n$, étant un sous-groupe ; donc$n$ et $-n$ sont dans H, et l'un d'eux est > 0.

Considérons $H_+^* = \{n \in H \mid n > 0\}$. Cet ensemble est non vide, comme on vient de le voir, donc cet ensemble a un minimum, que nous notons b. Nous montrons que $H = b\mathbb{Z}$. Pour ce faire, il faut montrer que $H \subset b\mathbb{Z}$ et $b\mathbb{Z} \subset H$. Pour montrer que $b\mathbb{Z} \subset H$, prenons $a \in b\mathbb{Z}$ quelconque et montrons que $a \in H$. Comme $a \in b\mathbb{Z}$, on a $a = bn$, $n \in \mathbb{Z}$. Supposons d'abord $n \geq 0$; alors $a = b + b + \cdots + b$ (n fois), donc $a \in H$, puisque H est un sous-groupe contenant b ; si $n < 0$, on a $a = -(b(-n))$ et $b(-n)$ est dans H d'après l'argument juste avant ; comme H est un sous-groupe, il contient aussi l'opposé de $b(-n)$, i.e. a, donc $a \in H$.

Montrons maintenant que $H \subset b\mathbb{Z}$. Soit donc $a \in H$ et supposons d'abord que $a > 0$. Par division euclidienne, nous avons $a = bq + r, 0 \leq r < b$. Donc $r = a - bq$ est dans H, car a et bq le sont (nous avons vu ci-dessus que $bZ \subset H$), et que H est un sous-groupe. Si r était non nul, on aurait $r \in H^*, r < b$, ce qui est impossible, car b est le minimum de H^*. Donc on doit avoir $r = 0, eta = bq \in b\mathbb{Z}$. Supposons maintenant que $a < 0$. Alors $-a > 0$ et $-a \in H$ puisque H est un sous-groupe. Donc, par ce que nous venons de voir, $-a \in b\mathbb{Z}$ et enfin $a \in bZ$. Ceci implique $H \subset b\mathbb{Z}$. □

Comme $b\mathbb{Z}$ est un sous-groupe (exercice 16), on obtient

Corollaire 2.16. *Les sous-groupes de* $\mathbb{Z}$ *sont les ensembles* $b\mathbb{Z}$, $b \in \mathbb{N}$.

On *classifie* ainsi tous les sous-groupes de $\mathbb{Z}$, car ils sont tous distincts, quand b varie dans $\mathbb{N}$.

Nous énonçons un dernier résultat, dont la preuve est analogue à celle de la proposition 2.8.

Proposition 2.17. *Soit H un sous-groupe du groupe H. Avec la loi $(a, b) \mapsto ab$, héritée de G, H est un groupe.*

On dit souvent que la loi sur H est *induite* par celle de G.

On peut représenter un monoïde, ou un groupe, par sa *table de multiplication* : chaque ligne, et chaque colonne, de cette table est indexée par un élément, et à l'intersection de la ligne a et de la colonne b, on met le produit de a par b. Ce tableau est fini si le monoïde est fini.

On dit qu'un sous-monoïde P d'un monoïde M (un sous-groupe H d'un groupe G) est *engendré* par une partie S de M (resp de G) si $S \subset P$ (resp. $S \subset H$), et si tout élément de P (resp. de H) s'écrit comme un produit d'éléments de S (resp. d'élements de S et de leurs inverses), répétitions permises. Notons que l'élément neutre est considéré être égal au produit vide, donc il sera toujours engendré.

On dit que S est un *système générateur* de P (resp. H).

Exemple 2.18. *1. Considérons le monoïde $\mathbb{N}$ avec l'addition ; il est engendré par 1 : en effet, tout élément de $\mathbb{N}$ est somme de plusieurs 1.*

2. Le groupe $\mathbb{Z}$ est engendré par 1. En effet, tout entier est somme de 1 et de -1, répétés plusieurs fois.

3. $\mathbb{N}$ avec l'addition a pour sous-monoïde $\mathbb{N}\backslash\{1\}$. Ce dernier pour système générateur $\{2, 3\}$. La preuve est laissée au lecteur.

4. Le monoïde multiplicatif $\mathbb{N}^*$ est engendré par l'ensemble des nombres premiers ; c'est une conséquence du théorème fondamental de l'arithmétique.

5. Le groupe multiplicatif $\mathbb{Q}_+^*$ est aussi engendré par l'ensemble des nombres premiers ; mais pour engendrer $\mathbb{Q}_+$, il faut ajouter -1, ou n'importe quel nombre rationnel < 0.

Exercice 1. *Parmi les ensembles suivants, dire lesquels sont des monoïdes ou des groupes pour l'addition usuelle : $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}_+, \mathbb{R}_+, \mathbb{Z}_-, \mathbb{Q}_-, \mathbb{R}_-, \mathbb{R}_+^*, \mathbb{Q}_+^*$. Dire aussi lesquels sont sous-monoïde ou sous-groupe d'un autre.*

Exercice 2. *Mêmes questions pour la multiplication dans les ensembles suivants : $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}_+, \mathbb{R}_+, \mathbb{R}_+^*, \mathbb{Q}_+^*, \mathbb{Z}^*$.*

Exercice 3. *Sur $\mathbb{Q}$, on définit une loi, notée $*$ par : $a*b = ab+a+b$. Montrer que Q devient un monoïde, d'élément neutre 0 ; montrer que tout élément a un inverse, sauf -1. Montrer que $Q\setminus\{-1\}$ est un sous-monoïde, qui devient un groupe avec la loi induite. Idée : utiliser $ab + a + b + 1 = (a + 1)(b + 1)$.*

Exercice 4. *Montrer que $\mathcal{P}(X)$ avec la loi $\cup$ (resp. $\cap$) est un monoïde avec élément neutre $\emptyset$) (resp. X).*

Exercice 5. *Montrer par un exemple que la soustraction sur $\mathbb{Z}$ n'est pas une loi associative.*

Exercice 6. *Même chose pour la division dans $\mathbb{Q}^*$.*

Exercice 7. *1) Comment calcule-t-on l'inverse d'un produit dans un groupe ?*

2) Calculer l'inverse de $a^{-1}bc^{-1}abcb^{-1}$.

3) Calculer $c^{-1}b^{-1}aa^{-1}bcadaa^{-1}d^{-1}$.

4) Que vaut l'élément de la question 2 quand le groupe est commutatif ?

Exercice 8. *On dit que a et b* commutent*, ou que a* commute avec *b, si $ab = ba$. Montrer que si a et b commutent avec c, alors ab^{-1} commute avec c (a, b, c sont des éléments d'un groupe).*

Exercice 9. *Soit G un groupe et H un sous-ensemble de G. Montrer que H est un sous-groupe si et seulement si on a les deux propriétés suivantes :*

(i) H est non vide ;

(ii) $\forall a, b \in H, ab^{-1} \in H$.

Exercice 10. *Montrer que $\mathbb{N} \setminus \{1, 2, 4\}$ est un sous-monoïde de N, mais que $N \setminus \{1, 4\}$ ne l'est pas.*

Exercice 11. *On définit sur $\mathcal{P}(X)$ une loi Δ par : $A\Delta B = (A \setminus B) \cup (B \setminus A)$. Montrer que c'est un groupe d'élément neutre $\emptyset$, et que l'inverse de A est A (on peut raisonner avec des dessins).*

Exercice 12. *Montrer que l'ensemble, noté X^X, des fonctions $X \to X$ est un monoïde avec la composition des fonctions (on rappelle que la composée $g \circ f$ des deux fonctions f et g est définie par $(g \circ f)(x) = g(f(x))$.*

Exercice 13. *Montrer que l'intersection de deux sous-monoïdes d'un monoïde est un sous-monoïde. Même chose avec deux sous-groupes d'un groupe.*

Exercice 14. *Soit M un monoïde et $a \in M$. On définit pour $n \in N$ la* puissance n*-ème de a par : $a^n = a \cdot \ldots \cdot a$ (n facteurs tous égaux à a) ; en particulier, $a^0 = 1$, $a^1 = a$, $a^2 = aa$, $a^3 = aaa$, et ainsi de suite. Noter que le parenthésage du produit importe peu, car le produit est associatif. Montrer que pour $n, m \in \mathbb{N}$, on a : $a^n \cdot a^m = a^{n+m}$ et $(a^n)^m = a^{nm}$.*

Exercice 15. *Dans un monoïde M, soit A un sous-ensemble. On note A^n l'ensemble des produits de n éléments de A : $A^n = \{a_1 a_2 \cdots a_n | \forall i = 1, \ldots, n, a_i \in A\}$. En particulier, $A_0 = \{e\}$, où e est l'élément neutre de M et $A^1 = A$. Montrer que $\bigcup_{n \geq 0} A^n$ est un sous-monoïde de M contenant A ; on dit que c'est le sous-monoïde* engendré par *A. Montrer que c'est le plus petit (pour l'ordre d'inclusion) des sous-monoïdes de M contenant A. En particulier si $A = \{a\}$, $A^n = \{a^n\}$ et $\bigcup_{n \geq 0} A^n = \{a^n | n \in \mathbb{N}\} = \{1, a, a^2, \ldots\}$.*

Exercice 16. *Soit b un entier. Montrer que $\{bn | n \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$ additif.*

Exercice 17. *Montrer que si H est un sous-groupe du groupe G, alors $HH = H$.*

Exercice 18. *Soit M l'ensemble des matrices carrées d'ordre n sur $\mathbb{R}$. Montrer que M est un groupe pour l'addition des matrices. Montrer que M est un monoïde pour la multiplication des matrices.*

Exercice 19. *Si G est un groupe et $a \in G$, on définit a^n comme dans l'exercice 14, pour $n \in \mathbb{N}$; et on définit $a^{-n} = (a^n)^{-1}$. Montrer que les égalités de l'exercice 14 sont valables pour $n, m \in \mathbb{Z}$.*

Exercice 20. ** Le lecteur aura sans doute remarqué qu'il y a un petit problème dans les exercices 14, 15, et 19. Dans 15, par exemple, on considère des produits du type abc : ceci signifie-t-il $(ab)c$ ou $a(bc)$? Pas d'importance, ils sont égaux par associativité. Attention, qu'en est-il de $(ab)(cd)$ et $(a(bc))d$? Après un moment de réflexion, on voit que : $(ab)(cd) = ((ab)c)d = (a(bc))d$, où dans les deux égalités, on n'utilise que l'associativité. Le lecteur pourra démontrer que dans le produit $a_1 a_2 \cdots a_n$, le résultat ne dépend pas du parenthésage choisi ; il faut, entre autres, définir la notion de parenthésage. Le lecteur pourra déjà se convaincre en montrant que $(a(bc))(de) = ((ab)(cd))e$, en n'utilisant que l'associativité.*

Exercice 21. *Soit M un monoïde et A, B des sous-ensembles de M. On définit leur produit AB par $AB = \{ab | a \in A, b \in B\}$. Montrer que $\mathcal{P}(M)$ devient ainsi un monoïde d'élément neutre $\{1\}$. Soit P un sous-ensemble de M contenant l'élément neutre de M ; montrer que P est un sous-monoïde de M si et seulement si $PP = P$.*

Exercice 22. ** Considérons le monoïde, noté X^X, de l'exercice 12. Quels éléments de X^X sont inversibles ? Si $|X| = n$, combien d'éléments X^X a-t-il ? Si $|X| = n$, combien y a-t-il d'éléments inversibles dans le monoïde X^X ?*

Exercice 23. *Soit $\mathbb{R}$ avec la loi $a * b = ab - 2(a+)b + 6$. Prouvez que la loi $*$ est : a) commutative ; b) associative ; c) avec un élément neutre ; d) quels éléments de R sont inversibles pour $*$?*

Exercice 24. ** Soit $E = \{x, 1-x, 1/x, 1/(1-x), x/(x-1), (x-1)/x\}$, avec la composition de fonctions. Prouver que E est un groupe. Trouver tous les sous-groupes de E.*

Exercice 25. *Pour la loi $*$ suivante sur l'ensemble X, dire si elle est commutative, associative, admet un élément neutre. Si $*$ admet un neutre, trouvez les éléments inversibles.*

a) $X = \mathbb{N}$ avec $*$ définie respectivement par : $a * b = pgdc(a, b), ppmc(a, b), a^b$.

b) $X = \mathbb{Z}$ avec $*$ définie respectivement par : $a * b = b, \min(a, b), \max(a, b), 2ab - a - b + 1$.

Exercice 26. *Vérifiez que $[0, 1) \subset \mathbb{R}$ est un groupe avec la loi $x_1 * x_2$ définie par : $x_1 * x_2 = x_1 + x_2$ si $x_1 + x_2 < 1$, $= x_1 + x_2 - 1$ si $x_1 + x_2 \geq 1$.*

Exercice 27. *Vérifiez qu'avec la multiplication matricielle, l'ensemble suivant est un groupe :*

$$\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\}$$

b) Trouvez tous les sous-groupes de ce groupe.

Exercice 28. *Soit $A \subset \mathbb{Z}$ avec l'addition. Dire si A est un sous-monoïde ou un sous-groupe (ou aucun des deux) si A est un des ensembles suivants :*

a) $\{$entiers pairs$\}$;

b) $\{0, 4, 5, 6, 7, \ldots\}$;

c) $\{\ldots, -5, -4, -3, 0, 2, 4, 5, 6, ...\}$;

d) l'ensemble des entiers impairs.

Exercice 29. ** Soit M un monoïde et X un ensemble. Sur l'ensemble E des fonctions de X dans M, on définit un produit par : $(fg)(x) = f(x)g(x)$.*

a) Montrer que est un monoïde.

b) Trouver les éléments inversibles de E.

c) Montrer que E est un groupe si M l'est.

Exercice 30. *On définit une loi de composition $*$ dans $\mathbb{N}$ par : $n * m = 0$ si nm est divisible par un carré, et $n * m = nm$ dans le cas contraire. Montrer $*$ est associative, mais que $\mathbb{N}$ n'a pas d'élément neutre pour ce produit.*

Exercice 31. *Si l'on interprète le produit $a \cdot b$ pour $a, b \in R_+$ comme l'aire d'un rectangle, comment peut- on interpréter les deux produits $(ab)c$ et $a(bc)$, et en déduire leur égalité ? Que veut dire la commutativité ?*

Exercice 32. *Soit G un groupe tel que $\forall x \in G$, $x^2 = 1$. Montrer que G est commutatif.*

Exercice 33. *Soit n un entier naturel. Montrer que les classes $[x]$ modulo n forment un monoïde avec la multiplication $[x][y] = [xy]$. Il faut montrer qu'elle est bien définie. Montrer que l'ensemble des classes $[x]$, où x est premier avec n, forme un groupe avec cette multiplication. Utiliser le théorème de Bezout.*

3 Actions de groupe

Définition 3.1. *Une* action à gauche *d'un groupe G sur un ensemble E est une fonction $G \times E \to E$, notée (comme une multiplication) $(g, e) \mapsto ge$, telle que pour tous g, g' dans G et e dans E, on ait :*
(i) $1e = e$ *; (ii)* $g(g'e) = (gg')e$.

On dit aussi que G *agit* sur E, ou encore *opère* sur E.

Définition 3.2. *Soit G un groupe agissant sur E à gauche et $e \in E$.*
*(i) L'*orbite *de e est le sous-ensemble $\{ge | g \in G\}$ de E.*
(ii) Le stabilisateur *de e est le sous-ensemble $\{g \in G | ge = e\}$ de G.*

Intuitivement, l'orbite de e est l'ensemble des *points* (éléments de E) qu'on peut atteindre à partir de e en faisant agir sur e un élément de G. Le stabilisateur de e, par contre, est l'ensemble des éléments de G dont l'action sur e ne fait rien (ne déplace pas e). On notera $Orb(e)$ l'orbite de e, et G_e le stabilisateur de e.

Exemple 3.3. *1. Faisons agir le groupe additif $\mathbb{R}$ sur l'ensemble des nombres complexes $\mathbb{C}$ par : $ge = g + e$ (ici $g \in R$ et $e \in \mathbb{C}$). L'orbite de e est l'ensemble des $g + e, g \in \mathbb{R}$, et peut être vue géométriquement comme la droite horizontale qui passe par e. Le stabilisateur de e est réduit à $\{0\}$.*

2. Prenons pour G le groupe à deux éléments, noté multiplicativement ; donc $G = \{1, x\}$ et $x^2 = 1$. Prenons $A = \{a, b, c\}$ avec l'action : $xa = a, xb = c, xc = b$. L'action est entièrement définie par ces trois égalités, à cause de 3.1 (i). Pour vérifier 3.1 (ii), il suffit de prendre $g = g' = x$ (puisque g ou $g' = 1$ dans (ii) le rend évident). On a $x(xa) = xa = a = 1a - (xx)a$; $x(xb) = xc = b = 1b = (xx)b$; et de manière analogue, $x(xc) = (xx)c$.

L'orbite de a est $\{a\}$, celle de b est $\{b, c\}$, et c'est aussi celle de c. Le stabilisateur de a est G, et celui de b, et de c, est $\{1\}$.

Théorème 3.4. *Soit G un groupe agissant à gauche sur un ensemble E.*

(i) Le stabilisateur d'un élément de E est un sous-groupe de G.

(ii) E est réunion disjointe des orbites.

(iii) Si G et E sont finis, la cardinalité d'une orbite est égale à $|G|/|G_e|$, où e est un élément de l'orbite, et G_e le stabilisateur de e.

Dans le cas fini, on note $|G|/|G_e| = [G : G_e]$, appelé l'*indice*[1] de G_e dans G. Notons que la cardinalité d'un groupe est aussi souvent appelé son *ordre*.

Dans les exemples 3.3, les stabilisateurs sont visiblement des sous-groupes. De plus, le plan complexe $\mathbb{C}$ est réunion disjointe des droites horizontales ; et $\{a, b, c\}$ est la réunion disjointe de $\{a\}$ et de $\{b, c\}$.

Démonstration. (i) Soit $e \in E$. Alors le stabilisateur de e est $H = \{g \in G | ge = e\}$. On a $1 \in H$ car $1e = e$, d'après 3.1 (i). De plus, si $g, h \in H$, alors $(gh)e = g(he)$ (d'après 3.1 (ii)) $= ge$ (puisque $h \in H$) $= e$ (puisque $g \in$) ; donc $gh \in H$. Enfin, on a $g^{-1}e = g^{-1}(ge)$ (puisque $g \in H$) $= (g^{-1}g)e = 1e = e$, par 3.1 (ii) et (i). D'où $g^{-1} \in H$. D'après la définition 2.13, H est donc un sous- groupe de G.

(ii) Il suffit de montrer qu'il existe une relation d'équivalence $\sim$ sur E dont les classes d'équivalences sont les orbites. Définissons $\sim$ par : e e' s'il existe $g \in G$ tel que $e' = ge$ (c'est-à-dire, e' appartient à l'orbite de e). Cette relation est réflexive, car $e = 1e$. Elle est symétrique, car $e' = ge \Rightarrow g^{-1}e' = e$, en faisant agir g^{-1} sur les deux membres de la première égalité, et en appliquant 3.1 (ii) et (i). La relation $\sim$ est aussi transitive car si $e' = ge$ et $e'' = g'e'$, alors $e'' = g'(ge) = (g'g)e$, par 3.1 (ii). C'est donc bien une relation d'équivalence. La classe d'équivalence de e est par définition $\{e' \in E | e' \sim e\} = \{e' \in E | \exists g \in G, e' = ge\}$, c'est-à-dire l'orbite de e.

(iii) On définit une fonction $f : G \to O$ où O est l'orbite de e, par $f(g) = ge$; cette fonction est bien définie et surjective. Soit $H = G_e$; montrons que l'image réciproque d'un élément ge de O est $gH = \{gh | h \in H\}$; on a en effet $g' \in f^{-1}(ge) \Leftrightarrow f(g') = ge \Leftrightarrow g'e = ge \Leftrightarrow g^{-1}g'e = e \Leftrightarrow g^{-1}g' \in H \Leftrightarrow g' \in gH$. Or la cardinalité de gH est $|H|$, car $h \mapsto gh, H \to gH$ est une bijection. Comme les images réciproques de f ont toute la même cardinalité $|H|$, et f étant surjective, on a $|O| = |G|/|H|$. □

1. On dit aussi *index*, qui est le mot anglais.

Lorsque G agit sur un ensemble E, on appelle *représentant* d'une orbite un élément de cette orbite ; un *système de représentants* est un sous-ensemble de E qui rencontre chaque orbite en un seul élément.

Corollaire 3.5. *Soit G un groupe fini agissant sur un ensemble fini E. Soit S un système de représentants des orbites. On a*

$$|E| = \sum_{e \in S} |G|/|G_e|.$$

Rappelons que $|G|/|G_e|$ est un entier (théorème 3.4 (iii)). On appelle parfois cette égalité l'*équation aux classes*.

Démonstration. Cela découle du théorème 3.4 (ii) et (iii). □

Définition 3.6. *Soit E un groupe et G un sous-groupe de E. Définissons une action à gauche du groupe G sur l'ensemble E par : ge est le produit dans le groupe E de g par e. Cette action s'appelle l'action de G par* translation à gauche *sur E. C'est bien une action, car E étant un groupe, on a $1e = e$, et $(gg')e = g(g'e)$. Introduisons la notation suivante : pour $e \in E$, $Ge = \{ge | g \in G\}$. Ce sous-ensemble de E s'appelle la* classe à droite *de e modulo G, ou le* translaté de G à droite *par e.*

Théorème 3.7. *Soit E un groupe fini et G un sous-groupe de E. Dans l'action définie en 3.6, toutes les orbites ont le même nombre d'éléments. Une telle orbite est de la forme Ge, pour un e. Ces orbites sont disjointes et E est égal à leur réunion dans E.*

Le nombre d'orbites est appelé l'*indice* de G dans E, noté $[E : G]$. Dans ce cas, notant $e_1, \ldots, e_k$ des représentant des orbites, $k = [E : G]$, on a

$$E = \bigcup_{1 \leq i \leq k} Ge_i, \tag{1}$$

où la réunion est disjointe.

Démonstration. Soit $e \in E$. L'orbite de e est par définition $\{ge | g \in G\}$, c'est-à-dire c'est Ge. Définissons une fonction $\gamma : G \to Ge$ par $\gamma(g) = ge$. Cette fonction est surjective, c'est-à-dire son image est Ge. Elle est aussi injective, car si $\gamma(g) = \gamma(g')$, on a $ge = g'e$, d'où en multipliant à droite par e^{-1}, $g = g'$. Donc γ est une bijection $G \to Ge$, et le nombre d'éléments de l'orbite Ge est égal à celui de G. □

Corollaire 3.8. *Soit G un groupe fini et H un sous-groupe. Alors $|H|$ divise $|G|$.*

Ce résultat est appelé le *théorème de Lagrange.*

Démonstration. En appliquant le théorème 3.7 (avec E, G remplacés par G, H), on trouve que G est réunion disjointe de sous-ensembles qui ont tous le même nombre d'éléments $|H|$. Si n est le nombre de ces sous-ensembles, on a donc $|G| = n|H|$. □

Exercice 34. *On fait agir le sous-groupe $n\mathbb{Z}$ sur $\mathbb{Z}$ par translation. Quelles sont les orbites ? Combien y en a-t-il ?*

Exercice 35. *On fait agir $(\mathbb{R}, +)$ sur $\mathbb{C}$ à gauche par $(x, z) \mapsto e^{ix}z$. Vérifier que c'est bien une action. Quelles sont les orbites ?*

Exercice 36. *On définit une fonction $G \times G \to G, (g, x) \mapsto gxg^{-1}$. Montrer que c'est une action à gauche de G sur lui-même : $g \cdot x = gxg^{-1}$. Quelle est l'orbite de 1 ? Montrer que $x \in G$ a une orbite réduite a un élément si et seulement si x est dans le* centre *$C(G)$ de G, où $C(G) = \{x \in G | \forall g \in G, xg = gx\}$. Montrer que $C(G)$ est un sous-groupe de G.*

Exercice 37. *Deux éléments g, g' d'un groupe G sont dits* conjugués *s'il existe x dans G tel que $g' = xgx^{-1}$. Montrer que la conjugaison est une relation d'équivalence. Les classes sont appelées* classes de conjugaison*. Montrer que les classes de conjugaison sont les orbites de l'action définie dans l'exercice 36.*

Exercice 38. *Montrer qu'un sous-groupe H de G est normal si et seulement s'il est réunion de classes de conjugaison (voir exercice 37).*

Exercice 39. *Soit $G = \mathbb{Z}/2\mathbb{Z}$. On considère l'action de G sur $\mathbb{C}$ définie par : $[0] \cdot z = z$ et $[1] \cdot z = \bar{z}$.*

a) Vérifier que c'est bien une action.

b) Décrire les orbites et les stabilisateurs.

c) Montrer que l'ensemble des orbites est en bijection avec $\mathbb{R} \times \mathbb{R}_+$.

Exercice 40. *Soit $G = \mathbb{Z}/2\mathbb{Z}$, qu'on fait opérer sur $\mathbb{C}^*$ par : $[0] \cdot z = z$ et et $[1] \cdot z = z^{-1}$. Répondre pour cette action aux questions a) et b) de l'exercice 39. Montrer que l'ensemble des orbites est en bijection avec $E = H \cup [1, 0) \cup (0, 1]$, où $H = \{a + bi \in \mathbb{C} | b > 0\}$.*

Exercice 41. *On fait agir le groupe G des racines n-èmes de l'unité sur $\mathbb{C}$ par : $e^{2ik\pi/n} \cdot z = e^{2ik\pi/n}z$. Vérifier que c'est bien une action, et montrer que toute orbite a n éléments. Décrire ces orbites. Montrer que l'ensemble des orbites est en bijection avec l'ensemble $\{z \in \mathbb{C}^* | 0 \leq arg(z) < 2\pi/n\}$.*

Exercice 42. *Dans les hypothèses du théorème 3.7, montrer que le nombre d'orbites, c'est-à-dire de classes à droite modulo G, est $|E|/|G|$. Ce nombre s'appelle l'*indice *du sous-groupe G de E, et on le note $[E : G]$.*

Exercice 43. *Soit G un groupe fini agissant à gauche sur E. Soit O une orbite, $e \in O$ et H le stabilisateur de e. Montrer que la fonction qui a une classe à gauche gH modulo H associe ge est une fonction bien définie et bijective de l'ensemble des classes à gauche modulo H dans l'orbite O. En déduire que $|O| = |G|/|H|$ (utiliser l'exercice 42).*

Exercice 44. *Montrer que si le groupe G agit sur deux ensembles disjoints non vides, il agit aussi naturellement sur leur réunion. Montrer qu'il y a au moins deux orbites.*

Exercice 45. *Soit G un groupe agissant sur E. Montrer que G agit aussi sur $E \times E$ par : $g(e, e') = (ge, ge')$. Montrer que si $|E| \geq 2$, il y a au moins deux orbites pour cette action de G sur $E \times E$ (on l'appelle l'*action diagonale*).*

Exercice 46. ** Soit G un groupe agissant sur E. Montrer que G agit sur E^n, $n \geq 1$ par : $g(e_1, e_2, \ldots, e_n) = (ge_1, ge_2, , ge_n)$. Montrer que si $|E| \geq 2$, alors il y a au moins 2^{n-1} orbites pour cet action.*

Exercice 47. ** Soit G un groupe fini agissant à gauche sur l'ensemble fini E. On note $Fix(g) = \{e \in E | ge = e\}$, et $Stab(e) = \{g \in G | ge = e\}$ (le stabilisateur de e, aussi noté précédemment G_e).*

a) Montrer que si $ge = e'$ alors $Stab(e') = gStab(e)g^{-1}$.

b) Déduire que si e, e' sont dans la même orbite C, alors $|Stab(e)| = |Stab(e')|$; ce nombre est noté $stab(C)$.

c) Montrer que $|C|stab(C) = |G|$.

d) Déduire que $\sum_{e \in C} |Stab(e)| = |G|$, pour toute orbite C.

e) Montrer que $\sum_{g \in G} |Fix(g)| = \sum_{e \in E} |Stab(e)|$.

f) Déduire que $(1/|G|) \sum_{g \in G} |Fix(g)|$ est égal au nombre d'orbites de l'action de G sur E. Cette formule s'appelle la formule de Burnside.

Exercice 48. *Soit G un groupe abélien de cardinalité nm, où n et m sont premiers entre eux. Soit H et K deux sous-groupes de G tel que $|H| = n$ et $|K| = m$. Montrer que G est isomorphe à $H \times K$.*

4 Homomorphismes, sous-groupes normaux et quotients

Définition 4.1. *Un* homomorphisme *de groupes est une fonction f d'un groupe G dans un groupe G' telle que*

$$\forall g, g' \in G, f(gg') = f(g)f(g').$$

Autrement dit, f préserve la multiplication, ou plus précisément, transforme la multiplication de G en celle de G'. On remarquera que si G est noté additivement et G' multiplicativement, la dernière égalité s'écrira : $f(g+g') = f(g)f(g')$. Il y a deux autres cas, laissés au lecteur.

Exemple 4.2. *1. Prenons $G = (\mathbb{R}, +)$ et $G' = (\mathbb{R}_+^*, \cdot)$. Soit $f(x) = e^x$. Alors $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$. La fonction f est donc un homomorphisme du groupe G vers le groupe G'. Cette fonction a une fonction réciproque $g : G' \to G$; c'est l'homomorphisme défini par $g(x) = \ln(x)$; on a $\ln(xy) = \ln(x) + \ln(y)$, donc g est un homomorphisme $G' \to G$.*

2. Soit $G = (\mathbb{C}^*, \cdot)$ et $G' = (\mathbb{R}_+^*)$. La fonction qui au nombre complexe z associe son module $|z|$ est un homomorphisme de groupes : $|zz'| = |z||z'|$.

3. Soit $G = (\mathbb{Z}, +)$, G' un groupe quelconque et $a \in G'$. La fonction $G \to G', n \mapsto a^n$ est un homomorphisme. En effet, $a^{n+m} = a^n a^m$ (exercice 19).

Proposition 4.3. *Soit $f : G \to G'$ un homomorphisme de groupes. Alors*
(i) $f(1) = 1$;
(ii) $\forall g \in G, f(g^{-1}) = f(g)^{-1}$.

Ainsi, un homomorphisme de groupes se comporte comme il faut vis-à-vis de la structure de groupe (produit, inverse, élément neutre). En particulier, l'inverse de l'image d'un élément par un homomorphisme est égal à l'image de l'inverse de cet élément.

Démonstration. (i) On a $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$. En multipliant par l'inverse de $f(1)$ (dans G'), on trouve $1 = f(1)$ (attention : on écrit 1 pour l'élément neutre de G et de G' ; le contexte montre duquel il s'agit : par exemple dans $1 = f(1)$, le premier 1 est dans G' puisqu'il est dans l'image de f, et le second 1 est dans G, puisqu'on lui applique f. Le lecteur qui aime les points sur les i pourra écrire $f(1_G) = 1_{G'}$, etc. . .).

(ii) On a par (i) $f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1$. Donc l'unicité de l'inverse (proposition 2.12) oblige $f(g)^{-1} = f(g^{-1})$. □

Proposition 4.4. *Les homomorphismes de groupes préservent les sous-groupes par image directe et inverse.*

Voir les exercices 53 et 55.

Définition 4.5. *Soit $f : G \to G'$ un homomorphisme de groupes. Son* noyau*, noté $N(f)$, est $\{g \in G | f(g) = 1\}$.*

Autrement dit, $N(f) = f^{-1}(1)$.

L'importance de cette notion vient entre autres du théorème qui suit.

On note souvent $N(f) = \ker(f)$ à cause du mot allemand Kern signifiant noyau.

Théorème 4.6. *Un homomorphisme $f : G \to G'$ est injectif si et seulement si $N(f) = \{1\}$.*

Pour vérifier que f est injectif, il suffit de vérifier que $N(f) \subset \{1\}$, autrement dit que

$$f(g) = 1 \Rightarrow g = 1.$$

Démonstration. On a déjà $1 \in N(f)$, d'après la proposition 4.3 (i), donc $\{1\} \subset N(f)$.

Supposons f injective, et soit $g \in N(f)$. Alors $f(g) = 1 = f(1)$ (par la même proposition que ci-dessus), donc $g = 1$ par injectivité. D'où $N(f) = \{1\}$.

Supposons maintenant que $N(f) = \{1\}$ et soient $g, g' \in G$ tels que $f(g) = f(g')$. Alors (astuce !), $1 = f(g)^{-1}f(g') = f(g^{-1})f(g')$ (par la proposition 4.3 (ii)) $= f(g^{-1}g')$. Donc $g^{-1}g' \in N(f) = \{1\}$ et donc $g^{-1}g' = 1$ par multiplication par g à droite de chaque côté ; enfin $g = g'$. Ceci montre que f est injective. □

Théorème 4.7. *Si $f : G_1 \to G_2, g : G_2 \to G_3$ sont des homomorphismes de groupes, il en est de même pour $g \circ f : G_1 \to G_3$.*

Nous laissons la démonstration de ce théorème au lecteur.

Définition 4.8. *Un sous-groupe normal, ou distingué, d'un groupe G est un sous-groupe H tel que $\forall h \in H, \forall g \in G, g^{-1}hg \in H$.*

On dit que deux éléments x, y de G sont *conjugués* s'il existe $g \in G$ tel que $y = gxg^{-1}$. Cette relation est une relation d'équivalence, comme on le vérifie, appelée la *conjugaison*, et ses classes d'équivalence sont appelées les *classes de conjugaison*. Voir les exercices 36 et 37.

Un sous-groupe H est donc normal si et seulement s'il est réunion de classe de conjugaison. Autrement dit : si $g \in H$ et si g' est conjugué à g, alors $g' \in H$. Voir l'exercice 38.

La notion de sous-groupe normal est reliée de très près à celle d'homomorphisme (bien que ça ne saute pas aux yeux, à première vue). En effet, nous avons le théorème suivant.

Théorème 4.9. *Soit $f : G \to G'$ un homomorphisme de groupes. Alors $N(f)$ est un sous-groupe normal de G.*

Démonstration. Démonstration On a déjà $1 \in N(f)$, d'après la proposition 4.3. Si $g, g' \in N(f)$, alors $f(gg') = f(g)f(g') = 1 \cdot 1 = 1$, donc $gg' \in N(f)$. De plus, $f(g^{-1}) = f(g)^{-1}$ (d'après la proposition 4.3) $= 1^{-1} = 1$, donc $g^{-1} \in N(f)$. Donc $N(f)$ est un sous-groupe. Montrons qu'il est normal : si $h \in N(f)$ et $g \in G$, alors $f(g^{-1}hg) = f(g^{-1}h)f(g) = f(g^{-1})f(h)f(g) = f(g)^{-1}1f(g) = f(g)^{-1}f(g) = 1$, d'où $g^{-1}hg \in N(f)$. C'est donc bien un sous-groupe normal. □

On notera que dans un groupe commutatif, tout sous-groupe est normal ; en effet, $g^{-1}hg = hg^{-1}g = h$ est alors dans H. La notion de sous-groupe normal n'acquiert toute son importance que dans le cas non commutatif. Comme nous manquons pour le moment d'exemples de groupes non commutatifs, il faudra patienter pour voir des exemples significatifs de sous-groupes normaux.

Dans la suite de ce chapitre, nous allons voir que tout sous-groupe normal s'obtient comme dans le théorème 4.9, i.e. comme noyau d'un homomorphisme. On peut en fait même dire que la notion d'homomorphisme de groupes est équivalente à celle de sous-groupe normal, en un sens bien précis (cf. exercice 52).

Nous avons vu au chapitre précédent la notion de classe à droite : si N est un sous-groupe de G, une classe à droite modulo N est un sous-ensemble de G de la forme Ng où $g \in G$. De même, une *classe à gauche* modulo N est de la forme gN.

Notation Si A, B sont deux parties du groupe G, nous notons $AB = \{ab | a \in A, b \in B\}$, c'est-à-dire l'ensemble de tous les produits d'un élément de A par un élément de B ; nous l'appellerons le *produit* de A par B.

Théorème 4.10. *Soit N un sous-groupe normal d'un groupe G.*

(i) Pour tout $g \in G$, on a $gN = Ng$. Donc toute classe à gauche modulo N est une classe à droite, et vice-versa.

(ii) Pour tous $g, g' \in G$, on a $(gN)(g'N) = (gg')N$.

(iii) L'ensemble des classes (à gauche ou à droite) modulo N forme un groupe sous la multiplication définie par le produit des parties de G ; l'élément neutre est $1N = N$.

Nous appellerons $gN = Ng$ la classe de g modulo le sous-groupe normal N.

Démonstration. (i) Si $x \in gN$, alors on a $x = gn$ pour un certain $n \in N$. Donc $x = gng^{-1}g = n'g$, où nous avons posé $n' = gng^{-1}$; N étant normal, n' est dans N, d'où $x \in Ng$ et donc $gN \subset Ng$. De manière analogue, on montre l'inclusion inverse. D'où l'égalité.

(ii) Le produit des parties de G est associatif (voir exercice 21). De plus $gN = \{g\}N$. On a donc $(gN)(g'N) = gNg'N = g(Ng')N = g(g'N)N$ (d'après (i)) $= (gg')(NN)$. De plus, $NN = N$, car N est un sous-groupe (voir exercice 21). Donc $(gN)(g'N) = (gg')N$.

(iii) D'après (ii), l'ensemble des classes à gauche modulo N forme un monoïde d'élément neutre N. De plus, $(gN)(g^{-1}N) = (gg^{-1})N = 1N = N$, donc c'est un groupe. □

Définition 4.11. *Soit N un sous-groupe normal d'un groupe G. L'ensemble des classes modulo N, avec le produit défini au théorème 4.10, s'appelle le* groupe quotient *de G par N, noté G/N.*

Théorème 4.12. *Soit N un sous-groupe normal d'un groupe G. La fonction qui à un élément g de G associe sa classe modulo N est un homomorphisme surjectif de G dans G/N, de noyau N.*

La fonction $G \to G/N$ décrite ci-dessus s'appelle l'*homomorphisme canonique* (ou *naturel*), ou encore *projection canonique*, de G dans G/N.

Lemme 4.13. *On a : $gN = N \Leftrightarrow g \in N$.*

Démonstration. □

Preuve du théorème 4.12. Le fait que c'est un homomorphisme résulte de la formule (ii) du théorème 4.10. Le noyau est l'ensemble des g tels que $gN = N$ (puisque N est l'élément neutre de G/N) ; mais cette égalité implique $g = g \cdot 1 \in N$, et vice versa : $g \in N \Rightarrow gN \subset NN = N$ et $N = g(g^{-1}N) \subset gN$, puisque $g^{-1} \in N$; donc $gN = N$. □

Corollaire 4.14. *Dans les hypothèses du théorème 4.12, on suppose G fini. Alors $|G| = |N||G/N|$.*

Démonstration. Soit p la projection canonique $G \to G/N$. On vérifie que ses fibres sont les classes modulo N ; et que celles-ci on toutes même cardinalité $|N|$. D'où l'égalité. □

La construction du quotient contient comme cas particulier celle du quotient de $\mathbb{Z}$ par un sous-groupe de $\mathbb{Z}$. Un tel sous-groupe est de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$. Les éléments $\mathbb{Z}/n\mathbb{Z}$ sont les $i + n\mathbb{Z}$, c'est-à-dire les classes de la congruence modulo n. On note aussi $i+n\mathbb{Z} = [i]$. Dans $\mathbb{Z}/n\mathbb{Z}$, on additionne comme suit : $[i]+[j] = [i+j]$, autrement dit $(i+n\mathbb{Z})+(j+n\mathbb{Z}) = (i+j)+n\mathbb{Z}$, conformément à ce qui précède.

Théorème 4.15. *Soit $f : G \to G'$ un homomorphisme de groupes et N son noyau. Soit $p : G \to G/N$ l'homomorphisme canonique. Il existe un unique homomorphisme $\bar{f} : G/N \to G'$ tel que $f = \bar{f} \circ p$.*

On appelle ce théorème *propriété universelle du quotient*. On la représente souvent par un diagramme (qui est dit *commutatif*).

Démonstration. 1. L'unicité de $\bar{f}$ se prouve ainsi : soit x un élément de G/N, donc $x = gN$, $g \in G$. Autrement dit $x = p(g)$. Alors $\bar{f}(x) = \bar{f}(p(g) = \bar{f} \circ p(g) = f(g)$. Donc $f(x)$ est uniquement déterminé.

2. Définissons $\bar{f}$ par $\bar{f}(gN) = f(g)$. Alors f est bien définie : si en effet $gN = g'N$, alors $g' \in gN \Rightarrow g = gn$, pour un $n \in N$, d'où $f(g') = f(g)f(n) = f(g)$, puisque $f(n) = 1$, N étant le noyau de f. La fonction $\bar{f}$ est un homomorphisme car $\bar{f}(gNg'N) = \bar{f}(gg'N)$ (par le théorème 4.10 (ii)) $= f(gg') = f(g)f(g') = \bar{f}(gN)\bar{f}(g'N)$. □

Définition 4.16. *Un* isomorphisme *d'un groupe G vers un groupe G' est un homomorphisme bijectif.*

Deux groupes sont dits isomorphes *s'il existe un isomorphisme de l'un vers l'autre. Notation : $G \simeq G'$.*

Exemple 4.17. *Soit G le groupe commutatif, noté multiplicativement, $G = \{1, a, b\}$ avec $ab = 1, a^2 = b, b^2 = a$. De même, soit G' le groupe commutatif, noté additivement, $G' = \{0, u, v\}$, avec $u + v = 0, u + u = v, v + v = u$. La fonction f, définie par $f(1) = 0, f(a) = u, f(b) = v$ est un isomorphisme de G vers G'. De plus, la fonction g, définie par $g(1) = 1, g(a) = b, g(b) = a$ est un isomorphisme de G vers lui-même.*

Proposition 4.18. *Si $f : G \to G'$ est un homomorphisme de groupes bijectif, alors $f^{-1} : G' \to G$ est un isomorphisme.*

Corollaire 4.19. *Dans les hypothèses du théorème 4.15, $\bar{f}$ est injectif; si f est de plus surjectif, $\bar{f}$ est un isomorphisme.*

Démonstration. Si $\bar{f}(gN) = e'$ (le neutre de G'), alors $f(g) = e'$ et $g \in N$. Donc $gN = N$, le neutre de G/N. Donc f est injectif, d'après le théorème 4.6.

De plus, si f est surjectif et si $g' \in G'$, il existe $g \in$ tel que $g' = f(g)$. Alors $g' = \bar{f}(p(g))$. Donc $\bar{f}$ est surjectif. □

Corollaire 4.20. *Dans les hypothèses du théorème 4.15, $Im(f)$ est isomorphe à $G/Ker(f)$.*

Une conséquence de ceci est le *théorème chinois*. Notons d'abord la notion de *produit de groupes* : voir l'exercice 67.

Théorème 4.21. *Soit $n = n_1 \cdots n_k$, $n, n_1, \ldots n_k \in \mathbb{N}^*$, où les n_i sont des entiers premiers entre eux deux à deux. Alors la fonction*

$$x \mod n \mapsto (x \mod n_1, \ldots, x \mod n_k), \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

est un isomorphisme de groupes bien défini.

Démonstration. Considérons la fonction $\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}, x \mapsto (x \mod n_1, \ldots, x \mod n_k)$. C'est un homomorphisme de groupes, dont le noyau est l'intersection des noyaux des homomorphismes canoniques $\mathbb{Z} \to \mathbb{Z}/n_i$ (exercice 77) ; le noyau de ce dernier homomorphisme est $n_i\mathbb{Z}$, et l'intersection des $n_i\mathbb{Z}$ est $n\mathbb{Z}$ car les n_i sont premiers entre eux deux à deux. Par le théorème 4.15 et le corollaire 4.19, la fonction de l'énoncé est donc un homomorphisme de groupes injectif ; comme les deux côtés ont la même cardinalité, il est aussi surjectif. □

Définition 4.22. *Un groupe G est dit* cyclique *s'il existe un homomorphisme surjectif $\mathbb{Z} \to G$.*

Il s'agit bien entendu de $\mathbb{Z}$ additif ($\mathbb{Z}$ multiplicatif n'est pas un groupe).

Proposition 4.23. *Pour tout entier naturel n, $\mathbb{Z}/nZ$ est cyclique. En particulier Z est cyclique.*

Démonstration. L'homomorphisme canonique $\mathbb{Z} \to Z/n\mathbb{Z}$ est en effet surjectif. Pour $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ est isomoprhe à $\mathbb{Z}$. □

Théorème 4.24. *Un groupe G est cyclique si et seulement s'il existe un élément $a \in G$ tel que tout élément de G soit de la forme $a^n, n \in Z$.*

Un tel élément a s'appelle un *générateur* du groupe cyclique G, et on dit que a *engendre* G. Pour la notation a^n, voir l'exercice 19.

Démonstration. Si G est cyclique, il existe un homomorphisme surjectif $f : \mathbb{Z} \to G$. Posons $a = f(1)$. Soit $g \in G$, quelconque. Comme f est surjectif, il existe $n \in \mathbb{Z}$ tel que $f(n) = g$. Si $n \geq 0$, alors $f(n) = f(1 + 1 + \cdots + 1)$ (n fois) $= f(1)f(1)\cdots f(1)$ (n fois) $= a^n$. Si $n < 0$, alors $f(n) = f(-(-n)) = f(-n)^{-1}$ (par la proposition 4.3) $= (a^{-n})^{-1}$ (par ce que nous venons de voir) $= a^n$. Donc, tout élément de G est de la forme a^n, $n \in \mathbb{Z}$.

Réciproquement, si tout élément de G est de la forme a^n, définissons une fonction $f : Z \to G$, par $f(n) = a^n$. Elle est surjective par hypothèse, et c'est un homomorphisme par la loi des exposants, voir l'exercice 19. □

Théorème 4.25. *Soit G un groupe cyclique. S'il est infini, il est isomorphe à $\mathbb{Z}$. S'il est fini, il existe $n \in \mathbb{N}^*$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

En particulier, un groupe cyclique est toujours commutatif.

Démonstration. Par hypothèse, il existe un homomorphisme surjectif $h : Z \to G$. Si $N(h) = \{0\}$, h est injectif d'après le théorème 4.6, donc bijectif, et c'est un isomorphisme. Si $N(h) \neq \{0\}$, $N(h) = n\mathbb{Z}$ pour un entier naturel $n \geq 1$ (théorème 2.15). Il existe alors d'après le corollaire 4.19 un isomorphisme $h : \mathbb{Z}/n\mathbb{Z} \to G$. □

L'*ordre* d'un élément g d'un groupe G est le plus petit $k \in \mathbb{N}^*$ tel que $g^k = 1$; si un tel k n'existe pas, g est dit d'*ordre infini*.

Théorème 4.26. *Soit G un groupe, $g \in G$ et H le sous-groupe engendré par g. L'ordre de g est égal à la cardinalité de H, qui est un groupe cyclique. S'il est fini, égal à k, alors l'ensemble des $n \in \mathbb{Z}$ tels que $g^n = 1$ est $k\mathbb{Z}$.*

Démonstration. On a $H = \{g^n | n \in \mathbb{Z}\}$. Si g est d'ordre infini, H est infini.

Supposons maintenant que g est d'ordre fini k. Alors $g^k = 1$, donc $H^+ = \{g^n | n \in \mathbb{N}\} = \{1, g, \ldots, g^{n-1}$; de plus tout $g^n, n < 0$ est égal g^{n+Nk}, avec $n + Nk > 0$ pour N assez grand, donc $H \subset H^+$; donc H est fini.

Dans ce cas aussi, les éléments $1, g, \ldots, g^{n-1}$ sont tous distincts : en effet, $g^i = g^j$ avec $0 \leq i \leq j \leq n - 1$, implique $g^{j-i} = 1$, et comme $0 \leq j - i < n$, on doit avoir $j = i$. Donc $|H| = k$.

Par la loi des exposants, la fonction $h : n \mapsto g^n, \mathbb{Z} \to H$ est un homomorphisme surjectif ; donc H est un groupe cyclique. Si H est fini, il est isomorphe à $\mathbb{Z}/\ell Z$, où $\ell\mathbb{Z}$ est le noyau de h. Alors $\ell = |H|$, et $\ell = k$, l'ordre de k, et par définition du noyau, l'ensemble des $n \in \mathbb{Z}$ tels que $g^n = 1$ est $k\mathbb{Z}$. □

Le corollaire 3.8 implique donc le

Corollaire 4.27. *Dans un groupe fini G, l'ordre d'un élément divise $|G|$, et $g^{|G|} = 1$.*

Exercice 49. ** Soit H un sous-groupe d'un groupe G. Montrer que les assertions suivantes sont équivalentes :*

(i) H est normal.

(ii) $\forall g \in G, gH = Hg$.

(iii) $\forall g, g' \in G, (gH)(g'H) = (gg')H$.

(iv) $\forall g \in H, (gH)^{-1} = (g^{-1})H$ (pour $A \subset G$, on pose ici $A^{-1} = \{a^{-1} | a \in A\}$).

Exercice 50. *Montrer qu'un sous-groupe H d'indice 2 d'un groupe G est nécessairement normal.*

Exercice 51. ** On définit un* homomorphisme de monoïdes *comme une fonction f d'un monoïde M dans un monoïde M' telle que $f(1) = 1$ et que : $\forall m, m' \in M, f(mm') = f(m)f(m')$.*

(i) Montrer que la fonction $D : M \to \mathbb{R}, D(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc$ est un homomorphisme du monoïde multiplicatif des matrices carrées d'ordre 2 sur $\mathbb{R}$ dans le monoïde multiplicatif $\mathbb{R}$.

(ii) Montrer que la fonction qui à une partie A de X associe 0 si $|A|$ pair, 1 si $|A|$ impair, est un homomorphisme du monoïde $(\mathcal{P}(X), \Delta)$ dans $\mathbb{Z}/2\mathbb{Z}$ additif.

(iii) Montrer que si M est un monoïde et $a \in M$, la fonction $n \mapsto a^n$ est un homomorphisme de $\mathbb{N}$ additif dans M.

Exercice 52. *Montrer que tout sous-groupe normal d'un groupe est le noyau d'un certain homomorphisme.*

Exercice 53. *Soit $f : G \to G'$ un homomorphisme de groupes. Soit H un sous-groupe de G. Montrer que $f(H)$ est un sous-groupe de G'.*

Exercice 54. *(Mêmes hypothèses que dans l'exercice 53). On suppose que f est surjectif et que H est normal. Montrer que $f(H)$ est normal dans G'.*

Exercice 55. *Soit $f : G \to G'$un homomorphisme de groupes. Montrer que si H est un sous-groupe de G', alors $f^{-1}(H)$ est un sous-groupe de G.*

Exercice 56. *Même chose, en ajoutant 'normal" après "sous-groupe".*

Exercice 57. *Soit H, N des sous-groupes d'un groupe G. On suppose que N est normal. Montrer que $HN = NH$, et que HN est un sous-groupe de G.*

Exercice 58. *Montrer que le sous-groupe $n\mathbb{Z}$ ($n \geq 1$) de $\mathbb{Z}$ est isomorphe à $\mathbb{Z}$.*

Exercice 59. *Soit $f : \mathbb{Z} \to G$ un homomorphisme surjectif et H un sous-groupe de G. Définir un homomorphisme surjectif $f^{-1}(H) \to H$. Utiliser l'exercice 58 pour montrer que H est un groupe cyclique.*

Exercice 60. ** Une* congruence *d'un groupe (ou d'un monoïde) G est une relation d'équivalence $\sim$ sur G telle que : $\forall g, g', h, h' \in G, g\ g'$ et $h\ h' \Rightarrow gh\ g'h'$.*

a) Soit $\sim$ une congruence du groupe G. Montrer que la classe de 1 est un sous-groupe normal N de G. Montrer que $g \sim h$ implique $g^{-1} \sim h^{-1}$. Montrer que la classe de g modulo $\sim$ est $gN = Ng$.

b) Montrer que si N est un sous-groupe normal de G, on a : $\forall g, h \in G, gh^{-1} \in N \Leftrightarrow h^{-1}g \in N$. Montrer que la relation $\sim$ sur G définie par : $g \sim h \Leftrightarrow gh^{-1} \in N$, est une congruence de G (notée parfois $g \equiv h \mod N$). Montrer que la classe de g pour $\sim$ est $gN = Ng$.

c) Soit $f : G \to G'$ un homomorphisme de groupes. Montrer que la relation $\sim$ sur G définie par : $g\ h \Leftrightarrow f(g) = f(h)$, est une congruence de G. Montrer que la classe de g est $f^{-1}(f(g)) = gN(f) = N(f)g$.

Exercice 61. *Soit G un groupe et $a \in G$. Montrer que la fonction $\ell : G \to G, \ell(g) = aga^{-1}$ est un isomorphisme de G dans G.*

Exercice 62. ** Soit G l'ensemble des fonctions de $\mathbb{C}$ vers $\mathbb{C}$, de la forme $z \mapsto az+b$, où $a, b \in \mathbb{C}, a \neq 0$. Montrer qu'avec la composition des fonctions, G est un groupe non commutatif. Soit N l'ensemble des fonctions de la forme $z \mapsto z+b$; montrer que N est un sous-groupe normal de G. Soit H l'ensemble des fonctions de la forme $z \mapsto az, a \neq 0$; montrer que H est un sous-groupe de G, qui n'est pas normal.*

Exercice 63. *Montrer que si $f : G \mapsto G'$ est un homomorphisme surjectif et si G est commutatif, alors G' est commutatif.*

Exercice 64. *Montrer que $x+n\mathbb{Z}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x est premier avec n.*

Exercice 65. *Montrer que $n+6\mathbb{Z} \mapsto n+3\mathbb{Z}$ est un homomorphisme surjectif bien défini de $\mathbb{Z}/6\mathbb{Z}$ vers $\mathbb{Z}/3\mathbb{Z}$. Quel est son noyau ?*

Exercice 66. ** Généraliser l'exercice précédent à $\mathbb{Z}+ab\mathbb{Z} \mapsto \mathbb{Z}+a\mathbb{Z}$ ($a, b \in \mathbb{N}^*$).*

Exercice 67. *Le* produit cartésien *de deux groupes G et G' est l'ensemble $G \times G'$ avec la loi $(g, g')(g_1, g'_1) = (gg_1, g'g'_1)$. Montrer que c'est un groupe.*

Exercice 68. *Montrer que $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Aide : définir $n \mapsto (n+2\mathbb{Z}, n+3\mathbb{Z})$ de $\mathbb{Z}$ vers $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et utiliser le corollaire 4.19.*

Exercice 69. *Déterminer les ordres des éléments de $\mathbb{Z}/12\mathbb{Z}$ (attention à la notation additive).*

Exercice 70. *Montrer que si $g \in G$ est d'ordre k, alors $\{g^0, g^1, \ldots, g^{k-1}\}$ est un sous-groupe de G ayant k éléments et isomorphe à $\mathbb{Z}/k\mathbb{Z}$.*

Exercice 71. *Montrer que l'intersection de deux sous-groupes normaux est un sous-groupe normal.*

Exercice 72. ** Soient $K \subset H \subset G$ des groupes, où K et H sont normaux dans G. Montrer que $gK \mapsto gH$ est un homomorphisme surjectif bien défini de $G \times K$ dans $G \times H$ (ceci généralise l'exercice 16).*

Exercice 73. *Soit A une partie du groupe G. Montrer que $C = \{g \in G | \forall a \in A, ga = ag\}$ et $N = \{g \in G | gAg^{-1} = A\}$ sont des sous-groupes de G, et que C est un sous-groupe normal de N.*

Exercice 74. *Trouver un isomorphisme (s'il en existe) entre les groupes suivants :*

a) $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/3Z \times \mathbb{Z}/4\mathbb{Z}$.

b) $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3Z$. Indication : montrer qu'il existe un élément d'ordre 4 dans l'un des deux.

c) $\mathbb{R}_+^* \times \{1, -1\}$ et $\mathbb{R}^*$ (avec la multiplication).

Exercice 75. *Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les diviseurs de n.*

Exercice 76. *Montrer qu'un groupe de cardinalité p est isomorphe à $Z/p\mathbb{Z}$.*

Exercice 77. *Soit f (resp. g) un homomorphisme du groupe G dans le groupe A (resp. B). On définit $\varphi : G \to A \times B$ par $\varphi(x) = (f(x), g(x))$. Montrer que φ est un homomorphisme de groupes (voir exercice 67) et que $N(\varphi) = N(f) \cap N(g)$.*

Exercice 78. *Soit G un groupe d'exposant n, c'est-à-dire tel que $\forall g \in G$, on a $g^n = 1$. Montrer que la fonction $G \times \mathbb{Z}/n\mathbb{Z} \to G, (g, i) \mapsto g^i$ est bien définie.*

Exercice 79. *Un groupe est dit* simple *s'il n'a pas d'autre sous-groupes normaux que $\{1\}$ et lui-même. Montrer que le groupe additif $\mathbb{Z}/p\mathbb{Z}$ est simple si et seulement si p est premier.*

Exercice 80. ** Montrer que si H est un sous-groupe d'indice 2 d'un groupe G, alors H est normal et G/H est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.*

Exercice 81. ** Soit G un groupe, $a \in G, b \in G$. On suppose que les ordres de a et b sont premiers entre eux.*

a) Si G est commutatif, montrer que l'ordre de ab est le produit des ordres de a et de b.

b) Le résultat a) est-il vrai si G n'est pas commutatif ? Ou si les ordres ne sont pas premiers entre eux ?

Exercice 82. ** Prouver que le groupe $(\mathbb{Q}, +)$ n'est pas cyclique.*

Exercice 83. ** Prouver que le groupe quotient $\mathbb{Q}/\mathbb{Z}$ est infini mais que tous ses éléments sont d'ordre fini.*

Exercice 84. ** Trouver cinq groupes non-isomorphes d'ordre 16.*

Exercice 85. *Soit $X = \{x_1, x_2, x_3, \ldots, x_n\}$, $n \geq 1$, un ensemble à n éléments. Définir sur l'ensemble des fonctions $\{1, 2, \ldots, n\} \to \mathbb{Z}/2\mathbb{Z}$ une structure de groupe et montrer que ce groupe est isomorphe à $(\mathcal{P}(X), \Delta)$, où Δ dénote la différence symétrique.*

Exercice 86. *Soit $\phi : G \to \mathbb{C}^*$ un homomorphisme de groupes. Montrer que si G est fini alors $\forall g \in G$, $\phi(g)$ est une racine de l'unité.*

Exercice 87. *Un sous-groupe H du groupe G est dit* caractéristique *si pour tout automorphisme ϕ de G, on a $\phi(H) \subset H$. Montrer qu'un sous-groupe caractéristique de G est toujours normal. Indication : montrer d'abord que pour tout $a \in G$, $g \mapsto aga^{-1}$ est un automorphisme de G.*

Exercice 88. ** Un sous-groupe H du groupe G est dit* maximal *si $H \neq G$, et si pour tout sous-groupe K de G, on a : $H \subset K \Rightarrow H = K$ ou $K = G$. Montrer que l'intersection de tous les sous-groupes maximaux de G est un sous-groupe normal de G.*

Exercice 89. *Prouver que le groupe défini à l'exercice 6.18 (? ? ?) est isomorphe à $(\mathbb{R}, +)$.*

Exercice 90. *Si H est un sous-groupe de G, montrer que $gH \mapsto Hg^{-1} = (gH)^{-1}$ est une bijection entre les classes à gauche modulo H et les classes à droite. Le nombre de classes à gauche (ou à droite) s'appelle l'*indice *de H dans G.*

Exercice 91. *Montrer que si H est un sous-groupe de G, alors H est normal si et seulement si : $\forall u, v \in G, uv \in H \Leftrightarrow vu \in H$.*

Exercice 92. ** Soit $G = \mathbb{R}^*$ (groupe multiplicatif) qui agit sur $X = \mathbb{R}^2 \setminus \{(0,0)\}$ par $\alpha(x,y) = (\alpha x, \alpha y), \alpha \in \mathbb{R}^*$.*

a) Décrire les orbites ;

b) Montrer que l'ensemble des orbites est en bijection avec $S^1 = \{z \in \mathbb{C} || z| = 1\}$;

c) Montrer que X est un groupe (avec la multiplication de $\mathbb{C}$), qui est isomorphe à $S^1 \times \mathbb{R}_+^*$.

Exercice 93. *Dans un groupe abélien, on suppose que a est d'ordre n et b d'ordre m. Montrer que l'ordre de ab n'est pas le ppmc de a et b en général.*

Exercice : soit G un groupe agissant à gauche sur un ensemble E. Soit A une partie de E. On note $g \cdot A = \{g \cdot a | g \in G\}$. Soit $H = \{g \in G | g \cdot A = A\}$ et $K = \{g \in G | \forall a \in A, g \cdot a = a\}$. Montrer que H est un sous-groupe de G, et que K est un sous-groupe normal de H

5 Groupes symétriques

Définition 5.1. *Soit $n \geq 1$. Le* groupe symétrique *de degré n est l'ensemble des bijections de l'ensemble $\{1, 2, \ldots, n\}$ dans lui-même. Une telle bijection s'appelle une* permutation. *La notation pour le groupe symétrique est S_n.*

Théorème 5.2. *Le groupe symétrique S_n est un groupe sous la composition des fonctions.*

La démonstration est laissée au lecteur. Regardons plutôt comment on représente une permutation. Prenons $n = 5$; alors la permutation σ définie par $\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 1, \sigma(5) = 3$ est représentée par $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$, ou plus simplement par 24513. L'inverse de σ est $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$ ou 41523. L'élément neutre est la fonction identité de $\{1, 2, 3, 4, 5\}$, c'est-à-dire la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 12345$.

Considérons la permutation $\alpha = 51432$. Alors $\sigma \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$. On a évidemment $\sigma^{-1} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$, c'est-à-dire l'identité.

Proposition 5.3. *Il y a $n!$ permutations dans S_n.*

Par exemple, $S_3 = \{123, 132, 213, 231, 312, 321\}$ a 6 éléments.

Démonstration. Toute permutation dans S_n se représente de manière unique par un *mot* $i_1 i_2 \cdots i_n$, où $\{i_1, \ldots, i_n\} = \{1, 2, \ldots, n\}$; les i_j sont distincts et leur ensemble est exactement $\{1, 2, \ldots, n\}$. On a donc n choix pour i_1, puis $n-1$ choix pour i_2, etc... Donc le nombre de permutations est $n(n-1)\cdots 2 \cdot 1 = n!$. □

Définition 5.4. *Une inversion d'une permutation $\sigma \in S_n$ est un couple $(\sigma(i), \sigma(j))$ tel que $i < j$ et $\sigma(i) > \sigma(j)$. Le nombre d'inversions de σ est noté $\ell(\sigma)$.*

Par abus, on écrira simplement $\sigma(i)\sigma(j)$ pour l'inversion. Par exemple, les inversions de 24513 sont $21, 41, 43, 51, 53$: il y en a 5, donc $\ell(\sigma) = 5$.

Définition 5.5. *Une transposition adjacente est une permutation τ dans S_n qui échange deux valeurs consécutives i et $i+1$ dans S_n, c'est-à-dire telle que $\tau(i) = i+1, \tau(i+1) = i$ et $\tau(j) = j$ si $j \in \{1, \ldots, n\} \setminus \{i, i+1\}$.*

Lemme 5.6. *Soit σ une permutation dans S_n et τ la transposition adjacente dans S_n qui échange i et $i+1$. Soit $\alpha = \sigma \circ \tau$. Alors α a une inversion de plus ou de moins que σ, selon que $\sigma(i) < \sigma(i+1)$ ou $\sigma(i) > \sigma(i+1)$.*

Prenons par exemple $\sigma = 24513$ et τ qui échange 3 et 4. Alors $\alpha = \sigma \circ \tau = 24153$ (c'est-à-dire qu'on a échangé les 3ème et 4ème nombres dans σ, à savoir 5 et 1) ; comme $\sigma(3) = 5 > 1 = \sigma(4)$, α a une inversion de moins : en effet, les inversions de α sont les mêmes que celles de σ, sauf 51.

Démonstration. Écrivons $\sigma = a_1 a_2 \cdots a_n$. On a alors $\alpha = \sigma \circ \tau = a_1 \cdots a_{i-1} a_{i+1} a_i \cdots a_n$, c'est-à-dire que α s'obtient à partir de σ en y échangeant le i-ème et le $(i+1)$-ème nombre. Si $\sigma(i) < \sigma(i+1)$, c'est-à-dire que $a_i < a_{i+1}$,aia_{i+1} n'est pas une inversion de σ, et $a_{i+1}a_i$ est une inversion de α. Si par contre $a_i > a_{i+1}$, alors aia_{i+1} est une inversion de σ, et $a_{i+1}a_i$ n'est pas une inversion de α. Comme toute autre inversion de σ se retrouve dans α, et vice-versa, le lemme s'en déduit. □

Théorème 5.7. *Toute permutation σ est un produit de $\ell(\sigma)$ transpositions adjacentes.*

Démonstration. (récurrence sur $\ell(\sigma)$) Si $\ell(\sigma) = 0$, σ est l'identité, qui correspond au produit vide. Supposons $\ell(\sigma) > 0$. Alors on ne peut pas avoir $\sigma(1) < \sigma(2) < \cdots < \sigma(n)$. Il existe donc i tel que $\sigma(i)\sigma(i+1)$. Soit τ la transposition adjacente qui échange i et $i+1$ et $\alpha = \sigma \circ \tau$. D'après le lemme 5.6, $\ell(\alpha) = \ell(\sigma) - 1$, donc α est, par hypothèse de récurrence, égal à un produit de $\ell(\sigma) - 1$ transpositions adjacentes. Donc $\sigma = \alpha \circ \tau^{-1} = \alpha \circ \tau$ (car $\tau = \tau^{-1}$) est un produit de $\ell(\sigma)$ transpositions adjacentes. □

La preuve ci-dessus est parfaitement algorithmique. Écrivons $(i, i+1)$ pour la transposition adjacente qui échange i et $i+1$ et regardons $\sigma = 24513$. On a

$$24513 = 24153 \circ (3,4);$$
$$24153 = 21453 \circ (2,3);$$
$$21453 = 12453 \circ (1,2);$$
$$12453 = 12435 \circ (4,5);$$
$$12435 = 12345 \circ (3,4) = (3,4).$$

D'où

$$\sigma = 24153 \circ (3,4) = 21453 \circ (2,3) \circ (3,4) = \ldots = (3,4) \circ (4,5) \circ (1,2) \circ (2,3) \circ (3,4).$$

Corollaire 5.8. *Soit $\epsilon : S_n \to \{-1, 1\}, \epsilon(\sigma) = (-1)^{\ell(\sigma)}$. Alors ϵ est un homomorphisme de S_n dans le groupe multiplicatif $\{-1, 1\}$; il est surjectif si $n \geq 2$.*

On appelle $\epsilon(\sigma)$ la *signature* de σ.

Démonstration. Pour montrer que σ est un homomorphisme, il suffit de montrer que

$$\ell(\sigma \circ \alpha) \equiv \ell(\sigma) + \ell(\alpha) \mod 2.$$

en effet, on aura alors

$$\epsilon(\sigma \circ \alpha) = (-1)^{\sigma \circ \alpha} = (-1)^{\ell(\sigma)+\ell(\alpha)} = (-1)^{\ell(\sigma)}(-1)^{\ell(\alpha)} = \epsilon(\sigma)\epsilon(\alpha).$$

Démontrons donc cette congruence par récurrence sur $\ell(\alpha)$. Si $\ell(\alpha) = 0$, α est l'identité, et c'est clair. Si $\ell(\alpha) > 0$, nous pouvons écrire $\alpha = \beta \circ \tau$, où $\tau = (i, i+1)$ et $\ell(\beta) = \ell(\alpha) - 1$ (lemme 5.6). Alors, par hypothèse de

récurrence, $\ell(\sigma \circ \beta \equiv \ell(\sigma) + \ell(\beta) \mod 2$.. Par ailleurs, le lemme 5.6 montre que $(\sigma \circ \beta) \circ \tau$ a une inversion de plus ou de moins que $\sigma \circ \beta$. Donc

$$\ell(\sigma \circ \alpha) = \ell(\sigma \circ \beta \circ \tau) \equiv \ell(\sigma \circ \beta) + 1 = \ell(\sigma) + \ell(\beta) + 1 = \ell(\sigma) + \ell(\alpha) \mod .2,$$

ce qui démontre la congruence.

Si $n \geq 2$, on a $\epsilon(\sigma) = -1$, pour $\sigma = (1, 2)$, et σ est surjective. □

Corollaire 5.9. *Si $n \geq 2$, le noyau de ϵ est un sous-groupe normal de S_n, qui a $n!/2$ éléments.*

Ce groupe s'appelle le groupe alterné, noté A_n ; les permutations dont la signature est 1 sont appelées *paires*, les autres *impaires*.

Démonstration. A_n est un sous-groupe normal d'après le théorème 4.9. Si $n \geq 2$, S_n est la réunion disjointe des deux sous-ensembles A_n et $S_n\ A_n$, qui ont autant d'éléments l'un que l'autre ($\sigma \mapsto \sigma \circ (1, 2)$ est une bijection de A_n dans $S_n\ A_n$). Donc $|A_n| = n!/2$, d'après la proposition 5.3. □

Définition 5.10. *Un* cycle *de longueur $k \geq 2$ est une permutation σ dans S_n telle qu'il existe k entiers distincts $j_1, \ldots, j_k$ dans $\{1, \ldots, n\}$ satisfaisant :*

$$\sigma(j_1) = j_2, \sigma(j_2) = j_3, \ldots, \sigma(j_{k-1}) = jk, \sigma(j_k) = j_1,$$

et

$$\forall i \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_k\}, \sigma(i) = i.$$

*On appelle $\{j_1, \ldots, j_k\}$ l'*orbite *du cycle. Deux cycles sont dits* disjoints *si leurs orbites sont disjointes. Une* transposition *est un cycle de longueur 2. Une permutation circulaire dans S_n est un cycle de longueur n.*

On dit *k-cycle* pour cycle de longueur k. Il n'y a pas de 1-cycle. Un *point fixe* d'une permutation σ est un i tel que $\sigma(i) = i$.

Par exemple, $\sigma = 24351$ est un cycle de longueur 4, d'orbite $\{1, 2, 4, 5\}$, puisque $\sigma(1) = 2, \sigma(2) = 4, \sigma(4) = 5, \sigma(5) = 1$ et que $\sigma(3) = 3$. On note le cycle $(j_1, j_2, \ldots, jk)$, avec les notations de la définition 5.10. Ainsi, le cycle ci-dessus se représente par $(1, 2, 4, 5)$; mais aussi par $(2, 4, 5, 1), (4, 5, 1, 2)$ ou $(5, 1, 2, 4)$. La permutation 14325 est une transposition, puisque c'est le cycle $(2, 4)$, et 31524 est la permutation circulaire $(1, 3, 5, 4, 2)$.

Théorème 5.11. *Toute permutation s'écrit de manière unique comme un produit de cycles deux à deux disjoints.*

Nous n'allons pas démontrer ce théorème, mais l'illustrer par la décomposition d'une permutation particulière. Prenons $\sigma = 729158436$ dans S_9. Nous partons de 1 et écrivons ses images sous σ, σ^2, etc..., jusqu'à ce qu'on retrouve 1 : $\sigma(1) = 7, \sigma(7) = 4, \sigma(4) = 1$. Ceci nous donne le cycle $(1, 7, 4)$. Continuant avec 2, le plus petit entier qui n'est pas apparu jusqu'ici, nous voyons que $\sigma(2) = 2 : 2$ est point fixe de σ. Nous continuons avec 3 : $\sigma(3) = 9, \sigma(9) = 6, \sigma(6) = 8, \sigma(8) = 3$, ce qui nous donne le cycle $(3, 9, 6, 8)$. Le seul nombre qui reste est 5, qui est point fixe. D'où la décomposition

$$\sigma = (1, 7, 4) \circ (3, 9, 6, 8).$$

On remarque que deux cycles disjoints commutent. On peut donc écrire

$$\sigma = (3, 9, 6, 8) \circ (1, 7, 4),$$

et c'est à cette commutation près qu'il y a unicité de la décomposition en cycles.

Remarquons que pour $n \geq 3$, S_n n'est pas commutatif ; en effet, les transpositions $(1, 2)$ et $(2, 3)$ ne commutent pas.

On appelle *multi-ensemble* un ensemble avec des répétitions d'éléments ; le nombre de fois qu'un élément est répété s'appelle la *multiplicité* de cet élément. Par, exemple $\{1, 1, 1, 2, 3, 5, 5, 8\}$ est un multi-ensemble, où la multiplicité de 1 est 3, et où celle de 5 est 2, et où les éléments 2, 3 et 8 sont chacun de multiplicité 1. Ce multi-ensemble est différent de $\{1, 1, 2, 3, 5, 5, 8\}$.

Définition 5.12. *Le* type cyclique *d'une permutation est le multi-ensemble des longueurs de ses cycles dans son écriture en produit de cycles deux à deux disjoints, en y incluant autant de 1 qu'elle a de poinst fixes.*

Par exemple, le type cyclique de la permutation de S_{10}, égale à $(1, 2)(3, 4, 5)(6, 7, 8)$ est $\{1, 1, 2, 3, 3\}$, car elle a les deux points fixes 10 et 9, un 2-cycle, et deux 3-cycles.

Définition 5.13. *Deux éléments g, h d'un groupe G sont dits* conjugués *s'il existe $a \in G$ tel que $g = aha^{-1}$.*

Proposition 5.14. *La conjugaison est une relation d'équivalence de G.*

La preuve est dans l'exercice 37.

Théorème 5.15. *Deux permutations sont conjuguées si et seulement si elles ont même type cyclique.*

Lemme 5.16. *(conjugaison d'un k-cycle) On a*

$$\sigma \circ (j_1, \ldots, j_k) \circ \sigma^{-1} = (\sigma(j_1), \ldots, \sigma(j_k).$$

Proposition 5.17. *Soit G un groupe et $a \in G$. La fonction $g \mapsto aga^{-1}$ est un automorphisme de G.*

Démonstration. La bijection réciproque est obtenue en remplaçant a par son inverse. On a $agha^{-1} = aga^{-1}aha^{-1}$: c'est bien un homomorphisme. □

Preuve du théorème 5.15. □

Corollaire 5.18. *Soit $p(n)$ le nombre de k-uplets décroissants (au sens large) d'entiers naturels ≥ 1 dont la somme est n. Alors le nombre de classes de conjugaison de S_n est $p(n)$.*

Démonstration. □

Théorème 5.19. *(Cayley) Tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique S_n.*

Démonstration. 1. Soit G un groupe fini de cardinal n. Pour tout $g \in G$, soit $\sigma_g : G \to G, x \mapsto gx$. Alors σ_g est une bijection $G \to G$. En effet, pour tous $x, y \in G$, $y = \sigma_g(x)$ est équivalent à $y = gx$, ce qui est équivalent à $x = g^{-1}y$; donc tout y dans G a un unique antécédant par σ_g.

2. On a $\sigma_{gh}(x) = ghx = \sigma_g(hx) = \sigma_g \circ \sigma_h(x)$; ceci implique que $\sigma_{gh} = \sigma_g \circ \sigma_h$. Donc la fonction $\phi : g \mapsto \sigma_g$ est un homomorphisme de G vers le groupe S_G des bijections de G dans G : en effet, la dernière égalité implique $\phi(gh) = \phi(g) \circ \phi(h)$.

3. L'homorphisme ϕ est injectif car $\sigma_g = id$ implique $g = ge = \sigma_g(e) = id(e) = e$, donc le noyau de σ est réduit à e.

4. Soit $b : G \to [n]$ une bijection. Soit $u : S_G \to S_n$ la fonction $u(\sigma) = b \circ \sigma \circ b^{-1}$. Alors u est isomorphisme de groupes. En effet, pour tous $\sigma_1, \sigma_2 \in S_G$, on a $u(\sigma_1 \circ \sigma_2) = b \circ \sigma_1 \circ \sigma_2 \circ b^{-1} = b \circ \sigma_1 \circ b^{-1} \circ b \circ \sigma_2 \circ b^{-1} = u(\sigma_1) \circ u(\sigma_2)$.

5. La fonction $u \circ \phi : G \to S_n$ est un homomorphisme de G vers S_n ; il est injectif, car u et *phi* sont injectifs ; son image est un sous-groupe de S_n. Donc $u \circ \phi$ définit un isomorphisme de G vers un sous-groupe de S_n. □

Exercice 94. *Décomposer en cycles disjoints les permutations suivantes :* $347219586, 315274968, 987654321$.

Exercice 95. *Montrer que l'inverse d'un cycle de longueur k est un cycle de longueur k ; comment obtient-on sa représentation ?*

Exercice 96. *Combien y a-t-il de permutations circulaires dans S_n ?*

Exercice 97. *Combien y a-t-il de transpositions dans S_n ?*

Exercice 98. *Quel est le nombre d'inversions de la permutation $n(n-1)(n-2)\cdots 21$ de S_n ? Montrer que c'est le nombre maximum d'inversions d'une permutation dans S_n.*

Exercice 99. *Quel est l'ordre d'un cycle de longueur k ? Quel est l'ordre de $(123)\circ(45)$? de $(12)(34)(5678)$?*

Exercice 100. ** Montrer que l'ordre d'une permutation est le ppmc des longueurs des cycles de sa décomposition en cycles disjoints.*

Exercice 101. *Vérifier que $\{id, (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe de S_4.*

Exercice 102. *Vérifier que si l'on note $\sigma_i = (i, i+1)$, alors*
$|i-j| \geq 2 \Rightarrow \sigma_i\sigma_j = \sigma_j\sigma_i$,
$|i-j| = 1 \Rightarrow \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$,
$|i-j|0 \Rightarrow \sigma_i\sigma_j = id$.
On omet ici le symbole $\circ$, et la composition est vue comme un produit.

Exercice 103. *Soit $\alpha \in S_n$ et α le cycle de longueur k : $\alpha = (j_1, \ldots, j_k)$. Montrer que $\sigma \circ \alpha \circ \sigma^{-1}$ est le cycle $(\sigma(j_1), \ldots, \sigma(j_k))$.*

Exercice 104. *Montrer que deux cycles de longueur k sont conjugués dans S_n (utiliser l'exercice 103).*

Exercice 105. ** Généralisant l'exercice 104, montrer que deux permutations dans S_n sont conjuguées si et seulement si pour tout k, ces deux permutations ont le même nombre de cycles de longueur k dans leur décomposition en cycles disjoints (théorème 5.11).*

Exercice 106. ** On définit la* table d'inversions *$T(\sigma)$ de $\sigma \in S_n$ par $T(\sigma) = (a_2, \ldots, a_n)$, où : $a_k =$ le nombres d'inversions $(\sigma(i), \sigma(j))$ avec $\sigma(i) = k$. Donner un exemple. Montrer que $\sigma \mapsto T(\sigma)$ est une fonction injective, d'image $E = \{(a_2, \ldots, a_n) \in \mathbb{N}^{n-1} | \forall i, 0 \leq a_i \leq i-1\}$.*

Exercice 107. *On considère l'ensemble $A = \{1, \ldots, n\}$. Soit $\sigma \in S_n$. On définit une action à gauche de S_n sur A^k par $\sigma(i_1, \ldots, i_k) = (\sigma(i_1), \ldots, \sigma(i_k))$. Vérifier que c'est bien une action. Déterminer le stabilisateur d'un élément.*

Exercice 108. *Décomposer la permutation*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 7 & 3 & 1 & 10 & 6 & 2 & 8 & 4 \end{pmatrix}$$

en produit de cycles disjoints et trouver son ordre dans S_{10}.

Exercice 109. *Soit* $H = \{id, (1,2)\}$, *et* $K = \{id, (1,2,3), (1,3,2)\}$ *des sous-groupes de* S_3.

a) Trouvez-en les classes à gauche et à droite.

b) Sont-ils normaux ?

Exercice 110. *Pour le sous-groupe* H *de l'exercice 101, écrire les six classes à droite (resp. à gauche) de* H *dans* S_4. *Ce sous-groupe est-il normal ?*

Exercice 111. *Soit* $H = \{\sigma \in S_8 | \sigma(8) = 8\} \subset S_8$.

a) Prouver que H *est un sous-groupe de* S_8.

b)Trouver l'indice de H *dans* S_8.

c) Combien y a-t-il dans H *d'éléments d'ordre* 7 *?*

d) Est-ce que H *est normal dans* S_8 *?*

Exercice 112. *Montrer que le groupe* S_n *est engendré par les deux permutations* $(1,2)$ *et* $(1,2,\ldots,n)$, *c'est-à-dire que toute permutation s'écrit comme un produit ne comportant comme facteurs que ces permutations. Aide : Calculer* $(1,2,\ldots,n)^i(1,2)(1,2,\ldots,n)^{-i}$.

Exercice 113. *Soit* $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 9 & 10 & 7 & 4 & 1 & 5 & 2 & 3 & 8 \end{pmatrix}$ *et* $b = (12345)(159)(249)$ *dans* S_{10}. *Calculer les ordres des éléments* $a, b, a \circ b, b \circ a, a^{1974}$ *et* b^{1975}. *Attention : les cycles ci-dessus ne sont pas disjoints.*

Exercice 114. *Considérons les deux permutation suivantes dans* S_9 *:* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 5 & 1 & 7 & 6 & 8 & 3 \end{pmatrix}$ *et* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 9 & 2 & 3 & 8 & 4 & 6 & 5 \end{pmatrix}$.

a) Écrire σ *et* τ *comme produits de cycles disjoints.*

b) Trouver l'ordre de σ *et de* τ.

c) Écrire σ *et* τ *comme produit de transpositions.*

d) Dire si σ *et* τ *sont paires ou impaires.*

Exercice 115. *Soit* G *un groupe ; on note, pour* $a \in G$, ℓ_a *la fonction de* G *dans* G *définie par* $\ell_a(g) = aga^{-1}$. *Montrer que* $\varphi : a \mapsto \ell_a$ *est un homomorphisme de* G *dans le groupe des bijections de* G *dans* G.

Exercice 116. *Montrer que le groupe de l'exercice 24 est isomorphe à* S_3.

6 Groupes linéaires

On rappelle que le déterminant du produit de deux matrices carrées de même ordre est égal au produit de leurs déterminant. On rappelle aussi que les coefficients de l'inverse d'une matrice sont des fractions, dont le dénominateur est le déterminant de la matrice, et dont les numérateurs sont certain mineurs de la matrice. De plus, le déterminant de l'inverse d'une matrice inversible est l'inverse de son déterminant. On rappelle encore que si on échange deux colonnes (resp. lignes) d'une matrice carrée, alors son déterminant est multiplié par -1, et que le déterminant de la matrice identité est 1.

Dans la suite, on pose $\mathbb{K} = \mathbb{C}, \mathbb{Q}$ ou $\mathbb{R}$.

Proposition 6.1. *Soit n un entier naturel non nul. L'ensemble des matrices carrées d'ordre n sur $\mathbb{K}$, de déterminant non nul, est un groupe sous la multiplication ; l'élément neutre est la matrice identité I_n. La fonction déterminant est un homomorphisme surjectif de $GL_n(\mathbb{K})$ vers $\mathbb{K}^*$ (multiplicatif).*

Démonstration. Le produit des matrices est associatif, et la matrice I_n est élément neutre pour le produit des matrices carrées d'ordre n.

Le déterminant du produit AB de deux matrices carrées A, B d'ordre n est le produit de leurs déterminants ; si ceux-ci sont non nuls, on a $\det(AB) \neq 0$. Donc les ensembles considérés dans l'énoncé forment un monoïde.

Les formules d'inversion des matrices carrées montrent que si A est carrée de déterminant non nul, à coefficient dans $\mathbb{K}$, alors son inverse est aussi à coefficients dans $\mathbb{K}$. Donc ces ensembles forment un groupe. □

Définition 6.2. *Avec les notations de la proposition 6.1, on note $GL_n(\mathbb{K})$ le groupe considéré, et on l'appelle le* groupe linéaire d'ordre n sur $\mathbb{K}$.

Corollaire 6.3. *On a $GL_n(\mathbb{Q}) \subset GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$, et chacun est sous-groupe du suivant.*

Définition 6.4. *On note $SL_n(\mathbb{K})$ l'ensemble des matrices dans $GL_n(\mathbb{K})$ de déterminant 1.*

Proposition 6.5. *$SL_n(\mathbb{K})$ est un sous-groupe normal de $GL_n(\mathbb{K})$, et $GL_n(\mathbb{K})/SL_n(\mathbb{K}) \simeq \mathbb{K}^*$.*

Le groupe $SL_n(\mathbb{K})$ est appelé le *groupe spécial linéaire* d'ordre n sur $\mathbb{K}$.

Démonstration. C'est parce que le déterminant du produit de deux matrices de déterminant 1 est aussi de déterminant 1, que le déterminant de la matrice identité est 1, et que le déterminant de l'inverse d'une matrice de déterminant 1 est aussi de déterminant 1.

Comme $SL_n(\mathbb{K})$ est le noyau de la fonction déterminant, il est normal dans $GL_n(\mathbb{K})$. La fonction déterminant de $GL_n(\mathbb{K})$ vers $\mathbb{K}^*$ est surjective : en effet, le déterminant de la matrice diagonale dont les éléments diagonaux sont $a, 1, \dots 1$, est a ; d'où l'isomorphisme par le corollaire 4.20. □

Proposition 6.6. *L'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{Z}$, de déterminant 1, est un sous-groupe de l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{Z}$, de déterminant 1 ou -1, qui est un sous-groupe de $GL_n(\mathbb{Q})$.*

Démonstration. Cela découle des formules qui donnent l'inverse d'une matrice : comme le déterminant est ± 1, les coefficients de l'inverse sont des entiers. □

Définition 6.7. *L'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{Z}$, de déterminant 1 (resp. de déterminant 1 ou -1) est noté $SL_n(\mathbb{Z})$ (resp. $GL_n(\mathbb{Z})$).*

Proposition 6.8. *$SL_n(\mathbb{Z}) \subset GL_n(\mathbb{Z}) \subset GL_n(\mathbb{Q})$, et chacun est un sous-groupe du suivant. De plus, $SL_n(\mathbb{Z})$ est un sous-groupe de $SL_n(\mathbb{Q}$.*

Démonstration. Si $A, B \in SL_n(\mathbb{Z})$, alors leur produit est à coefficients dans $\mathbb{Z}$; de plus, $\det(AB) = \det(A)\det(B) = 1$, donc $AB \in SL_n(\mathbb{Z})$. Clairement $I_n \in SL_n(\mathbb{Z})$. Enfin, par les formules d'inversion, $A^{-1} \in SL_n(\mathbb{Z})$. □

On appelle *matrice de la permutation* $\sigma \in S_n$ la matrice $P(\sigma)$ dont l'élément i, j est 1 si $\sigma(j) = i$, et 0 sinon.

Par exemple, la matrice de la permutation $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1, \sigma(4) = 4$ est la matrice $P_{2314} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Proposition 6.9. *La fonction $\sigma \mapsto P(\sigma)$ est un homomorphisme de groupes de S_n dans $GL_n(\mathbb{Z})$. Le déterminant de $P(\sigma)$ est égal à la signature $\epsilon(\sigma)$ de σ.*

Démonstration. Soit $M = P(\alpha)P(\beta)$, où $\alpha, \beta \in S_n$. On $M_{i,k} = \sum_j P(\alpha)_{i,j}P(\beta)_{j,k}$. Pour que cette somme soit non nulle, comme tous les termes sont ≥ 0, il faut qu'au moins un terme soit non nul ; pour que le terme correspondant à j dans cette somme soit non nulle, il faut que $i = \alpha(j)$ et $j = \beta(k)$; donc $i = \alpha \circ \beta(k)$; dans ce dernier cas, la somme vaut 1, sinon elle vaut 0. On a donc $M = P(\alpha \circ \beta)$ et la fonction est bien un homomorphisme de groupes.

Ecrivons $\sigma = \tau_1 \circ \cdots \circ \tau_k$ comme un produit de transpositions adjacentes. On a alors $P_\sigma = P_{\tau_1} \circ \cdots \circ P_{\tau_k}$, par ce qui précède. Or, pour une matrice P_τ, $\tau = (i, i+1)$, son déterminant est -1, car si on échange les deux colonnes i et $i+1$, on obtient la matrice identité. Donc $\det(P_\sigma) = (-1)^k = sgn(\sigma)$, par le corollaire 5.8, puisque la signature d'une transposition adjacente est -1. □

Les résultats suivants révèlent d'autres liens entre les permutations et les matrices. Nous ne les démontrerons pas (on peut trouver une preuve du premier dans les notes de cours [5], Théorème 20.2). Le second est lié à l'algorithme de Gauss-Jordan.

Théorème 6.10. *Le déterminant d'une matrice $A = (a_{ij})$, carrée d'ordre n, est égal à*

$$\sum_\sigma \epsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n},$$

où la somme est sur toutes les permutations de $\{1, \ldots, n\}$.

Théorème 6.11. *(décomposition de Bruhat) L'ensemble $GL_n(\mathbb{K})$ est réunion disjointe des $n!$ ensembles $T_n(\mathbb{K})P(\sigma)T_n(\mathbb{K})$, où $\sigma \in S_n$, et où T_n est l'ensemble des matrices triangulaires supérieures inversibles.*

Exercice 117. *Prouver que l'ensemble des matrices de la forme* $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, *$a \in \mathbb{R}$, est un sous-groupe du groupe $GL_2(\mathbb{R})$. Montrer qu'il est isomorphe à $\mathbb{R}$.*

Exercice 118. *Montrer que l'ensemble $T_n(\mathbb{K})$ des matrices triangulaires supérieures inversibles est un sous-groupe de $GL_n(\mathbb{K})$. On appelle* tore *d'ordre n l'ensemble des matrices carrées d'ordre n qui sont diagonales, avec des éléments diagonaux dans $\mathbb{K}^*$. Montrer que cet ensemble est un sous-groupe de $T_n(\mathbb{K})$.*

Exercice 119. *On définit pour toute fonction* $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ *la matrice* $P(f)$ *carrée d'ordre* n *comme suit : le coefficient* $i, j)$ *est égal à 1 si* $i = f(j)$*, et il vaut 0 dans les autres cas. Montrer que* $f \mapsto P(f)$ *est un homomorphisme de monoïdes du monoïde des endofonctions de* $\{1, 2, \ldots, n\}$ *dans le monoïde multiplicatif des matrices* $M_n(\mathbb{N})$*. Indication : imiter la première partie de la preuve de la proposition 6.9.*

Exercice 120. ** On note* $SL_2(\mathbb{N})$ *l'ensemble des matrices carrées d'ordre 2 à coefficients dans* $\mathbb{N}$*. Montrer que c'est un sous-monoïde de* $M_2(\mathbb{N})$*, et qu'il est engendré par les deux matrices* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Exercice 121. *Montrer que* $SL_n(\mathbb{K})$ *est un sous-groupe normal de* $GL_n(\mathbb{K})$.

Exercice 122. ** Montrer que* $GL_2(\mathbb{Z})$ *est engendré par les matrices*

$$P(q) = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}, q \in \mathbb{Z}.$$

Exercice 123. *Déduire de l'exercice 122 que* $SL_2(\mathbb{Z})$ *est engendré par les deux matrices*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Exercice 124. *Déduire de l'exercice 122 que* $GL_2(\mathbb{Z})$ *est engendré par les deux matrices*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Exercice 125. *Montrer que* $SL_n(\mathbb{Z})$ *est un sous-groupe normal de* $GL_n(\mathbb{Z})$ *et que* $GL_n(\mathbb{Z})/SL_n(\mathbb{Z}) \simeq \{1, -1\}$ *(multiplicatif).*

Exercice 126. *Montrer que l'inverse d'une matrice de permutation est sa transposée.*

Exercice 127.

Exercice 128.

7 Groupes abéliens finis

Définition 7.1. *Soit* p *un nombre premier. Un* p-groupe *est un groupe fini dont la cardinalité est une puissance de* p.

Exemple 7.2. *Un exemple de p-groupe abélien est le groupe*

$$\mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \mathbb{Z}/p^{r_s}\mathbb{Z}, \tag{2}$$

ou $s \in \mathbb{N}, r_1, \ldots, r_s \in \mathbb{N}^*$, avec $r_1 \geq \cdots \geq r_s$. En effet, sa cardinalité est $p^{r_1+\cdots+r_s}$.

Définition 7.3. *On dit qu'un groupe G est d'*exposant $n \in \mathbb{N}^*$ *si pour tout $g \in G$ on a $g^n = 1$.*

Tout groupe fini G est d'exposant $|G|$, d'après le corollaire 4.27. En particulier, tout p-groupe est d'exposant une puissance de p. La réciproque est une conséquence du résultat suivant.

Théorème 7.4. *Tout groupe abélien fini, qui a pour exposant une puissance de p, est isomorphe à un groupe de la forme (2). En particulier, c'est un p-groupe.*

Dans la suite, nous notons les groupes abéliens additivement. En particulier nous notons ng au lieu de g^n ; donc $ng = g + \cdots + g$ (n fois), et l'ordre de g est le plus petit entier naturel n non nul tel que $ng = 0$.

Lemme 7.5. *Soit A un groupe abélien fini, qui a pour exposant une puissance de p.*

(i) Soit $b \in A$ tel que $p^r b \neq 0$ et que $p^r b$ est d'ordre p^m. Alors b est d'ordre p^{m+r}.

(ii) Soit $a_1 \in A$ un élément d'ordre p^{r_1} maximum dans A. Soit A_1 le sous-groupe engendré par a_1. Soit $\bar{b}$ un élément dans A/A_1 d'ordre p^r. Il existe alors un élément $b \in A$ d'ordre p^r dont l'image est $\bar{b}$ par l'homomorphisme canonique $f : A \to A/A_1$.

Démonstration. (i) On a $p^{m+r}b = 0$. Donc l'ordre de b divise p^{m+r} (théorème 4.26). Si $p^n b = 0$, alors on doit avoir $n > r$ (sinon $p^r b = 0$). Supposons que $n < r + m$; alors $n - r < m$ et on a $p^{n-r}p^r b = 0$, contredisant que l'ordre de $p^r b$ est p^m. Donc $n \geq r + m$, donc l'ordre de b est p^{m+r}.

(ii) Soit $b \in A$ dont l'image dans A/A_1 est $\bar{b}$. Comme $p^r\bar{b} = 0$, on $p^r b \in A_1$, donc $p^r b = na_1$ pour un entier n. L'ordre p^r de $\bar{b}$ est $\leq$ l'ordre de b, puisque celui-ci est image homomorphe de celui-là ; donc si $na_1 = 0$, nous avons notre b du lemme. Supposons maintenant que $na_1 \neq 0$; donc $n \neq 0$, et écrivons $n = p^k\mu$, où μ est premier avec p ; donc $k < r_1$ (sinon $na_1 = 0$). Alors μa_1 est aussi un générateur de A_1 (une conséquence de l'exercice 64), et il est donc d'ordre p^{r_1}. Alors $p^k\mu a_1$ est d'ordre p^{r_1-k}. Comme $p^r b = p^k(\mu a_1)$,

l'ordre de b est p^{r+r_1-k} par (i). Par maximalité de r_1, on a $r+r_1-k \leq r_1$, donc $r \leq k$. Donc $p^r b = p^k(\mu a_1) = p^r c$, où $c = p^{k-r}\mu a_1 \in A_1$; donc $f(c) = 0$. Soit $a = b - c$. Alors $f(a) = f(b) - f(c) = 0$, et a est envoyé sur $\bar{b}$ par l'homomorphisme canonique f, et $p^r a = p^r(b-c) = p^r b - p^r c = 0$. Comme l'ordre de a est $\leq p^r$, son ordre est p^r. □

Preuve du théorème 7.4. Au lieu de parler de produit de groupes, nous allons parler de *somme directe interne*. Un groupe abélien A est dit somme directe interne de ses sous-groupes $A_1, \ldots, A_s$ si tout élément de A a une unique expression $h_1 + \cdots + h_s$, où chaque h_i est dans A_i. On écrit

$$A = A_1 \oplus \cdots \oplus A_s.$$

Dans ce cas, l'homomorphisme canonique $A_1 \times \cdots \times A_s \to A, (h_1, \ldots, h_s) \mapsto h_1 + \cdots + h_s$ est un isomorphisme de groupes.

Soit a_1, A_1 comme dans le lemme 7.5 (ii). Si A_1 est le groupe trivial, alors tout élément de A est d'ordre 1, donc A est trivial ; le résultat est vrai dans ce cas (avec $s = 0$). Supposons que A_1 n'est pas le groupe trivial. Le groupe A/A_1 est de cardinalité plus petite que celle de A, par le corollaire 4.14. Il a pour exposant une puissance p. Donc par hypothèse de récurrence sur la cardinalité, on peut supposer que

$$A/A_1 = \bar{A}_2 \oplus \cdots \oplus \bar{A}_s, \tag{3}$$

où les groupes $\bar{A}_j$ sont cycliques d'ordre p^{r_j}, avec $r_2 \geq \cdots \geq r_s$.

Soit $\bar{a}_j$ un générateur du groupe $\bar{A}_j$; en utilisant le lemme 7.5 (ii), on peut trouver $a_j \in A$ de même ordre p^{r_j} que $\bar{a}_j$, et dont l'image par $\pi : A \to A/A_1$ est $\bar{a}_j$. Soit A_j le groupe engendré par a_j ; c'est un groupe cyclique de cardinalité p^{r_j}. Nous montrons que A est somme directe de $A_1, A_2, \cdots, A_s$, ce qui finira la preuve.

Soit x dans A et $\bar{x}$ son image par π. Par (3), il existe des entiers $m_2, \ldots, m_s$ tels que $\bar{x} = m_2 a_2 + \ldots + m_s a_s$. Donc $\pi(x) = m_2\bar{a}_2 + \cdots + m_s a_s$, et par suite, $x - m_2 a_2 - \cdots - m_s a_s \in N(\pi) = A_1$, donc $x - m_2 a_2 - \cdots - m_s a_s = m_1 a_1$, $m_1 \in \mathbb{Z}$, et enfin $x = \sum m_i a_i$.

Donc tout x dans A s'écrit $x = \sum m_i a_i$. Pour montrer que cette écriture est unique, supposons que $\sum m_i a_i = 0$ et montrons que chaque terme $m_i a_i$ est nul. Appliquant π, on trouve $m_2\bar{a}_2 + \cdots + m_s a_s = 0$. Comme la somme (3) est directe, on doit avoir $m_j\bar{a}_j = 0$ pour chaque $j = 2, \ldots, s$. Donc, l'ordre de $\bar{a}_j$ étant p^{r_j}, celui-ci divise m_j ; donc $m_j a_j = 0$, puisque l'ordre de a_j est aussi p^{r_j}. Enfin $0 = m_1 a_1$. □

Théorème 7.6. *Tout groupe abélien fini est isomorphe à un produit fini de groupes cycliques, qui sont de la forme $\mathbb{Z}/p^r\mathbb{Z}$, p premier, $r \geq 1$.*

Pour un groupe abélien A et un entier n, on pose $A(n) = \{x \in A | nx = 0\}$. Alors $A(n)$ est un sous-groupe de A, comme on peut le vérifier facilement.

Lemme 7.7. *Soit A un groupe abélien fini d'exposant mn, où m, n sont des entiers naturels premiers entre eux. Alors A est somme directe des deux sous-groupes $A(n)$ et $A(m)$.*

Démonstration. Il existe des entiers u, v tels que $um + vn = 1$ (théorème de Bezout). Soit $x \in A$. Alors $x = (um + vn)x = (um)x + (vn)x$. On a $m((vn)x) = (mvn)x = mn(vx) = 0$, puisque A est d'exposant mn. Donc $(vn)x \in A(m)$. De même, $(um)x \in A(n)$. Donc $x \in A(n) + A(m)$.

Pour montrer que la somme $A(n) + A(m)$ est directe, il suffit de montrer que l'intersection de ces deux sous-groupes est nulle. Soit $x \in A(m) \cap A(n)$. Alors $mx = nx = 0$. Donc $x = (um + vn)x = u(mx) + v(nx) = 0$. □

Preuve du théorème 7.6. Soit $n = |A|$; alors n est un exposant de A (corollaire 4.27). Il découle, par récurrence sur k, du lemme 7.7 que si $n = p_1^{n_1} \cdots p_k^{n_k}$, où les p_i snt des nombres premiers distincts et les n_i des entiers naturels, alors A est somme directe des sous-groupes $A(p_i^{n_i})$. Ce dernier sous-groupe est d'exposant $p_i^{n_i}$. Il découle du théorème 7.4 qu'il est somme directe de sous-groupes cycliques de la forme $\mathbb{Z}/p^r\mathbb{Z}$. Donc A est somme directe de tels sous-groupes cycliques. □

Corollaire 7.8. *Tout groupe abélien fini est isomorphe à un produit de groupes cycliques de la forme*

$$\mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_s\mathbb{Z}, \tag{4}$$

où les c_i sont des entiers naturels ≥ 2, et où $c_1|c_2|\cdots|c_s$.

Démonstration. On sait que tout groupe abélien fini est isomorphe à un produit de groupes de la forme $\mathbb{Z}/p^r\mathbb{Z}$, p premier, $r \geq 1$. En remarquant que $\mathbb{Z}/p^0\mathbb{Z} = \mathbb{Z}/\mathbb{Z}$ est le groupe trivial, qui agit comme un élément neutre dans les produits cartésiens, on peut donc supposer que A est isomorphe à un produit

$$\prod_{1 \leq i \leq k, 1 \leq j \leq s} \mathbb{Z}/p_i^{r_{i,j}}\mathbb{Z},$$

où les p_i sont des nombres premiers distincts, et où on a pour tout i

$$r_{i,1} \leq \cdots \leq r_{i,s}.$$

Posons $c_j = \prod_{1\leq i\leq k} p_i^{r_{i,j}}$. Alors $c_1|\cdots|c_s$. De plus A est isomorphe à

$$\prod_{1\leq j\leq s}\prod_{1\leq i\leq k} \mathbb{Z}/p_i^{r_{i,j}}\mathbb{Z},$$

qui est, par le théorème chinois 4.21, isomorphe à

$$\prod_{1\leq j\leq s} \mathbb{Z}/c_j\mathbb{Z}.$$

□

Corollaire 7.9. *Tout groupe abélien fini, dont la cardinalité est divisible par un nombre premier p, possède un élément d'ordre p et donc un sous-groupe de cardinalité p.*

Démonstration. Soit G ce groupe. Par les résultats précédents, on peut supposer que G est un produit de groupe cycliques. L'un d'eux a une cardinalité divisible par p. On est donc ramené à G cyclique : $G = \mathbb{Z}/n\mathbb{Z}$, avec $n = pk$; alors $k + n\mathbb{Z}$ est d'ordre p dans G. □

On peut montrer que les décompositions apparaissant dans le corollaire 7.8 sont uniques. Précisément : si le groupe dans ce corollaire est isomorphe à un groupe $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$, où $2 \leq d_1|d_2|\cdots|d_t$, alors $s = t$ et $c_1 = d_1, \ldots, c_s = d_s$. Pour une preuve on peut voir [4].

De même, la décomposition du théorème 7.6 est unique. Ceci signifie que si deux groupe sont isomorphes, le multi-ensemble [2] des puissances des nombres premiers qui apparaissent dans la décomposition, sont les mêmes. Voir aussi [4].

Le fait que ces deux théorèmes d'unicité se ramènent l'un à l'autre est expliqué dans l'exercice 132.

Exercice 129. *En utilisant le théorème chinois, trouver un groupe de la forme (4) isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Exercice 130. *Montrer que dans un groupe abélien fini A, il existe pour tout diviseur d de $|A|$, un sous-groupe d'ordre d (c'est en quelque sorte une réciproque du théorème de Lagrange pour les groupes abéliens). Indication : commencer par un groupe cyclique ; puis continuer par un produit de groupes.*

2. Un multi-ensemble est un ensemble où l'on peut répéter des éléments.

Exercice 131. *Ecrire toutes les décompositions de la forme du corollaire 7.8 pour un groupe de cardinalité 2016. Remarque : on peut ainsi compter les groupes abéliens de cardinalité 2016 à isomorphisme près ; ça se généralise pour toute cardinalité ; donner d'autre exemples.*

Exercice 132. ** A toute suite $(c_1, \dots, c_s)$ d'entiers, telle que $s \geq 0$, $2 \leq c_1 | c_2 | \cdots | c_s$, on associe le multi-ensemble des puissances (non triviales) de nombres premiers divisant les c_i. Exemple : $(2, 12, 84) \mapsto \{2, 2^2, 2^2, 3, 3, 7\}$. Montrer qu'on obtient une bijection. En déduire par la construction dans la preuve du corollaire 7.8 que l'unicité dans le théorème 7.6 et celle dans le corollaire 7.8 se ramènent l'une à l'autre.*

Exercice 133. *Montrer que si deux permutations sont conjuguées, alors elles ont la même signature. Montrer que la signature d'un k-cycle σ est $(-1)^{k-1}$, c'est-à-dire : la parité de σ est l'opposée de celle de k. Indication : commencer par $c = (1, 2, \dots, k)$.*

Exercice 134. *Déterminer $A(m)$ lorsque $A = \mathbb{Z}/n\mathbb{Z}$.*

Exercice 135.

Exercice 136.

Exercice 137.

Exercice 138.

8 Monoïdes et groupes libres

Soit A un ensemble, qu'on appellera ici *alphabet*, et dont les éléments sont appelés des *lettres*. Un *mot sur* A est une suite finie d'éléments de A ; on inclut la suite vide, qu'on appelle le *mot vide*. Avec la *concatenation*, l'ensemble des mots sur A, noté A^*, devient un monoïde ; on appelle concatenation de deux mots $(a_1, \dots, a_n)$ et $(b_1, \dots, b_m)$, où $n, m \geq 0, a_i, b_j \in A$, le mot $(a_1, \dots, a_n, b_1, \dots, b_m)$. Ce produit est clairement associatif, et l'élément neutre est le mot vide, que nous notons 1.

Chaque lettre est aussi un mot, et nous écrivons a pour (a). Clairement, le mot $(a_1, \dots, a_n)$ est le produit des ses lettres, c'est-à-dire ce mot est $a_1 \cdots a_n$. Nous adopterons cette notation pour les mots, c'est-à-dire sans les parenthèses. La *longueur* du mot $a_1 \cdots a_n$ est n.

Le monoïde A^* est appelé *monoïde libre*, ce qui est justifié par la propriété universelle suivante.

Théorème 8.1. *Soit A un alphabet et $f : A \to M$ une fonction de A dans un monoïde. Il existe un unique homomorphisme de monoïdes $\bar{f} : A^* \to M$ tel que $f = \bar{f} \circ i$, où $i : A \to A^*$ est l'injection canonique $i(a) = a$.*

On peut ainsi dire que le monoïde libre est engendré par les lettres dans A, et qu'il n'y a pas d'autre relation entre ses éléments que celle imposées par l'associativité.

Démonstration. □

Nous allons voir qu'il existe un groupe qui a une propriété universelle analogue. Pour ceci, nous avons besoin de la notion de *congruence de monoïdes*. Une congruence d'un monoïde M est une relation d'équivalence $\sim$ sur M telle que : $\forall g, g', h, h' \in M, g \sim g'$ et $h \sim h' \Rightarrow gh \sim g'h'$. Le quotient $M/\sim$ est alors un monoïde et la projection canonique $M \to M/\sim$ un homomorphisme de monoïdes.

Soit A un alphabet et définissons une copie $\bar{A}$ de A, en ce sens qu'il y a une bijection $A \to \bar{A}, a \mapsto \bar{a}$. On suppose que A et $\bar{A}$ sont disjoints. Soit $X = A \cup \bar{A}$. Soit $\sim$ la congruence du monoïde libre X^* engendrée par les relations $a\bar{a} \sim 1$, $\bar{a}a \sim 1$, pour tout $a \in A$. Concrètement, cela signifie que $u \sim v$ si et seulement s'il existe $n \geq 0$, et une suite de mots $u = u_0, u_1, \ldots, u_n = u$, telles que pour tout $i = 1, \ldots, n$, il existe une factorisation $u_{i-1} = xfy, u_i = xgy$ et une lettre $a \in A$ tel qu'on ait $f = a\bar{a}, g = 1$, ou $f = \bar{a}a, g = 1$, ou $f = 1, g = a\bar{a}$, ou $f = 1, g = \bar{a}a$.

Par exemple, $ab\bar{b}\bar{a}aba \sim aba\bar{b}b$, car on a la suite $ab\bar{b}\bar{a}aba, a\bar{a}aba, aba, aba\bar{b}b$. On montre que la relation ainsi définie est une congruence. Soit alors $F(A) = X^*/\sim$. C'est un monoïde et la projection canonique $p : X^* \to F(A)$ est un homomorphisme de monoïdes. On a alors un homomorphisme de monoïdes $j : A^* \to F(A)$, qui est le composé de l'injection canonique $A^* \to X^*$, suivi de p.

Théorème 8.2. *$F(A)$ est un groupe et l'homomorphisme de monoïdes j est injectif. Notons i sa restriction à A.*

Soit $f : A \to G$ une fonction de A dans un groupe. Il existe un unique homomorphisme de groupes $\bar{f} : F(A) \to G$ tel que $f = \bar{f} \circ i$.

On appelle $F(A)$ le *groupe libre sur A*.

Démonstration. □

Un *facteur* d'un mot w dans un monoïde libre est un mot u tel qu'il existe des mots x, y tels que $w = xuy$.

On appelle *mot réduit* un mot dans le monoïde libre $\{A \cup \bar{A}\}^*$ qui ne contient aucun facteur $a\bar{a}$, ni $\bar{a}a$, $a \in A$.

Théorème 8.3. *Tout mot w dans $\{A \cup \bar{A}\}^*$ est congru modulo $\sim$ à un unique mot réduit. Il s'obtient à partir de w en supprimant itérativement tous les facteurs $\bar{a}a$ et $a\bar{a}$, dans l'ordre qu'on veut.*

Démonstration. □

Exercice 139. *Montrer que la fonction longueur est un homomorphisme de monoïdes $A^* \mapsto \mathbb{N}$. Montrer que c'est l'unique homomorphisme qui envoie chaque lettre sur 1, en utilisant le théorème 8.1.*

Exercice 140. *Montrer en utilisant le théorème 8.2 qu'il existe un unique homomorphisme de groupes $F(A) \to \mathbb{Z}$ qui envoie toute lettre $a \in A$ sur 1. Montrer que la restriction de cette fonction à A^* est l'homomorphisme longueur de l'exercice 139. Calculer des images d'éléments de $F(A)$, et vérifier que ce n'est pas la longueur du mot réduit en général. On appelle* longueur algébrique *cette fonction sur le groupe libre.*

Exercice 141. *Un mot dans $\{A \cup \bar{A}\}^*$ est dit* cycliquement réduit *si : soit il est vide ; soit il est réduit, et si a, b étant sa première et sa dernière lettre, on a $a \neq \bar{b}$ (on étend la fonction $a \mapsto \bar{a}$ à $A \cup \bar{A}$ par la condition $\bar{\bar{a}} = a, \forall a \in A$). Donner des exemples. Montrer que tout élément de A^* est cycliquement réduit. Montrer que pour tout $g \in F(A)$, il existe $w \in \{A \cup \bar{A}\}^*$ qui est cycliquement réduit et tel que g soit conjugué à w.*

Exercice 142.

Exercice 143.

Exercice 144.

9 Théorèmes d'isomorphisme

Le premier théorème d'isomorphisme n'est rien d'autre que le corollaire 4.20.

Théorème 9.1. *(Premier théorème d'isomorphisme) Soit $f : G \to G'$ un isomorphisme de groupes. Alors f induit un isomorphisme de groupes $\bar{f} : G/N(f) \to Im(f)$.*

Théorème 9.2. *(Premier théorème d'isomorphisme, variante) Soit $f : G \to G'$ un isomorphisme de groupes, et N un sous-groupe normal de G tel que $N \subset N(f)$. Alors f induit un homomorphisme de groupes $\bar{f} : G/N \to G'$.*

Démonstration. On pose $\bar{(}f)(gN) = f(g)$. Etc... □

Théorème 9.3. *(Deuxième théorème d'isomorphisme) Soient G un groupe, N un sous-groupe normal de G et H un sous-groupe de G. Alors $H \cap N$ est un sous-groupe normal de H, N est un sous-groupe normal du sous-groupe $HN = NH$ de G, et $H/(H \cap N)$ est isomorphe à HN/N.*

Démonstration. 1. L'intersection de deux sous-groupes de G est un sous-groupe, donc $H \cap N$ est un sous-groupe de G ; comme il est contenu dans H, c'est un sous-groupe de H.

Si $a \in H \cap N$ et $b \in H$, alors $bab^{-1} \in H$, car H est un sous-groupe ; de plus $bab^{-1} \in N$, car N est un sous-groupe normal. Donc $bab^{-1} \in H \cap N$, ce qui prouve que $H \cap N$ est un sous-groupe normal de H.

2. Si $g \in HN$, alors $g = hn, h \in H, n \in N$; donc $g = hnh^{-1}h \in NH$, car $hnh^{-1} \in N$, celui-ci étant normal. Ceci montre que $HN \subset NH$, et l'inclusion réciproque est démontrée de manière analogue. Donc $HN = NH$.

3. Soit $g \in N$, et $a \in NH$. Alors $a = nh, n \in N, h \in H$, donc $aga^{-1} = nhgh^{-1}n^{-1} \in N$, car n, hgh^{-1}, n^{-1} sont dans N, celui-ci étant normal. Donc N est un sous-groupe normal de NH.

4. Considérons l'homomorphisme canonique $p : HN \to HN/N$, et l'injection canonique $i : H \to HN$. Soit $f = p \circ i : H \to HN/N$. Nous montrons plus loin que f est surjectif et que $N(f) = H \cap N$. On en déduit par le premier théorème d'isomorphisme que HN/N est isomorphe à $H/(H \cap N)$.

5. Le noyau de f est l'ensemble des $h \in H$ tels que $p(h) = p(i(h)) = 1$. C'est-à-dire que que h appartienne à $N(p) = N$. C'est donc bien $H \cap N$.

6. Considérons un élément de HN/N. On peut l'écrire sous la forme $p(hn), h \in H, n \in N$. Comme $N = N(p)$, on a $p(hn) = p(h)p(n) = p(n) = p \circ i(n)$. Donc $p \circ i$ est surjectif. □

Théorème 9.4. *(Troisième théorème d'isomorphisme) Soit G un groupe, et N, M des sous-groupes normaux de G tels que $M \subset N$. Alors M est un sous-groupe normal de N, N/M est un sous-groupe normal de G/M, et G/N est isomorphe à $(G/M)/(N/M)$.*

Démonstration. 1. M est un sous-groupe de G, et un sous-ensemble de N ; c'est donc un sous-groupe de N, par un vérification immédiate des trois

points de la définition 2.13. Si $m \in M, n \in N$, alors $n^{-1}mn \in N$, car N est un sous-groupe normal de G.

2. Les éléments de N/M sont les classes nM modulo M, $n \in N$. Ce sont donc des éléments de G/M. Soit $p : G \to G/M$ l'homomorphisme canonique. On a $p(N) = \{nM, n \in N\}$; donc $p(N) = N/M$ est un sous-groupe de G/M. C'est un sous-groupe normal, car p est surjectif (exercice 54).

3. On a $p^{-1}(N/M) = N$. En effet, si $n \in N$, alors $p(n) \in p(N) = N/M$. Et si $p(g) \in N/M$, alors gM est de la forme $gM = nM, n \in M$. Donc $g \in N$, car M est un sous-groupe qui contient M.

4. Soit $q : G/M \to (G/M)/(N/m)$ l'homomorphisme canonique. Alors $q \circ p : G \to (G/M)/(N/M)$ est un homomorphisme, qui est surjectif, car p, q sont surjectifs. Le noyau de $q \circ p$ est $p^{-1}(N(q)) = p^{-1}(N/M) = N$; donc, par le premier théorème d'isomorphisme, $(G/M)/(N/m)$ est isomorphe à G/N. □

Exercice 145. *Soit $f : G \to G', g : G' \to G''$ des homomorphismes de groupes. Montrer que $N(g \circ f) = f^{-1}(N(f))$.*

Exercice 146. *On considère un homomorphisme surjectif $f : G \to G'$. Soit N' un sous-groupe normal de G' et $N = f^{-1}(N')$. Montrer que N est un sous-groupe normal de G, et que G/N est isomorphe à G'/N'.*

Exercice 147. *Soit d, n des entiers tels que d divise n. Vérifier que $n\mathbb{Z}$ est un sous-groupe de $d\mathbb{Z}$.*

Montrer que le groupe $d\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/(n/d)\mathbb{Z}$. Indication : considérer l'homomorphisme $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto dx \mod n$. Montrer que son noyau est $(n/d)\mathbb{Z}$ et que son image est $d\mathbb{Z}/n\mathbb{Z}$.

Montrer que le théorème 9.4 appliqué à cette situation donne l'isomorphisme $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}$.

Exercice 148. ** Montrer que tous les sous-groupes et tous les quotients de Z/nZ sont de la forme $\mathbb{Z}/d\mathbb{Z}$, $d|n$. Commencer par $n = 12$.*

10 Théorèmes de Sylow

Soit un groupe fini G de cardinalité $|G| = p^n m$, avec p premier ne divisant pas m.

On dit qu'un sous-groupe de G est un *p-sous-groupe de Sylow* si sa cardinalité est p^n.

On dit que H est un *sous-groupe de Sylow* de G s'il existe un nombre premier p tel que H soit un p-sous-groupe de Sylow.

Théorème 10.1 (Premier théorème de Sylow)**.** *Soit G un groupe fini. Alors, pour tout nombre premier p, et toute puissance p^s divisant $|G|$, le groupe G possède un sous-groupe d'ordre p^s. En particulier, G contient un p-sous-groupe de Sylow.*

Théorème 10.2 (Deuxième théorème de Sylow)**.** *Soit G un groupe fini. Pour chaque diviseur premier p de $|G|$, les p-sous-groupes de Sylow sont conjugués.*

Théorème 10.3 (Troisième théorème de Sylow)**.** *Soit G un groupe fini, et p un diviseur premier de G. Soit N_p le nombre de p-sous-groupes de Sylow de G. Alors $N_p \equiv 1 \mod p$.*

Nous ne prouvons que les deux premiers théorèmes de Sylow.

Preuve du théorème 10.1. Considérons l'action de G sur lui-même par conjugaison. Les orbites de cardinalité 1 sont les $\{g\}$, $g \in C(G)$. Pour les autres orbites, choisissons des représentants $x_1, \ldots, x_r$.

Par le corollaire 3.5, on a donc

$$|G| = |C(G)| + \sum_{x_i \notin C(G)} |G|/|C(x_i)|,$$

où $C(x_i)$ est le stabilisateur de x_i dans l'action par conjugaison. On distingue deux cas.

Premièrement, p ne divise pas $|C(G)|$. Alors p ne divise pas $|G|/|C(x_i)|$ pour un certain i. D'où p^s divise $|C(x_i)|$. On a aussi $|C(x_i)| < |G|$, car $x_i \notin C(G)$. Par récurrence, $C(x_i)$ possède un sous-groupe H d'ordre p^s, qui est aussi un sous-groupe de G d'ordre p^s.

Deuxièmement, p divise $|C(G)|$. Alors $C(G)$ possède un élément d'ordre p, disons c (corollaire 7.9). Soit H_0 le sous-groupe engendré par c. C'est un groupe cyclique de cardinalité p ; H_0 est un sous-groupe normal de G, car $c \in C(G)$. Donc G/H_0 est un groupe de cardinalité $|G|/p$ (corollaire 4.14). Par récurrence, G/H_0 possède un sous-groupe d'ordre p^{s-1}, disons K. Soit $H = \pi^{-1}(K)$, où π est le morphisme naturel $G \to G/H_0$. Alors H un sous-groupe de G qui contient H_0, H_0 est un sous-groupe normal de H, et $H/H_0 \simeq K$, car $\pi|H : H \to K$ est surjectif. D'où $|H| = |H_0| \cdot |K| = p^s$. □

Preuve du théorème 10.2. Soit $|G| = p^n m$, m premier avec p. Fixons un p-sous-groupe de Sylow S, et considérons un autre p-sous-groupe de Sylow S'. Désignons par $\mathcal{T}$ l'ensemble des translatés à droite de S : $\mathcal{T} = \{Sg | g \in G\}$,

avec $|\mathcal{T}| = m$: en effet, par le théorème 3.7, les translatés à droite de S sont disjoints, chacun a cardinalité $p^n = |S|$, et leur réunion est G.

Le groupe S' agit sur $\mathcal{T}$ par produit à droite : si $s \in S'$, $Sg \cdot s = Sgs$. Notons S'_T le stabilisateur de $T \in \mathcal{T}$ dans cette action ; c'est un sous-groupe de S'. Notons aussi $T_1, T_2, \ldots$ des représentants des orbites de cette action. En appliquant le corollaire 3.5 à cette action, on obtient

$$m = |\mathcal{T}| = \sum_i |S'|/|S'_{T_i}|.$$

Notons que tous les $|S'|/|S'_{T_i}|$ divisent p^n, alors que p ne divise pas m. Il doit donc y avoir au moins un i tel que $|S'|/|S'_{T_i}|$ soit égal à 1, d'où $S' = S'_{T_i}$: donc tout $s' \in S'$ stabilise T_i ; posons $T_i = Sg$. On a donc $\forall s \in S', Sgs = Sg$, donc $gs \in Sg$, d'où $s \in g^{-1}Sg$. On en tire $S' \subset g^{-1}Sg$, d'où $S' = g^{-1}Sg$, par égalité des cardinalités. Les sous-groupes S et S' sont donc conjugués. □

Exercice 149. *Quels sont les sous-groupes de Sylow d'un groupe cyclique ? Utiliser l'exercice 75.*

Exercice 150. *Quels sont les sous-groupes de Sylow de S_3 ?*

Exercice 151. *Combien S_4 a-t-il de p-sous-groupes de Sylow pour $p = 2$ et $p = 3$?*

11 Conjugaison

Deux éléments g, g' d'un groupe G sont dits *conjugués* s'il existe x dans G tel que $g' = xgx^{-1}$.

Lemme 11.1. *Soit G un groupe.*

(i) g, g' sont conjugués si et seulement s'il existe y dans G tel que $g' = y^{-1}gy$.

(ii) g, g' sont conjugués si et seulement s'il existe a, b dans G tel que $g = ab$ et $g' = ba$.

(iii) Si G est commutatif, g, g' sont conjugués si et seulement s'ils sont égaux.

Proposition 11.2. *La conjugaison est une relation d'équivalence.*

Une classe d'équivalence s'appelle une *classe de conjugaison.*

Proposition 11.3. *Un élément g de G n'est conjugué qu'à lui-même si et seulement s'il commute avec tous les éléments de G. L'ensemble de ces éléments est un sous-groupe normal de G, appelé le* centre *de G.*

Proposition 11.4. *On définit une fonction $G \times G \to G, (g, x) \mapsto gxg^{-1}$. C'est une action à gauche de G sur lui-même : $g \cdot x = gxg^{-1}$, dont les orbites sont les classes de conjugaison.*

On définit la fonction γ_g de G dans G telle que

$$\forall x \in G, \gamma_g(x) = gxg^{-1}.$$

Proposition 11.5. *La fonction γ_g est un automorphisme de G ; son inverse est la fonction $\gamma_{g^{-1}}$.*

Un tel automorphisme de G s'appelle un *automorphisme intérieur* de G. Rappelons que les automorphismes de G forment un groupe sous la composition des fonctions ; ce groupe est noté $Aut(G)$.

Proposition 11.6. *La fonction $g \mapsto \gamma_g$ est un homomorphisme de G vers $Aut(G)$. Son noyau est le centre de G.*

Proposition 11.7. *L'ensemble des automorphismes intérieurs de G est un sous-groupe normal de $Aut(G)$.*

Plus généralement, on dit que deux parties A, B deux sont conjuguées s'il existe $g \in G$ tel que $B = gAg^{-1}$ $(= \{gag^{-1} | g \in G\}$. On parlera donc deux *sous-groupes conjugués*, par exemple.

Ceci s'exprime aussi par l'action par conjugaison de G sur l'ensemble des parties de G : c'est l'action $g \cdot A = gAg^{-1}$. C'est une action à gauche.

On appelle *normalisateur* de A l'ensemble des g dans G tels que $gAg^{-1} = A$; autrement dit, c'est le stabilisateur de A dans l'action ci-dessus. C'est donc un sous-groupe de G.

Le *centralisateur* de A est l'ensemble des g dans G tels que $gag^{-1} = a$ pour tout $a \in A$; de manière équivalente $ga = ag$, c'est-à-dire que g commute avec tous les éléments de A.

Proposition 11.8. *Soit A une partie de G. Le centralisateur de A est un sous-groupe normal du normalisateur de A.*

Si A est un sous-groupe de G, alors A est un sous-groupe normal de son normalisateur, et celui-ci est le plus grand sous-groupe de G dans lequel A est un sous-groupe normal

Exercice 152. *On dit que deux matrices carrées A, B de même taille sont* conjuguées *s'il existe une matrice carrée inversible P de même taille telle que $B = P^{-1}AP$. Montrer qu'alors $\mathrm{Tr}(A) = \mathrm{Tr}(B)$ et $\det(A) = \det(B)$. Montrer qu'elles on même polynôme caractéristique.*

Exercice 153. *Un élément de la forme $x\gamma_y(x^{-1})$ de G, avec $x, y \in G$, s'appelle un* commutateur *de G. Montrer que de manière équivalente c'est un élément de la forme $xyx^{-1}y^{-1}$.*

Exercice 154. *Montrer que, sauf pour $n = 2$, le centre de S_n est trivial.*

12 Solutionnaire

La plupart des solutions ne sont qu'esquissées.

1 On a $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}, \mathbb{N} \subset \mathbb{Q}+ \subset \mathbb{R}_+$ et ce sont des monoïdes et sous-monoïdes. Cependant $\mathbb{Q}_+^*$ et $\mathbb{R}_+^*$ ne le sont pas (car ils n'ont pas d'élément neutre). De plus, $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$, qui l'est de $\mathbb{R}$.

2 On a $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ et $\mathbb{Z}^*, \mathbb{N} \subset \mathbb{Q}_+ \subset \mathbb{R}_+$ et ce sont des monoïdes et sous-monoïdes. De plus $\mathbb{Q}_+^*$ *est un sous-groupe de $\mathbb{R}_+^*$.

3 $0 * b = b = b * 0$, $\forall b$, donc 0 est le neutre. $(-1) * b = -1$, $\forall b$, donc -1 n'a pas d'inverse, car $(-1) * b = 0$ (le neutre) est impossible. Notez que la fonction $f : \mathbb{Q} \setminus -1 \to \mathbb{Q}*$ définie par $f(x) = x+1$ est une bijection telle que $f(a * b) = ab + a + b + 1 = (a + 1)(b + 1) = f(a)f(b)$ et $f(0) = 1$ (0 étant le neutre pour $*$ dans $\mathbb{Q} \setminus \{-1\}$ et 1 le neutre pour la multiplication usuelle dans $\mathbb{Q}^*$). C'est un premier exemple d'isomorphisme de groupes.

4 On a $(A \cup B) \cup C = A \cup (B \cup C)$,$\forall A, B, C \in \mathcal{P}(X)$; $A \cup \emptyset = A = \emptyset \cup A$; donc $\emptyset$ est le neutre pour $\cup$). On a $(A \cap B) \cap C = A \cap (B \cap C)$,$\forall A, B, C \in \mathcal{P}(X)$; $A \cap X = A = X \cap A$; donc X est le neutre pour $\cap$).

5 $(3 - 2) - 1 = 0, 3 - (2 - 1) = 3 - 1 = 2, 0 \neq 2$.

6 $(4/2)/2 = 2/2 = 1, 4/(2/2) = 4/1 = 4$.

9 Supposons que H soit un sous-groupe. Alors $e \in H \Rightarrow$ (i) ; pour (ii) soient $a, b \in H$, on a $b^{-1} \in H$, donc $ab^{-1} \in H$.

Réciproquement, supposons que (i) et (ii) soient satisfaits. Soit $a \in H$ (car H non vide). On a $e = aa^{-1} \in H$. Soit $b \in H$; alors $b^{-1} = eb^{-1} \in H$. Soient $a, b \in H$, on a $a, b^{-1} \in H$ et donc par (ii), $ab = a(b^{-1})^{-1} \in H$.

10 $\mathbb{N} \setminus \{1, 2, 4\} = \{0, 3, 5, 6, 7, \ldots\}$ est bien un sous-monoïde de $\mathbb{N}$, avec l'addition. Mais comme $2 + 2 = 4$, $\mathbb{N} \setminus \{1, 4\} = \{0, 2, 3, 5, 6, \ldots\}$ n'est pas un sous-monoïde.

11 $(A\Delta B)\Delta C = \{x \in X | x \,\text{appartient à un seul ou aux trois sous-ensembles}\, A, B \,\text{et}\, C\} = A\Delta(B\Delta C)$, car $A\delta B = \{x | (x \in A \,\text{et}\, x \neq B) \,\text{ou}\, (x \in A \,\text{et}\, x \in B)\} =$

$\{x|x$ appartient à un seul des deux sous-ensembles A et $B\}$. Le neutre est $\emptyset$ car $A\Delta\emptyset = A$ et l'inverse de A est A lui-même car $A\Delta A = \emptyset$, $\forall A$.

12 Le neutre est id_X, la fonction *identité* de X, définie par $id_X(x) = x, \forall x \in X$.

13 Soient A et B deux sous-monoïdes de M. Comme $e \in A$ et $e \in B$, on a $e \in A \cap B$. De plus, si $a, b \in A \cap B$, alors $a, b \in A$ et $a, b \in B$, donc $ab \in A$ et $ab \in B$, car A et B sont des sous-monoïdes ; on a donc $ab \in A \cap B$. Notez que ce résultat est également vrai pour une intersection de plus de deux ou même une intersection d'une infinité de sous-monoïdes. Notez que la réunion $A \cup B$ de deux sous-monoïdes n'en est pas nécessairement un. Par exemple $(2\mathbb{N}) \cup (3\mathbb{N})$ n'est pas un sous-monoïde de $\mathbb{N}$, car $2 + 3 = 5 \notin (2\mathbb{N}) \cup (3\mathbb{N})$.

14 Par induction sur m prouvons : $\forall n, a^n a^m = a^{n+m}$.

(1) $a^n a^0 = a^n 1 = a^n = a^{n+0}$; vrai pour $m = 0$.

(2) $a = na^{m+1} = a^n(a^m a) = (a^n a^m)a = a^{n+m}a = a^{n+m+1}$, par l'associativité et la définition $a^{n+1} = a^n a$.

Par induction sur m prouvons : $\forall n, (a^n)^m = a^{nm}$.

(1) $(a^n)^1 = a^n = a^{n1}$; $(a^n)^0 = 1 = a^{n0}$, donc c'est vrai pour $m = 0$ et $m = 1$.

(2) $(a^n)^{m+1} = (a^n)^m (a^n)^1$ (d'après la première partie) $= a^{nm}a^n = a^{nm+m}$ (idem) $= a^{n(m+1)}$.

15 $(a_1 a_2 \dots a_n)(b_1 b_2 \dots b_m) = a_1 a_2 \dots a_n b_1 b_2 \dots b_m \in A^{n+m}$ si $a_1 a_2 \dots a_n \in A_n$ et $b_1 b_2 \dots b_m \in A_m$.

16 On a $0 = b0$; de plus $bn + bm = b(n + m)$ et $b(-n) + (bn) = 0$. Donc $\{bn|n \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$, noté $n\mathbb{Z}$.

17 $h_1 h_2 \in HH \Rightarrow h_1 h_2 \in H$ et $h \in H \Rightarrow h = 1h \in HH$.

22 Les éléments inversibles sont les bijections $X \to X$. La cardinalité de X^X est n^n, et il y a $n!$ éléments inversibles.

32 On a $aa = 1$, donc $a = a^{-1}$. Donc $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

34 Les orbites sont $Orb(0) = n\mathbb{Z}, Orb(1) = n\mathbb{Z} + 1, \dots, Orb(n - 1) = n\mathbb{Z} + n - 1$. Il y en a n.

35 $0 \cdot z = e^0 z = z$; $(x + y) \cdot z = e^{i(x+y)}z = e^{ix}e^{iy}z = x\dot{(}y \cdot z)$. Les orbites sont $\{z||z| = r\}$, $r \geq 0$, les cercles centrés en O de rayon $r \geq 0$. On a $Stab(0) = \mathbb{R}$, et si $z \neq 0$, $Stab(z) = 2\pi\mathbb{Z}$, où $Stab(z) = Gz$, le stabilisateur de z.

36 $(g_1 g_2) \cdot x = (g_1 g_2)x(g_1 g_2)^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = g_1 \cdot (g_2 \cdot x)$; $Orb(1) = \{g1g^{-1}|g \in G\} = \{1\}$. On a $1 = |Orb(x)| = |\{gxg^{-1}|g \in G\}| \Leftrightarrow \forall g \in G, gxg^{-1} = x \Leftrightarrow \forall g \in G, gx = xg \Leftrightarrow x \in C(G) = \{x \in G|xg = gx\}$.

37 Réflexivité : $g = ege^{-1}$, où e est l'élément neutre. Symétrie : si $g' = xgx^{-1}$, alors $g = x^{-1}g'(x^{-1})^{-1}$. Transitivité : si $g' = xgx^{-1}$ et $g'' = yg'y^{-1}$, alors $g'' = yxgx^{-1}y^{-1} = yxg(yx)^{-1}$.

La classe d'équivalence de g est $\{xgx^{-1}|x \in G\}$, qui est l'orbite $\{x \cdot g|x \in G\}$ de g sous l'action de 36.

39 a) $[1] \cdot ([1] \cdot z) = [1] \cdot \bar{z} = z = [0] \cdot z = ([1] + [1]) \cdot z$.

b) Si z est réel, son orbite est $\{z\}$; si z n'est pas réel, son orbite est $\{z, \bar{z}\}$. Dans le premier cas, le stabilisateur est G, et dans le second, c'est $[0]$.

c) À $(a, b) \in \mathbb{R} \times \mathbb{R}^+$, on associe l'orbite $\{a\}$ si $b = 0$, et l'orbite $\{a + bi, a - bi\}$ si $b < 0$.

40 Les orbites à un élément sont $\{1\}$ et $\{-1\}$; toutes les autres orbites ont deux éléments. Le stabilisateur de 1 est G, ainsi que celui de -1 ; le stabilisateur d'un autre élément est $\{[0]\}$. À un élément de E, on associe son orbite ; on obtient une bijection, car on vérifie que pour tout $z \in \mathbb{C}^*$, son orbite rencontre E en exactement un élément.

41 Une orbite est l'ensemble des sommets d'un polygone régulier à n côtés centré en l'origine. Un tel polygone a exactement un sommet z avec $arg(z) \in [0, 2\pi/n)$.

50 Pour tout $g \in G \setminus H$, G est réunion disjointe de H et Hg. Alors G est réunion disjointe de H et $g^{-1}H$, quelque soit $g \in G \setminus H$. Donc, pour $g \in G \setminus H$, $G \cup Hg = G \cup gH$ (réunion disjointe), et par suite $gH = Hg$. Donc H est normal.

49 (i) $\Rightarrow$ (ii) et (ii) $\Rightarrow$ (iii) sont respectivement les points (i) et (ii) dans la démonstration du théorème 4.10.

(iii) $\Rightarrow$ (i) : On a $g^{-1}hg \in (g-1H)(gH) = (g^{-1}g)H \subset H \Rightarrow g^{-1}hg \in H$ et H est normal.

(ii) $\Rightarrow$ (iv) : $gH)^{-1} = (Hg)^{-1} = \{(hg)^{-1}|h \in H\} = \{g^{-1}h^{-1}|h \in H\} = \{g^{-1}h'|h' \in H\} = g^{-1}H$.

(iv) $\Rightarrow$ (i) : $g^{-1}hg \in g^{-1}Hg = (gH)^{-1}g = Hg^{-1}g = H$.

51 (i) On reconnaît la fonction déterminant. On sait que $\det(AB) = (\det A)(\det B)$. Le lecteur fera le calcul.

(ii) On a $|A \cup B| = |A| + |B| + |A \cap B|, |A\Delta B| = |A \cup B| - |A \cap B| = |A| + |B| - 2|A \cap B|$. Donc $|A\Delta B| = |A| + |B| \mod 2$.

(iii) $n + m \mapsto a^{n+m} = a^n a^m, 0 \mapsto 1$.

53 Soit $g' \in f(H)$; alors $g' = f(h)$ pour un $h \in H$. Donc $(g')^{-1} = (f(h))^{-1} = (f(h^{-1})) \in f(H)$ car $h^{-1} \in H$. De plus $e' = f(e)$: le neutre de G' est bien dans $f(H)$. Si $g'_1, g'_2 \in f(H)$, alors $g'_1 = f(h_1)$ et $g'_2 = f(h_2)$ pour $h_1, h_2 \in H$; d'où $g'_1 g'_2 = f(h_1)f(h_2) = f(h_1 h_2) \in f(H)$ car $h_1 h_2 \in H$, H étant un sous-groupe.

54 Soit $g' \in G', g' = f(g), g \in G$; alors $g' f(h) g'^{-1} = f(g)f(h)f(g'^{-1}) = f(ghg'^{-1}) \in f(H)$.

55 $h_1, h_2 \in f^{-1}(H') \Rightarrow f(h_1), f(h_2) \in H' \Rightarrow f(h_1)f(h_2) = f(h_1h_2) \in H' \Rightarrow h_1h_2 \in f^{-1}(H')$. De plus, $f(1) = 1 \rightarrow 1 \in f^{-1}(H')$. Enfin, $h \in f^{-1}(H') \Rightarrow f(h^{-1}) = f(h)^{-1} \in H' \Rightarrow h^{-1} \in f^{-1}(H')$.

56 Si $h \in f^{-1}(H')$, alors $f(h) = h' \in H'$. Alors pour tout $g \in G$, $f(ghg^{-1}) = f(g)h'f(g)^{-1} \in H'$, donc $ghg^{-1} \in H$.

57 On a $hnh'n' = hh'(h'^{-1}nh') \in HN$. $HN = \bigcup_{h\in H} hN \bigcup_{h\in H} Nh = NH$.

58 Tous les groupes cycliques infinis sont isomorphes.

59 $f^{-1}(H) \xrightarrow{f} H$ est un homomorphisme surjectif et $f^{-1}(H) \subset \mathbb{Z} \Rightarrow f^{-1}(H) = n\mathbb{Z}$. Donc H est cyclique car $nZ \cong \mathbb{Z}$.

60 a) $gng^{-1} \sim g1g^{-1} \sim 1 \Rightarrow gNg^{-1} \subset N, \forall g \in G$; $g \sim h \Rightarrow gh^{-1} \sim 1 \Rightarrow h^{-1} \sim g^{-1}$; $gn \sim g1 = g = 1g \sim ng \Rightarrow Ng = [g] = gN$.

b) $gh^{-1} \in N \Leftrightarrow g \in Nh \Leftrightarrow g \in hN$ (car $Nh = hN$) $\Leftrightarrow h^{-1}g \in N$. Il est facile de vérifier que $\sim$ est une relation d'équivalence, même pour un sous-groupe quelconque. De plus $g_1 \sim g_2$ et $h_1 \sim h_2$ implique $g_1g_2^{-1} \in N, h_1h_2^{-1} \in N$; alors $(g_1h_1)(g_2h_2)^{-1} = g_1g_2h_2^{-1}h_1^{-1} \in g_1Ng_2^{-1} = Ng_1g_2^{-1} \subset NN \subset N$, d'où $g_1h_1 \sim g_2h_2$. La classe de 1 modulo $\sim$ est l'ensemble des g telle $g \in N$; c'est donc N. On conclut en utilisant a).

c) On a vu au chapitre 1 que c'est une relation d'équivalence. De plus $g_1 \sim g_2$ et $h_1 \sim h_2 \Rightarrow f(g_1) = f(g_2)$ et $f(h_1) = f(h_2)$ d'où $f(g_1h_1) = f(g_1)f(h1) = f(g_2)f(h_2) = f(g_2h_2)$. Donc $g_1h_1\ g_2h_2$. On a finalement $[1] = f^{-1}(1) = N(f)$ et $[g] = f^{-1}(f(g)) = gN(f) = N(f)g$ par a).

61 $ag_1g_2a^{-1} = (ag_1a^{-1})(ag_2a^{-1})$, donc ℓ est un homomorphisme. C'est un isomorphisme, car $Ker\ell = \{g|aga^{-1} = 1\} = \{1\}$ et ℓ est surjectif puisque $\ell(a^{-1}ga) = g$.

62 Écrivons, pour simplifier, $az + b$ pour la fonction $z \mapsto az + b$. On a $(a_1z + b_1) \circ (a_2z + b_2) = a_1(a_2z + b_2) + b_1 = a1a_2z + (a_1b_2 + b_1)$; $(a_2z + b_2) \circ (a_1z + b_1) = a2(a_1z + b1) + b_2 = a_1a_2z + (a_2b_1 + b_2)$; donc G n'est pas commutatif, car $a_1b_2 + b1 \neq a_2b_1 = b_2$ en général (par exemple si $b_1 = 1$ et ${}_a1 = a_2 = b_2 = 0$). On a $az' + b = z \Rightarrow a^{-1}z - a^{-1}b = z'$; $(az + b)^{-1} = a^{-1}z + (-a^{-1}b)$; $(az + b) \circ (z + b') \circ (a^{-1}z - a^{-1}b) = (az + ab' + b) \circ (a^{-1}z - a^{-1}b) = z - b + ab' + b = z + ab' \in N$; $az \circ a'z = (aa')z$; $(az+b)\circ(a'z)\circ(a^{-1}z-a^{-1}b) = (aa'z+b)\circ(a^{-1}z-a^{-1}b) = a'z-a'b+b \neq a'z$ si $a' \neq 1$ et $b \neq 0$.

63 $g'_1, g'_2 \in G \Rightarrow g'_1 = f(g_1), g'_2 = f(g_2) \Rightarrow g'_1g'_2 = f(g_1g_2) = f(g_2g_1) = g'_2g'_1$.

65 $\{0, 1, 2, 3, 4, 5\} \xrightarrow{f} \{0, 1, 2\}, f(0) = f(3) = 0, f(1) = f(4) = 1, f(2) = f(5) = 2; N(f) = \{0, 3\}$.

66 $p([i]) = [i], p : \mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z}$; p est bien défini car $i \equiv j \mod abi \Rightarrow$

$j \mod a$.

67 Le neutre est (e, e) ; $(g, g')^{-1} = (g^{-1}, g'^{-1})$.

68 On vérifie que cette fonction est un homomorphisme surjectif, de noyau $6\mathbb{Z}$.

69 0 est (comme dans tout groupe noté additivement) le seul élément d'ordre 1. $\{1, 5, 7, 11\}$: ordre 12 ; $\{2, 10\}$: ordre 6 ; $\{4, 8\}$: ordre 3 ; $\{3, 9\}$: ordre 4 ; $\{6\}$: ordre 2.

70 A cause de l'ordre k de g, les suite bi-infinie $\ldots, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots$ a pour période minimum k. Donc $H = \{g^n, \in \mathbb{Z}\}$ est un ensemble de cardinalité k, et c'est un sous-groupe, par la loi des exposants. La fonction $\mathbb{Z} \to H, n \mapsto H$ est un homomorphisme (pour la la même raison), et il est surjectif.

75 $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la projection canonique ; la fonction $H \mapsto p^{-1}(H)$ est une bijection de l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ vers l'ensemble des sous-groupes de $\mathbb{Z}$ qui contiennent $n\mathbb{Z}$; ceux-ci sont de la forme $d\mathbb{Z}$, d divise n.

93 Il existe un groupe et un élément d'ordre 2. Le carré de cet élément est d'ordre 1.

94 $(1, 3, 7, 5) \circ (2, 4) \circ (6, 9), (1, 3, 5, 7, 9, 8, 6, 4, 2), (1, 9) \circ (2, 8) \circ (3, 7) \circ (4, 6)$.

95 $(j_1, j_2, \ldots, j_k)^{-1} = (j_k, j_{k-1}, \ldots, j_2, j_1)$.

96 $(n-1)!$.

97 $\binom{n}{2}$.

98 $\binom{n}{2}$ est le nombre d'inversions de cette permutation, car c'est le cardinal de l'ensemble $\{(j, i) | n \geq j > i \geq 1\}$. L'ensemble d'inversions d'une permutation est toujours contenu dans l'ensemble précédent.

99 $k; 6; 4$.

101 Écrire la table de multiplication. Ce groupe est isomorphe $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

102 Si $|i - j| \geq 2$, alors σ_i et σ_j sont des cycles disjoints, donc ils commutent. Si $|i - j| = 1$, on peut supposer sans perte de généralités que $j- = i + 1$; alors le calcul montre que $\sigma_i \sigma_j \sigma_j$ envoie i sur $i + 2$, $i + 1$ sur $i + 1$ et $i + 2$ sur i, et qu'il en est de même pour $\sigma_j \sigma_i \sigma_i$; comme σ_i et σ_j laissent fixe tout $k \notin \{i, i + 1, i + 2\}$, on a bien $\sigma_i \sigma_j \sigma_j = \sigma_j \sigma_i \sigma_i$. Pour conclure, on remarque que $\sigma_i^2 = id$.

103 Si $j \notin \{\sigma(j_1), \ldots, \sigma_(j_k)\}$, alors $\sigma \circ \alpha \circ \sigma^{-1}(j) = j$, car $\alpha(\sigma^{-1}(j) = \sigma^{-1}(j)$. De plus, $\sigma \circ \alpha \circ \sigma^{-1}(\sigma(j_i)) = \sigma(j_{i+1})$, $1 \leq i \leq k-1$, et $\sigma \circ \alpha \circ \sigma^{-1}(j_k) = \sigma(j_1)$.

106 L'ensemble E a $n!$ éléments, car on a 2 choix pour a_2, 3 choix pour a_3,..., et n choix pour a_n.

Le fait que l'image de la fonction T est contenue dans E résulte de ce que a_k est égal à la cardinalité d'un ensemble de cardinalité au plus $k-1$; en effet, dans la définition de a_k, on $\sigma(i) = k$ et $\sigma(j) = 1, 2, \ldots, k-1$.

Le fait que l'image de T est exactement E résulte de ce que T est injective.

Montrons que la fonction T est injective. On se donne donc un $n-1$-uplet $T(\sigma) = a_2, \ldots, a_n$; on doit donc avoir $\sigma = unv$, la concaténation des 3 mots u, n et v, où la longueur de v est a_n. Par récurrence sur n, la permutation uv est entièrement déterminée par sa table d'inversion $(a_2, \ldots, a_{n-1})$.

107 On a $(i_1, \ldots, i_k) = \sigma(i_1, \ldots, i_k) = (\sigma(i_1), \ldots, \sigma(i_k))$ si et seulement si $\forall j = 1, \ldots, k$, $\sigma(i_j) = i_j$. Donc le stabilisateur de $(i_1, \ldots, i_k)$ est l'ensemble des permutations dans S_n qui fixent tous les éléments de l'ensemble $I = \{i_1, \ldots, i_k\}$; c'est un sous-groupe de S_n, isomorphe à $S_{n-|I|}$.

117 La fonction qui envoie la matrice indiquée sur a est un isomorphisme de groupes vers $\mathbb{R}$ avec l'addition.

122 Posons $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. On a $ABA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, (ABA)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$.

Soit H le sous-groupe de $GL_2(\mathbb{Z})$ engendré par les matrices $P(q), q \in \mathbb{Z})$. Il s'agit de montrer que $H = GL_2(\mathbb{Z})$. On a déjà $A = P(1)P(0) \in H, B = (P(0)P(1))^{-1} \in H$. Donc $J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in H, -I_2 \in H$.

Soit M dans $GL_2(\mathbb{Z})$. Si M n'a que deux coefficients non nuls, ces deux coefficients ne sont pas dans la même ligne, ni la même colonne ; notez que $P(0) = P(0)^{-1}$. Donc, quitte à multiplier par $P(0)$, M est l'une des quatre matrices diagonales avec des coefficients 1 ou -1 sur la diagonale : c'est donc l'une des 4 matrices $I_2, -I_2, P(0)J, JP(0)$, et elle est dans H.

On peut donc supposer que M a au moins 3 coefficicients non nuls. Ecrivons $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On peut se ramener à $b \neq 0$, quitte à multiplier à gauche par $P(0)$, à ce que les deux coefficients de la première ligne sont non nuls Quitte à multiplier à droite par $P(0)$, on peut se ramener à $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, avec $|a| \geq |b| > 0$. Alors, il existe $q \in \mathbb{Z}$ tel que $a = bq + r, 0 \leq r < |b|$. Alors $M = NP(q)$, où $N = \begin{pmatrix} b & r \\ c' & d' \end{pmatrix}$. Alors la somme des valeurs absolues des coefficients de la première ligne de N est plus petite que celle de M. Par hypothèse de récurrence, on est ramené à $M = \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}$. Comme

le déterminant est ± 1, on doit avoir $d = \pm 1$. Si $d = 1$, $M = B^{-c} \in H$. Si $d = -1$, alors on multiplie par $JP(0)$, et on est ramené à $d = 1$.

123 Si $M \in SL_2(\mathbb{Z})$ est un produit de matrices $P(q)$, ce produit doit comporter un nombre pair de telles matrices ; en effet le déterminant de $P(q)$ est -1, et $\det(M) = 1$. On utilise les identités $P(q)P(r) = P(q)P(0)P(0)P(r)$, $P(q)P(0) = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q$, et similairement pour $P(0)P(r)$.

124 On a $P(q) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q P(0)$.

129 On a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

Références

[1] François Bergeron, Théorie des groupes, Notes de cours, UQàM, 2011. 1

[2] Christophe Hohlweg, Théorie des groupes, Notes de cours, UQàM, 2018. 1

[3] Jacques Labelle, Christophe Reutenauer, Algèbre 1, Notes de cours, UQàM, 1998. 1

[4] Serge Lang, Algebra, 42

[5] Christophe Reutenauer, Algèbre linéaire 2, Notes de cours, UQàM. 37