INTRODUCTION À LA THÉORIE DES GROUPES
MAT 2600

ABRAHAM BROER

Références

[1] M.A. Armstrong, *Groups and symmetry*,U.T.M., Springer-Verlag, New York, 1988.
[2] J.D. Dixon, *Problems in group theory*, Dover reprint, New York, 1973.
[3] D.S. Dummit et R.M. Foote, *Abstract Algebra, third edition*, 2004.
[4] N. Jacobson, *Basic algebra I*, W.H. Freeman, San Francisco 1974.
[5] D.J.S. Robinson, *A course in the theory of groups*, GTM **80**, Springer-Verlag, New York, 1996.
[6] W.R. Scott, *Group theory*, Dover reprint, New York, 1987.

1. Définitions et notions élémentaires

1.1. **Introduction.** Dans les mathématiques plusieurs *orientations* sont utilisées, ou langues, ou modes de penser, d'argumenter ou de communiquer. Comme la langue géométrique, analytique, topologique, probabiliste, statistique, fonctionnelle, algébrique, fonctorielle, et cetera. Chaque mathématicien devrait au moins maîtriser les éléments de base de chaque orientation. Dans ce cours on donnera une introduction à l'orientation algébrique, à l'aide de la notion de base de groupe.

Partout dans les mathématiques des *groupes* jouent des rôles considérables, mais aussi dans les autres domaines scientifiques comme la physique (e.g., la mécanique quantique) ou la chimie (e.g., la cristallographie). Souvent les groupes décrivent les symétries d'une structure : le groupe des mouvements dans l'espace, le groupe de Lorentz, le groupe symétrique, le groupe de monodromie, le groupe de tresses, le groupe de l'icosaèdre, le groupe d'une équation de degré 5, et cetera. Chaque fois qu'il y a des symétries dans un problème scientifique, il y a un certaine groupe associé et en règle générale ça vaut la peine d'expliciter ce groupe.

Un *groupe* est un ensemble muni d'une opération associative, où on suppose qu'il existe un neutre (qui "ne fait rien") et que chaque élément a un inverse ("on peut neutraliser chaque élément").

Voici quelques exemples typiques.

L'ensemble des nombres entiers $\mathbb{Z}$ avec l'opération $+$ usuelle. On a bien sûr l'associativité, $(a+b)+c = a+(b+c)$, le nombre 0 est le neutre, $a+0 = 0+a = a$, et l'inverse du nombre a est $-a$, $a+(-a) = (-a)+a = 0$. C'est un groupe *commutatif*, c'est à dire que $a+b = b+a$ est toujours vrai.

L'ensemble des fractions non-zéro $\mathbb{Q}-\{0\}$ avec l'opération la multiplication usuelle $\cdot$. L'associativité est vrai, $(x\cdot(y\cdot z)) = x\cdot(y\cdot z)$, le neutre est 1, parce que $1\cdot x = x\cdot 1 = x$ pour chaque x, et l'inverse de x est $x^{-1} = 1/x$, parce que $x\cdot x^{-1} = x^{-1}\cdot x = 1$. C'est aussi un groupe commutatif, $x\cdot y = y\cdot z$.

Date: September 9, 2011.

Soit $M :=$ { I, II, III, IV,..., XI, XII} l'ensemble des heures sur une montre de douze heures et l'opération + est définie comme $h_1 + h_2 = h_3$ si et seulement si h_2 heures plus tard que h_1 heures il est h_3 heure sur la montre. Par exemple, X+ X=VIII. Maintenant le neutre est XII, l'inverse de III est IX, de IV est VIII, et cetera. C'est un groupe commutatif d'ordre fini.

Un exemple d'un groupe non-commutatif est le groupe linéaire général $\mathrm{GL}(n, \mathbb{R})$ des matrices réelles de taille $n \times n$ et de déterminant non-zéro :

$$\mathrm{GL}(n, \mathbb{R}) := \{A \text{ matrice réelle } n \times n | \ \det(A) \neq 0\}$$

avec l'opération $\cdot$, la multiplication matricielle usuelle. Dans l'algèbre linéaire on montre que cette multiplication est associative, la matrice identité $\mathbf{1}$ est le neutre ($A \cdot \mathbf{1} = \mathbf{1} \cdot A = A$), et chaque matrice réelle de déterminant non-zéro A a une matrice inverse de déterminant non-zéro A^{-1} (on a $A \cdot A^{-1} = A^{-1} \cdot A = \mathbf{1}$). Ce groupe n'est pas commutatif si $n > 1$, parce qu'il y a des matrices inversibles A et B telles que $A \cdot B \neq B \cdot A$.

Un autre exemple est le groupe symétrique S_n, l'ensemble de tous les bijections de $\{1, 2, \ldots, n\}$, avec la composition comme opération. Ce groupe joue un role important dans la théorie du déterminant d'une matrice carrée. La composition d'applications est toujours associative, le neutre est l'application identité et chaque bijection a un inverse (presque par définition). Si $n > 2$ le groupe symétrique n'est pas commutatif. C'est un autre exemple d'un groupe d'ordre fini.

Quelques exemples d'ensembles avec opération qui ne sont pas de groupes : $\mathbb{Z}$ avec opération $\cdot$ ou $-$; l'ensemble de toutes les applications injectives de $\mathbb{Z}$ dans $\mathbb{Z}$, avec la composition comme l'opération; l'ensemble de toutes les matrices $n \times n$ avec opération $X * Y := XY - YX$ ($n > 1$).

1.2. **Définitions.** Soyons plus exact maintenant.

Une *opération interne* $\circ$ (ou une *opération binaire*, ou un *produit*) sur un ensemble E est une application

$$E \times E \longrightarrow E \ : \ (a, b) \mapsto a \circ b.$$

Alors à chaque paire (sans exceptions !) ordonnée (a, b) d'éléments de E un nouvel élément de E (noté $a \circ b$) est uniquement associé.

À la place de $\circ$ on emploie aussi autres symboles comme $*, \bullet, \cdot, +, \triangle, \ldots$.

L'opération interne est *associative* si

$$(x \circ y) \circ z = x \circ (y \circ z)$$

pour chaque $x, y, z \in E$.

Un *demi-groupe* est une paire ordonnée $(E, \circ)$ d'un ensemble et d'une opération interne associative.

Exemples 1.1. Une opération bien connue sur $\mathbb{Z}$ est la soustraction $-$. Cette opération interne n'est pas associative, car par exemple $1-(2-3) \neq (1-2)-3$. Alors $(\mathbb{Z}, -)$ n'est pas un demi-groupe. Nous allons seulement étudier les opérations internes associatives, mais ils existent aussi des opérations internes très intéressantes, mais non-associatives. Par exemple, considérons l'ensemble de toutes les matrices $n \times n$ réelles anti-symétriques ($A = -A^t$, où A^t est la matrice transposée de A) avec l'opération interne "crochet de Lie"

$$A \times B := A \cdot B - B \cdot A,$$

où $\cdot$ est la multiplication de matrices usuelle. Alors $A \times B$ est aussi anti-symétrique.

Exercice 1.1. Montrer que le crochet de Lie $A \times B$ est une opération interne associative sur l'ensemble de toutes les matrices antisymétriques $n \times n$ *si et seulement si* $n \leq 2$. Montrer par contre que l'identité suivante de Jacobi est toujours satisfaite :

$$A \times (B \times C) + B \times (C \times A) + C \times (A \times B) = 0$$

et que $A \times B = -B \times A$. Ce sont les axiomes d'un anneau de Lie.

Soit $(E, \circ)$ un demi-groupe et soient x_1, x_2, x_3 et $x_4 \in E$. Alors par l'associativité de $\circ$ tous les produits

$$x_1 \circ (x_2 \circ (x_3 \circ x_4)) = x_1 \circ ((x_2 \circ x_3) \circ x_4) = (x_1 \circ (x_2 \circ x_3)) \circ x_4 =$$

$$= ((x_1 \circ x_2) \circ x_3) \circ x_4 = (x_1 \circ x_2) \circ (x_3 \circ x_4)$$

donnent le même élément de E. On écrit cet élément sans parenthèses comme

$$x_1 \circ x_2 \circ x_3 \circ x_4.$$

De façon analogue pour plus de termes. Si par contre l'opération interne $\circ$ n'est pas associative nous ne donnons pas à $x_1 \circ x_2 \circ x_3$ un sens.

L'opération interne est *commutative* si

$$x \circ y = y \circ x$$

pour chaque $x, y \in E$. Nous n'allons utiliser le symbole $+$ ("plus") que pour les opérations internes commutatives.

Un élément *neutre* (simultanément à gauche et à droite) pour une opération $\circ$ sur E est un élément $x \in E$ tel que

$$x \circ y = y \circ x = y$$

pour chaque $y \in Y$.

Un *monoïde* est un demi-groupe $(E, \circ)$ où l'opération interne possède un élément neutre. Nous obtenons un premier résultat. C'est un résultat facile à montrer, mais ce n'est pas évident.

Lemme 1.1. *Soit $(E, \circ)$ un monoïde. Alors l'opération interne $\circ$ ne possède qu'un seul élément neutre.*

Preuve. Par la définition de monoïde il existe un élément neutre, disons x. Supposons que y est aussi un élément neutre. Alors $y = x \circ y$ (parce que x est un neutre) et $x \circ y = x$ (parce que y est un neutre). Donc $x = y$. □

Alors on peut parler **du** *neutre* d'un monoïde $(M, \circ)$, parce que cet élément (qui existe par hypothèse d'un monoïde) est uniquement déterminé. Ce neutre est noté $\mathbf{1}_M$ (ou $\mathbf{1}$ s'il n'y a pas de confusion possible), si le symbole d'opération n'est pas $+$. Par contre, on écrit $\mathbf{0}_M$ ou $\mathbf{0}$ ("zéro") pour le neutre si l'opération interne du monoïde $(M, +)$ est notée $+$.

Exemples 1.2. Par exemple, $(\mathbb{Z}_{\geq 0}, +)$ est un monoïde avec neutre 0, mais $(\mathbb{Z}_{>0}, +)$ est seulement un demi-groupe. Aussi $(\mathbb{Z}, \cdot)$ est un monoïde, dans lequel le nombre 1 est le neutre.

Soit $M(n \times n, \mathbb{R})$ l'ensemble de toutes les matrices réelles de taille $n \times n$ et $\cdot$ la multiplication matricielle usuelle. Alors $(M(n \times n, \mathbb{R}), \cdot)$ est un monoïde, le neutre est la matrice identité $\mathbf{1}$.

Pour deux ensembles X et Y on écrit X^Y pour l'ensemble de toutes les applications $f : Y \longrightarrow X$. Si $Y = X$, la composition $f \circ g$ de deux applications $f, g \in X^X$ est définie comme d'habitude par

$$(f \circ g)(x) := f(g(x)).$$

Alors $(X^X, \circ)$ est un monoïde avec neutre l'application identité $\mathbf{1}$ (où $\mathbf{1}(x) = x$ pour chaque $x \in X$). On vérifie l'associativité :

$$(f_1 \circ (f_2 \circ f_3))(x) = f_1((f_2 \circ f_3)(x)) = f_1(f_2(f_3(x))) = (f_1 \circ f_2)(f_3(x)) = ((f_1 \circ f_2) \circ f_3)(x),$$

pour chaque $x \in X$ et $f_1, f_2, f_3 \in X^X$.

Soit $(E, \circ)$ un monoïde avec neutre $\mathbf{1}_E$. On dit que $x \in E$ a un *inverse* (simultanément à gauche et à droite) dans le monoïde s'il existe un élément $y \in E$ tel que

$$x \circ y = y \circ x = \mathbf{1}_E.$$

Lemme 1.2. *Soit $(E, \circ)$ un monoïde. Il est impossible qu'un élément de E a plus qu'un inverse.*

Preuve. Supposons que y et z sont deux inverses de x dans le monoïde avec neutre $\mathbf{1}_E$. Alors

$$y = y \circ \mathbf{1}_E = y \circ (x \circ z) = (y \circ x) \circ z = \mathbf{1}_E \circ z = z.$$

Ici on a utilisé les propriétés du neutre $\mathbf{1}_E$, de l'associativité et d'un inverse. Donc $y = z$. □

Alors dans un monoïde un peut parler de *l'inverse* de x si x possède un inverse, parce que cet élément est uniquement déterminé. Cet inverse de x est noté x^{-1}, si l'opération n'est pas $+$. Mais on écrit $-x$ pour l'inverse si l'opération interne est le $+$. Mais nous ne donnons pas de sens à x^{-1} (ni à $-x$) si x n'a pas d'inverse (ou si c'est inconnu si x possède un inverse ou non).

Un *groupe* est un monoïde dont tous les éléments possèdent un inverse. Donc on peut parler du neutre du groupe et de l'inverse de chaque élément.

Un groupe *abélien*[1] (ou *commutatif*) est un groupe dont l'opération interne est commutative.

Un critère pour qu'un demi-groupe soit un groupe est donné dans l'exercice suivant.

Exercice 1.2. [2] Soit E un ensemble avec une opération interne associative notée $\circ$. On suppose l'existence d'un élément $e \in E$ avec les propriétés suivantes.

(i) Pour chaque $a \in E$ on a $e \circ a = a$ (on dit que e est un *neutre à gauche*),

(ii) Pour chaque $a \in E$ il existe un $b \in E$ tel que $b \circ a = e$ (on dit que *l'inverse à gauche* existe).

Alors $(E, \circ)$ est un groupe.

Exercice 1.3. L'ensemble des matrices $n \times n$ de coefficients entières et de déterminant non-zéro, avec l'opération $\cdot$ (la multiplication matricielle) est un monoïde mais pas un groupe.

[1] Niels Henrik Abel, mathématicien norvégien, 1802-1829.

[2] Dans un exercice on demande de montrer toutes les affirmations données.

Exercice 1.4. Un groupe dans lequel chaque élément est son propre inverse (i.e., $x = x^{-1}$) est abélien.

Exercice 1.5. Soit $(G, +)$ un groupe abélien fini.

(i) Supposons $x \in G$ est un élément tel que $x + x = \mathbf{0}$. Si $x \neq \mathbf{0}$ alors l'ordre de G est pair. Indice: montrer que G est la réunion disjointe d'un certain nombre de jumeaux $\{a, a + x\}$, ce qui implique que l'ordre de G est pair.

(ii) Soit x la somme de tous les éléments du groupe. Alors $x + x = \mathbf{0}$ et si l'ordre de G est impair alors $x = \mathbf{0}$.

Exercice 1.6. Soit $n \in \mathbb{Z}_{\geq 1}$. Le groupe *cyclique* d'ordre n est la paire $(C_n, \cdot)$, où

$$C_n := \{e^{2\pi ik/n} \in \mathbb{C};\ k \in \mathbb{Z}\} = \{z \in \mathbb{C}; z^n = 1\}$$

est l'ensemble des n racines n-ièmes de 1 dans $\mathbb{C}$ et où $\cdot$ est la multiplication des nombres complexes. Si on écrit $\rho := e^{2\pi i/n}$ alors

$$C_n = \{1, \rho, \rho^2, \rho^3, \ldots, \rho^{n-1}\}$$

a exactement n éléments et $\rho^n = 1$, $\rho^{-1} = \rho^{n-1}$.

Exercice 1.7. Fixons $n \geq 2$.

(i) La rotation du plan réel par $2\pi k/n$ radian (ou par $360k/n$ degrés) est réalisée par la matrice orthogonale

$$\begin{pmatrix} \cos 2\pi k/n & -\sin 2\pi k/n \\ \sin 2\pi k/n & \cos 2\pi k/n \end{pmatrix}$$

et la réflection par rapport de la droite qui à l'angle $\pi k/n$ radian (ou par $180k/n$ degrés) avec l'axe de x est réalisée par la matrice orthogonale

$$\begin{pmatrix} \cos 2\pi k/n & \sin 2\pi k/n \\ \sin 2\pi k/n & -\cos 2\pi k/n \end{pmatrix}.$$

(ii) Le group *diédral* est la paire $(D_n, \cdot)$, où

$$D_n := \left\{ \begin{pmatrix} \cos 2\pi k/n & -\sin 2\pi k/n \\ \sin 2\pi k/n & \cos 2\pi k/n \end{pmatrix};\ k \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} \cos 2\pi k/n & \sin 2\pi k/n \\ \sin 2\pi k/n & -\cos 2\pi k/n \end{pmatrix};\ k \in \mathbb{Z} \right\}$$

est une certaine collection de $2n$ matrices orthogonales et où $\cdot$ est la multiplication matricielle. C'est un groupe non-commutatif si et seulement si $n > 2$. Décrire les éléments qui sont leur propre inverse.

(iii) Écrivons

$$\rho := \begin{pmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{pmatrix} \text{ et } \sigma := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Alors

$$\sigma^2 = \rho^n = \mathbf{1} \text{ et } \sigma\rho\sigma = \rho^{-1} = \rho^{n-1}$$

et

$$D_n = \{\rho^i \sigma^j;\ 0 \leq i < n, 0 \leq j < 2\}.$$

(On remarque le suivant. Soit M une matrice 2×2 orthogonale quelconque. Alors $M \in D_n$ si et seulement si M transforme le "n-gon régulier" sur soi-même.)

Exercice 1.8. Soit $(M, \circ)$ un monoïde. On écrit

$$M^\times := \{m \in M | \ \ m \text{ possède un inverse dans le monoîde } (M, \circ)\}.$$

Montrer que $x \circ y \in M^\times$ si x et $y \in M^\times$, et montrer que la paire $(M^\times, \circ)$ (où $\circ$ est l'opération interne sur $M^\times$ induite par l'opération interne sur M) est un groupe.

On a par exemple $(M(n, \mathbb{R})^\times, \cdot) = (\mathrm{GL}(n, \mathbb{R}), \cdot)$ et $((X^X)^\times, \circ) = (S_n, \circ)$, si $X = \{1, 2, \ldots, n\}$. Décrire $(\mathbb{Z}^\times, \cdot)$.

1.3. **Notation.** Dans un groupe $(G, \circ)$ on écrit souvent ab à la place de $a \circ b$ (sauf si le symbole de l'opération interne est le $+$, dans ce cas on ne supprime jamais le symbole $+$).

Souvent on dénote un groupe $(G, \circ)$ par son ensemble G seulement. Dans ce cas il faut que se soit clair par le contexte quelle opération interne $\circ$ est prise. Si le symbole de l'opération interne n'est pas explicitement donné on utilise généralement $x \cdot y$ ou xy pour l'opération interne. Mais si le groupe est abélien on écrit généralement (mais pas exclusivement) $x + y$ pour l'opération.

Soit $(G, \circ)$ un groupe. On pose $x^0 := \mathbf{1}_G$, $x^1 := x$ et x^{-1} pour l'inverse de x. On définit par induction sur l'entier $n \geq 0$

$$x^n := (x^{n-1}) \circ x \text{ et } x^{-n} := x^{-n+1} \circ x^{-1}.$$

Par exemple, $x^5 = x \circ x \circ x \circ x \circ x$ et $x^{-2} = x^{-1} \circ x^{-1}$. De façon analogue, si $(G, +)$ est un groupe abélien avec opération interne $+$ on définit $0x = \mathbf{0}$, $1x := x$ et $-1x = -x$ pour l'inverse de x et par induction sur l'entier n

$$nx := ((n-1)x) + x \text{ et } \ -nx := (-n+1)x + (-x).$$

Si l'opération interne n'est pas $+$, alors $2x$ n'est pas défini, et si l'opération interne est notée par $+$ alors x^2 n'est pas défini a priori.

Exercice 1.9. Soit $(G, \circ)$ un groupe et $x \in G$. Alors pour n et $m \in \mathbb{Z}$ on a

$$x^{n+m} = x^n \circ x^m \text{ et } (x^n)^{-1} = x^{-n}.$$

1.4. **Homomorphisme de groupes.** Un *homomorphisme* ou un *morphisme* (de groupes) entre deux groupes $(G, \circ)$ et $(K, *)$ est une application $\phi : G \longrightarrow K$ telle que

$$\phi(x \circ y) = \phi(x) * \phi(y)$$

pour chaque x et $y \in G$.

Un *monomorphisme* est un homomorphisme injectif, ça veut dire que $x \neq y \in G$ implique que $\phi(x) \neq \phi(y) \in K$.

Un *épimorphisme* est un homomorphisme surjectif, ça veut dire que pour chaque $k \in K$ il existe au moins un élément $g \in G$ tel que $\phi(g) = k$.

Un *isomorphisme* est un homomorphisme bijectif, ça veut dire que pour chaque $k \in K$ il existe un seul élément $g \in G$ tel que $\phi(g) = k$. Cet élément g est noté $\phi^{-1}(k)$.

Un *endomorphisme* est un homomorphisme d'un groupe dans lui-même, alors si $(G, \circ) = (K, *)$.

Un *automorphisme* est un endomorphisme bijectif. L'ensemble de tous les automorphismes d'un group G est noté $\mathrm{Aut}(G)$.

Exemples 1.3. Le déterminant $\det : \mathrm{GL}(n,\mathbb{R}) \longrightarrow \mathbb{R}^\times$ définit un homomorphisme entre $(\mathrm{GL}(n,\mathbb{R}),\cdot)$ et $(\mathbb{R}^\times,\cdot)$ (rappel : $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$). Parce que (par l'algèbre linéaire)

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

pour toutes les matrices $n \times n$ A et B. Le déterminant est un épimorphisme (pourquoi?).

L'exponentiel $\exp : \mathbb{R} \longrightarrow \mathbb{R}^\times$ définit un homomorphisme de groupes entre $(\mathbb{R},+)$ et $(\mathbb{R}^\times,\cdot)$, parce que

$$\exp(x+y) = \exp(x) \cdot \exp(y).$$

C'est un monomorphisme mais pas un épimorphisme (pourquoi ?).

L'exponentiel $\exp : \mathbb{C} \longrightarrow \mathbb{C}^\times$ définit un homomorphisme de groupes entre $(\mathbb{C},+)$ et $(\mathbb{C}^\times,\cdot)$, parce que $\exp(x+y) = \exp(x) \cdot \exp(y)$. Maintenant c'est un épimorphisme mais pas un monomorphisme (pourquoi ?).

L'application inverse-transposé $\mathrm{GL}(n,\mathbb{R}) \longrightarrow \mathrm{GL}(n,\mathbb{R})$ qui applique une matrice A à son inverse transposé $(A^t)^{-1} (= (A^{-1})^t)$ est un automorphisme de $(\mathrm{GL}(n,\mathbb{R}),\cdot)$.

Dans la théorie des groupes on considère deux groupes comme équivalent ou "essentiellement les mêmes groupes" s'il existe un isomorphisme entre les deux groupes. Cette idée d'isomorphisme est extrêmement importante.

Exercice 1.10. Soit

$$G := \left\{ \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} ;\ \phi \in \{0, 2\pi/3, 4\pi/3\} \right\}$$

et $\cdot$ la multiplication matricielle usuelle. Alors $(G,\cdot)$ est un groupe.

Soit $H := \{a,b,c\}$ avec l'opération interne $\blacklozenge$ définie par la table de composition

$\blacklozenge$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Alors $(H,\blacklozenge)$ est un groupe.

Les deux groupes $(G,\cdot)$ et $(H,\blacklozenge)$ sont isomorphes. Tous les groupes de cardinalité trois sont "essentiellement le même groupe".

Exercice 1.11. Si $\phi : G \longrightarrow K$ est un isomorphisme de groupes, alors l'application inverse $\phi^{-1} : K \longrightarrow G$ est aussi un isomorphisme de groupes. La composition $\phi \circ \psi$ de deux automorphismes ϕ et ψ de G donne une opération interne sur $\mathrm{Aut}\, G$; $(\mathrm{Aut}\, G, \circ)$ est un groupe, le *groupe d'automorphismes* de G.

Exercice 1.12. Chaque élément $g \in G$ définit un automorphisme c_g de G par *conjugaison*, défini par

$$c_g(x) := gxg^{-1}.$$

L'application $c : G \longrightarrow \mathrm{Aut}\, G$ définie par $c(g) := c_g$ donne un homomorphisme de groupes.

Exercice 1.13. Soit $n > 2$ et $(G, \cdot)$ un groupe. Supposons il existe $a, b \in G$ tels que $a^n = b^2 = \mathbf{1}_G$ et $ba = a^{-1}b$ et n est le plus petit $n \geq 1$ tel que $a^n = \mathbf{1}$. Montrer qu'il existe un monomorphism du groupe diédral D_n (exercice 1.6) dans G.

Le *noyau* d'un homomorphisme $\phi : G \longrightarrow K$ (dénoté par $\operatorname{Ker}\phi$) est défini comme

$$\operatorname{Ker}\phi := \{g \in G |\ \phi(g) = \mathbf{1}_K\},$$

où $\mathbf{1}_K$ est le neutre du groupe K. Alors le noyau est l'ensemble des éléments de G qui sont envoyés vers le neutre de H. L'*image* de ϕ est définie comme d'habitude par

$$\operatorname{Im}\phi := \{\phi(g) |\ g \in G\}.$$

Lemme 1.3. *Soit $\phi : G \longrightarrow K$ un homomorphisme entre les groupes $(G, \circ)$ et $(K, *)$. Alors $\phi(\mathbf{1}_G) = \mathbf{1}_K$ et pour chaque $g \in G$ on a $\phi(g^{-1}) = (\phi(g))^{-1}$.*

Preuve. On utilise que si $x^2 = x$ dans un groupe, alors $x = \mathbf{1}$. Preuve : $x^2 = x$ implique que $x^2 \cdot x^{-1} = x \cdot x^{-1}$, donc $x = \mathbf{1}$. On a maintenant

$$\phi(\mathbf{1}_G) = \phi(\mathbf{1}_G \circ \mathbf{1}_G) = \phi(\mathbf{1}_G) * \phi(\mathbf{1}_G),$$

donc $\phi(\mathbf{1}_G) = \mathbf{1}_K$. Le reste de la preuve est laissé comme exercice. □

Lemme 1.4. *Un homomorphisme $\phi : G \longrightarrow K$ est un monomorphisme si et seulement si le noyau de ϕ ne contient que le neutre de G.*

Preuve. Le noyau contient au moins le neutre de G. Supposons que ϕ est un monomorphisme, alors $g \neq \mathbf{1}_G$ implique que $\phi(g) \neq \phi(\mathbf{1}_G) = \mathbf{1}_K$. Donc $g \notin \operatorname{Ker}\phi$.

Par contre, supposons que $\operatorname{Ker}\phi = \{\mathbf{1}_G\}$ et $x \neq y \in G$. Alors $x \circ y^{-1} \neq \mathbf{1}_G$ et $\phi(x \circ y^{-1}) \neq \mathbf{1}_K$. Alors $\phi(x) * \phi(y^{-1}) = \phi(x) * \phi(y)^{-1} \neq \mathbf{1}_K$ et $\phi(x) \neq \phi(y)$. Donc l'application ϕ est injective. □

Exercice 1.14. Soit $\log : (\mathbb{R}^{\times}_{>0}, .) \longrightarrow (\mathbb{R}, +)$ le logarithme. Vérifier les deux lemmes précédents dans ce cas.

Exercice 1.15. Trouver tous les homomorphismes $\phi : C_n \longrightarrow D_n$ et $\psi : D_n \longrightarrow C_n$ entre le groupe cyclique et le groupe diédral, si $n = 2, 3, 4$.

2. Permutations et groupe symétrique

Le groupe des permutations d'un ensemble fini est un des plus importants groupes finis. On va établir quelques propriétés.

Soit E un ensemble. On dit qu'une application $f : E \longrightarrow E$ a un inverse, s'il existe une application $g : E \longrightarrow E$ telle que les deux compositions $f \circ g$ et $g \circ f$ sont l'application identité

$$f(g(x)) = g(f(x)) = x,$$

pour chaque $x \in E$. Cette application g est unique (pourquoi?) et notée souvent f^{-1}, l'inverse de f. On dit que f est une bijection ou une permutation de E. L'ensemble de toutes les permutations (ou bijections) de E est notée

$$S_E.$$

On écrit $S_n := S_E$ dans le cas particulier où $E = \{1, 2, 3, \ldots, n\}$.

Si f_1 et $f_2 \in S_E$, alors la composition $f_1 \circ f_2$, définie par $(f_1 \circ f_2)(x) := f_1(f_2(x))$, est aussi un élément de S_E. La règle d'associativité est satisfaite :

$$(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3),$$

pour chaque $f_1, f_2, f_3 \in S_E$. Preuve :

$$\begin{aligned} ((f_1 \circ f_2) \circ f_3)(x) &= ((f_1 \circ f_2)(f_3(x)) \\ &= f_1(f_2(f_3(x))) \\ &= f_1((f_2 \circ f_3)(x)) \\ &= (f_1 \circ (f_2 \circ f_3))(x) \end{aligned}$$

pour chaque $x \in E$; d'où le résultat.

La paire $(S_E, \circ)$ est appelée le *groupe symétrique* sur E.

Exercice 2.1. La cardinalité de S_n est $n!$.

Exercice 2.2. Si $\beta : E \longrightarrow F$ est une bijection entre deux ensembles, trouver un isomorphisme entre S_E et S_F. Combien d'isomorphismes différents existent-t-ils entre S_E et S_F si E et F ont 2 ou 3 éléments?

Une permutation $f \in S_E$ est connue si (et seulement si) l'image de chaque élément de E est connue. Si $E = \{a, b, \ldots, z\}$ est un ensemble fini on peut donner toutes les images de f dans un tableau

$$f = \begin{pmatrix} a & b & \ldots & z \\ f(a) & f(b) & \ldots & f(z) \end{pmatrix}.$$

Par exemple, si $E = \{1, 2, 3, 4, 5\}$, alors

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

est l'application $f : \{1, 2, 3, 4, 5\} \longrightarrow \{1, 2, 3, 4, 5\}$ où

$$f(1) = 2, f(2) = 3, f(3) = 4, f(4) = 1 \text{ et } f(5) = 5.$$

Il y a une application inverse pour f, donc $f \in S_E = S_5$. On obtient l'inverse f^{-1} de f en changeant les deux lignes dans un tableau de f :

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

Soit maintenant

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

alors la composition est

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = g \circ f.$$

(Vérifier! On va de droite à gauche.)

Une permutation $f : E \longrightarrow E$ est dite *cyclique* d'ordre m, ou un m-cycle, s'ils existent m éléments différents $x_1, x_2, \ldots, x_m \in E$ tels que $f(x_i) = x_{i+1}$, pour $1 \leq i < m$, $f(x_m) = x_1$ et $f(x) = x$ pour chaque autre $x \in E$ (si $x \in E \backslash \{x_1, \ldots, x_m\}$). Et on écrit $f = (x_1, x_2, \ldots, x_m)$.

Exercice 2.3. On a $(x_1, x_2, \ldots, x_m) = (x_2, x_3, \ldots, x_m, x_1) \in S_E$.

On remarque que dans S_5 on a

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

puis

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

et

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

Exercice 2.4. Calculer dans S_5

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \circ (1,2,3,4,5) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \circ (1,5) \circ (1,5,4) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

On dit que les cycles $(x_1, \ldots, x_m)$ et $(y_1, \ldots, y_k)$ sont *disjoints*, si $x_i \neq y_j$ pour chaque i et j.

Exercice 2.5. Si les cycles $f = (x_1, \ldots, x_m)$ et $g = (y_1, \ldots, y_k)$ sont disjoints alors f et g commutent, ça veut dire $f \circ g = g \circ f$.

Proposition 2.1. *Si la cardinalité $n := |E|$ de E est finie, alors chaque permutation dans S_E est une composition finie de cycles deux à deux disjoints.*

Par exemple, dans S_9 on a

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 5 & 6 & 4 & 3 & 1 & 2 & 9 \end{pmatrix} = (1,7) \circ (2,8) \circ (3,5,4,6) = (1,7) \circ (2,8) \circ (3,5,4,6) \circ (9).$$

Preuve. Par induction sur n. Si $n = 1$, il n'y a qu'une seule permutation : l'identité qui est un 1-cycle (e), si $E = \{e\}$. Supposons $n > 1$ et choisissons $x \in E$. Soit f une permutation. Considérons

$$x, f(x), f^2(x) := f(f(x)), f^3(x) := f(f(f(x))), \ldots$$

Ils existent $n_1 < n_2$ tels que $f^{n_1}(x) = f^{n_2}(x)$, parce que $n < \infty$. Après la composition avec $(f^{-1})^{n_1}$ on obtient un entier positif $m (= n_2 - n_1)$ tel que $x = f^m(x)$. Choisissons un tel m de façon minimal, alors les éléments

$$x, f(x), f^2(x), \ldots, f^{m-1}(x)$$

sont tous différents.

Si $E_1 := \{x, f(x), f^2(x), \ldots, f^{m-1}(x)\} = E$ alors $n = m$ et f est le n-cycle

$$f_1 := (x, f(x), f^2(x), \ldots, f^{n-1}(x))$$

et on est prêt. Sinon f permute aussi les éléments dans le complément $E_2 := E\backslash E_1$. C'est à dire, si $y \in E_2$ alors $f(y) \in E_2$, car sinon il existe un m tel que $f(y) = f^m(x)$ donc $y = f^{m-1}(x) \in E$, contradiction. Donc la restriction du permutation f sur E_2 est aussi une permutation de E_2.

Par induction cette permutation f_2 de E_2 est une composition finie de cycles deux à deux disjoints

$$f_2 = \sigma_1 \circ \sigma_2 \circ \dots \sigma_s.$$

Chaque σ_i est de la forme $(x_1, x_2, \dots, x_m)$ où chaque $x_i \in E_2$. On peut interpréter chaque σ_i et f_2 comme permutation de E, fixant chaque élément de E_1. Maintenant

$$f = (x, f(x), f^2(x), \dots, f^{m-1}(x)) \circ \sigma_1 \circ \sigma_2 \dots \sigma_s,$$

parce que si $e \in E_2$, alors $f(e) = f_2(e)$ sinon il existe un i tel que $e = f^i(x)$. Donc f est une composition de cycles deux à deux disjoints. □

Exercice 2.6. Soit $f = (x_1, x_2, \dots, x_m)$ un m-cycle et $g \in S_E$. Montrer que $g \circ f \circ (g^{-1})$ est le m-cycle $(y_1, y_2, \dots, y_m)$ avec $y_i := g(x_i)$.

Par exemple, si $f = (1, 4, 3)$ et $g = (1, 2) \circ (3, 4, 5)$ dans S_9, alors

$$g \circ f \circ g^{-1} = (g(1), g(4), g(3)) = (2, 5, 4).$$

Exercice 2.7. Chaque permutation $f \in S_n$ est un produit de 2-cycles de la forme $(i, i+1)$, où $1 \leq i < n$. Par exemple,

$$(1,2,3,4,5,6,7,8) = (1,2) \circ (2,3) \circ (3,4) \circ (4,5) \circ (5,6) \circ (6,7) \circ (7,8) \text{ et } (1,3) = (2,3) \circ (1,2) \circ (2,3).$$

2.1. **Matrices de permutation.** Prenons $E := \{1, 2, \dots n\}$. Nous allons associer à chaque permutation une matrice $n \times n$ de coefficients réels (où de coefficients dans un autre corps comme $\mathbb{C}$, $\mathbb{Q}$ ou $\mathbb{F}_q$, voyez plus loin). Si $f \in S_n$, alors la matrice L_f est définie comme $(L_f)_{ji} = 1$ si $j = f(i)$ et $(L_f)_{ji} = 0$ si $j \neq f(i)$, pour $i, j \in E$. La matrice L_f est appelée la *matrice de permutation* associée à la permutation f. Soit

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n := \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

la base naturelle de l'espace vectoriel $\mathbb{R}^n$ de vecteurs colonnes. La matrice L_f est aussi déterminée par la propriété

$$L_f e_i = e_{f(i)}$$

pour $i \in E$. Si $f, g \in S_n$, alors

$$(L_f L_g) e_i = L_f e_{g(i)} = e_{f(g(i))} = e_{(f \circ g)(i)} = L_{f \circ g} e_i,$$

pour chaque $i \in E$. Donc $L_f L_g = L_{f \circ g}$, ça veut dire le produit des deux matrices de permutation f et g est la matrice de permutation associée à la composition $f \circ g$. Il suit que l'application

$$L : S_n \longrightarrow \mathrm{GL}(n, \mathbb{R});\ L(f) := L_f$$

est un homomorphisme de groupes.

Exemples pour $n = 3$.

$$L_{(1,2,3)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, L_{(1,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, L_{(2,3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

et en effet $L_{(1,2,3)} = L_{(1,2)}L_{(2,3)}$.

On peut identifier l'ensemble de matrices $\{L_f |\ f \in S_n\}$ comme l'ensemble de matrices $n \times n$ ayant un et un seul coefficient 1 dans chacune de ses lignes et de ses colonnes; ses autres coefficients étant 0. Notons cet ensemble de matrices par P_n.

Lemme 2.1. *Le déterminant de $L \in P_n$ est 1 ou -1.*

Preuve. Après une permutation des lignes de L on obtient la matrice identité ayant déterminant 1. □

On définit le *signe* $\mathrm{sg}(f)$ d'un élément de S_n comme le déterminant de sa matrice de permutation L_f.

Lemme 2.2. *On a $\mathrm{sg}(f)\mathrm{sg}(g) = \mathrm{sg}(f \circ g)$ pour $f, g \in S_n$.*

Preuve. On a $L_{f\circ g} = L_f L_g$ et $\det(L_f L_g) = \det(L_f)\det(L_g)$. □

Donc le signe est aussi un homomorphisme de groupes. Les permutations de signe $+1$ sont appelées *paires* et ceux de signe -1 sont appelées *impaires*.

Exercice 2.8. Soit f est un produit d'un certain nombre de permutations cycliques, dont n_m sont de longueur m, où $m = 1, 2, \ldots$. Mettons $N := \sum_m n_m(m-1)$. Montrer que $\mathrm{sg}(f) = (-1)^N$.

Exercice 2.9. Il pourrait exister un problème logique avec cette définition du signe à l'aide du déterminant, dépendant de la définition du déterminant adoptée ! Pour cette raison nous donnons une définition alternative du sg.

Considérons l'ensemble $\mathbb{R}[x_1, \ldots, x_n]$ de tous les polynômes $F(x_1, \ldots, x_n)$ dans les variables $x_1, \ldots, x_n$ et des coefficients réels. Pour une permutation $\pi \in S_n$ et un polynôme F on définit un autre polynôme $\pi * F$ ainsi :

$$(\pi * F)(x_1, x_2, \ldots, x_n) := F(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)});$$

c-à-d, on remplace le variable x_i par le variable $x_{\pi(i)}$. Par exemple, si $F = x_1^2 + 7x_2x_3$ on a

$$(1,2)*F = x_2^2+7x_1x_3; (1,3,2)*F = x_3^2+7x_1x_2; (2,3)*[(1,2)*F] = (2,3)*(x_2^2+7x_1x_3) = x_3^2+7x_1x_2.$$

(i) Montrer que

$$\pi_1 * [\pi_2 * F] = (\pi_1 \circ \pi_2) * F,$$

pour chaque $F \in \mathbb{R}[x_1, \ldots, x_n]$ et $\pi_1, \pi_2 \in S_n$.

(ii) Fixons le polynôme $\Delta := \prod_{1\le i<j\le n}(x_i - x_j)$. Montrer que pour chaque $\pi \in S_n$, il existe un signe $\epsilon(\pi) \in \{1, -1\}$ tel que

$$\pi * \Delta = \epsilon(\pi)\Delta.$$

(En fait, $\epsilon(\pi) = (-1)^{\ell(\pi)}$, où $\ell(\pi)$ est le nombre de pairs $i < j$ tels que $\pi(i) > \pi(j)$ (appelé *inversion*).)

(iii) Montrer que

$$\epsilon : S_n \longrightarrow \{1, -1\} : \pi \mapsto \epsilon(\pi)$$

est un homomorphisme de groupes.

(iv) Montrer que $\mathrm{sg} = \epsilon$. [Puisque les 2-cycles $(i, i+1)$ (où $1 \leq i < n$) engendrent S_n, il suffit de montrer $\mathrm{sg}((i, i+1)) = \epsilon((i, i+i) = -1)$.]

Exercice 2.10. Une permutation f de S_n est paire si et seulement si f est la composition d'un nombre pair de 2-cycles. Une permutation f est paire si et seulement si f est la composition d'un nombre de 3-cycles.

Les permutations paires

$$\mathrm{Alt}_n := \{f \in S_n;\ \mathrm{sg}(f) = 1\}$$

avec l'opération interne la composition $\circ$ des permutations forme un groupe : le groupe *alterné* d'ordre n. C'est le noyau de l'homomorphisme sg.

Exercice 2.11. La cardinalité du groupe alterné Alt_n est $n!/2$.

3. Corps et groupes linéaires

Pour être capable de donner encore plus d'exemples de groupes, il faut introduire la notion de corps ("field", en anglais). On a vu sa définition très vite dans l'algèbre linéaire, mais pas beaucoup de ses propriétés. L'essentiel est qu'on peut faire de l'algèbre linéaire sur un corps quelconque.

Par définition un corps est un ensemble K avec deux opérations internes commutatives fixées, notées $+$ et $\cdot$, satisfaisant plusieurs axiomes.

Premièrement, la paire $(K, +)$ soit un groupe abélien; le neutre pour le $+$ est noté $\mathbf{0}$ et l'inverse de x est $-x$.

Puis, la paire $(K, \cdot)$ soit un monoïde commutatif, le neutre est noté $\mathbf{1}$.

Les deux éléments spéciaux $\mathbf{0}$ et $\mathbf{1}$ soient différents.

Chaque élément $k \neq \mathbf{0}$ dans K est supposé d'avoir un inverse pour le $\cdot$, noté x^{-1}.

Finalement, les deux opérations internes soient liées par la loi de la distributivité:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

pour chaque $x, y, z \in K$.

La convention est que dans une formule $\cdot$ prend une priorité plus élevée que $+$, par exemple

$$x + y \cdot z + t := x + (y \cdot z) + t, \text{ et } x \cdot y + z \cdot t := (x \cdot y) + (z \cdot t).$$

Aussi on supprime souvent le symbole $\cdot$, par exemple

$$xyz + t := x \cdot y \cdot z + t.$$

Ici $x, y, z, t \in K$.

Comme pour chaque groupe additif nk est définie pour chaque entier n et chaque $k \in K$. Mais $\mathbb{Z}$ n'est pas nécessairement un sous-ensemble de K !

Exercice 3.1. Soit $N \geq 1$ un nombre naturel. Définissons

$$K = \mathbb{Q}(\sqrt{N}) := \{a + b\sqrt{N}; a, b \in \mathbb{Q}\} \subset \mathbb{R}.$$

Montrer que K est un corps, avec les opérations $+$ et $\cdot$ induites par celles de $\mathbb{R}$.

Le plus petit corps contient seulement deux éléments et est noté $\mathbb{F}_2$. Les deux éléments sont appelés $\mathbf{0}$ et $\mathbf{1}$ et on a

$$\mathbf{0} = \mathbf{0} + \mathbf{0} = \mathbf{1} + \mathbf{1} = \mathbf{0} \cdot \mathbf{0} = \mathbf{0} \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{0}$$

et

$$\mathbf{1} = \mathbf{0} + \mathbf{1} = \mathbf{1} + \mathbf{0} = \mathbf{1} \cdot \mathbf{1}.$$

Il faut penser de $\mathbf{0}$ comme "pair" et de $\mathbf{1}$ comme "impair", par exemple $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$ est interprété comme "impair fois impair est impair". On calcule "modulo 2". En fait, $\mathbb{F}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ (le montre de deux heures), avec les opérations comme dans le petit cours d'arithmétique.

Il existe aussi un corps de trois éléments $\mathbb{F}_3 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$. Les tableaux des deux opérations internes sont :

$+$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{0}$
$\mathbf{2}$	$\mathbf{2}$	$\mathbf{0}$	$\mathbf{1}$

et

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{2}$	$\mathbf{0}$	$\mathbf{2}$	$\mathbf{1}$

Il y a un sens ici à adopter le symbole "$\mathbf{2}$" parce que $2\mathbf{1} = \mathbf{1} + \mathbf{1} = \mathbf{2}$. Mais $\mathbf{2} + \mathbf{1} = \mathbf{0}$. On calcule "modulo 3" et $\mathbb{F}_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

Il existe un corps de quatre éléments $\mathbb{F}_4 = \{\mathbf{0}, \mathbf{1}, a, b\}$. Les tableaux des opérations internes sont :

$+$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$	b	a
a	a	b	$\mathbf{0}$	$\mathbf{1}$
b	b	a	$\mathbf{1}$	$\mathbf{0}$

et

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	a	b
a	$\mathbf{0}$	a	b	$\mathbf{1}$
b	$\mathbf{0}$	b	$\mathbf{1}$	a

Maintenant il n'y a pas de sens à adopter le symbole $\mathbf{2}$ à la place de a ou b, parce que $2 \cdot \mathbf{1} = \mathbf{1} + \mathbf{1} = \mathbf{0}$, et donc $2 \cdot \mathbf{1}$ n'est pas un nouvel élément. Pour chaque élément x de $\mathbb{F}_4$ on a $2x = x + x = \mathbf{0}$. L'élément a satisfait l'égalité $a^2 + a + 1 = 0$ et après tout on n'a pas vraiment besoin d'un symbole b, parce que $b = a^2 = a + 1$. Maintenant $\mathbb{F}_4 \not\simeq \mathbb{Z}/4\mathbb{Z}$!

Exercice 3.2. Calculer le déterminant des matrices

$$\begin{pmatrix} a & a & \mathbf{1} \\ \mathbf{1} & b & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & a \end{pmatrix}, \quad \begin{pmatrix} a & b & \mathbf{1} \\ \mathbf{1} & b & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & a \end{pmatrix}, \quad \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} \\ x & y & z \\ x^2 & y^2 & z^2 \end{pmatrix}$$

de coefficients dans le corps $\mathbb{F}_4$, pour n'importe quels x, y, z. Et ses inverses?

Exercice 3.3. Vérifier que $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_4$ sont des corps. Trouver un corps de 5 éléments. Essayer de montrer qu'il n'existe pas un corps de 6 éléments. (Indice : On a $6\mathbf{1} = \mathbf{0}$ et soit $2\mathbf{1} \neq \mathbf{0}$ ou $3\mathbf{1} \neq \mathbf{0}$, contradiction.)

En fait, on peut montrer que la cardinalité d'un corps fini est toujours une puissance d'un nombre premier, et il existe essentiellement seulement un corps fini $\mathbb{F}_q$ de la cardinalité $q = p^m$, où p est un nombre premier et m un entier positif. Nous ne montrons pas ces propositions ici (voyez par exemple [4, p.277-8]).

Si K est un corps, on indique le groupe multiplicatif par $K^\times$ (alors l'ensemble est $K\backslash\{\mathbf{0}\}$ et l'opération interne est le produit $\cdot$).

Dès qu'on fixe un corps K, on peut définir la notion d'espace linéaire et application linéaire sur K; des matrices avec coefficients dans K; l'addition et la multiplication matricielle; le déterminant d'une matrice sera un élément de K; le rang; l'inverse; l'existence d'inverse si et seulement si le déterminant n'est pas $\mathbf{0}$; les formes bilinéaires symétriques; le groupe $\mathrm{GL}(n, K)$; le groupe $\mathrm{SL}(n, K)$; le groupe orthogonale $\mathrm{O}(n, K)$; $\mathrm{SO}(n, K)$ et cetera.

Mais la partie de l'algèbre linéaire qui utilise la relation d'ordre $\leq$, comme "un produit scalaire défini positif", ne se généralise pas tout de suite pour tous les corps.

Si le corps est fini, les groupes linéaires sont aussi finis. Par exemple, la cardinalité de $\mathrm{GL}(n, \mathbb{F}_q)$ est $(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})$. (Preuve : On peut choisir q^n-1 vecteurs pour la première colonne, après on peut choisir encore $(q^n - q)$ vecteurs pour la deuxième colonne linéairement indépendant de la première, après on peut choisir $(q^n - q^2)$ vecteurs pour la troisième colonne linéairement indépendant avec les deux premières, etc.)

Exercice 3.4. Soit g un élément de

$$\mathrm{O}(4, \mathbb{F}_2) = \{g \in \mathrm{GL}(4, \mathbb{F}_2);\ g \cdot g^t = 1\}.$$

Montrer qu'il y a deux possibilités. Soit chaque ligne et chaque colonne de g contient un unique coefficient $\mathbf{1}$ (une matrice de permutation), ou chaque ligne et chaque colonne de g contient un unique coefficient $\mathbf{0}$. Est-ce que la même est vraie pour $\mathrm{O}(5, \mathbb{F}_2)$ ou $\mathrm{O}(4, \mathbb{F}_3)$? Montrer que $\mathrm{O}(3, \mathbb{F}_2)$ est isomorphe à S_3.

Exercice 3.5. Pour un corps K nous posons $K[T]$ pour l'ensemble des polynômes en variable T et coefficients dans K. La notion de degré est comme d'habitude (le plus grand exposant de T qui apparaît). Montrer qu'on peut diviser avec reste :

Soient f et g deux polynômes dans $K[T]$, où $g \neq 0$. Alors ils existent deux polynômes q et r dans $K[T]$ tels que

$$f = qg + r$$

et si $r \neq 0$ le degré de r est plus petit que le degré de g.

Exercice 3.6. Comme dans le petit cours d'arithmétique donner une définition du $\mathrm{pgcd}(f, g)$ et montrer qu'ils existent deux polynômes a et b tels que

$$af + bg = \mathrm{pgcd}(f, g).$$

On peut généraliser d'autres propriétés des polynômes de coefficients réels. Comme la factorisation unique (la notion de "nombre premier" est remplacée par "polynôme irréductible"). Et que chaque polynôme de degré n a au plus n solutions dans un corps. Nous donnons une preuve.

Proposition 3.1. *Soit $F(T) = a_0 + a_1T + a_1T^2 + \ldots + a_nT^n$ un polynôme de degré n de coefficients a_i dans un corps K et on suppose que $a_n \neq \mathbf{0}$. Alors F a au plus n racines, c'est à dire, il existe au plus n éléments différents $k \in K$ tels que*

$$F(k) := a_0 + a_1k + a_1k^2 + \ldots + a_nk^n = \mathbf{0}$$

dans K.

Preuve. Par induction sur n. Si $n = 0$, il n'y a aucune racine (parce que $a_0 \neq \mathbf{0}$). Supposons $k \in K$ est une solution. Par la division avec reste (exercice 3.5) il existe un polynôme $G(T)$ de degré $n-1$ et un scalaire $c \in K$, tels que $F(T) = (T-k)G(T) + c$. Donc $c = F(k) = 0$ et $F(T) = (T-k)G(T)$. Soit k' une solution de $F(T) = (T-k)G(T) = \mathbf{0}$, alors $k' - k = \mathbf{0}$ où $G(k') = \mathbf{0}$. Par induction on peut supposer que $G(T) = \mathbf{0}$ a au plus $n-1$ solutions différents dans K, donc $F(T) = \mathbf{0}$ a au plus n solutions différents dans K. □

L'équation $2x = 0$ a une solution dans un corps, mais deux dans $\mathbb{Z}/4\mathbb{Z}$.

Exercice 3.7. Trouver tous les zéros de $F(T) := T^6 + aT^5 + bT^4 + \mathbf{1}$ dans le corps $\mathbb{F}_4$. Et les zéros de $F'(T)$ (le dérivé de F)?

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA