PETIT COURS D'ARITHMÉTIQUE

ABRAHAM BROER

1. Introduction

Nous allons rappeler quelques propriétés élémentaires et bien connues des nombres entiers, rencontrées déjà dans le cours MAT1500. Par exemple, que chaque nombre entier est un produit de nombres premiers, et ce produit est unique à permutation près. Comme point de départ nous prenons l'idée qu'on sait compter !

Les nombres entiers se trouvent vraiment à la base de toutes les mathématiques, leur *existence* est un de ses axiomes même ! On suppose que les nombres entiers existent. Mais après, en acceptant les nombres naturels, on *construit* les nombres entiers négatifs, les fractions, les nombres réels et les nombres complexes.[1] Nous rappelons des définitions des fractions et des nombres réels.

2. Un rappel de définitions

Essayez avant tout de vous rappeler ou de vous imaginer comment les nombres naturels peuvent être caractérisé exactement (peut-être à l'école primaire ?), et puis l'addition et la multiplication.

L'idée est qu'il est possible de compter aussi loin qu'on veut à partir de 1 :

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$$

Les nombres qu'on obtient ainsi sont les nombres naturels. Donc implicitement, chaque nombre naturel a un unique successeur et chaque nombre sauf 1 a un unique nombre naturel comme prédécesseur.

Il existe essentiellement un unique ensemble $\mathbb{N}$ (l'ensemble des nombres naturels) avec un élément spécial noté 1, dont chaque élément a un unique *successeur* et dont chaque élément sauf 1 a un *unique prédécesseur*, et aucun sous-ensemble contenant 1 a la même propriété. En particulier, si $S \subseteq \mathbb{N}$ est un sous-ensemble avec les deux propriétés que $1 \in S$ et que avec $s \in S$ aussi son successeur est dans S, alors on a nécessairement que $S = \mathbb{N}$.

Nous allons accepter l'existence de $\mathbb{N}$. En consqence nous allons aussi accepter le principe d'induction mathématique ! Supposons que $P(n)$ est une préposition logique qui dépend du nombre naturel $n \in \mathbb{N}$. Supposons que $P(1)$ est vraie et que pour chaque $n \in \mathbb{N}$ la préposition $P(n)$ implique $P(n')$, où n' est le successeur de n. Alors, parce que $P(1)$ implique $P(2)$ et $P(1)$ est vraie, on a que $P(2)$ est aussi vraie. Donc $P(3)$ est vraie. Donc $P(4)$ est vraie. Et cetera. Donc $P(n)$ est vraie pour chaque $n \in \mathbb{N}$, parce qu'on peut compter jusqu'à n. De façon analogue pour les *définitions* inductives.

Date: August 31, 2009.

[1] L. Kronecker (1823-1891, un mathématicien allemand) a dit que Dieu a créé les nombres entiers et tout le reste est le travail d'homme. Voir le bouquin très lisible : Eric Temple Bell, Men of Mathematics, New York, Simon and Schuster, 1986. La bibliothèque a une version française.

Pour donner la définition d'addition sur $\mathbb{N}$ correctement, il faut nécessairement utiliser l'induction (c'est à dire : une propriété définissantes de l'ensemble des nombres naturels !).

Soit $n \in \mathbb{N}$ on va définir $n+m \in \mathbb{N}$ par induction sur m. Si $m = 1$ nous *définissons* $n+1$ comme le successeur (unique) de n. Supposons que $n+m$ a été défini. Alors on *définit* :

$$n + (m+1) := (n+m) + 1$$

(c'est à dire, le successeur de $n+m$). Alors par le principe d'induction on a maintenant défini $n+m$ pour chaque $n, m \in \mathbb{N}$.

Nous pouvez voir (comme on pourrait demander un enfant de 7 ans) que

$$a + b = b + a \text{ et } (a+b) + c = a + (b+c) \ :$$

Preuve. Soient $a, b \in \mathbb{N}$. Nous allons montrer par induction sur n que $(a+b)+n = a+(b+n)$. Si $n = 1$, alors $(a+b)+1 = a+(b+1)$ par définition de $+$. Supposons maintenant que $(a+b)+n = a+(b+n)$. Alors

$$\begin{aligned}
(a+b)+(n+1) &= ((a+b)+n)+1 \quad \text{(par définition de } +) \\
&= (a+(b+n))+1 \quad \text{(par hypothèse d'induction)} \\
&= a+((b+n)+1) \quad \text{(par définition de } +) \\
&= a+(b+(n+1)) \quad \text{(par définition de } +).
\end{aligned}$$

Donc par induction nous avons montré la règle d'associativité.

Pour montrer la commutativité, nous commençons par montrer que $a+1 = 1+a$ par induction sur a. Si $a = 1$ on a la tautologie $1+1 = 1+1$. Supposons que $a+1 = 1+a$. Alors

$$(a+1)+1 = (1+a)+1 = 1+(a+1)$$

et on conclut par induction.

Fixons a. Nous allons montrer par induction sur n que $a+n = n+a$. On vient de montrer le cas ou $n = 1$. Supposons maintenant que $a+n = n+a$, alors on a en utilisant l'associativité

$$a+(n+1) = (a+n)+1 = (n+a)+1 = 1+(n+a) = (1+n)+a = (n+1)+a.$$

On conclut par induction. □

Rappelez-vous la définition de "a est plus petit que b", pour des nombres naturels a et b. On a $n < m$ (ou $m > n$) si et seulement si il existe un $a \in \mathbb{N}$ tel que $m = n+a$. Si $n < m$ et $m < k$ alors $n < k$ (pourquoi ?). Pour deux nombres naturels a et b il existe trois alternatives : $a < b$ ou $b < a$ ou $a = b$ (pourquoi ?). On écrit $a \leq b$ si $a = b$ ou si $a < b$.

Exercice 2.1. Montrer que chaque sous-ensemble non-vide S de $\mathbb{N}$ *contient* un *unique* élément qui est plus petit que tous les autres éléments de S.

La définition du produit de deux nombres naturels ? Soit $n, m \in \mathbb{N}$ on définit $n \cdot m \in \mathbb{N}$ par induction sur n. Si $n = 1$ on définit $1 \cdot m := m$. Supposons $n \cdot m$ a été défini. Alors on pose $(n+1) \cdot m := (n \cdot m) + m$.

Pouvez vous voir pourquoi

$$a \cdot b = b \cdot a,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)\ ?$$

Exercice 2.2. Montrer la règle de distributivité:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

pour chaque $a, b, c \in \mathbb{N}$.

Puis, à partir de $\mathbb{N}$ on *construit* par induction l'ensemble des nombres entiers

$$\mathbb{Z} := \{\ldots, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots\}$$

en ajoutant à l'ensemble $\mathbb{N}$ un nombre appelé 0 premièrement (donc 0 n'était pas encore dans $\mathbb{N}$) et puis successivement pour chaque nombre naturel n un nouveau nombre appelé $-n$ (alors $-n$ n'était pas encore dans $\{-(n-1), -(n-2), \ldots, -1, 0, 1, 2, \ldots\}$). On obtiendra une extension unique des opérations $+$ et $\cdot$ tels que

$$n + (-n) = (-n) + n = 0,\ (-1) \cdot n = (-n),\ 0 + n = n + 0 = n,$$

pour chaque $n \in \mathbb{N}$. Les règles d'associativité, de commutativité et de distributivité restent vrai. On pose $-(-n) := n$ et $-0 := 0$, pour $n \in \mathbb{N}$. Et $a - b := a + (-b)$. Si $n \in \mathbb{N}$ on pose $|n| = |(-n)| = n$ et $|0| = 0$. On a $|a||b| = |ab|$ et $|a + b| \leq |a| + |b|$.

3. Division avec reste

En général, on ne peut pas diviser un nombre entier par un autre nombre entier et obtenir un nombre entier. Mais on peut diviser avec reste, comme on a vu dans MAT1500. Par exemple, si on divise 3599 par 112 on aura un reste :

$$3599 = 32 \cdot 112 + 15.$$

Théorème 3.1 (Division avec reste)**.** *Soient $a, b \in \mathbb{Z}$, où $b \neq 0$. Alors il existe deux unique nombres entiers, q, r tel que*

$$a = qb + r \text{ et } 0 \leq r < |b|.$$

Preuve. Premièrement nous allons montrer que si $a \geq 0$ et $b > 0$, alors il existe q et r tels que $a = qb + r$ et $0 \leq r < b$. Nous procédons par induction sur a. Si $a = 0$ alors $a = 0 = 0 \cdot b + 0$. Soit $0 < a$. Supposons par induction qu'il existe q' et r' tels que $a = q'b + r'$ et $0 \leq r' < b$. Il y a deux cas possible. (1) Si $r' + 1 = b$. Alors $a + 1 = q'b + r' + 1 = q'b + b = (q' + 1) \cdot b + 0$. (2) Si $r' + 1 < b$. Alors $a + 1 = q' \cdot b + (r' + 1)$. Donc il existe q et r tels que $a + 1 = qb + r$.

D'une manière analogue on montre le cas où $a \leq 0$ et $b > 0$.

Supposons maintenant $b < 0$. Alors $-b > 0$ et nous venons de montrer qu'ils existent q et r tels que $a = q(-b) + r$ et $0 \leq r < |b|$. Donc $a = (-q)b + r$.

Il reste à montrer l'unicité. Supposons que $a = qb + r$, $a = q'b + r'$, $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors $0 \leq |r - r'| < |b|$ et $|r - r'| = |q' - q| \cdot |b|$. Donc $0 \leq |q' - q| \cdot |b| < |b|$, et $0 \leq |q' - q| < 1$. Donc le nombre entier $|q' - q|$ est 0, d'où $q' = q$. Aussi $r = a - qb = a - q'b = r'$. □

On dit que "b divise a", ou $b|a$, s'il existe $q \in \mathbb{Z}$ tel que $a = qb$ (alors un tel q est unique). Propriétés élémentaires :

$$c|b \wedge\ b|a \Rightarrow c|a$$

$$b|a \wedge\ b|a' \Rightarrow b|(na + ma') \ \forall n, m \in \mathbb{Z}$$

$$\forall b:\ b|0\ \text{ et } \forall a:\ 1|a$$

$$b|a \Leftrightarrow |b| \mid |a|$$

$$b|a \wedge\ (a \neq 0)\ \Rightarrow |b| \leq |a|.$$

4. Le pgcd

Si $(a, b) \neq (0, 0)$, on définit le $\text{pgcd}(a, b)$ comme le plus grand diviseur commun de a et b, ou

$$\text{pgcd}(a, b) := \text{Max}\{d; d|a \wedge d|b\}.$$

Et on définit $\text{pgcd}(0, 0) := 0$. On a $\text{pgcd}(n, 0) = |n|$.

Lemme 4.1. *Soient $a, b, q, r \in \mathbb{Z}, b \neq 0$, tels que $a = qb + r$. Alors*

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

Preuve. Soit $d \in \mathbb{N}$ tel que $d|a$ et $d|b$, donc $d|(a - qb) = r$. Si $d \in \mathbb{N}$ tel que $d|b$ et $d|r$, donc $d|(qb + r) = a$. Donc l'ensemble des diviseurs en commun de a et b est égal à l'ensemble des diviseurs en commun de b et r. Donc par définition $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. □

Le lemme donne une suggestion pour calculer le pgcd itérativement, l'algorithme d'Euclide. Nous donnons seulement un exemple.

$$\begin{aligned}
\text{pgcd}(1057, 315) &= \text{pgcd}(315, 112)\ \ (\text{parce que } 1057 = 3 \cdot 315 + 112) \\
&= \text{pgcd}(112, 91)\ \ (\text{parce que } 315 = 2 \cdot 112 + 91) \\
&= \text{pgcd}(91, 21)\ \ (\text{parce que } 112 = 1 \cdot 91 + 21) \\
&= \text{pgcd}(21, 7)\ \ (\text{parce que } 91 = 4 \cdot 21 + 7) \\
&= \text{pgcd}(7, 0)\ \ (\text{parce que } 21 = 3 \cdot 7 + 0) \\
&= 7
\end{aligned}$$

Théorème 4.1. *Soient $a, b \in \mathbb{Z}$. Alors il existe $x, y \in \mathbb{Z}$ tel que*

$$xa + yb = \text{pgcd}(a, b).$$

Preuve. Nous pouvons supposer que $a \neq 0$, parce que sinon $\text{pgcd}(a, b) = |b| = 0 \cdot a + (\pm 1)b$. Soit $S \subset \mathbb{N}$ le sous-ensemble défini par

$$S := \{n \in \mathbb{N}; \exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}:\ xa + yb = n\}$$

On a $|a| \in S$, donc S n'est pas vide. Soit s le plus petit élément de S, en particulier $s \leq |a|$ et il existe x, y tels que $xa + yb = s$. Soit $m = x'a + y'b \in S$ quelconque. Par division avec reste il existe q, r tels que $m = qs + r$ et $0 \leq r < s$, et

$$r = m - qs = (x'a + y'b) - q(xa + yb) = (x' - qx)a + (y' - qy)b.$$

Si $r > 0$, on aurait $r \in S$ et $r < s$, une contradiction avec le choix de s. Donc $r = 0$ et $s|m$. En particulier, s divise $|a|$ et $|b|$ ($|a| \in S$, et $|b| \in S$, si $b \neq 0$) et alors aussi a et b. Donc s est un diviseur commun de a et b et $s \leq \text{pgcd}(a, b)$.

Par contre, $\text{pgcd}(a, b)$ divise a et b, donc aussi $xa + yb = s$ et nécessairement $\text{pgcd}(a, b) \leq s$. Donc $s = \text{pgcd}(a, b) = xa + yb$. □

On peut aussi donner un algorithme (de Bézout) pour trouver x et y. Un exemple suffit peut-être.

Exemple 4.1. Nous calculons des x et y tels que $x \cdot 1057 + y \cdot 315 = \text{pgcd}(1057, 315)$. On commence par deux équations triviales et puis on utilise division avec reste :

$$\begin{aligned}
1 \cdot 1057 + 0 \cdot 315 &= 1057 \\
0 \cdot 1057 + 1 \cdot 315 &= 315 \\
1 \cdot 1057 + (-3) \cdot 315 &= 112 \quad (\text{parce que } 112 = 1057 - 3 \cdot 315) \\
(-2) \cdot 1057 + (7) \cdot 315 &= 91 \quad (\text{parce que } 91 = 315 - 2 \cdot 112) \\
3 \cdot 1057 + (-10) \cdot 315 &= 21 \quad (\text{parce que } 21 = 112 - 1 \cdot 91) \\
(-14) \cdot 1057 + (47) \cdot 315 &= 7 \quad (\text{parce que } 7 = 91 - 4 \cdot 21)
\end{aligned}$$

Donc $x = -14$ et $y = 47$. Les x et y ne sont pas unique, parce que on a aussi

$$(-14 + 315) \cdot 1057 + (47 - 1057) \cdot 315 = 301 \cdot 1057 - 1010 \cdot 315 = 7.$$

Exercice 4.1. Calculer $\text{pgcd}(987654321, 123456789)$. Trouver a, b tels que $-14a + 47b = \text{pgcd}(14, 47)$.

Corollaire 4.1. *Soient $a, b, d \in \mathbb{Z}$ tels que $d|a$ et $d|b$, alors $d|\text{pgcd}(a, b)$. Si $c = xa + yb$, pour certains $x, y \in \mathbb{Z}$, alors $\text{pgcd}(a, b)|c$.*

Preuve. Le nombre d divise $xa + yb$ pour chaque x, y, donc en particulier divise le $\text{pgcd}(a, b)$ (par le théorème). L'autre préposition est montrée dans la preuve du théorème. □

Un *nombre premier* est un nombre naturel $p > 1$ ayant seulement 1 et p comme diviseurs dans $\mathbb{N}$.

Corollaire 4.2. *Soit p un nombre premier. Si $p|a_1 a_2 \dots a_n$, alors il existe au moins un i tel que $p|a_i$.*

Preuve. Par induction sur n. Si $n = 1$, il n'y a rien à montrer. Supposons que si p divise un produit de moins que n facteurs, alors il divise au moins un des facteurs. Supposons que $p|a_1 a_2 \cdots a_n$ et que p ne divise pas a_n. Alors $\text{pgcd}(p, a_n) = 1$, donc il existe x, y tels que $xp + ya_n = 1$. Donc après multiplier par $(a_1 a_2 \cdots a_{n-1})$ on obtient que

$$(a_1 a_2 \cdots a_{n-1} x)p + y(a_1 a_2 \cdots a_{n-1} a_n) = a_1 a_2 \cdots a_{n-1}$$

est divisible par p, donc par l'hypothèse d'induction p divise l'un des a_i. □

5. Factorisation unique

Théorème 5.1. *Soit $1 < n$. Alors il existe un nombre naturel m et m nombres premiers $p_1, \dots, p_m$ tels que $n = p_1 p_2 \dots p_m$. Le nombre m est unique et les nombres premiers sont uniques à une permutation près des facteurs p_i.*

Preuve. Nous allons montrer l'existence d'une telle décomposition par induction sur n. Si n est premier, par exemple si $p = 2$, on prend $m = 1$ et $p_1 := n$. Sinon, ils existent $a, b \in \mathbb{N}$ tels que $n = ab$, $n > a > 1$, $n > b > 1$. Par l'hypothèse d'induction il existe s, t et décompositions $a = q_1 \cdots q_s$ et $b = r_1 \cdots r_t$, où les q_i et r_j sont premiers. Donc $n = q_1 \cdots q_s r_1 \cdots r_t$ est un produit de $s + t$ nombres premiers.

Maintenant nous montrons l'unicité par induction sur n. Si n est premier, c'est clair. Supposons que n n'est pas premier et

$$n = p_1 \cdots p_m = q_1 \cdots q_s,$$

où les p_i et q_j sont premiers et $m \geq 1, s \geq 1$. p_m divise n et est premier, donc divise un des facteurs q_i. Possiblement après renuméroter on peut supposer que ce facteur est q_s. Mais q_s est aussi premier, donc $p_m = q_s$. Soit n' tel que $n = n' p_m = n' q_s$. Alors

$$n' = p_1 \cdots p_{m-1} = q_1 \cdots q_{s-1},$$

et donc par induction $m - 1 = s - 1$ et (possiblement après renuméroter les $q_1, \dots, q_{s-1}$) on a $p_i = q_i$ pour chaque i. Alors par induction nous avons montré l'unicité. □

Exercice 5.1. Le théorème ne dit pas si le nombre de nombres premiers différents est fini ou non. Montrer qu'il existe un nombre infini de nombres premiers.

6. Relations d'équivalence

Soit X un ensemble. Une *relation* (binaire) sur X est un sous-ensemble $R \subseteq X \times X$ du produit cartésien. On utilisera la notation

$$x \sim y :\iff (x, y) \in R.$$

On dit que c'est une *relation d'équivalence* si les trois propriétés suivantes sont satisfaites :

(1) $x \sim x$ pour chaque $x \in X$ (réflexivité);
(2) $x \sim y$ implique $y \sim x$ (symétrie);
(3) $x \sim y$ et $y \sim z$ implique $x \sim z$ (transitivité).

Si $\sim$ est une relation d'équivalence sur X et $x \in X$ on écrit

$$\mathrm{Cl}(x) := \{y \in X; x \sim y\},$$

la *classe d'équivalence contenant* x. Une *classe d'équivalence* est un sous-ensemble de la forme $\mathrm{Cl}(x)$ pour un $x \in X$.

Proposition 6.1. *Soit $\sim$ une relation d'équivalence sur un ensemble X.*

(i) On a $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ si et seulement si $x \sim y$.
(ii) Supposons Cl et Cl' sont deux classes d'équivalence. Si $\mathrm{Cl} \neq \mathrm{Cl}'$ alors Cl et Cl' sont disjoints.
(ii) X est la réunion disjointe de ses classes d'équivalence.

Preuve. (i) Si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$, alors $x \in \mathrm{Cl}(x) = \mathrm{Cl}(y)$, donc $x \sim y$. Si $x \sim y$ et $z \in \mathrm{Cl}(x)$, alors $z \sim x$ et par la transitivité $z \sim y$, d'où $z \in \mathrm{Cl}(y)$. (ii) et (iii) suivent de (i). □

On écrit $X/\sim$ pour l'ensemble des classes d'équivalence et on a une application

$$\mathrm{Cl} : X \longrightarrow X/\sim : x \mapsto \mathrm{Cl}(x).$$

Faites attention: une classe d'équivalence C peut être vu comme un *élément* de $X/\sim$ ou comme un *sous-ensemble* de X. On a $x \sim y$ si et seulement si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.

6.1. **Les fractions.** Maintenant on va rappeler comment on définit les fractions. Soit

$$X = \{(n, d) \in \mathbb{Z}^2; d \neq 0\},$$

avec la relation d'équivalence

$$(n, d) \sim (n', d') \iff nd' = n'd \text{ (une égalité dans } \mathbb{Z}).$$

Nous vérifions la transitivité. Si $(n, d) \sim (n', d')$ et $(n', d') \sim (n'', d'')$ alors $nd' = n'd$ et $n'd'' = n''d'$. Donc

$$(nd'' - n''d)d' = nd'd'' - n''dd' = nd'd'' - n'dd'' = nd'd'' - nd'd'' = 0,$$

et parce que $d' \neq 0$ il suit que $nd'' = n''d$, d'où $(n, d) \sim (n'', d'')$.

La classe d'équivalence de (n, d) est appelé une *fraction*, et s'écrit comme d'habitude comme $\frac{n}{d}$:

$$\frac{n}{d} := \mathrm{Cl}(n, d).$$

On a $\frac{n}{d} = \frac{n'}{d'}$ si et seulement si $\mathrm{Cl}(n, d) = \mathrm{Cl}(n', d')$ si et seulement si $nd' = n'd$. Maintenant

$$\mathbb{Q} := X/\sim = \{\frac{n}{d}; d \neq 0\}$$

est l'ensemble des fractions.

On définit l'addition et la multiplication sur $\mathbb{Q}$ par

$$\frac{n}{d} \cdot \frac{n'}{d'} := \frac{nn'}{dd'}; \ \frac{n}{d} + \frac{n'}{md'} := \frac{nd' + n'd}{dd'}.$$

Il y a quelque chose à faire encore ! Les formules sont données en termes de représentants de classes d'équivalence; changer les représentants ne change pas les classes, mais change les formules. Vérifions par exemple que l'addition est *bien-définie*. Supposons $\frac{n}{d} = \frac{r}{s}$ et $\frac{n'}{d'} = \frac{r'}{s'}$. Il faut vérifier si

$$\frac{nd' + n'd}{dd'} = \frac{rs' + r's}{ss'},$$

c'est à dire si

$$(nd' + n'd)ss' = (rs' + r's)dd'.$$

On a $ns = rd$ et $n's' = r'd'$ et donc on a en effet

$$(nd' + n'd)ss' = ns \cdot d's' + n's' \cdot ds = rd \cdot d's' + r'd' \cdot ds = (rs' + r's)dd'.$$

On considère $\mathbb{Z}$ comme un sous-ensemble par l'inclusion $\mathbb{Z} \longrightarrow \mathbb{Q}; n \mapsto \frac{n}{1}$. Il y a une extension de l'ordre partiel : soit $\frac{n}{d}$ et $\frac{n'}{d'}$ deux fractions où on peut supposer que $d, d' \in \mathbb{N}$. On écrit

$$\frac{n}{d} \leq \frac{n'}{d'} \iff nd' \leq n'd$$

et $|\frac{n}{d}| := \frac{|n|}{|d|}$.

6.2. **Modulo n.** Pour chaque entier n on a une relation d'équivalence $\equiv (\mathrm{mod}\ n)$ sur $\mathbb{Z}$. On écrit $a \equiv a'(\mathrm{mod}\ n)$ et on dit que a est *congruent à a' modulo n* si $n|(a-a')$, ou si a et a' ont le même reste après division par n :

$$a \equiv a'(\mathrm{mod}\ n) \iff n|(a-a').$$

Pour n fixé, ça donne une relation d'équivalence sur $\mathbb{Z}$, parce que

(1) $a \equiv a(\mathrm{mod}\ n)$ (on a $n|(a-a)$);

(2) $a \equiv a'(\mathrm{mod}\ n) \iff a' \equiv a(\mathrm{mod}\ n)$ (on a $n|(a-a') \iff n|(a'-a)$);

(3) $a \equiv a'(\mathrm{mod}\ n)$ et $a' \equiv a''(\mathrm{mod}\ n) \Rightarrow a \equiv a''(\mathrm{mod}\ n)$, (on a $n|(a-a')$ et $n|(a'-a'') \Rightarrow n|(a-a'')$.)

Écrivons $\overline{a} = \mathrm{Cl}(a)$ pour la classe d'équivalence de a pour l'équivalence $\equiv (\mathrm{mod}\ n)$, donc

$$\overline{a} := \{m \in \mathbb{Z};\ m \equiv a(\mathrm{mod}\ n)\} = \{a + mn;\ m \in \mathbb{Z}\}.$$

Donc $\overline{a} = \overline{a'}$ si et seulement si $a \equiv a'(\mathrm{mod}\ b)$.

On écrit $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv (\mathrm{mod}\ n)$ pour l'ensemble des classes d'équivalence pour $\equiv (\mathrm{mod}\ n)$.

Addition et multiplication respectent la relation d'équivalence modulo n

$$\overline{a} + \overline{a'} := \overline{a+a'}; \overline{a} \cdot \overline{a'} := \overline{aa'}.$$

Exercice 6.1. (i) Montrer que $+$ et $\cdot$ sont bien définies et que les règles de commutativité, transitivité et distributivité sont satisfaites.

(ii) Montrer que si $n \neq 0$, alors $\mathbb{Z}/n\mathbb{Z}$ est d'ordre fini $|n|$.

Preuve. Par exemple la règle de distributivité

$$\begin{aligned}
\overline{a_1} \cdot (\overline{a_2} + \overline{a_3}) &= \overline{a_1} \cdot \overline{(a_2 + a_3)} \ \text{(par la définition de } +) \\
&= \overline{a_1 \cdot (a_2 + a_3)} \ \text{(par la définition de } \cdot) \\
&= \overline{a_1 a_2 + a_1 a_3} \ \text{(par la distributivité dans } \mathbb{Z}) \\
&= \overline{a_1 a_2} + \overline{a_1 a_3} \ \text{(par la définition de } +) \\
&= \overline{a_1} \cdot \overline{a_2} + \overline{a_1} \cdot \overline{a_3} \ \text{(par la définition de } \cdot)
\end{aligned}$$

□

Par exemple, si $n = 2$, alors $\mathbb{Z}/2\mathbb{Z}$ a deux éléments $\overline{0}$="Pair" et $\overline{1}$="Impair'. On a

$$\overline{0} + \overline{0} = \overline{0},\ \overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1},\ \overline{1} + \overline{1} = \overline{2} = \overline{0},\ \overline{0} \cdot \overline{0} = \overline{0},\ \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0},\ \overline{1} \cdot \overline{1} = \overline{1}.$$

Proposition 6.2. *a et n sont relativement premier si et seulement si il existe un $x \in \mathbb{Z}$ tel que $\overline{a} \cdot \overline{x} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Preuve. Si $\mathrm{pgcd}(a,n) = 1$ alors il existe x et y tels que $xa + yn = 1$. On a $\overline{n} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, donc $\overline{xa} + \overline{yn} = \overline{xa} = \overline{1}$. Par contre, si $\overline{ax} = \overline{1}$, alors $\overline{ax - 1} = \overline{0}$, donc $ax - 1$ est divisible par n, disons $ax - 1 = -yn$. Alors $ax + yn = 1$, et donc a et n sont relativement premier. □

6.3. **Nombres réels.** (Les deux sous-sections finales ne seront pas utilisées dans le cours Algèbre 1.) On donnera une définition d'un nombre réel (est-ce qu'on a déj donné dans un de vos cours une définition d'un nombre réel, pas basée sur l'intuition géométrique ?) Une suite $(a_i)_{i\in\mathbb{N}}$ où $a_i \in \mathbb{Q}$ est appelé une suite de Cauchy, si pour chaque $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, il existe un $N \in \mathbb{N}$ tel que $|a_i - a_j| \leq \epsilon$ pour chaque $i, j \geq N$. Chaque fraction $a \in \mathbb{Q}$ définit une suite de Cauchy $(a_i)_{i\in\mathbb{N}}$, si on pose $a_i = a$ pour chaque $i \in \mathbb{N}$. Soit X la collection de toutes les suites de Cauchy. On définit une relation d'équivalence sur X, comme $(a_i)_{i\in\mathbb{N}} \sim (a'_i)_{i\in\mathbb{N}}$ si et seulement si pour chaque $\epsilon \in \mathbb{Q}, \epsilon > 0$ il existe un $N \in \mathbb{N}$ tel que pour chaque $i \geq N$ on a $|a_i - a'_i| \leq \epsilon$.

Les classes d'équivalence $X/\sim$ sont appelées "nombres réels" et $\mathbb{R} := X/\sim$. Comment définir la somme et le produit de deux "nombres réels"?

Une autre dfinition courante de nombre réel (pas basée sur l'intuition) est basée sur les coupures de Dedekind.

6.4. **Nombres p-adiques.** Presque la même définition définit un autre genre de nombre, nommé *p-adique*, étrange mais quand-même très utile. Pour chaque nombre premier p, il existe une autre valeur absolue $|x|_p$ sur $\mathbb{Q}$ que celui d'habitude. Soit $\frac{n}{d}$ une fraction. Écrit $n = p^i n'$, où $p \not| n'$, et $d = p^j d'$ où $p \not| d'$. On définit alors

$$|\frac{n}{d}|_p := p^{j-i} \text{ (dans } \mathbb{Q}).$$

Donc un entier est petit pour cette valeur absolue si et seulement si cet entier est divisible par une haute puissance de p.

Une suite $(a_i)_{i\in\mathbb{N}}$ où $a_i \in \mathbb{Q}$ est appelé une suite p-adique de Cauchy, si pour chaque $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, il existe un $N \in \mathbb{N}$ tel que $|a_i - a_j|_p \leq \epsilon$ pour chaque $i, j \geq N$. Chaque fraction $a \in \mathbb{Q}$ définit une suite de Cauchy $(a_i)_{i\in\mathbb{N}}$, si on pose $a_i = a$ pour chaque $i \in \mathbb{N}$. Soit X_p la collection de toutes les suites p-adique de Cauchy. On définit une relation d'équivalence sur X_p, comme $(a_i)_{i\in\mathbb{N}} \sim (a'_i)_{i\in\mathbb{N}}$ si et seulement si pour chaque $\epsilon \in \mathbb{Q}, \epsilon > 0$ il existe un $N \in \mathbb{N}$ tel que pour chaque $i \geq N$ on a $|a_i - a'_i|_p \leq \epsilon$.

Les classes d'équivalence $X_p/\sim$ sont appelées *nombres p-adique* et $\mathbb{Q}_p := X_p/\sim$. Comment définir la somme et le produit de deux nombres p-adique ?

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

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

4. Sous-groupes et théorème de Lagrange

4.1. **Sous-groupes.** Considérons le sous-ensemble de permutations

$$V_4 := \{(1), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$$

de S_4. On voit que V_4 a la propriété remarquable que la composition de deux de ses éléments est encore un élément de V_4. La même chose pour les inverses. Alors $(V_4, \circ)$ est soi-même un groupe et on dit que V_4 est un sous-groupe de S_4. Ce groupe est appelé *le quatre groupe de Klein*[3] (c'est un groupe isomorphe au groupe $(\mathbb{F}_4, +)$).

En général, on dit qu'un groupe $(H, \circ)$ est un *sous-groupe* d'un groupe $(G, *)$ si $H \subseteq G$ et

$$h_1 \circ h_2 = h_1 * h_2$$

pour chaque h_1 et $h_2 \in H$. Ici $h_1 * h_2$ a un sens, parce que $H \subseteq G$. Une autre manière de dire la même chose est que $(H, \circ)$ est un sous-groupe de $(G, *)$ si et seulement si l'application induite par l'inclusion

$$H \subseteq G : \ h \mapsto h$$

est un homomorphisme de groupes.

Presque toujours on adopte les même symboles pour les deux opérations (l'un sur H et l'autre sur G), et on écrit

$$H < G.$$

Par exemple $(\{1, -1\}, \cdot)$ est un sous-groupe de $(\mathbb{Q}^\times, \cdot)$, mais pas un sous-groupe de $(\mathbb{Z}, +)$.

Soit $H < G$ un sous-groupe. A priori on a deux neutres ($\mathbf{1}_H$ et $\mathbf{1}_G$) et a priori chaque $h \in H$ a deux inverses (l'un dans le groupe H et l'autre dans le groupe G). Heureusement, nous pouvons montrer que les deux neutres sont le même élément, et les deux inverses sont égaux aussi. Alors il n'aura pas de confusion de parler du neutre ou de l'inverse d'un h.

Lemme 4.1. *Soit $(H, \circ)$ un sous-groupe de $(G, *)$. Alors les neutres $\mathbf{1}_H$ de H et $\mathbf{1}_G$ de G coïncident. Chaque élément $h \in H$ a un inverse $k \in H$ dans le groupe $(H, \circ)$ et un inverse $y \in G$ dans le groupe $(G, *)$. Ces deux inverses k et y coïncident aussi.*

Preuve. On a $\mathbf{1}_H = \mathbf{1}_H \circ \mathbf{1}_H = \mathbf{1}_H * \mathbf{1}_H$, parce que $H < G$. Soit $x \in G$ l'inverse de $\mathbf{1}_H$ dans le groupe G, alors

$$\mathbf{1}_G = x * \mathbf{1}_H = x * (\mathbf{1}_H * \mathbf{1}_H) = (x * \mathbf{1}_H) * \mathbf{1}_H = \mathbf{1}_G * \mathbf{1}_H = \mathbf{1}_H,$$

parce que $\mathbf{1}_G$ est le neutre de G. Donc les neutres coïncident. Soit $k \in H$ l'inverse de $h \in H$, ça veut dire que $h \circ k = k \circ h = \mathbf{1}_H$. Donc on a aussi que $h * k = k * h = \mathbf{1}_G$ et il suit que k est l'inverse de h dans G.

Pour la preuve on peut aussi utiliser lemme 1.3. □

Supposons H est un sous-ensemble d'un groupe G avec l'opération interne $\circ$. Il est naturel de se demander si H avec la même opération soit un sous-groupe. Pour ça il faut au moins que $H \circ H \subseteq H$, ça veut dire $h_1 \circ h_2 \in H$ pour chaque $h_1, h_2 \in H$. Sinon, $\circ$ n'est pas une opération interne sur H. Si cela est le cas, l'associativité est immédiat et $(H, \circ)$ est alors un demi-groupe. Si

[3]Felix Klein, mathématicien allemand, 1849-1925.

la cardinalité de H est finie et H n'est pas vide, $(H, \circ)$ est automatiquement un groupe, comme sera démontré dans l'exercice suivant.

Exercice 4.1. Supposons $H \subseteq G$ est un sous-ensemble non-vide de cardinalité finie d'un groupe quelconque $(G, \circ)$, tel que $H \circ H \subseteq H$. Alors $(H, \circ)$ est un sous-groupe de $(G, \circ)$.

Mais si la cardinalité de H n'est pas finie, alors $(H, \circ)$ n'est pas nécessairement un sous-groupe si $H \circ H \subseteq H$. Par exemple, si $(G, \circ) = (\mathbb{R}^\times, \cdot)$ est le groupe multiplicatif des nombres réels et H est le sous-ensemble de tous les nombres de valeur absolu plus grand que 1,

$$H = \{x \in \mathbb{R};\ |x| > 1\}.$$

Dans ce cas $H \cdot H \subseteq H$, mais $(H, \cdot)$ n'est pas un groupe. Alors il faut supposer plus.

Proposition 4.1. *Soit H un sous-ensemble d'un groupe $(G, \circ)$. Alors $(H, \circ)$ est un sous-groupe de $(G, \circ)$ si et seulement si H satisfait les trois propriétés suivantes.*

(a) Pour chaque h_1 et h_2 de H on a aussi $h_1 \circ h_2 \in H$.

(b) Le neutre $\mathbf{1}_G$ de G est un élément de H, donc $\mathbf{1}_G \in H$.

(c) Pour chaque $h \in H$, l'inverse de h dans G est aussi dans H, donc $h^{-1} \in H$.

Preuve. Un sous-groupe satisfait les trois propriétés. Supposons que $H \subseteq G$ satisfait les propriétés. Alors $\circ$ définit une opération interne associative sur H, par (a), et parce que $\circ$ est une opération interne associative sur le groupe G. Le neutre $\mathbf{1}_G \in H$ est aussi un neutre pour $(H, \circ)$, parce que $\mathbf{1}_G \circ h = h \circ \mathbf{1}_G = h$ pour chaque $h \in H$ (par (b)). Et par (c) chaque $h^{-1} \in H$ et $h \circ h^{-1} = h^{-1} \circ h = \mathbf{1}_G$, donc chaque élément $h \in H$ a un inverse dans $(H, \circ)$. Donc $(H, \circ)$ est un groupe, et donc un sous-groupe de $(G, \circ)$. □

Exercice 4.2. Énumérer tous les sous-groupes de S_3 et D_4 (les symétries d'un carré, ex. 1.7).

Exemples 4.1. Soit K un corps. L'ensemble de toutes les matrices $n \times n$ de coefficients dans K, inversibles et triangulaires supérieures est noté $B(n, K)$. On dénote l'ensemble des matrices diagonales inversibles par $T(n, K)$, et l'ensemble des matrices triangulaires supérieures et unitaires (la seule valeur propre est $\mathbf{1} \in K$) par $U(n, K)$. Alors

$$T(n, K) < B(n, K) < \mathrm{GL}(n, K),\ U(n, K) < B(n, K) \text{ et } U(n, K) < \mathrm{SL}(n, K) < \mathrm{GL}(n, K).$$

Parfois on dit que $T(n, K)$ est le *sous-groupe (standard) de Cartan*[4] et $B(n, K)$ le *sous-groupe (standard) de Borel*[5] de $\mathrm{GL}(n, K)$.

L'ensemble $\mathrm{O}(n, K)$ de toutes les matrices X de dimension $n \times n$ à coefficients dans K telles que $X \cdot X^t = \mathbf{1}$ est un sous-groupe de $\mathrm{GL}(n, K)$, appelé le *groupe orthogonal*.

L'ensemble $\mathbf{U}(n)$ de toutes les matrices complexes X de dimension $n \times n$ telles que $X \cdot \overline{X}^t = \mathbf{1}$ est un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$, appelé le *groupe unitaire*. Ici, $\overline{X}$ est la matrice conjuguée complexe, ça veut dire $(\overline{X})_{ij} = \overline{X_{ij}}$.

Il existe aussi un critère un peu plus court.

[4] Élie Cartan, mathématicien français, 1869-1951.

[5] Armand Borel, mathématicien suisse, 1923-2003.

Exercice 4.3. Soit H un sous-ensemble d'un groupe $(G, \circ)$. Alors $(H, \circ)$ est un sous-groupe de $(G, \circ)$ si et seulement si H a les deux propriétés suivantes.

(a) $H \neq \emptyset$ (H n'est pas vide)

(b) Si $x, y \in H$ aussi $x \circ y^{-1} \in H$.

Un autre critère utile est que $H \subseteq G$ est un sous-groupe si et seulement si H est l'image d'un homomorphisme dans G. Ça suit de la proposition suivante.

Proposition 4.2. *L'image* $\operatorname{Im}\phi$ *d'un homomorphisme de groupes* $\phi : K \longrightarrow G$ *est un sous-groupe de* G *et le noyau* $\operatorname{Ker}\phi$ *est un sous-groupe de* K*.*

Un sous-ensemble $H \subseteq G$ *d'un groupe* G *est un sous-groupe de* G si et seulement si *il existe un homomorphisme de groupes* $\phi : K \longrightarrow G$ *telle que* $H = \operatorname{Im}\phi$*.*

Preuve. Nous allons utiliser le critère précédant. Clairement $\operatorname{Im}\phi$ n'est pas vide. Supposons $x, y \in \operatorname{Im}\phi$, alors ils existent $a, b \in K$ tels que $\phi(a) = x$ et $\phi(b) = y$, alors

$$xy^{-1} = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(a \circ b^{-1}) \in \operatorname{Im}\phi.$$

(on a utilisé Lemme 1.3.) Donc $\operatorname{Im}\phi$ est un sous-groupe de G. La preuve que $\operatorname{Ker}\phi < K$ est analogue. La deuxième partie est évidente (n'est-ce pas ?) □

Exercice 4.4. Chaque monomorphisme $\phi : H \longrightarrow G$ induit un isomorphisme entre H et le sous-groupe $\operatorname{Im}\phi$ de G.

Exemples 4.2. L'ensemble de matrices $n \times n$ de permutation est un sous-groupe de $GL(n, \mathbb{R})$, parce que c'est l'image de $L : S_n \longrightarrow \mathrm{GL}(n, \mathbb{R})$.

L'ensemble $\mathrm{SL}(n, K)$ de toutes les matrices de coefficients dans un corps K et de déterminant $\mathbf{1}$ est un sous-groupe de $\mathrm{GL}(n, K)$, parce que c'est le noyau de l'homomorphisme det : $GL(n, K) \longrightarrow K^{\times}$.

Le groupe alterné Alt_n est un sous-groupe de S_n parce que c'est le noyau de l'homomorphisme signe sg.

Exercice 4.5. Montrer que le *centre*

$$Z(G) := \{g \in G;\ \forall x \in G : gx = xg\}$$

est un sous-groupe de G utilisant le morphisme conjugaison $c : G \longrightarrow \operatorname{Aut} G$.

Lemme 4.2. *Soit* G *un groupe. Alors l'intersection d'une famille quelconque de sous-groupes de* G *est aussi un sous-groupe de* G*.*

Preuve. Cette intersection n'est pas vide, parce que $\mathbf{1}_G$ est dans chaque sous-groupe de G. Soient x et y dans l'intersection, donc $xy^{-1} \in H$ pour chaque sous-groupe H de la famille de sous-groupes. Donc xy^{-1} est dans l'intersection. Il suit que l'intersection est un sous-groupe de G. □

Exemples 4.3. En particulier, si $H < G$ et $K < G$ aussi $(H \cap K) < G$. On a aussi que si $H < K$ et $K < G$ alors $H < G$.

Alors $\mathrm{SO}(n, K) := \mathrm{SL}(n, K) \cap \mathrm{O}(n, K)$ est un sous-groupe de $\mathrm{GL}(n, K)$, de $\mathrm{SL}(n, K)$ et de $\mathrm{O}(n, K)$. Et $\mathrm{S}\mathbf{U}(n) := \mathrm{SL}(n, \mathbb{C}) \cap \mathbf{U}(n)$ est un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$, de $\mathrm{SL}(n, \mathbb{C})$ et de $\mathbf{U}(n)$.

Exercice 4.6. Montrer que

$$\mathrm{SO}(2,\mathbb{R}) = \{\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}; \phi \in \mathbb{R}\}$$

et

$$\mathbf{SU}(2) = \{\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix};\ z,w \in \mathbb{C}, |z|^2 + |w|^2 = 1\}.$$

Calculer $\mathbf{SU}(n) \cap U(n,\mathbb{C})$ et $\mathrm{SO}(n,\mathbb{R}) \cap B(n,\mathbb{R})$. Calculer les centres de $\mathrm{GL}(n,\mathbb{C})$, $\mathbf{SU}(n)$, $U(n,\mathbb{C})$, C_n et D_n.

Il existe une manière facile de produire des sous-groupes du groupe orthogonal. Soit $F \subseteq \mathbb{R}^n$, par exemple un cube ou un tétraèdre dans $\mathbb{R}^3$. Alors

$$\{g \in \mathrm{O}(n,\mathbb{R});\ g(F) \subseteq F\}$$

est un sous-groupe de $\mathrm{O}(3,\mathbb{R})$. Ce sont des exemples de groupes de symétries.

4.2. **Sous-groupe engendré par un sous-ensemble.** On peut définir des sous-groupes de G par générateurs. Soit $S \subseteq G$ un sous-ensemble d'un groupe. Le sous-groupe de G *engendré par* S est défini comme étant le plus petit sous-groupe de G contenant S. Plus précisément, c'est l'intersection de tous les sous-groupes $K < G$ contenant S comme sous-ensemble. On écrit $< S >$ pour ce sous-groupe. Les éléments de S sont des *générateurs* de H dans le sens suivant. Chaque élément x de $< S >$ s'écrit comme

$$x = s_1 s_2 \cdots s_n,$$

où $n \in \mathbb{Z}_{\geq 0}$ et s_i ou $s_i^{-1} \in S$ pour chaque i. Le produit vide est par définition le neutre de G.

Preuve. Soit

$$K := \{s_1 s_2 \cdots s_n \in G;\ n \in \mathbb{Z}_{\geq 0} \text{ et } \forall_{1 \leq i \leq n} s_i \text{ ou } s_i^{-1} \in S\}.$$

On a que K est un sous-groupe de G, parce que $\mathbf{1}_G \in K$ (le produit vide), $K \cdot K \subseteq K$ et l'inverse $s_n^{-1} \cdots s_2^{-1} s_1^{-1}$ de $s_1 s_2 \cdots s_n$ est aussi dans K. Évidemment $S \subseteq K$. Soit H un sous-groupe de G contenant S. Alors chaque expression $s_1 s_2 \cdots s_n$ est dans H et donc $K \subseteq H$. Il suit que K est exactement l'intersection de tous les sous-groupes de G contenant S et le plus petit sous-groupe de G contenant S. □

Exemples 4.4. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\{\overline{1}\}$.

Soit $S = \{(1,2),(2,3),(3,4),\ldots,(n-1,n)\} \subset S_n$. Alors $< S >= S_n$, parce que chaque permutation est un produit de 2-cycles de la forme $(i, i+1)$. On a que

$$< \{(12)(34),(13)(24)\} >= V_4$$

dans S_4.

Le sous-ensemble $\{\rho, \sigma\}$ engendre le groupe diédrale D_n de l'exercise 1.6.

Exercice 4.7. Soit S l'ensemble des produits de pairs de 2-cycles (pas nécessairement disjoints) dans S_n. Montrer que $< S >= \mathrm{Alt}_n$. Montrer que Alt_n est aussi le sous-groupe engendré par l'ensemble de tous les 3-cycles.

Exercice 4.8. Soit K un corps. Pour $k \in K$ et $0 \leq i, j \leq n$ soit $E_{ij}(k)$ la matrice $n \times n$ élémentaire définie par $E_{ij}(k)_{rr} := \mathbf{1}$ (si $1 \leq r \leq n$), $E_{ij}(k)_{ij} := k$ et $E_{ij}(k)_{rs} := \mathbf{0}$ si $r \neq s$ et $(r, s) \neq (i, j)$. Montrer que $\mathrm{SL}(n, K)$ est le sous-groupe de $\mathrm{GL}(n, K)$ engendré par toutes les matrices élémentaires $E_{ij}(k)$. (Utiliser l'algorithme de Gauss de l'algèbre linéaire.)

Exercice 4.9. Soit H le sous-groupe de $\mathrm{GL}(2, \mathbb{R})$ engendré par les deux matrices

$$A := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};\ B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

c.-à-d., $H =< A, B >$. Mopntrer que $H = \mathrm{SL}(2, \mathbb{Z})$, la collection des matrices avec coefficients entiers et déterminant 1.

Exercice 4.10. Le sous-groupe engendré par $S \subseteq G$ est abélien si et seulement si $st = ts$ pour chaque $s, t \in S$.

Exemple 4.5. Les sous-groupes de $(\mathbb{Z}, +)$ sont les

$$n\mathbb{Z} := \{nm;\ m \in \mathbb{Z}\}$$

pour $n \in \mathbb{Z}_{\geq 0}$. Par exemple $15\mathbb{Z} \cap 18\mathbb{Z} \cap 10\mathbb{Z} = 90\mathbb{Z}$.

Preuve. Ce sont vraiment des sous-groupes. Soit $H \neq \{0\}$ un sous-groupe. Soit n le plus petit entier positif dans H, et supposons que $n\mathbb{Z} \neq H$, alors il existe un $m \in H$ qui n'est pas divisible par n. Par division avec reste ils existent des entiers r, s tels que $m = sn + r$, où $0 < r < n$. Mais $-sn \in H$ (pourquoi ?), donc $r \in H$ qui est plus petit que n. Contradiction. Donc $n\mathbb{Z} = H$. □

Exercice 4.11. Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{ppcm}(a, b)\mathbb{Z}$ et $< a\mathbb{Z} \cup b\mathbb{Z} >= \mathrm{pgcd}(a, b)\mathbb{Z}$.

Exercice 4.12. Soit $a \in G$, alors le sous-groupe $< a >:=< \{a\} >$ est isomorphe à $(\mathbb{Z}, +)$ si $| < a > | = \infty$ et isomorphe à C_n (le groupe cyclique d'ordre n) si $| < a > | = n < \infty$. Montrer que si $| < a > | = n < \infty$ alors n est le plus petit entier n tel que $a^n = \mathbf{1}$.

4.3. **Sous-groupe dérivé.** Soit G un groupe et soient $x, y \in G$ deux éléments. Le *commutateur* de la paire (x, y) est l'élément

$$[x, y] := xyx^{-1}y^{-1} \in G.$$

Alors $xy = [x, y]yx$ et $[x, y][y, x] = \mathbf{1}$. Soit S l'ensemble de tous les commutateurs

$$S := \{[x, y];\ x, y \in G\}.$$

En général S n'est pas un sous-groupe de G. Le sous-groupe de G engendré par S est dénoté par $[G, G]$ ou G' et appelé le *sous-groupe dérivé* de G.

Puis on peut définir $G'' := (G')'$ (le sous-groupe dérivé du sous-groupe dérivé de G), $G^{(3)} := G'''$ et cetera.

On dit qu'un groupe est *résoluble* si $G^{(n)} = \mathbf{1}$ pour n assez grand.

$$G \supseteq G' \supseteq G'' \supseteq G^{(3)} \supseteq G^{(n)} = \mathbf{1}.$$

Exercice 4.13. Soit K un corps. Montrer que chaque sous-groupe H de $B(n, K)$ est résoluble. Indice : Calculer $B(n, K)'$ et $B(n, K)''$.

On va montrer plus loin que le sous-groupe dérivé est l'intersection des noyaux de tous les homomorphismes de G vers un groupe abélien. On montre déjà

Lemme 4.3. *Pour chaque homomorphisme $\phi : G \longrightarrow A$, où A est abélien on a que $G' \subseteq \operatorname{Ker}\phi$.*

Preuve. On a $\phi([x,y]) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \mathbf{1}_A$, parce que l'opération interne de A est commutative. Donc $S \subseteq \operatorname{Ker}\phi$, impliquant que $G' =< S >\subseteq \operatorname{Ker}\phi$, parce que $\operatorname{Ker}\phi$ est un sous-groupe de G. □

Exercice 4.14. Soit $G = \mathrm{Alt}_4$ et $A = C_3 =< \rho := e^{2\pi i/3} >$. Soit l'application $\phi : G \longrightarrow A$ définie par $\phi(x) = 1$ si $x \in V_4$; et

$$\phi((1,2,3)) = \phi((1,3,4)) = \phi((2,4,3)) = \phi((1,4,2)) = \rho;$$
$$\phi((1,3,2)) = \phi((2,3,4)) = \phi((1,2,4)) = \phi((1,4,3)) = \rho^2.$$

Vérifier que ϕ est un homomorphisme. Conclure que $V_4 \supseteq [\mathrm{Alt}_4, \mathrm{Alt}_4]$.

Maintenant un résultat classique de Galois.

Proposition 4.3. *On a (i) $[S_n, S_n] = \mathrm{Alt}_n$, (ii) $[\mathrm{Alt}_n, \mathrm{Alt}_n] = \{\mathbf{1}\}$ si $1 \leq n \leq 3$; $[\mathrm{Alt}_4, \mathrm{Alt}_4] = V_4$ et $[\mathrm{Alt}_n, \mathrm{Alt}_n] = \mathrm{Alt}_n$ si $n \geq 5$.*

Preuve. Pour (i), on a que $[S_n, S_n] \subseteq \mathrm{Alt}_n$ parce que Alt_n est le noyau d'un homomorphisme vers un group abélien. Si $n = 2$ la proposition est claire, alors on peut supposer que $n \geq 3$. Soient $1 \leq i, j, k \leq n$ trois entiers différents. Alors le trois-cycle $(i,j,k) \in [S_n, S_n]$ est un commutateur, parce que

$$[(i,j),(i,k)] = (i,j) \circ (i,k) \circ (i,j) \circ (i,k) = (i,j,k).$$

Donc le sous-groupe engendré par tous les 3-cycles est contenu dans $[S_n, S_n]$. Mais ce sous-groupe est Alt_n. Donc $\mathrm{Alt}_n < S'_n$, donc (i).

(ii) Pour $n = 3$ c'est clair, parce que Alt_3 est cyclique d'ordre 3 donc abélien.

Pour $n = 4$. On a

$$[(1,2,3),(1,2,4)] = (1,2) \circ (3,4)$$

et de façon analogue pour les deux autres produits disjoints de deux 2-cycles. Donc $V_4 \subseteq [\mathrm{Alt}_4, \mathrm{Alt}_4]$. Dans la dernière exercice on a vu que V_4 est le noyau d'un homomorphisme vers un groupe abélien, d'où l'égalité.

Pour $n \geq 5$ on a

$$(1,2,3) = [(1,2,4),(1,3,5)]$$

et de façon analogue tous les autres 3-cycles sont des commutateurs dans Alt_n. Mais Alt_n est engendré par les 3-cycles, donc $[\mathrm{Alt}_n, \mathrm{Alt}_n] = \mathrm{Alt}_n$. □

Corollaire 4.1. *Alors S_n est résoluble si et seulement si $n \leq 4$.*

Remarque. Les solutions de l'équation quadratique $x^2 + bx + c = 0$ sont données par la formule

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Une telle formule a été trouvée aussi pour les équations de degré trois et quatre dans le 16-ième siècle. Mais pour plusieurs siècles on n'était pas capable de trouver des formules semblables pour

des degrés plus élevés. Premièrement c'étaient Abel[6] et Ruffini qui montraient qu'il n'en existent pas (Abel quand il avait 19 ans, la preuve de Ruffini était douteuse) ! Un peu plus tard Galois[7] montrait aussi que c'est impossible d'en trouver. Il trouvait une relation profonde entre la théorie des équations et la théorie des groupes. Le point clé était que l'équation général de degré n est résoluble par des radicaux si et seulement si S_n est résoluble (donc par le corollaire si et seulement si $n \leq 4$).

Les coefficients du polynôme $x^n + b_1 x^{n-1} + \ldots + b_n$ sont des combinaisons des racines $x_1, x_2, \ldots, x_n$ comme on voit quand on fait l'expansion de $\prod_{i=1}^{n}(x - x_i)$ et on compare les coefficients. Par exemple, $b_n = \prod_{i=1}^{n}(-x_i)$ et $b_1 = \sum_{i=1}^{n}(-x_i)$. Ces combinaisons ne dépendent pas de l'ordre des solutions on a pris, donc sont invariants par toutes les permutations des solutions. Ainsi apparaît le groupe des permutations dans la théorie des équations !

4.4. **Théorème de Cayley.** On peut interpréter chaque groupe comme un sous-groupe de permutations. C'est un résultat classique de Cayley[8].

Proposition 4.4. *Chaque groupe $(G, *)$ est isomorphe à un sous-groupe du groupe symétrique S_G.*

Preuve. A chaque $g \in G$ on associe la bijection $T_g : G \longrightarrow G$ (pas un homomorphisme de groupes !) définie par

$$T_g(x) := g * x$$

pour $x \in G$. On a $T_g \circ T_h = T_{g*h}$, parce que

$$(T_g \circ T_h)(x) = T_g(T_h(x)) = T_g(h * x) = g * (h * x) = (g * h) * x = T_{g*h}(x)$$

pour chaque $x \in G$. L'application inverse de T_g est $T_{g^{-1}}$. Donc l'application

$$T : G \longrightarrow S_G \text{ avec } T(g) := T_g$$

est un homomorphisme de groupes. Pour montrer que T est un monomorphisme il suffit de montrer que le noyau est trivial. Supposons donc que $g \in \operatorname{Ker} T$, alors $T_g = \mathbf{1}$, donc

$$g * x = T_g(x) = \mathbf{1}(x) = x,$$

pour chaque $x \in G$. Donc $g = \mathbf{1}_G$ et le noyau est trivial. Donc T est un monomorphisme et G est isomorphe au sous-groupe

$$\{T_g; g \in G\} < S_G.$$

□

4.5. **Théorème de Lagrange.** Soit $H < G$ un sous-groupe d'un groupe $(G, \circ)$. Pour $g \in G$ on définit le sous-ensemble $g \circ H$, le *translaté à gauche* de H par g, comme

$$g \circ H := \{g \circ h;\ h \in H\},$$

et de façon analogue $H \circ g$, le translaté à droite de H par g. Évidemment $g \circ H = (g \circ h) \circ H$ comme sous-ensembles de G, pour chaque $h \in H$.

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

[7]Évariste Galois, étudiant de l'école normale, 1811-1832.

[8]Arthur Cayley, mathématicien anglais, 1821-1895.

Pour $H < G$ un sous-groupe d'un groupe $(G, \circ)$ on désigne par G/H ("G modulo H") l'ensemble des translatés à gauche de H par les éléments de G. Alors on peut interpréter $g \circ H$ soit comme *sous-ensemble* de G, soit comme *élément* de G/H. Il faut bien comprendre la différence !!

Il y a une application surjective *naturelle*

$$\nu_H : \ G \longrightarrow G/H; \ \nu_H(g) := g \circ H.$$

Bien sûr, ici $g \circ H$ est vu comme un élément de G/H, pas comme un sous-ensemble de G.

Cette application n'est pas un homomorphisme de groupes, par la simple raison qu'on n'a pas défini une opération interne sur l'ensemble G/H. Si $g \circ H$ et $k \circ H$ sont considérés comme sous-ensembles de G, on peut définir un autre sous-ensemble de G :

$$g \circ H \circ k \circ H := \{g \circ h_1 \circ k \circ h_2; \ h_1, h_2 \in H\}.$$

Mais, en général cet ensemble est la réunion de plusieurs translatés à gauche par des éléments de G (montrer ça).

Lemme 4.4. *Soit $H < G$ un sous-groupe d'un groupe $(G, \circ)$. Alors chaque élément de G est contenu dans un seul translaté à gauche de H, et dans un seul translaté à droite. Si deux translatés à gauche de H sont différents alors leur intersection est vide. Il y a une bijection entre H et le translaté $g \circ H$.*

Preuve. Soit $g \in G$, alors $g = g \circ \mathbf{1}_G \in g \circ H$, donc g est contenu dans le translaté $g \circ H$. Supposons que g est aussi contenu dans $x \circ H$ pour $x \in G$. Alors il existe un $h \in H$ tel que $g = x \circ h$, alors $g \circ H = (x \circ h) \circ H = x \circ H$, donc les deux translatés coïncident. La bijection est $h \mapsto g \circ h$ avec l'inverse $x \in g \circ H \mapsto g^{-1} \circ x$. □

Le nombre d'éléments $O(G)$ dans un groupe G s'appelle *l'ordre de G*. *L'ordre* $O(g)$ d'un élément $g \in G$ est l'ordre du sous-groupe engendré par g, ou

$$O(g) := O(< g >).$$

Si $H < G$, le nombre de translatés à gauche de H s'appelle *l'indice de H dans G* et se dénote $(G : H)$ ou $O(G/H)$.

Théorème 4.1 (Théorème de Lagrange)**.** [9] *Soient $H < K$ et $K < G$ des sous-groupes. Alors*

$$(G : H) = (G : K)(K : H).$$

En particulier

$$O(G) = (G : K) \cdot O(K)$$

et si $O(G) < \infty$, alors $O(K)$ est un diviseur de $O(G)$.

Si $g \in G$, alors $O(g)$ est un diviseur de $O(G)$.

Preuve. On a que H est aussi un sous-groupe de G et le groupe G est la réunion disjointe de ses différents translatés à gauche de H, par le lemme précédent. Chaque translaté à gauche gH est en bijection avec H, donc a la même cardinalité que H et on voit que $O(G) = (G : H) \cdot O(H)$.

[9] Joseph Louis Lagrange, mathématicien français, 1736-1813.

Soient xH et yK deux translatés. Si l'intersection n'est pas vide, alors $xH \subseteq yK$ et il y a une bijection entre K/H (les translatés à gauche de H contenus dans K) et les translatés à gauche de H contenus dans yK par l'application $kH \mapsto ykH$. Donc chaque translaté à gauche de K contient $(K : H)$ translatés à gauche de H. Alors $(G : H) = (G : K)(K : H)$.

Les autres affirmations suivent de cette formule. □

Remarque. On pourrait définir un sous-monoïde N d'un monoïde $(M, \circ)$ (d'une façon évidente), et le translaté à gauche $m \circ N$. Mais l'analogue du théorème ne serait plus valide. C'est ça peut-être la plus grande différence entre la théorie des monoïdes et la théorie des groupes !

Exercice 4.15. Soit G un groupe tel que $O(G)$ est un nombre premier p. Alors G est isomorphe à C_p et est engendré par chaque élément qui n'est pas le neutre. C_p est le seul groupe (fini ou non) (à isomorphisme près) ayant seulement deux sous-groupes différents.

Exercice 4.16. Soit G un groupe fini et soit $g \in G$. On a que $O(g)$ est le plus petit nombre entier m tel que $g^m = \mathbf{1}$. Si $g^r = \mathbf{1}$, alors r est divisible par $O(g)$. On a que $g^{O(G)} = \mathbf{1}$. Pour chaque i on a que $O(g^i)$ divise $O(g)$.

Lemme 4.5. *Soit G un groupe et $x, y \in G$ d'ordre fini tels que $xy = yx$. Soit m le plus petit commun multiple de $O(x)$ et $O(y)$; n le plus grand commun diviseur de $O(x)$ et $O(y)$ et $a := m/n$. Alors*

$$a|O(xy) \text{ et } O(xy)|m.$$

En particulier, si $O(x)$ et $O(y)$ sont relativement premiers et $xy = yx$ alors $O(xy) = O(x)O(y)$.

Preuve. Ils existent q et r relativement premiers tels que $O(x) = nq$, $O(y) = nr$. Remarquons que $a = qr$. On a, car x et y commutent,

$$(xy)^m = x^m y^m = x^{nqr} y^{nqr} = \mathbf{1}$$

et donc par l'exercice précédent $O(xy)|m$.

On va montrer que $O((xy)^n) = a$. D'abord $O((xy)^n)$ divise a, car

$$((xy)^n)^a = (xy)^{na} = (xy)^m = \mathbf{1}.$$

Supposons que $O((xy)^n) \neq a$, alors il existe un premier p tel $p|a$ et $O((xy)^n)$ divise même l'entier a/p. On peut supposer que p divise q (sinon on change x et y). Donc p ne divise pas r et il existe un entier q' tel que $q = q'p$. Alors

$$1 = ((xy)^n)^{a/p} = x^{nq'r} y^{nq'r} = x^{nq'r}$$

et il suit que $O(x) = nq$ divise $nq'r$ et donc q divise $q'r$ et $q = q'p$ divise q' (car q et r sont relativement premiers). On trouve une contradiction, donc $O((xy)^n) = a$. Par l'exercice précédent on obtient que $a|O(xy)$. □

Proposition 4.5. *Soit A un groupe abélien fini. Soit m le plus grand ordre d'un élément de A (appelé l'exposant de A). Pour chaque $a \in A$ on a que $O(a)$ divise m.*

Preuve. Choisissons un élément $g \in A$ tel que $O(g) = m$. Soit $a \in A$ et supposons que $O(a)$ ne divise pas m. Alors il existe un nombre premier p tel que la multiplicité de p dans $O(a)$ est plus élevée que dans m, disons $m = p^r m'$, $O(a) = p^s n'$, $s > r$ et p ne divise ni m' ni n'. Posons $x = g^{p^r}$ et $y = a^{n'}$, alors $O(x) = m'$ et $O(y) = p^s$. Par le lemme précédent on aura $O(xy) = m'p^s > m'p^r = m$. Une contradiction. Alors $O(a)$ divise m après tout. □

Nous utilisons la proposition pour montrer que chaque sous-groupe fini du groupe multiplicatif d'un corps est nécessairement cyclique.

Proposition 4.6. *Chaque sous-groupe fini H du groupe multiplicatif $K^\times$ d'un corps K est cyclique, alors il existe un élément $h \in H$ tel que $H =< h >$. Donc pour chaque élément k de H il existe un $n \in \mathbb{Z}_{\geq 0}$ tel que $k = h^n$*

Preuve. Soit $m \leq O(H)$ le plus grand ordre d'un élément de H. Alors par l'exercice précédent l'ordre de chacun des éléments de H est un diviseur de m. Donc chaque $h \in H$ est une solution de l'équation $T^m - \mathbf{1} = \mathbf{0}$, alors cette équation de degré m a au moins $O(H)$ solutions. Mais par Proposition 3.1 une équation de degré m a au maximum m solutions dans K. On conclut que $m = O(H)$. Ça veut dire qu'il existe un élément $k \in H$ d'ordre $O(H)$, alors $H =< k >$ est isomorphe au groupe cyclique d'ordre $O(H)$. □

Exercice 4.17. Soit n un nombre naturel, alors $\mathbb{Z}/n\mathbb{Z}$ est un monoïde avec la multiplication dfinie dans le petit cours arithmétique. Posons $(\mathbb{Z}/n\mathbb{Z})^\times$ pour le groupe des classes inversibles. Si $\phi(n)$ dénote le nombre des entiers entre 0 et n qui sont relativement premiers avec n, montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ a $\phi(n)$ éléments. Par le théorème de Lagrange on a donc que $m^{\phi(n)} = 1$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Montrer maintenant :

Théorème 4.2 (Fermat-Euler)**.** [10] *Pour chaque pair de nombres entiers relativement premiers n et m on a que le reste de $m^{\phi(n)}$ après division par n est* 1*.*

En particulier, soit $n = 1000000$. On a que $m > 0$ est relativement premier avec n si et seulement si son dernier chiffre est $1, 3, 7$ ou 9, donc $\phi(n) = 400000$. Le théorème dit dans ce cas que si $m > 0$ a comme dernier chiffre $1, 3, 7$ or 9, alors les six derniers chiffres de $m^{400000} - 1$ sont tous 0.

Exercice 4.18. Soit p un nombre premier. Montrer que $(\mathbb{Z}/p\mathbb{Z}^\times, .)$ est un groupe cyclique d'ordre $p - 1$. Donc il existe un nombre m tel que pour chaque $0 < r < p$ il existe un exposant a tel que le reste de m^a par division par p est r. (Indice : $(\mathbb{Z}/p\mathbb{Z}, +, .)$ est un corps.)

4.6. **Le groupe** $(\mathbb{Z}/p^n\mathbb{Z})^\times$**.** [11] Soit p un nombre premier. Si $n \geq 2$, alors $\mathbb{Z}/p^n\mathbb{Z}$ n'est plus un corps et on ne peut plus conclure que le groupe multiplicatif $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique. En effet le groupe

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

n'est pas cyclique. Mais

$$(\mathbb{Z}/9\mathbb{Z})^\times =< \overline{2} >= \{\overline{2}^0 = \overline{1},\ \overline{2}^1 = \overline{2},\ \overline{2}^2 = \overline{4},\ \overline{2}^3 = \overline{8},\ \overline{2}^4 = \overline{7},\ \overline{2}^5 = \overline{5}\}.$$

[10] Pierre de Fermat, avocat et conseiller municipal français et mathématicien amateur, 1601-1665. Leonhard Euler, mathématicien suisse, 1707-1783.

[11] **Pas de matière examen !**

Proposition 4.7. *(i) Soit p un nombre premier impair et $k \geq 1$. Alors le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $p^k - p^{k-1}$.*

En plus, si la classe de $b \in \mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^2\mathbb{Z})^\times$, alors sa classe modulo p^k est aussi un générateur de $(\mathbb{Z}/p^k\mathbb{Z})^\times$ pour chaque $k \geq 2$.

(ii) Le groupe $(\mathbb{Z}/2^k\mathbb{Z})^\times$ d'ordre 2^{k-1} est engendré par les classes de -1 (d'ordre 2) et de 5 (d'ordre 2^{k-2}). Ici $k \geq 3$.

On ne donne pas la preuve ici.

Remarque. En utilisant ces résultats on montre que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si n n'est pas divisible par 8, et engendré par exactement deux générateurs si n est un 8-multiple.

Ce sont des faits utilisés dans la théorie des nombres.

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

5. Les théorèmes d'isomorphisme

5.1. **Sous-groupes normaux.** Dans le petit cours d'arithmétique nous avons défini une opération interne + sur $\mathbb{Z}/n\mathbb{Z}$ par la formule

$$\overline{a} + \overline{b} := \overline{a+b}$$

ou la même formule avec une autre notation

$$(a + n\mathbb{Z}) \ + \ (b + n\mathbb{Z}) := (a + b + n\mathbb{Z}).$$

Avec cette opération $\mathbb{Z}/n\mathbb{Z}$ est un groupe et l'application naturelle $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto \overline{a}$ est un homomorphisme de groupes.

Est-ce que nous pouvons généraliser ça ? Pour un sous-groupe $H < G$ nous venons de définir l'ensemble des translatés G/H et l'application naturelle

$$\nu_H : G \longrightarrow G/H : \nu_H(g) := g \circ H.$$

Si on met $\overline{g} := g \circ H$ pour la classe de g, il est naturel de poser la question si la formule

$$\overline{g_1} \bullet \overline{g_2} := \overline{g_1 \circ g_2} \tag{1}$$

définit une opération interne sur l'ensemble G/H, et que G/H devient un groupe avec $\bullet$. Et en plus, si $\nu_H : G \longrightarrow G/H$ est un homomorphisme dans ce cas.

La réponse est oui dans le cas où G est abélien, mais non en général.

Exercice 5.1. Montrer que si G est abélien et $H < G$, alors la formule (1) définit une opération interne *bien définie* sur G/H. Montrer que G/H avec cette opération est un groupe abélien.

Aussi l'exercice suivant donne une réponse partielle.

Exercice 5.2. Soit $f : G \longrightarrow K$ un homomorphisme avec noyau $N < G$ et image $F < K$. Montrer que le translaté $g \circ N$ est exactement le sous-ensemble de G des éléments qui ont la même image que g :

$$g \circ N = \{x \in G; f(x) = f(g)\},$$

et qu'il y a donc une bijection naturelle entre G/N et F. Une conclusion est que dans le cas de l'exercice on peut au moins identifier G/N avec un groupe.

Mais pour un sous-groupe général $H < G$, la formule (1) ne donne pas une opération interne sur l'ensemble G/H. Un translaté $g \circ H$ est déterminé par un $g \in G$, mais le représentant g n'est pas déterminé par le translaté $g \circ H$.

Exercice 5.3. Soit $H < G$ et posons $\overline{g} := g \circ H$ pour le translaté de g. Montrer que $\overline{g_1} = \overline{g_2}$ si et seulement si il existe un $h \in H$ tel que $g_1 = g_2 \circ h$.

Pour un exemple où la formule n'est pas bien définie, considérons $H := \{(1), (1,2)\} < S_3$. Alors $\overline{(1,3)} = \overline{(1,3) \circ (1,2)} = \overline{(1,2,3)}$. Si la formule (1) était bien définie on aurait

$$\overline{(1,3)} \bullet \overline{(2,3)} = \overline{(1,2,3)} \bullet \overline{(2,3)},$$

ou $\overline{(1,3) \circ (2,3)} = \overline{(1,2,3) \circ (2,3)}$, ou $\overline{(1,3,2)} = \overline{(1,2)}$, ou il existerait un $h \in H$ tel que $(1,3,2) \circ h = (1,2)$. Ce qui n'est pas le cas : une contradiction !

Nous allons approcher la formule d'une autre côté. Pour deux sous-ensembles X et Y d'un groupe $(G, \circ)$ on définit leur produit comme étant

$$X \circ Y := \{x \circ y; x \in X, y \in Y\} \subseteq G.$$

Comme d'habitude si l'opération est $+$ on définit la somme

$$X + Y := \{x + y;\ x \in X, y \in Y\}.$$

Par exemple, la somme de deux translatés $a + n\mathbb{Z}$ et $b + n\mathbb{Z}$ dans $\mathbb{Z}$ est un seul translaté $a + b + n\mathbb{Z}$. Le produit dans un groupe G de deux translatés à gauche (vus comme sous-ensembles de G) est la réunion de plusieurs translatés à gauches, mais en général plus que seulement un (montrer ça). On a évidemment l'inclusion

$$(g_1 \circ g_2) \circ H \subseteq g_1 \circ H \circ g_2 \circ H \tag{2}$$

mais l'inclusion peut être stricte. Pour un exemple, considérons $G := S_3$, $H := \{(1), (1,2)\}$, $g_1 := (1,3)$ et $g_2 := (2,3)$. Alors

$$(g_1 \circ g_2) \circ H = \{(1,3,2), (2,3)\}$$

et

$$g_1 \circ H \circ g_2 \circ H = \{(1), (1,2), (2,3), (1,3,2)\} = H \ \cup \ (g_1 \circ g_2 \circ H)$$

sont strictement différents.

Exercice 5.4. Montrer que la formule (1) donne une opération bien-définie sur G/H si et seulement si on a toujours l'égalité dans l'équation (2).

Quand pour un sous-groupe $H < G$ le produit de deux translatés (comme sous-ensembles de G) est toujours un seul translaté, alors l'opération (1) est bien définie dans G/H. On montrera facilement que G/H avec cette opération forme un groupe et la règle des homomorphismes serait satisfaite

$$\nu_H(g) \bullet \nu_H(k) = \nu_H(g \circ k).$$

Abstraitement, soient x et y deux éléments de G/H et $X \subset G$ et $Y \subset G$ les deux translatés de H correspondants. On multiplie X et Y comme sous-ensembles de G et par l'hypothèse $X \circ Y$ est un translaté Z qui correspond à un élément $z \in G/H$. Alors par définition $x \bullet y := z$. Nous n'avons pas choisi des représentants des translatés, donc la définition est bien cette fois.

On verra dans le théorème suivant que le sous-groupe H a cette propriété agréable *si et seulement si* H est le noyau d'un certain homomorphisme *si et seulement si* $ghg^{-1} \in H$ pour chaque $g \in G$ et $h \in H$ *si et seulement si* chaque translaté à gauche est simultanément un translaté à droite.

Théorème 5.1. *Soit $H < G$ un sous-groupe d'un groupe $(G, \circ)$. Alors les cinq prépositions suivantes sont équivalentes.*

(i) Pour chaque g et $k \in G$ le sous-ensemble $g \circ H \circ k \circ H$ de G est un seul translaté à gauche de H par un élément de G, ça veut dire $g \circ H \circ k \circ H = (g \circ k) \circ H$ pour chaque $g, k \in G$.

(ii) Il existe une opération interne $*$ sur l'ensemble G/H, pour laquelle $(G/H, *)$ est un groupe et pour laquelle l'application naturelle $\nu_H : G \longrightarrow G/H$ est un épimorphisme.

(iii) Il existe un groupe K et un homomorphisme $\phi : G \longrightarrow K$ tel que $H = \mathrm{Ker}(\phi)$.

(iv) On a $g \circ h \circ g^{-1} \in H$ pour chaque $g \in G$ et pour chaque $h \in H$.

(v) Chaque translaté à gauche de H par un élément de G est égal comme sous-ensemble de G à un translaté à droite de H par un élément de G, ça veut dire pour chaque $g \in G$ on a

$$g \circ H = H \circ g$$

comme sous-ensembles de G.

Preuve. Supposons (i) est vrai. Plus haut nous avons défini une opération interne bien-définie (par l'hypothèse) $\bullet$ sur l'ensemble de translatés à gauche G/H. On montre maintenant que $(G/H, \bullet)$ est un groupe.

L'associativité : soient $g_1 \circ H$, $g_2 \circ H$ et $g_3 \circ H$ trois translatés à gauche. Alors dans G/H on a

$$(g_1 \circ H \bullet g_2 \circ H) \bullet g_3 \circ H = (g_1 \circ g_2) \circ H \bullet g_3 \circ H = ((g_1 \circ g_2) \circ g_3) \circ H =$$

$$= (g_1 \circ (g_2) \circ g_3)) \circ H = g_1 \circ H \bullet (g_2 \circ H \bullet g_3 \circ H).$$

L'existence du neutre : $\mathbf{1}_G \circ H = H$ est un neutre pour $\bullet$, parce que

$$\mathbf{1}_G \circ H \bullet g \circ H = (\mathbf{1}_G \circ g) \circ H = g \circ H = (g \circ \mathbf{1}_G) \circ H = g \circ H \bullet \mathbf{1}_H \circ H$$

pour chaque $g \circ H \in G/H$.

L'existence des inverses : l'inverse $(g \circ H)^{-1}$ de $g \circ H \in G/H$ est $g^{-1} \circ H$, parce que

$$g \circ H \bullet g^{-1} \circ H = (g \circ g^{-1}) \circ H = \mathbf{1}_G \circ H = (g^{-1} \circ g) \circ H = g^{-1} \circ H \bullet g \circ H.$$

Donc $(G/H, \bullet)$ est un groupe. On a déjà vu que ν_H est surjective et que $\nu_H(g) \bullet \nu_H(k) = \nu_H(g \circ k)$, alors l'application naturelle est un épimorphisme. Alors (i) implique (ii).

Supposons (ii) est vrai. Le noyau de ν_H est

$$\{g \in G |\ \nu_H(g) = \mathbf{1}_{G/H} = \nu_H(\mathbf{1})\} = \{g \in G |\ g \circ H = H\} = H.$$

On peut prendre $(G/H, *)$ pour le groupe K et ν_H pour l'homomorphisme ϕ. Alors (ii) implique (iii).

Supposons (iii) est vrai, et que H est le noyau de ϕ, où $\phi : G \longrightarrow K$ est un homomorphisme entre les groupes $(G, \circ)$ et $(K, *)$. Pour $h \in H$ et $g \in G$ on a

$$\phi(g \circ h \circ g^{-1}) = \phi(g) * \phi(h) * \phi(g^{-1}) = \phi(g) * \mathbf{1}_K * \phi(g^{-1}) = \phi(g) * \phi(g^{-1}) = \mathbf{1}_H.$$

Donc $g \circ h \circ g^{-1} \in \operatorname{Ker} \phi = H$. Alors (iii) implique (iv).

Supposons que (iv) est vrai. Soit $g \in G$. Pour chaque $h \in H$ on a $g \circ h = (g \circ h \circ g^{-1}) \circ g \in H \circ g$. Donc $g \circ H \subseteq H \circ g$ et de façon analogue $H \circ g \subseteq g \circ H$. Alors (iv) implique (v).

Supposons que (v) est vrai. On calcule

$$g \circ H \circ k \circ H = g \circ k \circ H \circ H = (g \circ k) \circ H,$$

parce que $H \circ k = k \circ H$, par hypothèse et $H \circ H = H$, parce que $H < G$. Alors (v) implique (i). □

On dit que $H < G$ est un *sous-groupe normal* de G ou *sous-groupe distingué*, si une des prépositions dans le théorème est vraie pour H (donc si toutes les prépositions sont vraies). On écrit $H \lhd G$. Par abus de notation on prend le même symbole pour les opérations internes de G et G/H. Dans la théorie des nombres, c'est la théorie de $\mathbb{Z}$, il est absolument nécessaire d'aussi considérer les groupes quotients $\mathbb{Z}/n\mathbb{Z}$. Dans la théore des groupes il est absolument nécessaire d'aussi considérer les groupes quotients par des sous-groupes normaux. Abstrait, oui, mais cela donne exactement la force de l'algèbre : une grande flexibilité !

Exemple 5.1. (i) $\mathrm{Alt}_n \lhd S_n$, parce que Alt_n est le noyau de l'homomorphism sg et le groupe S_n/Alt_n a deux éléments. Par exemple,

$$(1,2,3)\circ \mathrm{Alt}_7 \ \circ (4,5)\circ \mathrm{Alt}_7 = (1,2,3,4,5,6)\circ \mathrm{Alt}_7 \in S_7/\mathrm{Alt}_7\,.$$

(ii) $\mathrm{SL}(n,K) \lhd \mathrm{GL}(n,K)$, parce que $\mathrm{SL}(n,K)$ est le noyau du déterminant. Nous écrivons

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mathrm{SL}(2,\mathbb{R})$$

pour le translaté à gauche dans le groupe quotient $K := \mathrm{GL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{R})$. Alors le neutre de K est

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

et

$$\overline{\begin{pmatrix} 5 & 10 \\ 13 & 27 \end{pmatrix}}^{-1} = \overline{\begin{pmatrix} \frac{1}{10} & -1 \\ \frac{1}{10} & 1 \end{pmatrix}}.$$

(iii) Soit $H = V_4$ le 4-groupe de Klein vu comme sous-groupe de $G = \mathrm{Alt}_4$. Pour chaque $f \in V_4$, aussi $gfg^{-1} \in V_4$ pour chaque $g \in \mathrm{Alt}_4$ (même pour $f \in S_4$), donc $H \lhd G$. On a $O(G/H) = 3$, donc

$$G/H \simeq C_3.$$

Un générateur est par exemple $\sigma = \overline{(1,2,3)} = (1,2,3)\circ H$, et $G/H = \{\sigma, \sigma^2, \sigma^3 = \mathbf{1}_{G/H}\}$.

Exercice 5.5. Si $H < G$ et $(G:H) = 2$, montrer que $H \lhd G$. Donner un exemple d'un sous-groupe qui n'est pas distingué et d'index 3.

Exercice 5.6. Pour un sous-ensemble $X \subset G$ d'un groupe on définit $X^{-1} = \{x^{-1}; x \in X\}$. Soit $H < G$ un sous-groupe. Alors $H \lhd G$ *si et seulement si* pour chaque translaté à gauche $g \circ H$ on a $(g\circ H)^{-1} = g^{-1}\circ H$.

Exercice 5.7. Montrer que $U(n,K) \lhd B(n,K)$ mais $U(n,K)$ n'est pas normal dans $\mathrm{GL}(n,K)$. Ici $n > 1$ et K un corps. Montrer que $C_n \lhd D_n$. Déterminer les sous-groupes normaux de S_3.

Exercice 5.8. Soit H un sous-groupe du centre de G. (i) Montrer que $H \lhd G$. (ii) Supposons que G/H est cyclique (ça veut dire que G/H est engendré par un seul élément). Montrer que G est abélien.

Exercice 5.9. Soit S un sous-ensemble de G, tel que $gsg^{-1} \in S$ pour chaque $s \in S$ et $g \in G$. Montrer que $< S > \lhd G$. Montrer que $V_4 \lhd S_4$ et $G' \lhd G$.

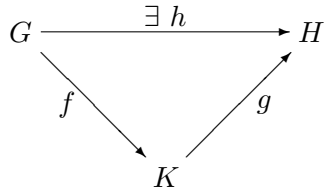
Exercice 5.10. Montrer que l'intersection d'une famille quelconque de sous-groupes normaux est un sous-groupe normal.

Exercice 5.11. Soit $H < G$ un sous-groupe caractéristique, c-à-d pour chaque automorphisme $\phi \in \mathrm{Aut}(G)$ on a $\phi(H) = H$. Montrer que $H \lhd G$. Montrer que le centre et le sous-groupe dérivé sont des sous-groupes caractéristiques.

Exercice 5.12. Soit $N \lhd G$ un sous-groupe normal. Pour $x \in G$ écrit $\overline{x} \in G/N$ pour le translaté qui contient x. Montrer que $O(\overline{x})$ est le plus petit entier positif n tel que $x^n \in N$. Si $O(N) = 46$ et $O(G) = 230$ montrer que pour chaque $x \in G$ on a que $x^5 \in N$.

5.2. **Le théorème fondamental des homomorphismes.** L'idée de fonction (ou d'application) en mathématiques n'a pas toujours été là : c'est difficile à imaginer maintenant qu'on a dû inventer ce concept à la fin du 17ième siècle. Aussi la réalisation qu'on devrait systématiquement étudier les homomorphismes entres les groupes est d'une date relativement récente, surtout popularisé par Nicolas Bourbaki[12] il y a seulement 50 ans, sous l'influence de Emmy Noether[13]. Dans les sections qui suivent nous allons donner les théorèmes de base sur des homomorphismes. Dans les autres sujets d'algèbre (espaces vectoriels, anneaux, modules, et cetera) on a des théorèmes semblables. Une fois qu'on comprend ces théorèmes pour la théorie des groupes, les théorèmes dans les autres sujets algébriques seront facile à comprendre. Le but est simple: on veut "factoriser" les homomorphismes dans des morceaux plus simples; un peu comme on factorise un entier comme produit de nombres premiers, ou une matrice inversible comme produit de matrices élémentaires.

En composant deux morphismes $f : G \longrightarrow K$ et $g : K \longrightarrow H$ on obtient un autre homomorphisme $h = g \circ f : G \longrightarrow H$:



Des informations sur f ou g donnent des informations sur h, et vice versa. Un exemple est donné par l'exercice suivant.

Exercice 5.13. On a

(i) $\mathrm{Im}\, h \subseteq \mathrm{Im}\, g$, donc si h est un épimorphisme, alors g est aussi un épimorphisme.

(ii) $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$, donc si h est un monomorphisme, alors f est aussi un monomorphisme.

Factoriser un homomorphisme $h : G \longrightarrow H$ comme $h = g \circ f$ peut être très utile pour la compréhension de h.

Exercice 5.14. Supposons $O(G) = 60$, $O(H) = 12$. Supposons qu'on peut factoriser l'homomorphisme $h : G \longrightarrow H$ comme $h = g \circ f$, où $f : G \longrightarrow K$ et $g : K \longrightarrow H$ et $O(K) = 35$. Montrer que $h(g) = \mathbf{1}_H$ pour chaque $g \in G$.

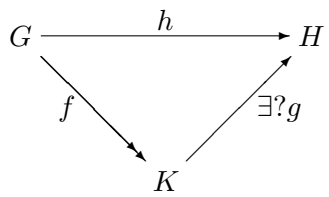
---

[12]Nicolas Bourbaki, le pseudonyme d'un groupe de mathématiciens, voir en.wikipedia.org/wiki/Bourbaki

[13]Emmy Noether, mathématicienne allemande, 1882 - 1935, "la mère de l'algèbre abstraite", voir en.wikipedia.org/wiki/Noether

Pour factoriser un homomorphisme le théorème suivant est fondamental.

Théorème 5.2 (Théorème fondamental des homomorphismes)**.** *Soit $h: G \longrightarrow H$ un homomorphisme et soit $f: G \longrightarrow K$ un épimorphisme.*



(i) Il existe un homomorphisme $g: K \longrightarrow H$ tel que $g \circ f = h$ si et seulement si

$$\ker f \subseteq \ker h.$$

(ii) Il existe au maximum un seul tel homomorphisme g.
(iii) On a $\mathrm{Im}(g) = \mathrm{Im}(h)$, donc g est un épimorphisme si et seulement si h est un épimorphisme.
(iv) On a $f(\mathrm{Ker}(h)) = \mathrm{Ker}(g)$, donc g est un monomorphisme si et seulement si

$$\mathrm{Ker}(f) = \mathrm{Ker}(h).$$

Preuve. (i) Si g existe, un exercice plus haut donne que $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$. Supposons maintenant que $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$. Nous définissons une application $g: K \longrightarrow H$. Soit $y \in K$. Il existe un $x \in G$ tel que $y = f(x)$ (parce que f est un épimorphisme). Alors on définit

$$g(y) := h(x).$$

Cette définition semble dépendre du choix de la pré-image x de y, il faut donc qu'on montre que g soit bien-définie. Si x' est une autre pré-image, $x'x^{-1} \in \mathrm{Ker}(f)$, parce que $f(x'x^{-1}) = f(x')f(x)^{-1} = yy^{-1} = \mathbf{1}_K$. Donc il existe un $z \in \mathrm{Ker}(f)$ tel que $x' = xz$. Par hypothèse $z \in \mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$, donc $h(z) = \mathbf{1}_H$ et

$$h(x') = h(xz) = h(x)h(z) = h(x).$$

Il suit que à cause de $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$ l'application g est bien définie.

Soient $y_1, y_2 \in K$. Il existent $x_1, x_2 \in G$ tels que $f(x_1) = y_1$, $f(x_2) = y_2$ et $f(x_1x_2) = y_1y_2$. Donc

$$g(y_1y_2) = h(x_1x_2) = h(x_1)h(x_2) = g(y_1)g(y_2).$$

Alors g est un homomorphisme tel que $h = g \circ f$.

(ii) Supposons on a aussi $h = g' \circ f$. Si $f(x) = y$, alors

$$g'(y) = g'(f(x)) = h(x) = g(y).$$

Donc $g' = g$.

(iii) est montré dans l'exercice plus haut.

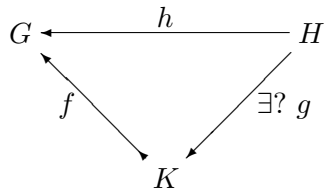
(iv) Soit $y \in \mathrm{Ker}\, g$ et $x \in G$ tel que $f(x) = y$. Alors par définition de g on a $g(y) = h(x) = \mathbf{1}_H$. Donc $x \in \mathrm{Ker}(h)$ et $\mathrm{Ker}(g) \subseteq f(\mathrm{Ker}(h))$. Si $y = f(x)$ où $x \in \mathrm{Ker}\, h$, alors $g(y) = h(x) = \mathbf{1}_G$ et $x \in \mathrm{Ker}\, h$, donc $y \in \mathrm{Ker}(g)$, ou $\mathrm{Ker}(g) \supseteq f(\mathrm{Ker}(h))$. □

Exercice 5.15. (i) Donner un exemple de deux homomorphismes $h : G \longrightarrow H$ et $f : G \longrightarrow K$ tels qu'il y a au moins deux homomorphismes différents $g_i : K \longrightarrow H$ tels que $h = g_i \circ f$ $(i = 1, 2)$.

(ii) Donner un exemple de deux homomorphismes $h : G \longrightarrow H$ et $f : G \longrightarrow K$ tels que $\ker f \subseteq \ker h$ mais qu'il n'y a pas d'homomorphismes $g : K \longrightarrow H$ tel que $h = g \circ f$.

Supposons on a un théorème sur une certaine classe d'homomorphismes, comme le théorème fondamental. Si on change les directions des flèches, monomorphismes par épimorphismes, Ker par Im, on trouve parfois un autre théorème. Mais la preuve peut être beaucoup plus facile (ou plus dure).

Exercice 5.16. Soit $h : H \longrightarrow G$ un homomorphisme et soit $f : K \longrightarrow G$ un monomorphisme.



(i) Il existe un homomorphisme $g : H \longrightarrow K$ tel que $f \circ g = h$ *si et seulement si*

$$\operatorname{Im} f \supset \operatorname{Im} h.$$

(ii) Il existe au maximum un seul tel homomorphisme g.

(iii) On a $\operatorname{Ker}(g) = \operatorname{Ker}(h)$, donc g est un monomorphisme si et seulement si h est un monomorphisme.

(iv) On a $f^{-1}(\operatorname{Im}(h)) = \operatorname{Im}(g)$, donc g est un épimorphisme si et seulement si

$$\operatorname{Im}(f) = \operatorname{Im}(h).$$

5.3. **Le premier théorème d'isomorphisme.** Chaque homomorphisme h factorise comme

$$h = \iota \circ \overline{h} \circ \nu_N$$

où ι est une inclusion, $\overline{h}$ un isomorphisme et ν_N l'homomorphisme naturel associé à un sous-groupe normale. Donc pour comprendre tous les homomorphismes il suffit de comprendre les inclusions, les isomorphismes et les homomorphismes naturels.

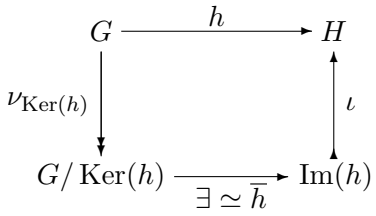
Théorème 5.3 (Premier théorème d'isomorphisme)**.** *Soit $h : G \longrightarrow H$ un homomorphisme. L'inclusion $\operatorname{Im}(h) \subseteq H$ induit un monomorphisme*

$$\iota : \operatorname{Im}(h) \longrightarrow H$$

défini par $\iota(x) := x$ pour $x \in \operatorname{Im}(h)$.

Alors il existe un unique isomorphisme $\overline{h}$ entre le groupe quotient $G/\operatorname{Ker}(h)$ et l'image $\operatorname{Im}(h)$ tel que

$$h = \iota \circ \overline{h} \circ \nu_{\operatorname{Ker}(h)} \ :$$



Preuve. Les noyaux de h et $\nu_{\ker(h)}$ sont égaux, donc par le théorème fondamental des homomorphismes il existe un monomorphisme $g:\ G/\operatorname{Ker}(h) \longrightarrow H$ tel que $h = g \circ \nu_{\mathrm{Ker}(h)}$ et $\operatorname{Im}(h) = \operatorname{Im}(g)$. Puis, on peut appliquer l'exercice avant avec l'homomorphisme g et le monomorphisme ι. Ça donne un morphisme $\overline{h}:\ G/\operatorname{Ker}(h) \longrightarrow \operatorname{Im}(g)$ tel que $\iota \circ \overline{h} = g$. Cet homomorphisme est un épimorphisme (parce que $\operatorname{Im}(h) = \operatorname{Im}(\iota) = \operatorname{Im}(g)$) et un monomorphisme (parce que g est un monomorphisme). Donc $\overline{h}$ est un isomorphisme et

$$\iota \circ \overline{h} \circ \nu_{\mathrm{Ker}(h)} = h.$$

□

Corollaire 5.1. *Soit $h:\ G \longrightarrow H$ un homomorphisme entre deux groupes finis. Alors*

$$O(\operatorname{Ker} h) \cdot O(\operatorname{Im} h) = O(G),$$

et $O(\operatorname{Im} h)$ divise le plus grand commun diviseur de $O(G)$ et de $O(H)$. Si $x \in G$, alors $O(h(x))$ divise le plus grand commun diviseur de $O(x)$ et de $O(H)$.

Preuve. On a $G/\operatorname{Ker}(h) \simeq \operatorname{Im}(h)$ par le théorème, donc $O(G)/O(\operatorname{Ker} h) = O(\operatorname{Im}(h))$. Les divisibilités suivent du théorème de Lagrange. Soit $k : < x > \longrightarrow H$ la restriction de h au sous-groupe $< x >$. L'image de k est $< h(x) >$, et le noyau de k est $< x > \cap\ \operatorname{Ker}(h)$. Donc le premier théorème d'isomorphisme donne l'existence d'un isomorphisme

$$< x > /(< x > \cap\ \operatorname{Ker}(h)) \simeq < h(x) > .$$

Puis on applique le théorème de Lagrange. □

Exercice 5.17. Soit $h:\ G \longrightarrow H$ un épimorphisme. Si $N \lhd H$, montrer que

$$G/h^{-1}(N) \simeq H/N.$$

5.4. **Le deuxième théorème d'isomorphisme.** Si H et K sont deux sous-groupes normaux de G, alors $(H \cap K) \lhd K$ et $H \lhd HK$, où $HK = \{hk;\ h \in H, k \in K\}$ est un sous-groupe de G. Le deuxième théorème d'isomorphisme suivant dit que les deux groupes quotients $K/(H \cap K)$ et HK/H sont isomorphes.

Soit $H < G$. On pose

$$N_G(H) := \{g \in G;\ \forall h \in H:\ ghg^{-1} \in H\}.$$

On l'appelle le *normalisateur* de H dans G. Évidemment on a

$$H \lhd\ N_G(H) < G$$

et le normalisateur est le plus grand sous-groupe de G qui contient H comme sous-groupe normale.

Exercice 5.18. Soient H, K et L trois sous-groupes de G, tels que $H \lhd K$ et $H \lhd L$. Montrer que le sous-groupe M de G engendré par K et L est contenu dans le normalisateur $N_G(H)$.

Théorème 5.4 (Deuxième théorème d'isomorphisme)**.** *Soient H et K deux sous-groupes de G tels que*

$$K < N_G(H).$$

Alors on a
(i) $KH = HK < G$;
(ii) $H \lhd HK$ et $H \cap K \lhd K$;
(iii) et

$$K/(H \cap K) \simeq HK/H.$$

Preuve. Soit $h : K \longrightarrow N_G(H)/H$ la restriction à $K \subseteq N_G(H)$ de l'homomorphisme naturel

$$\nu_H : N_G(H) \longrightarrow N_G(H)/H.$$

Le noyau de h est $H \cap K$, donc $(H \cap K) \lhd K$. L'image de h est

$$\mathrm{Im}(h) = \{kH;\ k \in K\}.$$

C'est un sous-groupe de $N_G(H)/H$. Par le premier théorème d'isomorphisme on obtient un isomorphisme

$$K/(H \cap K) \simeq \{kH;\ k \in K\}.$$

Le pré-image $\nu_H^{-1}(\mathrm{Im}(h)) = \{kh; k \in K, h \in H\} = KH$ est un sous-groupe de $N_G(H)$, et donc de G. On a

$$kh = (khk^{-1})k \in HK$$

donc $HK = KH < N_G(H)$. Soit maintenant $k : HK \longrightarrow N_G(H)/H$ la restriction de ν_H à $HK \subseteq N_G(H)$. Alors l'image de k est $\mathrm{Im}(h)$, et son noyau est $HK \cap H = H$. Par le premier théorème d'isomorphisme on obtient un isomorphisme

$$HK/H \simeq \{kH;\ k \in K\}.$$

En utilisant les deux isomorphismes on obtient un isomorphisme

$$HK/H \simeq K/(H \cap K).$$

□

Exercice 5.19. Soit K un corps. Utiliser le deuxième théorème d'isomorphisme pour montrer que $B(2,K)/U(2,K) \simeq T(2,K)$.

Exercice 5.20. Soit $G = \mathrm{Alt}_5$ et $H =< (1,2,3,4,5) >$. (i) Soit $g \in N_G H$ un élément d'ordre 5. Calculer l'ordre de $H < g >$ et conclure que $g \in H$ et $N_G H \neq G$.

(ii) Montrer que $(2,5)(3,4) \in N_G H$, et utiliser Lagrange pour montrer que $N_G H$ ne contient aucun élément d'ordre 3, i.e., aucun 3-cycle.

(iii) Montrer que Alt_5 contient 15 éléments d'ordre 2, et que ces éléments engendrent Alt_5. Conclure que $N_G H$ contient moins que 15 éléments d'ordre 2, et contient moins que 20 éléments en total.

(iv) Montrer que $N_G H =< (2,5)(3,4) > H$, d'ordre 10.

Exercice 5.21. Soit U un sous-espace vectoriel V sur un corps fixé. Définir sur V/U un structure d'espace vectoriel (appelé l'espace quotient). Formuler et montrer les versions des deux premiers théorèmes d'isomorphisme pour les espaces vectoriels.

5.5. **Le troisième théorème d'isomorphisme.** Si $N \subseteq M$ sont deux sous-groupes normaux, on peut "simplifier la fraction" $(G/N)/(M/N) \simeq G/M$.

Théorème 5.5 (Troisième théorème d'isomorphisme)**.** *Soient N et M deux sous-groupes normaux de G tels que*

$$N \subseteq M \subseteq G.$$

Alors
(i) $N \lhd M$;
(ii) On peut identifier M/N avec un sous-groupe normal de G/N;
(iii) et

$$(G/N)/(M/N) \simeq G/M.$$

Preuve. On a $N = \mathrm{Ker}(\nu_N) \subseteq \mathrm{Ker}(\nu_M) = M$, donc par le théorème fondamental des homomorphismes il existe un épimorphisme $g : G/N \longrightarrow G/M$ tel que $\nu_M = g \circ \nu_N$ avec noyau

$$\mathrm{Ker}(g) = \nu_N(M) = \{mN;\ m \in M\}.$$

Et comme $N \subseteq M$ l'ensemble de translatés $\{mN;\ m \in M\} \subseteq G/N$ s'identifie avec l'ensemble de translatés M/N. Donc par le premier théorème d'isomorphisme on obtient :

$$(G/N)/(M/N) \simeq G/M.$$

□

Exercice 5.22. Soient $N_0 \subset N_1 \subset N_2 \subset N_3$ quatre sous-groupes normaux d'un groupe G. Définissons

$$\overline{G} := G/N_0 \text{ et } \overline{N_i} := N_i/N_0 \lhd G/N_0,$$

pour $i = 1, 2, 3$. Puis, définissons

$$\overline{\overline{G}} := \overline{G}/\overline{N_1} \text{ et } \overline{\overline{N_i}} := \overline{N_i}/\overline{N_1} \lhd \overline{G}/\overline{N_1},$$

pour $i = 2$ et 3. Finalement, définissons

$$\overline{\overline{\overline{G}}} := \overline{\overline{G}}/\overline{\overline{N_2}} \text{ et } \overline{\overline{\overline{N_3}}} := \overline{\overline{N_3}}/\overline{\overline{N_2}} \lhd \overline{\overline{G}}/\overline{\overline{N_2}}.$$

Montrer que

$$\overline{\overline{\overline{G}}}/\overline{\overline{\overline{N_3}}} \simeq G/N_3.$$

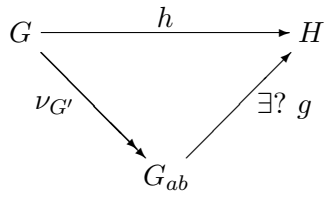
Exercice 5.23. Soient N et M deux sous-groupes normaux de G. Montrer que $G/(N \cap M)$ est isomorphe à un sous-groupe du produit cartésien $G/N \times G/M$.

5.6. **Morphismes vers un groupe abélien.** Pour un groupe G on écrit souvent G_{ab} à la place du groupe quotient G/G', où G' est le sous-groupe dérivé de G. C'est un groupe abélien, le plus grand groupe quotient de G qui est abélien.

Théorème 5.6. *Soit $h: G \longrightarrow H$ un homomorphisme. Alors il existe un (unique) homomorphisme $g: G_{ab} \longrightarrow H$, tel que*

$$h = g \circ \nu_{G'}$$

si et seulement si $\mathrm{Im}(h)$ *est abélien si et seulement si* $G' \subset \mathrm{Ker}(h)$.



Preuve. Si g existe, alors $\mathrm{Im}(h) = \mathrm{Im}(g)$ est l'image d'un groupe abélien G_{ab}, donc est abélien. Supposons $\mathrm{Im}(h)$ est abélien, donc $G' \subset \mathrm{Ker}(h)$ et on peut appliquer le théorème fondamental des homomorphismes. Ça donne l'existence de g, tel que $h = g \circ \nu_{G'}$. □

Exercice 5.24. Soit A un groupe abélien. Montrer que l'application $h \mapsto \overline{h}$ induit une correspondance biunivoque entre $\mathrm{Mor}(G, A)$ et $\mathrm{Mor}(G_{ab}, A)$. Ici $\mathrm{Mor}(G, A) = \{h: G \longrightarrow A;\ h \text{ est un morphisme}\}$ et $\overline{h}: G_{ab} \longrightarrow A$ est l'homomorphisme tel que $h = \overline{h}\nu_{G'}$.

Montrer que $\mathrm{Mor}(\mathrm{Alt}_n, A)$ contient seulement un élément si $n \geq 5$.

Exercice 5.25. Soit $N \lhd G$. Montrer que $N \lhd (G'N) \lhd G$; $G/G'N$ est abélien; $G'N/N = \nu_N(G')$ et $(G/N)' = (G'N)/N$.

5.7. **Le théorème de correspondance.** Si on connaît les sous-groupes (normaux) de G/N, on connaît aussi les sous-groupes (normaux) de G contenant N.

Théorème 5.7. *Soit $N \lhd G$ et $\nu: G \longrightarrow G/N$ l'application naturelle.*

(i) Les sous-groupes de G/N sont en correspondance biunivoque avec les sous-groupes de G qui contiennent N.

(ii) Les sous-groupes normaux de G/N sont en correspondance biunivoque avec les sous-groupes normaux de G qui contiennent N.

Les correspondances sont données par

$$G/N > K \mapsto \nu^{-1}(K) < G \quad \text{et } G > H \mapsto \nu(H) < G/N.$$

Preuve. Posons $\Omega := \{H < G;\ H \supset N\}$ et $\Psi := \{K < G/N\}$ et les applications $\phi: \Omega \longrightarrow \Psi$ et $\eta: \Psi \longrightarrow \Omega$ définies par $\phi(H) := \nu_N(H)$ et $\eta(K) := \nu_N^{-1}(K)$. Il faut montrer que $\phi \circ \eta = \mathbf{1}$ et $\eta \circ \phi = \mathbf{1}$. C'est facile est laissé comme exercice. □

Exercice 5.26. Soit $n \in \mathbb{Z}_{>0}$ un nombre entier. Décrire les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ en utilisant le théorème de correspondance.

Exercice 5.27. (i) Soit $G' \subset H < G$. Montrer que $H \lhd G$ en utilisant le théorème de correspondance.

(ii) Donner un exemple d'un sous-groupe $H \lhd G' \lhd G$, mais H n'est pas normal dans G.

(iii) Soit $\phi : G \longrightarrow G$ un automorphisme. Montrer que $\phi(G') = G'$, et plus généralement $\phi(G^{(n)}) = G^{(n)}$, pour chaque n.

(iv) On a $G' \lhd G$ et $G'' \lhd G'$. Montrer qu'on a aussi $G'' \lhd G$. Et plus généralement, si $N \lhd G$, alors $N^{(n)} \lhd G$ pour chaque n.

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

5.8. **Le théorème de Jordan–Hölder.** [14] Chaque nombre naturel a une décomposition primaire, qui est unique à une permutation des facteurs près. Quelque chose semblable est vrai pour chaque groupe fini.

On dit qu'un groupe K est *simple* si ses seuls sous-groupes normaux sont les sous-groupes triviaux K et $\{\mathbf{1}_K\}$. Un sous-groupe normal $N \lhd G$ est dit *maximal* si $N \neq G$ et s'il n'y a pas de sous-groupe normal $M \lhd G$ contenant N, sauf $M = N$ et $M = G$. Ou, ce qui est équivalent par le théorème de correspondance, $N \lhd G$ est maximal si et seulement si $N \neq G$ et G/N est simple.

Un des très grands théorèmes du 20-ième siècle est l'achèvement autour de 1981 de la classification de tous les groupes simple finis (à isomorphisme près, bien sûr). La preuve actuelle prend environ 5000 pages ![15] Exemples sont les groupes cycliques C_p, si p est un nombre premier; les groupes Alt_n, si $n > 4$ (un résultat de Galois [4, p.241]); ou les groupes $\mathrm{PGL}(n, \mathbb{F}_q)$, si $(n, q) \neq (2, 2)$ ou $(2, 3)$ [4, p.362] (ici, PGL est le groupe quotient de GL par le sous-groupe normal des matrices scalaire $c\mathbf{1}$), et des généralisations. Il y a plusieures séries de groupes simples dépendantes de paramètres (comme les exemples déjà données), et 28 groupes sporadiques, qui n'appartiennent pas à une série infinie. Le plus grand groupe simple sporadique s'appelle le monstre, et est d'ordre

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

construit (ou plutôt son existence montré) en 1981. Un théorème important utilisé est celui de Feit-Thompson (1963), qui dit qu'un groupe fini simple d'ordre impair est cyclique d'ordre premier. La preuve originale de ce résultat prend déjà 255 pages.

Si G est fini et non-trivial alors G contient toujours un sous-groupe normal maximal G_1. Si G_1 n'est pas trivial, il contient un sous-groupe normal maximal $G_2 \lhd G_1$ (mais G_2 n'est pas nécessairement un sous-groupe normal de G). On continue et on trouve une *suite de décomposition* (ou une suite de Jordan–Hölder) de G :

$$\{\mathbf{1}_G\} = G_s \lhd G_{s-1} \lhd G_{s-2} \lhd \ \ldots \ \lhd G_2 \lhd G_1 \lhd G_0 := G.$$

Par exemple :

$$\{\mathbf{1}\} \lhd \{\mathbf{1}, (1,2)(3,4)\} \lhd V_4 \lhd \ \mathrm{Alt}_4 \lhd S_4.$$

En général il y a plusieurs choix pour G_1, et puis pour G_2, etc. Toute de même la longueur d'une telle suite sera toujours la même, et les mêmes groupes simple G_i/G_{i+1} (à isomorphisme près) (les *facteurs simples* de G) vont apparaître avec les mêmes multiplicités. C'est ça le théorème de Jordan–Hölder.

Exercice 5.28. Trouver plusieures suites de décomposition du groupe $B(3, \mathbb{F}_3)$, des matrices 3×3 inversibles triangulaires de coefficients dans $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

Théorème 5.8 (Théorème de Jordan–Hölder)**.** *Soit G un groupe fini et soient*

$$G_s = \{\mathbf{1}_G\} \lhd G_{s-1} \lhd G_{s-2} \lhd \ \ldots \lhd G_2 \lhd G_1 \lhd G_0 = G,$$

[14] **Pas de matière examen !**

[15] Mais récemment on avait encore trouvé un trou dans la preuve, pour le remplir on a écrit tout un livre. Voir M. Aschbacher, The status of the classification of the finite simple groups, Notices of the American Mathematical Society, **51**, 2004, p. 736–740

et

$$K_t = \{\mathbf{1}_G\} \lhd K_{t-1} \lhd K_{t-2} \lhd \ldots \lhd K_2 \lhd K_1 \lhd K_0 = G,$$

deux suites de décomposition, en particulier $G_{i+1} \lhd G_i$ *et* $K_{i+1} \lhd K_i$ *sont maximal pour chaque* i.

Alors $s = t$ *et il existe une permutation* $\pi \in S_s$ *de* $\{1, 2, \ldots, s\}$ *telle que*

$$G_{i-1}/G_i \simeq K_{\pi(i)-1}/K_{\pi(i)},$$

pour chaque $1 \leq i \leq s$.

Lemme 5.1. *Soient* N *et* M *deux sous-groupes normaux d'un groupe* G. *Supposons que* $N \not\subset M$ *et que* M *est maximal. Alors* $(N \cap M) \lhd N$ *est aussi maximal, et*

$$N/(N \cap M) \simeq G/M.$$

Preuve. Parce que $G = N_G M$ et donc $N < N_G M$ on peut appliquer le deuxième théorème d'isomorphisme. On obtient $NM < G$ et un isomorphisme $NM/M \simeq N/N \cap M$. On a même que $NM \lhd G$, parce que si $g \in G$, $n \in N$, $m \in M$ on a $gnmg^{-1} = gng^{-1} \cdot gmg^{-1} \in NM$. Puisque $M \lhd NM \lhd G$ et M est un sous-groupe normal maximal il suit que $G = NM$ et $G/M \simeq N/N \cap M$. Le groupe G/M est simple, donc aussi le groupe $N/N \cap M$ est simple et $N \cap M \lhd N$ est maximal. □

Preuve du théorème. Nous montrons le théorème par induction sur la cardinalité de G. Le cas où $O(G) = 1$ est trivial. Donc supposons que le théorème est vrai pour tous les groupes d'ordre plus petit que $O(G)$. Et soient deux suites de décomposition données comme dans l'énoncé du théorème.

Par le lemme précédent $(G_1 \cap K_1) \lhd G_1$ et $(G_1 \cap K_1) \lhd K_1$ sont des sous-groupes maximaux. Soit

$$L_u = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ldots L_3 \lhd L_2 := (G_1 \cap K_1)$$

une suite de décomposition de $(G_1 \cap K_1)$. Alors

$$L_u = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd G_1$$

et

$$G_s = \{\mathbf{1}_G\} \lhd G_{s-1} \lhd G_{s-2} \lhd \ldots \lhd G_2 \lhd G_1$$

sont deux suites de décomposition de G_1. Par induction on obtient $s = u$ et on obtient aussi une permutation des facteurs simples. Donc aussi les facteurs simples des deux suites de G

$$L_s = \{\mathbf{1}_G\} \lhd L_{s-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd G_1 \lhd G$$

et

$$G_s = \{\mathbf{1}_G\} \lhd G_{s-1} \lhd G_{s-2} \lhd \ldots \lhd G_2 \lhd G_1 \lhd G$$

sont permutés.

Aussi

$$L_u = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd K_1$$

et

$$K_t = \{\mathbf{1}_G\} \lhd K_{t-1} \lhd K_{t-2} \lhd \ldots \lhd K_2 \lhd K_1$$

sont deux suites de décomposition de K_1, et par induction on a $t = u$. Donc $s = t$. Et les facteurs simples des deux suites de composition de G :

$$L_s = \{\mathbf{1}_G\} \lhd L_{s-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd K_1 \lhd G$$

et

$$K_s = \{\mathbf{1}_G\} \lhd K_{s-1} \lhd K_{s-2} \lhd \ \ldots \lhd K_2 \lhd K_1 \lhd G$$

sont permutés.

Parce que $G/K_1 \simeq G_1/L_2$ et $G/G_1 \simeq K_1/L_2$ par le lemme précédent, on a aussi que les facteurs simples des suites de composition de G :

$$L_s = \{\mathbf{1}_G\} \lhd L_{s-1} \lhd \ \ldots \lhd L_3 \lhd L_2 \lhd G_1 \lhd G$$

et

$$L_s = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ \ldots \lhd L_3 \lhd L_2 \lhd K_1 \lhd G$$

sont permutés.

Donc les facteurs simples des suites de décomposition énoncé dans le théorème sont permutés. □

Exemple 5.2. Les suites de décomposition de $\mathbb{Z}/12\mathbb{Z}$ sont

$$< 0 + 12\ \mathbb{Z} > \lhd \ < 6 + 12\ \mathbb{Z} > \lhd \ < 3 + 12\ \mathbb{Z} > \lhd \mathbb{Z}/12\mathbb{Z};$$

$$< 0 + 12\ \mathbb{Z} > \lhd \ < 6 + 12\ \mathbb{Z} > \lhd \ < 2 + 12\ \mathbb{Z} > \lhd \mathbb{Z}/12\mathbb{Z};$$

$$< 0 + 12\ \mathbb{Z} > \lhd \ < 4 + 12\ \mathbb{Z} > \lhd \ < 2 + 12\ \mathbb{Z} > \lhd \mathbb{Z}/12\mathbb{Z}.$$

Les trois facteurs simples sont $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ (à une permutation près).

Exercice 5.29. Soit $n = p_1^{m_1} \cdots p_s^{m_s}$ la décomposition primaire du nombre naturel n. Montrer que le groupe cyclique C_n a les facteurs simples C_{p_i} avec la multiplicité m_i.

Exercice 5.30. Si G est un groupe fini abélien et simple, alors G est cyclique d'ordre premier.

Exercice 5.31. Montrer qu'un groupe fini G est soluble (dans le sens que $G^{(n)} = \mathbf{1}$ pour $n >> 0$ si et seulement si les facteurs simples dans une suite de décomposition de G sont tous abélien.

Le grand problème irrésolu dans la théorie des groupes finis est de construire tous les groupes avec des facteurs simple de Jordan-Hölder donnés, appelé le problème d'extension. En particulier, soient donnés deux groupes simple G_1 et G_2. Trouver les groupes G (à isomorphisme près) ayant un sous-groupe normal N isomorphe à G_1 tel que le groupe quotient G/N est isomorphe à G_2.

6. Opérations d'un groupe sur un ensemble

Dans les sciences on considère souvent des groupes de symétries d'un objet X. L'objet peut être physique, comme un cristal ou un molécule, ou mathématique, comme une courbe dans l'espace. Alors chaque $g \in G$ est une symétrie: une application (par exemple une rotation) qui préserve la structure de X.

Nous considérons ici le cas ou X est un ensemble. En pratique, un ensemble a plus de structure (par exemple une opération interne ou une notion de distance) et on est souvent intéressé aux symmétries qui préservent ce structure aussi.

6.1. **Opérations.** Soit $(G, \circ)$ un groupe et X un ensemble. Une *G-action* (ou une action de G ou une *G-opération*) sur X est une règle

$$(g, x) \mapsto g \bullet x \in X,$$

pour chaque $g \in G$ et $x \in X$, satisfaisant les propriétés

$$\mathbf{1}_G \bullet x = x$$

$$(g_1 \circ g_2) \bullet x = g_1 \bullet (g_2 \bullet x))$$

pour chaque $g_1, g_2 \in G$ et $x \in X$. On dit que $(X, \bullet)$ est un *G-ensemble*, ou simplement que X est un G-ensemble (où la G-opération est fixée).

Soient X et Y deux G-ensembles. Une application $f : Y \longrightarrow X$ est une *G-application* si

$$f(g \bullet y) = g \bullet f(y),$$

pour chaque $g \in G$ et $y \in Y$. On définit de façon analogue les *G-bijections*.

Un *sous-G-ensemble* de X est un sous-ensemble Y d'un G-ensemble X tel que $g \bullet y \in Y$, pour chaque $g \in G$ et $y \in Y$. L'inclusion $Y \longrightarrow X$ est une G-application.

Exercice 6.1. L'intersection et la réunion d'une famille de sous-G-ensembles d'un G-ensemble sont aussi des sous-G-ensembles. Le complément d'un sous-G-ensemble est un sous-G-ensemble.

Un sous-G-ensemble non-vide de X qui ne contient pas un sous-G-ensemble propre non-vide s'appelle une *orbite* (ou une G-orbite) de X. Donc les orbites sont les plus petits G-sous-ensembles non-vide. Soit O une orbite et $x \in O$, on verra que

$$O = G \bullet x := \{g \bullet x; g \in G\}.$$

On dit que l'action sur X est *transitive*, si G opère avec seulement une seule orbite.

Soit $x \in X$, alors on appelle le *stabilisateur* de x le sous-groupe de G défini par

$$G_x := \{g \in G;\ g \bullet x = x\}.$$

Autre notations pour G_x sont $\mathrm{Stab}_G(x)$ ou $\mathrm{Stab}(x)$.

Le *noyau* de l'opération est

$$G_X := \{g \in G;\ \forall x \in X :\ g \bullet x = x\},$$

l'ensemble des éléments de G qui agissent trivialement sur X.

Exercice 6.2. Montrer que G_x est un sous-groupe de G et que $G_{g\bullet x} = gG_xg^{-1}$. Montrer que G_X est un sous-groupe normal de G.

On dénote

$$X^G := \{x \in X;\ \forall g \in G :\ g \bullet x = x\}$$

pour l'ensemble des *points fixes*. Une orbite contient seulement un élément x si et seulement si x est un point fixe.

On dénote l'ensemble des G-orbites de X par X/G (on va voir que les orbites sont disjointes). Donc un élément de l'ensemble X/G est une G-orbite de X. On verra que chaque x est dans une unique orbite; l'application surjective

$$\mathrm{Orb} :\ X \longrightarrow X/G$$

associe à chaque $x \in X$ l'unique G-orbite $\mathrm{Orb}(x)$ contenant x.

Exemple 6.1. Soit X un ensemble et G un sous-groupe de S_X. Alors $g \bullet x := g(x)$ définit une opération de G sur X. Soit H un sous-groupe de $\mathrm{GL}(n, \mathbb{R})$, alors H opère sur l'espace linéaire $\mathbb{R}^n$ par la multiplication matricielle.

Exemple 6.2. Soit $(G, \circ)$ un groupe, alors G opère sur soi-même par multiplication à gauche:

$$g \bullet x := g \circ x,$$

où $g, x \in G$. Soit H un sous-groupe de G (pas nécessairement normal), alors l'ensemble des translatés G/H devient un G-ensemble avec la G-opération

$$g \bullet (x \circ H) := (g \circ x) \circ H,$$

pour $g \in G$ et $x \circ H \in G/H$. Évidemment $\mathbf{1}_G \bullet (x \circ H) = x \circ H$ et $g_1 \bullet (g_2 \bullet (x \circ H)) = (g_1 \circ g_2) \bullet (x \circ H)$. Pour cette G-opération transitive on va adopter le même symbole (ici $\circ$) pour l'opération interne du groupe et la G-opération sur G/H. L'application naturelle $\nu : G \longrightarrow G/H$ est une G-application entre deux G-ensembles.

Exercice 6.3. Il existe d'autres opérations naturelles sur l'ensemble G/H, où $H < G$. Définissons $K := N_G(H)/H$. Montrer que

$$((g, nH), xH) \mapsto (g, nH) \bullet xH := gxn^{-1}H$$

donne une $G \times K$-opération bien définie sur G/H. Définir une opération de $G \times K$ sur $H\backslash G$, l'ensemble des translatés à droite.

Exercice 6.4. Le groupe diédral D_6 opère naturellement sur $\mathbb{R}^2$. Trouver ses orbites, ses stabilisateurs, ses points fixe. Décrire $\mathbb{R}^2/D_6$ par donner un représentant de chaque orbite.

Exercice 6.5. Un exemple important dans la théorie des nombres algébriques. Soit Σ la sphère de Riemann

$$\Sigma = \mathbb{C} \cup \{\infty\}.$$

Le groupe $\mathrm{SL}(2, \mathbb{R})$ agit sur Σ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet z := \frac{az + b}{cz + d}.$$

Par exemple,

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \bullet \infty := \frac{1\infty+1}{0\infty+1} = \infty;$$

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \bullet \infty := \frac{1\infty+0}{1\infty+1} = \frac{1+0}{1+1/\infty} = 1$$

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \bullet i := \frac{i+0}{i+1} = \frac{i+1}{2} = \begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix} \bullet i,$$

où $i^2 = -1$.

(a) Vérifier que les axiomes d'une action sont satisfaits.

(b) Montrer que $\mathrm{SL}(2,\mathbb{R})$ agit avec trois orbites. Calculer le noyau de l'opération et les stabilisateurs de i, $-i$, 1 et ∞.

(c) Chaque sous-groupe de $\mathrm{SL}(2,\mathbb{R})$ opère aussi sur Σ. Dessiner les orbites de $U(2,\mathbb{R})$ (le groupe des matrices triangulaire supérieures de valeurs propres 1), T_2 (les matrices diagonales de déterminant 1) et de $\mathrm{SO}(2)$ (les matrices orthogonales).

(d) Trouver un représentant dans chaque orbite de $\mathrm{SL}(2,\mathbb{Z})$ agissant sur Σ. Indice : le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par les deux matrices

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \text{et} \quad \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

(Pour montrer ça, utiliser la division avec reste !)

6.2. **Théorème fondamental des opérations.** Le théorème suivant donne la structure des G-ensembles. Chaque G-ensemble est la réunion disjointe de ses orbites et chaque orbite est en G-bijection avec un G/H pour un sous-groupe $H < G$.

Théorème 6.1. *Soit $(G,\circ)$ un groupe et $(X,\bullet)$ un G-ensemble.*

(i) X est la réunion disjointe de ses G-orbites.

(ii) Chaque $x \in X$ est contenu dans une unique G-orbite, notée $\mathrm{Orb}(x)$ *et*

$$\mathrm{Orb}(x) = G \bullet x := \{g \bullet x;\ g \in G\}.$$

(iii) Posons $H := \mathrm{Stab}_G(x)$. Alors il existe une G-bijection entre les G-ensembles $\mathrm{Orb}(x)$ *et G/H.*

Preuve. L'intersection de deux orbites est un G-sous-ensemble, donc par minimalité on obtient que si deux orbites ne sont pas disjointes, alors elles sont égales.

Pour $x \in X$ soit O_x l'intersection de tous les sous-G-ensembles contenant x. Alors O_x est un sous-G-ensemble contenant x, contenu dans chaque G-sous-ensemble contenant x. Supposons que O_x n'est pas une orbite. Alors il existe un sous-G-ensemble propre non-vide $E \subset O_x$ contenant x. Ce qui est une contradiction avec la construction de O_x. Alors chaque élément $x \in X$ est inclus dans une unique orbite et on a montré (i).

O_x contient $G \bullet x := \{g \bullet x;\ g \in G\}$ comme sous-ensemble, parce que O_x est un G-sous-ensemble. Mais $G \bullet x$ est soi-même un sous-G-ensemble contenant x, parce que $x = \mathbf{1}_G \bullet x$ et $g_1 \bullet (g_2 \bullet x) = (g_1 \circ g_2) \bullet x$. Donc $O_x = \{g \bullet x;\ g \in G\}$ et (ii) est montré.

Définissons l'application

$$\phi : \ G \bullet x \longrightarrow G/H$$

par $\phi(g \bullet x) := g \circ H$. Il faut d'abord montrer que ϕ est bien-définie, qu'elle ne dépend pas du choix de $g \in G$ pour représenter $g \bullet x \in O_x$. Donc supposons $g_1 \bullet x = g_2 \bullet x$. Alors $g_2^{-1} \circ g_1 \in H$, parce que

$$(g_2^{-1} \circ g_1) \bullet x = g_2^{-1} \bullet (g_1 \bullet x) = g_2^{-1} \bullet (g_2 \bullet x) = (g_2^{-1} \circ g_2) \bullet x = \mathbf{1}_G \bullet x = x,$$

donc ($g_2^{-1} \circ g_1 \in \mathrm{Stab}(x) = H$; alors $g_1 \circ H = g_2 \circ H$ et ϕ est bien-définie.

Pour chaque y in $\mathrm{Orb}(x) = G \bullet x$ il existe un $k \in G$ tel que $k \bullet x = y$. Alors $\phi(g \bullet y) = \phi(g \bullet (k \bullet x)) = \phi((g \circ k) \bullet x) = (g \circ k) \circ H = g \circ (k \circ H) = g \circ \phi(y)$, et ϕ est donc une G-application.

L'injectivité de ϕ : Si $\phi(g_1 \bullet x) = \phi(g_2 \bullet x)$, alors $g_1 \circ H = g_2 \circ H$. Donc, il existe un $h \in H$ tel que $g_1 = g_2 \circ h$. Alors

$$g_1 \bullet x = (g_2 \circ h) \bullet x = g_2 \bullet (h \bullet x) = g_2 \bullet x,$$

parce que $H = \mathrm{Stab}(x)$.

La surjectivité de ϕ : Soit $g \circ H \in G/H$ quelconque, alors $g \circ H = \phi(g \bullet x)$. □

6.3. **L'équation de classe.** Comme corollaire immédiat du Théorème 6.1 on obtient :

Corollaire 6.1 (Équation de classe)**.** *Soit X un G-ensemble fini. Alors*

$$|X| = \sum_{O \in X/G} |O| = |X^G| + \sum_{O \in X/G, |O|>1} |O|,$$

où X^G est l'ensemble des points fixe.

Soit $O \in X/G$ et $x \in O$. Alors

$$|O| = (G : \mathrm{Stab}_G(x)).$$

En particulier, la cardinalité de chaque orbite est un diviseur de l'ordre du groupe.

Exemple 6.3. Soit K en sous-groupe d'un groupe $(L, \circ)$. Alors K opère sur L par l'opération

$$k \bullet x := x \circ k^{-1},$$

$k \in K, x \in L$. Les K-orbites sont les translatés à gauche de K, les stabilisateurs sont tous triviaux et les orbites ont toutes la cardinalité $O(K)$. Donc l'équation de classes devient ici $O(L) = \sum_{O \in L/K} |O| = |L/K| \cdot O(K)$, et $|L/K|$ est l'index $(L : K)$. Donc on peut voir l'équation de classe comme une généralisation du théorème de Lagrange.

Exercice 6.6. Supposons un groupe cyclique d'ordre premier p opère sur un ensemble de $p^2 + p + 1$ éléments. Montrer qu'il existe au moins un point fixe.

6.4. **Existence de points fixe.** Une première application de la formule de classe est l'existence d'un point fixe pour certaines actions. Si l'ensemble X est trop petit pour un groupe G, alors G peut seulement opérer trivialement.

Lemme 6.1. *Soit p le plus petit diviseur premier d'un group fini G et soit X un G ensemble. Si x n'est pas un point fixe alors l'orbite contenant x a au moins p éléments. En particulier, si $X - X^G$ a moins que p éléments alors nécessairement G agit trivialement : $X = X^G$.*

Preuve. On a $|\mathrm{Orb}(x)|$ divise $O(G)$ et p est le plus petit diviseur de $O(G)$. □

Le lemme suivant est aussi presque trivial, mais ces applications sont nombreuses.

Lemme 6.2. *Soit p un nombre premier et P un groupe d'ordre p^r. Soit X un P-ensemble fini. Alors $|X| - |X^P|$ est divisible par p. En particulier, si p ne divise pas $|X|$, alors il existe un point fixe $x \in X^G$.*

Preuve. Soit O une orbite de X, alors la cardinalité de O divise la cardinalité de P, donc est une puissance de p. On a $|O| \neq 1$ si et seulement si O ne contient pas un point fixe si et seulement si p divise $|O|$. Par l'équation de classes il suit que $|X| - |X^P|$ est divisible par p. □

6.5. **Le théorème de Cayley généralisé.** Si G opère sur X, alors chaque g induit une bijection de X, d'où une application $G \longrightarrow S_X$. Les propriétés d'une opération impliquent que cette application est un morphisme. En effet, donner une action sur un ensemble est équivalent à donner un homomorphisme de groupe de G vers S_X. Les G-actions sur X sont en correspondance avec les homomorphismes $G \longrightarrow S_X$.

Théorème 6.2. *Soit G un groupe et X un ensemble.*

(i) Si $(g, x) \longrightarrow g \bullet x$ est une G-opération sur X, alors l'application $f : G \longrightarrow S_X$ définie par

$$[f(g)](x) := g \bullet x$$

est un homomorphisme de groupes avec noyaux G_X.

(ii) Si $f : G \longrightarrow S_X$ est un homomorphisme de groupes alors

$$(g, x) \mapsto g \bullet x := [f(g)](x)$$

est une G-opération sur X.

(iii) Les G-opérations sur X sont en correspondance biunivoque avec les homomorphismes

$$f : G \longrightarrow S_X.$$

Preuve. (i) Soit $(g, x) \mapsto g \bullet x$ une G-opération sur X et $[f(g)](x) := g \bullet x$. Alors

$$[f(g_1 \circ g_2)](x) = (g_1 \circ g_2) \bullet x = g_1 \bullet (g_2 \bullet x) = [f(g_1)]([f(g_2)](x)) = [f(g_1) \circ f(g_2)](x).$$

Donc f est un homomorphisme. La preuve de (ii) est similaire. La correspondance suit de (i) et (ii). □

Exercice 6.7. Supposons que $f : G \longrightarrow S_X$ correspond à l'opération $g \bullet x$. Montrer que le noyau de f est exactement le noyau de l'opération. Montrer que le noyau de l'opération est l'intersection de tous les stabilisateurs G_x.

Supposons que G agit transitivement sur X, et $x \in X$. Montrer que le noyau G_X est le plus grand sous-groupe normal de G contenu dans G_x.

Exercice 6.8. Pourquoi ce théorème est une généralisation du théorème de Cayley?

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

7. Applications dans la théorie des groupes

L'équation de classe est très simple et s'applique dans beaucoup de situations. Il y a beaucoup d'applications dans la topologie algébrique, la géométrie différentielle, la théorie de la représentation et dans d'autres sujets. Maintenant nous allons tirer des conséquences non-triviales dans la théorie des groupes finis soi-même.

Premièrement on va donner une condition suffisante pour qu'un sous-groupe soit normal, une généralisation du fait que si l'index d'un sous groupe est $(G : H) = 2$ alors $H \lhd G$. La preuve utilise l'action de G (et donc de H) sur G/H.

Proposition 7.1. *Soit $H < G$ tel que $p := (G : H)$ est le plus petit diviseur premier de $O(G)$. Alors $H \lhd G$.*

Preuve. Le groupe G agit sur $X := G/H$ par multiplication à gauche, alors son sous-groupe H agit aussi sur G/H par restriction et le plus petit diviseur premier de $O(H) \geq p$. Le translaté gH est un point fixe pour cette H-opération si et seulement si $hgH = gH$ pour chaque $h \in H$, donc si et seulement si $g^{-1}hg \in H$ ou $g \in N_G(H)$ (le normalisateur de H). Donc

$$|X^H| = |N_G H/H| = (N_G H : H) \geq 1$$

et

$$|X| - |X^H| = (G : H) - (N_G H : H) < p.$$

Par Lemme 6.1 on obtient que $X = X^H$, donc $N_G H = G$ et $H \lhd G$. □

Exercice 7.1. Soient $H < G$, $O(H) = m$, $O(G) = mk$ tel que le plus petit diviseur premier de m est $\geq k$. Montrer que $H \lhd G$.

Par exemple, si $O(G) = 140$ et $O(H) = 35$ donc $H \lhd G$.

Exercice 7.2. Soit G un groupe d'ordre 245 et X un G-ensemble d'ordre 244 et de 49 orbites. Montrer l'existence d'un point fixe.

7.1. **Action par conjugaison.** La deuxième application de l'équation de classe utilise l'action d'un groupe sur soi-même par conjugaison :

$$g \odot x := gxg^{-1},$$

pour $g \in G$ et $x \in X := G$.

Vérification : On a $\mathbf{1} \odot x = x$ et

$$g_1 \odot (g_2 \odot x) = g_1(g_2 \odot x)g_1^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = (g_1 g_2) \odot x,$$

et donc $(g, x) \mapsto g \odot x$ est vraiment une G-opération sur G.

Les G-orbites pour cette opération sont appelées *classes de conjugaison.* L'élément $x \in G$ est un point fixe pour cette action si et seulement si $gx = xg$ pour chaque g si et seulement si x est dans le centre $Z(G)$ de G. Le stabilisateur de $x \in X = G$ est appelé le *centralisateur* de x

$$\mathrm{Stab}(x) = \{g \in G; gx = xg\}.$$

Exemple 7.1. Soit $G = \mathbf{U}(n)$ le groupe des matrices unitaires. Dans le cours de l'algèbre linéaire on démontre que pour chaque $u \in G$ il existe un $v \in G$ tel que $v^{-1}uv = \Lambda$, où Λ est une matrice diagonale. En fait, on peut prendre pour la i-ème colonne de v un vecteur propre de u avec valeur propre Λ_{ii}. Si $f(t)$ est un polynôme unitaire de degré n dont tous les zéros sont de valeur absolue 1, alors il existe une seule classe de conjugaison dans G ayant $f(t)$ comme polynôme caractéristique. Donc il y a une bijection entre les classes de conjugaison de G et les polynômes unitaire de degré n dont chaque zéro est de valeur absolue 1.

On va utiliser l'action par conjugaison dans la preuve de la proposition suivante.

Proposition 7.2. *Soit P un groupe fini d'ordre p^r, où p est un nombre premier et $r > 0$. Alors le centre $Z(P)$ de P a au moins p éléments.*

L'ordre de $Z(P)$ n'est pas p^{r-1}, car sinon P n'est pas abélien et $P/Z(P)$ est cyclique. Mais, si P n'est pas abélien, alors $P/Z(P)$ n'est pas cyclique.

Preuve. Considérons l'action de P sur soi-même par conjugaison. Les points fixes forment le centre, donc $|P| - |Z(P)|$ est divisible par p, par Lemme 6.2. Donc p divise $|Z(P)|$. Mais le neutre est dans le centre, donc ils existent encore au moins $p-1$ autres éléments dans $Z(P)$.

Supposons que $P/Z(P)$ est cyclique de générateur $vZ(P)$, pour un $v \in P$. Donc pour chaque $x, y \in P$ ils existent $i, j \in \mathbb{Z}$ et $c_1, c_2 \in Z(P)$ tels que

$$x = v^i c_1 \text{ et } y = v^j c_2.$$

Donc

$$xy = v^i c_1 v^j c_2 = v^i v^j c_1 c_2 = v^{i+j} c_2 c_1 = v^j v^i c_2 c_1 = v^j c_2 v^i c_1 = yx,$$

parce que c_1 et c_2 commutent avec tous les éléments du groupe. Alors P est abélien et $P = Z(P)$.

Supposons que $|Z(P)| = p^{r-1}$, donc P n'est pas abélien. Le groupe quotient $P/Z(P)$ est cyclique d'ordre p, donc P est abélien. Contradiction. □

Exercice 7.3. Montrer qu'un group d'ordre p^2 est abélien, isomorphe à C_{p^2} ou à $C_p \times C_p$.

Exemple 7.2. Groupes d'ordre p^3 ne sont pas nécessairement abélien. Par exemple le groupe D_4 (isomorphe à $U(3, \mathbb{F}_2)$) d'ordre 8. Un autre exemple est le groupe des quaternions de Hamilton : $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ avec le centre $\{1, -1\}$ et les multiplications

$$i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik.$$

Q (six éléments d'ordre 4) n'est pas isomorphe à D_4 (seulement deux éléments d'ordre 4).

Exercice 7.4. Montrer qu'un groupe d'ordre p^s est résoluble.

7.2. **Théorème de Cauchy.** La troisième application est le théorème de Cauchy qui dit que pour chaque diviseur premier de l'ordre du groupe il existe un élément de tel ordre. Ce résultat est très utile. La preuve utilise aussi des actions.

Théorème 7.1 (Cauchy)**.** [16] *Soit G un groupe fini et soit p un diviseur premier de $|G|$. Alors le groupe contient au moins un élément d'ordre p.*

[16] Augustin-Louis Cauchy, mathématicien français, 1789-1857.

Soit n_p le nombre d'éléments de G d'ordre p et soit N_p le nombre de sous-groupes de G d'ordre p. Alors $n_p + 1$ et $N_p - 1$ sont divisible par p et $n_p = N_p(p-1)$, donc n_p est divisible par $p-1$.

Preuve. Dans cette preuve ce n'est pas G qui agit, mais un groupe cyclique $P =< \sigma >$ d'ordre p. Définissons sur l'ensemble

$$Y := \{(g_1, g_2, \ldots, g_p) \in G^p;\ g_1 g_2 \ldots g_p = \mathbf{1}_G\}.$$

une P-action par

$$\sigma \bullet (g_1, g_2, \ldots, g_p) := (g_2, g_3, \ldots, g_p, g_1),$$

la permutation cyclique des coefficients. Donc en effet σ^p agit trivialement, et si $g_1 g_2 \ldots g_p = \mathbf{1}$, alors

$$g_2 g_3 \ldots g_p g_1 = g_1^{-1} g_1 g_2 \ldots g_p g_1 = \mathbf{1}.$$

On va identifier les points fixes. On a que $(g_1, g_2, \ldots, g_p) \in Y^P$ si et seulement si

$$(g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

donc $g_1 = g_2 = g_3 = \ldots = g_p$, disons g, et $g_1 g_2 \ldots g_p = gg \ldots g = g^p = \mathbf{1}$. Donc

$$Y^P = \{(g, g, \ldots, g \in G^p); g^p = 1\}.$$

Si $g^p = 1$ alors $O(g) = p$ ou $O(g) = 1$ (c.-à-d. $g = \mathbf{1}_G$), parce que p est premier. D'où

$$|Y^P| = |\{g \in G;\ g^p = \mathbf{1}\}| = 1 + n_p.$$

L'application

$$\pi : Y \longrightarrow G^{p-1} :\ (g_1, g_2, \ldots, g_p) \mapsto (g_1, g_2, \ldots, g_{p-1})$$

est une bijection, parce que $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$. Donc

$$|Y| = O(G)^{p-1}.$$

Par l'équation de classe (ou par Lemme 6.2) on obtient que

$$|Y| - |Y^P| = O(G)^{p-1} - (1 + n_p)$$

est divisible par p. Par l'hypothèse p divise $O(G)$, donc $n_p + 1$ est divisible par p. En particulier, $n_p > 0$ et il existe un élément d'ordre p.

L'intersection de deux sous-groupes différents d'ordre p est $\{\mathbf{1}\}$, chaque groupe d'ordre p contient exactement $p-1$ éléments d'ordre p et chaque élément x d'ordre p est dans un unique sous-groupe d'ordre p (le sous-groupe $< x >$). Donc $n_p = N_p(p-1)$ et $pN_p - N_p + 1$ est divisible par p, donc $N_p - 1$ est divisible par p. □

Nous allons maintenant donner une preuve alternative (aussi utilisant des actions) pour l'existence d'un élément d'ordre p. Nous allons utiliser l'exercice suivant.

Exercice 7.5. Soit G un groupe et $n \in \mathbb{Z}_{>0}$ un entier avec la propriété suivante. Pour chaque sous-groupe $H < G$ tel que $H \neq G$ on a que n divise l'index $(G : H)$. Montrer que pour chaque G-ensemble fini X on a que

$$|X| \equiv |X^G| \mod n.$$

Preuve alternative de l'existence d'un élément d'ordre p, si p divise $O(G)$. Nous allons utiliser une preuve par induction sur $O(G)$. Si $O(G) = p$, alors G est cyclique d'ordre p et donc il existe en effet un élément d'ordre p. Supposons en suite le résultat soit vrai pour les groupes d'ordre $< O(G)$.

Supposons alors que p est un diviseur premier de l'ordre de G. Supposons qu'il existe un sous-groupe $H < G$ tel que $H \neq G$ et p divise $O(H)$. Par l'hypothèse d'induction il existe un $h \in H$ tel que $O(h) = p$, mais $h \in G$ donc on a trouvé G un élément d'ordre p dans G. Donc la preuve serait complète.

Supposons, par contre, que pour chaque sous-groupe $H < G$ tel que $H \neq G$ on a que p ne divise pas $O(H)$. En conséquence, pour chaque sous-groupe propre H on a que p divise l'index $(G : H)$. Cela implique que pour chaque G-action et chaque orbite Orb telle que $|\,\mathrm{Orb}\,| > 1$ on a p divise $|\,\mathrm{Orb}\,|$. Considérons maintenant l'action de G sur soi-même par conjugaison. L'équation de classe nous donne

$$O(G) = O(Z(G)) + \sum_{C,|C|>1} |C|,$$

où la somme est sur les classes de conjugaison d'ordre > 1, et donc cette somme est divisible par p. On obtient que $O(Z(G))$ est aussi divisible par p, et il suit que $Z(G) = G$ et donc G est abélien (car, par hypothse, G est le seul sous-groupe de G dont l'ordre est divisible par p).

Ainsi on peut supposer, en plus, que G est un groupe abélien. Soit maintenant $g \in G$ non-trivial. Si $O(g) = np$ alors $O(g^n) = p$ et on est prêt. Supposons alors que p ne divise pas $O(g) =: n$, et donc aussi que $H :=< g >\neq G$. Le groupe G est abélien, donc $H \lhd G$ et G/H est un groupe d'ordre $O(G)/n < O(G)$ et encore divisible par p. Par l'hypothèse d'induction on conclut qu'il existe un $k \in G$ tel que le translaté kH est d'ordre p dans le groupe quotient G/H, c-à-d, $kH \neq H$ et $k^pH = H$.

Parce que p et n sont relativement premier, il existe des entiers $a, b \in \mathbb{Z}$ tel que $1 = an + bp$. On a que $k^nH \neq H$, car sinon on aurait $k^nH = H$ et $kH = k^{an+bp}H = (k^nH)^a(k^pH)^b = H$, mais $kH \neq H$.

$k^pH = H$ implique qu'il existe un r tel que $k^p = g^r$ et donc $k^{np} = g^{rn} = 1$, car $n = O(g)$. Mais $k^nH \neq H$ implique que $k^n \notin H$, donc $k^n \neq 1$. On conclut que $O(k)$ divise np mais ne divise pas n, alors est de la forme $O(k) = mp$. Il suit que k^m est de l'ordre p et donc G contient un élément d'ordre p. □

Exercice 7.6. Si $7|O(G)$ et n_7 dénote le nombre d'éléments d'ordre 7, alors $n_7 \equiv 6 \mod 42$.

Calculer le nombre d'éléments d'ordre 7 dans Alt_7 et vérifier que c'est 6 modulo 42.

Exercice 7.7. Soit P un groupe d'ordre p^s et $t \leq s$. Utiliser le théorème de Cauchy et Proposition 7.2 pour montrer que P contient un sous-groupe d'ordre p^t.

Exercice 7.8. Considérons le groupe $G = \mathrm{GL}(3, \mathbb{F}_2)$. Montrer que $O(G) = 168$.

Posons

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ g_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ g_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix};\ g_4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix};$$

$$g_7 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} ; \; g_7^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Montrer que $O(g_i) = i$.

Si $C_G(x) = \{g \in G; gxg^{-1} = x\}$ est le centralisateur de $x \in G$, montrer que

$$C_G(g_1) = G; C_G(g_3) =< g_3 >; C_G(g_4) =< g_4 >; C_G(g_7) =< g_7 >=< g_7^{-1} >= C_G(g_7^{-1})$$

et

$$C_G(g_2) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} ; \; a, b, c \in \mathbb{F}_2 \}.$$

Posons n_i pour le nombre d'éléments de G d'ordre i. Montrer que

$$n_1 = 1, n_2 = 21, n_3 = 56, n_4 = 42, n_7 = 48$$

et $n_i = 0$ si $i \notin \{1, 2, 3, 4, 7\}$.

Montrer que les polynómes caractéristiques de g_7 et g_7^{-1} sont différents, et montrer qu'il y a deux classes de conjugaison d'éléments d'ordre 7, et six classes de conjugaison en total.

7.3. **Produits semi-direct.** [17] Les actions peuvent aussi être utiles pour construire ou décomposer des groupes. Si un groupe G opère sur un autre groupe N par des automorphismes on peut construire un produit semi-direct. Plus précisément, soit G et N deux groupes et

$$\phi : \; G \longrightarrow \operatorname{Aut} N$$

un homomorphisme de groupes (comparez avec le théorème de Cayley généralisé). Nous définissons le *produit semi-direct*

$$N \rtimes_\phi G$$

de N et G. L'ensemble de ce groupe est le produit cartésien $N \times G$ et l'opération interne est définie par

$$(n_1, g_1) \circ (n_2, g_2) := (n_1 \cdot [\phi(g_1)](n_2), g_1 g_2) \in N \times G.$$

Lemme 7.1. *$N \rtimes_\phi G$ est un groupe.*

Preuve. On a que $\phi : \; G \longrightarrow \operatorname{Aut} N$ est un homomorphisme de groupes. Alors pour $g_1, g_2 \in G$ et $n_1, n_2 \in N$ on a

$$[\phi(g_1)](n_1 n_2) = [\phi(g_1)](n_1) \cdot [\phi(g_1)](n_2) \tag{3}$$

(parce que $\phi(g_1)$ est un automorphisme de N) et

$$[\phi(g_1 g_2)](n_1) = [\phi(g_1) \circ \phi(g_2)](n_1) = [\phi(g_1)]([\phi(g_2)](n_1)) \tag{4}$$

(parce que ϕ est un homomorphisme et l'opération interne de $\operatorname{Aut} N$ est la composition d'applications).

[17] Ne fait pas partie de la matière examen

Vérifions maintenant l'associativité.

$$\begin{aligned}
&((n_1, g_1) \circ (n_2, g_2)) \circ (n_3, g_3) = \\
&= (n_1 \cdot [\phi(g_1)](n_2), g_1 g_2) \circ (n_3, g_3) \\
&= (n_1 \cdot [\phi(g_1)](n_2) \cdot [\phi(g_1 g_2)](n_3), g_1 g_2 g_3) \\
&= (n_1 \cdot [\phi(g_1)](n_2) \cdot [\phi(g_1)]([\phi(g_2)](n_3)), g_1 g_2 g_3) \text{ par (4)} \\
&= (n_1 \cdot [\phi(g_1)](n_2 \cdot [\phi(g_2)](n_3)), g_1 g_2 g_3) \text{ par (3)} \\
&= (n_1, g_1) \circ (n_2 \cdot [\phi(g_2)](n_3), g_2 g_3) \\
&= (n_1, g_1) \circ ((n_2, g_2) \circ (n_3, g_3)).
\end{aligned}$$

□

Exercice 7.9. Montrer que $(\mathbf{1}_N, \mathbf{1}_G)$ est le neutre de $N \rtimes_\phi G$, et trouver l'inverse de (n, g).

Définissons $A := \{(n, \mathbf{1}_G);\ n \in N\}$ et $B := \{(\mathbf{1}_N, g);\ g \in G\}$. Montrer que $A \lhd (N \rtimes_\phi G)$, $B < (N \rtimes_\phi G)$, $A \cap B = \{(\mathbf{1}_N, \mathbf{1}_G)\}$ et $AB = N \rtimes_\phi G$.

On peut caractériser les groupes qui sont isomorphes aux produits semi-directs. Le résultat principal est le suivant (comparez avec le deuxième théorème d'isomorphisme).

Proposition 7.3. *Supposons que H est un groupe avec deux sous-groupes A et B tels que $A \lhd H$, $A \cap B = \{\mathbf{1}_H\}$ et $AB = H$. Définissons $\phi : B \longrightarrow \operatorname{Aut} A$ par $\phi(b)(a) := bab^{-1}$. Alors $H \simeq (A \rtimes_\phi B)$.*

Preuve. L'application $\psi :\ A \rtimes_\phi B \longrightarrow H$ définie par

$$\psi(a, b) := ab$$

est un homomorphisme de groupes, parce que

$$\begin{aligned}
\psi((a_1, b_1) \circ (a_2, b_2)) &= \psi((a_1 \cdot [\phi(b_1)](a_2), b_1 b_2)) = a_1 \cdot [\phi(b_1)](a_2) \cdot b_1 b_2 = \\
&= a_1 \cdot b_1 a_2 b_1^{-1} \cdot b_1 b_2 = a_1 b_1 a_2 b_2 = \psi((a_1, b_1))\psi((a_2, b_2)).
\end{aligned}$$

C'est surjectif, parce que $H = AB$ et injectif parce que (a_1, b_1) est dans le noyau si et seulement si $a_1 b_1 = \mathbf{1}_H$, ou $a_1 = b_1^{-1}$, donc $a_1 \in A \cap B = \{\mathbf{1}_H\}$. Donc ψ est un isomorphisme de groupes. □

Exercice 7.10. Soit K un corps et B le groupe des matrices triangulaire supérieure inversibles, T le groupe des matrices diagonale inversibles et U le groupe des matrices triangulaire supérieure unitaires. Si $n = 3$:

$$B = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix};\ T = \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix};\ U = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

Montrer que B est un produit semi-direct de T et U.

Chaque groupe d'ordre pq est un produit semi-direct, où $p \neq q$ sont deux nombres premier.

Proposition 7.4. *Soit G un groupe d'ordre pq, où $p < q$ sont deux nombres premiers.*
Alors il existe un homomorphisme $\phi : C_p \longrightarrow \operatorname{Aut} C_q$ tel que

$$G \simeq C_q \rtimes_\phi C_p.$$

Si G est abélien, alors G est cyclique. Si p ne divise pas $q-1$, alors G est abélien et donc cyclique.

Preuve. Par le théorème de Cauchy il existe un sous-groupe $B < G$ d'ordre p et un sous-groupe $A < G$ d'ordre q. L'index de $(G : A) = p$ est le plus petit diviseur premier de $|G|$, donc $A \lhd G$ par Proposition 7.1. On a $A \cap B = \{\mathbf{1}_G\}$ et $AB = G$. Donc avec $\phi : B \longrightarrow \operatorname{Aut} A$ défini par $\phi(b)(a) := bab^{-1}$ on a $G \simeq A \rtimes_\phi B$, par le résultat plus haut. On a que G est abélien si et seulement si ϕ est trivial (ça veut dire $\phi(g) = \mathbf{1}$ pour chaque g) (exercice : montrer ça). Ici le groupe A est cyclique d'ordre q, disons avec générateur a. Alors $\phi(a)$ est aussi un générateur, donc il existe un unique $1 \leq i < q$ tel que $\phi(a) = a^i$. Par contre, $a \mapsto a^i$, où $1 \leq i < q$, définit un automorphisme de A. Donc $O(\mathrm{Aut}(A)) = q - 1$. Si ϕ n'est pas trivial, alors l'image $\phi(B)$ n'est pas trivial, donc isomorphe à B (parce que B est isomorphe au groupe cyclique d'ordre p, où p est premier). Donc $p = O(B)$ divise $O(\mathrm{Aut}(A)) = q - 1$. □

Remarque. Pour connaître les groupes non-abélien d'ordre pq il suffit de connaître $\operatorname{Aut} C_q$ et les homomorphismes $C_p \longrightarrow \operatorname{Aut} C_q$. Soit $C_q =< a >$, alors a^i est aussi un générateur si et seulement se i n'est pas divisible par q. Donc $\operatorname{Aut} C_q \simeq (\mathbb{Z}/q\mathbb{Z})^\times$. Nous avons démontré dans Proposition 4.6 que $(\mathbb{Z}/q\mathbb{Z})^\times$ est un groupe cyclique d'ordre $q-1$. Les homomorphismes $\phi : C_p \longrightarrow C_{q-1}$ sont déterminés par donner l'image d'un générateur (d'ordre p). Donc les homomorphismes non-triviaux sont en correspondance biunivoque avec les éléments d'ordre p de C_{q-1}. Si y est un générateur de C_{q-1} et $q - 1 = pm$, alors les éléments d'ordre p sont y^{im} où $1 \leq i < p$.

Exercice 7.11. Montrer directement que

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/210\mathbb{Z}.$$

mais que $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/420\mathbb{Z}$.

8. Théorèmes de Sylow

On a des résultats plus forts que celui de Cauchy, avec un peu plus de travail. Le résultat suivant n'est pas une curiosité, mais est fondamental. La plupart des preuves disponibles utilise des actions particulières.

Théorème 8.1 (Sylow). [18] *Soit G un groupe d'ordre $p^s m$, où $p \nmid m$ et p un nombre premier.*

(i) Pour chaque $1 \leq t \leq s$ il existe un sous-groupe $P < G$ d'ordre p^t.

(ii) Si P et Q sont deux sous-groupes de cardinalité p^s, alors il existe un $g \in G$ tel que

$$P = gQg^{-1}.$$

(iii) Soit N_{p^s} le nombre de sous-groupes de G de cardinalité p^s. On a que $N_{p^s} \equiv 1 \mod p$. Fixons un sous-groupe P d'ordre p^s. Alors $N_{p^s} = (G : N_G(P))$, donc N_{p^s} divise m.

Soit G un groupe d'ordre $p^s m$, où $p \nmid m$ et p premier. Un sous-groupe d'ordre p^s est appelé un *p-Sylow sous-groupe.*

Exercice 8.1. Chaque sous-groupe d'ordre p^t est contenu dans un p-Sylow-sous-groupe.

Exemple 8.1. Comme exemple d'utilisation du théorème de Sylow on va montrer qu'il n'existe pas un groupe simple d'ordre 36. Donc soit G un groupe d'ordre 36.

Si N_9 dénote le nombre de 3-Sylow sous-groupes, on a que $N_9 - 1$ est divisible par 3 et N_9 divise $36/9 = 4$. Donc $N_9 = 1$ ou 4. Si $N_9 = 1$, alors il existe un seul 3-Sylow-sous-groupe, donc est normal et propre et G n'est pas simple. Sinon on a quatre 3-Sylow-sous-groupes, donc l'action transitive par conjugaison sur l'ensemble des 3-Sylow-sous-groupes donne un homomorphisme non-trivial $\phi : G \longrightarrow S_4$ avec un noyau N. Alors $(G : N)$ divise $|S_4| = 24$ et donc $N \neq \{\mathbf{1}_G\}$. Alors G a un sous-groupe normal propre et G n'est pas simple.

Exercice 8.2. Il n'existe pas un groupe simple d'ordre 42, 84, 126, 140, ou 280. Indice: Montrer qu'il existe un sous-groupe normal de sept éléments.

Exercice 8.3. On connaît essentiellement les groupes d'ordre ≤ 15 :

Il existe essentiellement seulement un groupe d'ordre 1, 2, 3, 5, 7, 11, 13, 15 (le groupe cyclique).

Il existe seulement deux groupes non-isomorphes d'ordre 4, 6, 9, 10, 14.

Il existe seulement cinq groupes non-isomorphes d'ordre 8 (les groupes C_8,$C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 et Q ne sont pas isomorphes) et aussi cinq groupes non-isomorphes d'ordre 12.

(Indice pour ordre 12. Un 3-Sylow P_3 est C_3, un 2-Sylow P_2 est C_4 ou $C_2 \times C_2$. On a $N_3 = 1$ ou 4 et $N_4 = 1$ ou 3. G est abélien si et seulement si $N_4 = N_3 = 1$: deux possibilités. Si $N_3 = 1$ et $N_4 \neq 1$, alors $P_3 \lhd G$ et $G \simeq P_3 \rtimes_\phi P_2$ pour un homomorphisme non-trivial $\phi : P_2 \longrightarrow \operatorname{Aut} P_3$: ça donne aussi deux possibilités différents. Si $N_4 = 1$ et $N_3 \neq 1$, alors $P_2 \lhd G$ et $G \simeq P_2 \rtimes_\phi P_3$ pour un homomorphisme non-trivial $\phi : P_3 \longrightarrow \operatorname{Aut} P_2$; seulement possible si $P_2 \simeq C_2 \times C_2$: ça donne un groupe. Le cas $N_4 = 3$ et $N_3 = 4$ est impossible : sinon on aurait un élément d'ordre 1, huit éléments d'ordre 3 et au moins cinq éléments d'ordre deux ou quatre : c'est trop.)

[18] L. Sylow (1832-1918), mathématicien norvégien, voir http://www.gap-system.org/ history/Biographies/Sylow.html.

Exercice 8.4. Chaque groupe d'ordre p^2q possède un sous-groupe normal propre, où p, q sont des nombres premiers.

8.1. **Première preuve du théorème de Sylow.** Nous allons briser la preuve du théorème en deux parties.

Preuve d'existence de p-Sylow sous-groupes. Nous allons utiliser induction sur $O(G)$; si $O(G) = 1$ il n'y a rien à montrer. Supposons l'existence d'un p-Sylow sous-groupe pour les groupes d'ordre plus petit que $O(G) = p^s m$, où $p \not| m$.

Soit X la collection des éléments d'ordre p de G. On laisse G agir sur X par conjugaison. Par le théorème de Cauchy on a que

$$|X| = n_p \equiv p - 1 \mod p.$$

Donc il existe au moins une orbite (classe de conjugaison) $\mathrm{Orb}(s)$ telle que p ne divise pas son ordre. Le stabilisateur de s est égal au centralisateur $C_G s$ et p ne divise pas $|\mathrm{Orb}(s)| = O(G)/O(C_G s)$; donc p^s divise l'ordre de $C_G s$.

Si $C_G s \neq G$ on conclut par induction que $C_G s$ a un sous-groupe d'ordre p^s, et on est prêt. Sinon, $< s > \lhd C_G s = G$ et par induction $G/ < s >$ contient un sous-groupe Q d'ordre p^{s-1}, parce que $O(G/ < s >) = p^{s-1}m$. Par le théorème de correspondance il existe un sous-groupe P contenant s tel que $Q = P/ < s >$ et alors $|P/ < s > | = p^{s-1}$. Donc par Lagrange on a $|P| = p^s$ et on a trouvé un p-Sylow sous-groupe. □

Pour finir la preuve de (i) on utilise Exercice 7.7.

La partie restante de la preuve du théorème de Sylow. On suppose encore que $O(G) = p^s m$, $p \not| m$. Premièrement, soit Y la collection des p-Sylow sous-groupes de G; on vient de montrer que Y n'est pas vide. Le groupe G agit sur Y par conjugaison et agit possiblement avec plusieurs orbites. On va montrer qu'il n'y a qu'une. Soit P un p-Sylow sous-groupe quelconque.

Soit X le G-orbite d'une des p-Sylow sous-groupes, disons Q; donc

$$X = \mathrm{Orb}(Q) = \{gQg^{-1}; g \in G\} \subseteq Y.$$

Le stabilisateur de Q pour cette G-action est exactement le normalisateur $N_G Q$ et $Q \lhd N_G Q$. Donc $|X| = O(G)/O(N_G Q)$ divise m et p ne divise pas $|X|$.

Par restriction, le groupe P agit aussi sur X par conjugaison. On a, par Lemma 6.2 car P est un p-groupe,

$$|X| \equiv |X^P| \mod p.$$

Parce que $p \not| |X|$, il suit que $p \not| |X^P|$ et qu'il existe un point fixe pour P sur X, disons le p-Sylow sous-groupe $Q_1 \in X$. Cela veut dire que pour chaque $p \in P$ on a $pQ_1p^{-1} = Q_1$, ou que $P \subseteq N_G Q_1$.

Par le deuxième théorème d'isomorphisme PQ_1 est un sous-groupe d'ordre

$$O(P)O(Q_1)/O(P \cap Q_1),$$

alors $O(PQ_1)$ est de la forme p^t où $t \geq s$. Mais s est le maximum possible. Il suit que $O(PQ_1) = O(P) = O(Q_1) = p^s$ et $P = Q_1$.

La conclusion est que P est l'unique point fixe dans chaque G-orbite X. Mais deux G-orbites différentes sont disjointes, donc il n'existe qu'une seule G-orbite sur Y. C'est à dire, si P et Q sont deux p-Sylow sous-groupes, alors il existe un $g \in G$ tel que $Q = gPg^{-1}$.

Il suit aussi que N_{p^s} (le nombre de p-Sylow sous-groupes) est égal à $O(G)/O(N_G P) = (G : N_G P)$ et donc divise $O(G)/O(P) = m$.

Et finalement P est le seul point fixe sur $X = Y$ pour l'action de P par conjugaison, donc encore une fois par Lemme 6.2 on a

$$N_{p^s} = |Y| \equiv |Y^P| = 1 \mod p.$$

□

8.2. **Une autre preuve du théorème de Sylow.** [19] Nous allons présenter une deuxième preuve du théorème de Sylow, en utilisant d'autre actions.

Nous aurons besoin d'un résultat plus général. Pour un ensemble X et un entier positif n nous notons

$$\binom{X}{n} := \{A \subset X;\ |A| = n\},$$

pour la collection des sous-ensembles de cardinalité n. Nous avons choisi cette notation parce que

$$\left|\binom{X}{n}\right| = \binom{|X|}{n}.$$

Si X est un G-ensemble avec l'opération $g \bullet x$, alors $\binom{X}{n}$ devient aussi un G-ensemble avec l'opération

$$g \bullet A := \{g \bullet a;\ a \in A\} \in \binom{X}{n}.$$

Lemme 8.1. *Soit X un ensemble de cardinalité $|X| = p^s m$, où $p \nmid m$ et p un nombre premier. Et soit P un groupe d'ordre p^r, pour un $r \in \mathbb{Z}$.*

(i) Alors $\binom{|X|}{p^s} \equiv m \mod p$.

(ii) Supposons que X est un P-ensemble. Alors il existe un sous-P-ensemble Y de X de cardinalité p^s.

(iii) En particulier, si $s = 0$, il existe un point fixe dans X pour l'opération de P.

Preuve. On a

$$\binom{|X|}{p^s} = \binom{p^s m}{p^s} = \prod_{i=0}^{p^s-1} \frac{p^s m - i}{p^s - i}.$$

Soit $0 < i < p^s$, alors on peut écrire $i = p^{t_i} n_i$, où $p \nmid n_i$ et $0 \leq t_i < s$. Donc

$$\frac{p^s m - i}{p^s - i} = \frac{p^{s-t_i} m - n_i}{p^{s-t_i} - n_i}.$$

Le translaté $(p^{s-t_i} - n_i) + p\mathbb{Z} = -n_i + p\mathbb{Z}$ n'est pas $0 + p\mathbb{Z}$, donc il existe un inverse

$$(-n_i + p\mathbb{Z})^{-1} = r_i + p\mathbb{Z}$$

dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors on peut calculer dans $\mathbb{Z}/p\mathbb{Z}$:

[19] Ne fait pas partie de la matière examen

$$\begin{aligned}\binom{|X|}{p^s}+p\mathbb{Z} &= m\prod_{i=1}^{p^s-1}\frac{p^{s-t_i}m-n_i}{p^{s-t_i}-n_i}+p\mathbb{Z}\\ &= (m+p\mathbb{Z})\prod_{i=1}^{p^s-1}\left((p^{s-t_i}m-n_i)+p\mathbb{Z}\right)\left((p^{s-t_i}-n_i)+p\mathbb{Z}\right)^{-1}\\ &= (m+p\mathbb{Z})\prod_{i=1}^{p^s-1}(-n_i+p\mathbb{Z})\,(-n_i+p\mathbb{Z})^{-1}\\ &= m+p\mathbb{Z}.\end{aligned}$$

En particulier $\left|\binom{X}{p^s}\right|$ n'est pas divisible par p. Donc si P opère sur X il existe un point fixe dans $\binom{X}{P^s}$ par Lemme 6.2. Donc il existe un sous-P-ensemble de X de cardinalité p^s. □

Maintenant nous pouvons donner la deuxième preuve du théorème de Sylow.

Preuve du théorème de Sylow. Dans chaque partie de la preuve on va utiliser une autre action.

(i) Le groupe G agit sur $X = G$ par $g \bullet x := gx$ (la multiplication du groupe). Donc G agit aussi sur $Y := \binom{G}{p^s}$. Soit $A \in Y$; alors A est un sous-ensemble de G de p^s éléments.

Si A est même un sous-groupe de G, alors $\mathrm{Orb}(A) = \{gA;\ g \in G\} = G/A \subset \binom{G}{p^s}$ est la collection des translatés de A par un élément de G, donc $|\,\mathrm{Orb}(A)| = (G : A) = m$.

Supposons que A n'est pas un translaté d'un sous-groupe. Soit $a \in A$, alors $\mathbf{1}_G \in a^{-1}A$. Si $g \in \mathrm{Stab}(a^{-1}A)$ alors $g\mathbf{1} = g \in a^{-1}A$, donc $\mathrm{Stab}(a^{-1}A) \subset a^{-1}A$. Par hypothèse $a^{-1}A$ n'est pas un sous-groupe de G donc $|\,\mathrm{Stab}(a^{-1}A)| < p^s$ (strict) et

$$|\,\mathrm{Orb}(A)| = |\,\mathrm{Orb}(a^{-1}A)| = \frac{|G|}{|\,\mathrm{Stab}(a^{-1}A)|} > \frac{p^s m}{p^s} = m$$

et $|\,\mathrm{Orb}(A)|$ divise $p^s m$. Alors p divise $|\,\mathrm{Orb}(A)|$.

Donc p divise $|\,\mathrm{Orb}(A)|$ si et seulement si A n'est pas un translaté d'un sous-groupe.

Soit $Y' \subset Y$ la collection des translatés des sous-groupes d'ordre p^s. Un tel sous-groupe a exactement m translatés. Donc $N_{p^s} = \frac{|Y'|}{m}$ et on vient de montrer que $|Y| - |Y'|$ est un p-multiple. Par le lemme p divise $|Y| - m$, donc p divise aussi $|Y'| - m$ et $N_{p^s} - 1$. En particulier, $N_{p^s} \geq 1$, alors il existe un sous-groupe d'ordre p^s.

Pour finir la preuve de (i) on utilise Exercice 7.7.

(ii) Soient P et Q deux sous-groupes de cardinalité p^s. Laissons G agir maintenant sur $X = G$ par conjugaison. Donc il y a aussi une G-opération sur $Y = \binom{G}{p^s}$ définie par $g \odot A := \{gag^{-1}; a \in A\}$. On peut interpréter P et Q comme éléments de Y. Soit

$$Z := \mathrm{Orb}_G(P) = \{gPg^{-1};\ g \in G\}$$

sa G-orbite. On a $\mathrm{Stab}_G(P) = N_G P > P$, donc $|Z| = |G|/|N_G P|$ divise m.

Par restriction on peut aussi considérer Z comme Q-ensemble. Le groupe Q a cardinalité p^s, donc par Lemme 6.2 il y a un point fixe dans Z, disons $A = g^{-1}Pg$, pour cette opération de Q. Donc gQg^{-1} fixe P, ça veut dire que $gQg^{-1} \subset N_G(P)$.

L'image $\nu_P(gQg^{-1})$ par l'application naturelle $\nu_P : \ N_G(P) \longrightarrow N_G(P)/P$ est un sous-groupe de $N_G(P)/P$, donc son ordre est un diviseur de m. Mais $\nu_P(gQg^{-1})$ est aussi un groupe quotient de gQg^{-1}, donc son ordre divise p^s. Donc l'image est trivial et $gQg^{-1} \subset P$. Mais les deux sous-groupes P et gQg^{-1} ont cardinalité p^s, donc

$$P = gQg_{-1}.$$

D'où (ii).

Et Z est l'ensemble des sous-groupes de cardinalité p^s, donc par définition $|Z| = N_{p^s}$. Alors $N_{p^s} = (G : N_G(P))$. Alors (iii). □

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