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_n. 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 isomorphe à $(\mathbb{F}_4, +)$).

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,

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

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).

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. 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 4.10. 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 4.11. 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 4.12. 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 $G' \subseteq \mathrm{Ker}\,\phi$.*

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 $S \subseteq \mathrm{Ker}\,\phi$, impliquant que $G' =< S >\subseteq \mathrm{Ker}\,\phi$, parce que $\mathrm{Ker}\,\phi$ est un sous-groupe de G. □

Exercice 4.13. 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

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

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

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 de l'équation $x^n + bx^{n-1} + \ldots$ sont des combinaisons des racines $x_1, x_2, \ldots$ qui ne dépendent pas de l'ordre des solutions (comme la somme ou la produit de toutes les solutions), donc invariants par toutes les permutations des solutions. D'où apparaît le groupe symétrique 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 $h \in H$.

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.

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

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 différents 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 $O(G) = (G : H) \cdot O(H)$.

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 !

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

Exercice 4.14. 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 4.15. 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 $O(x)$ divise $nq'r$ et donc q divise $q'r$ et $q'p = q$ 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 4.16. 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 inversible. Si $\phi(n)$ dénote le nombre des entiers entre 0 et n qui sont relativement premier 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 4.17. 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

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

Proposition 4.7. *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 $k \geq 2$.

Pour la preuve nous aurons besoin d'un lemme. On utilise la notation que

$$p^i || a \iff p^i | a \ \text{ et } p^{i+1} \not| a.$$

Lemme 4.6. *Soit p un nombre premier, $a \in \mathbb{Z}$ et $k \geq 1$. Si $p = 2$ on suppose que $k \geq 2$.*

(i) Si $p^k || (a - 1)$ alors $p^{k+1} || (a^p - 1)$.

(ii) Si $p \neq 2$, on a $p^k || \left((1 + p)^{p^{k-1}} - 1\right)$.

(iii) On a $2^k || (5^{2^{k-2}} - 1)$.

[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 !**

Preuve. (i) Par hypothèse, il existe un entier b, tel que $a-1=bp^k$ et $p \not| b$. Alors

$$a^p=(1+bp^k)^p=\sum_{i=0}^{p}\binom{p}{i}b^ip^{ki}=1+p\cdot bp^k+\sum_{i=2}^{p-1}\binom{p}{i}b^ip^{ki}+b^pp^{kp}.$$

Si $2\leq i\leq p-1$ on a $p|\binom{p}{i}$ (parce que p est premier) et

$$1+ki\geq 1+2k=k+(k+1)\geq k+2,$$

donc

$$p^{k+2}|\binom{p}{i}b^ip^{ki}.$$

Aussi $k(p-1)\geq 2$ (ici on utilise que $k\geq 2$ si $p=2$), donc $kp\geq k+2$ et

$$p^{k+2}|\ b^pp^{kp}.$$

La conclusion est qu'il existe un $c\in\mathbb{Z}$ tel que

$$a^p=1+bp^{k+1}+cp^{k+2}.$$

Donc $a^p-1=p^{k+1}(b+cp)$ et $p^{k+2}\not|(a^p-1)$, parce que sinon p divise $b+cp$ et b, ce qui n'est pas le cas. Alors $p^{k+1}||\,(a^p-1)$.

(ii) et (iii) sont des conséquences de (i). □

Preuve de Proposition 4.7. Soit $a\in\mathbb{Z}$, alors $a+p^k\mathbb{Z}\in(\mathbb{Z}/p^k\mathbb{Z})^\times$ si et seulement si $p\not|a$. Donc l'ordre de $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est p^k-p^{k-1}.

Le cas où $k=1$ est montré dans la dernière exercice. Soit $b\in\mathbb{Z}$, tel que $b+p\mathbb{Z}\in(\mathbb{Z}/p\mathbb{Z})^\times$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$; donc son ordre est $p-1$. Soit d l'ordre de $b+p^2\mathbb{Z}$ dans $(\mathbb{Z}/p^2\mathbb{Z})^\times$, alors par Lagrange $d|p(p-1)=O((\mathbb{Z}/p^2\mathbb{Z})^\times)$. On a $b^d\equiv 1 \mod p^2$, et certainement $b^d\equiv 1 \mod p$ et $(b+p\mathbb{Z})^d=(1+p\mathbb{Z})$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, donc $(p-1)|d$ (par exercice 4.15). Alors il y a deux possibilités : $d=(p-1)$ ou $d=p(p-1)$, parce que p est premier.

Si $d=(p-1)$, considérons $b\cdot(1+p)$. Modulo p cet élément $b\cdot(1+p)$ reste un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, donc par l'argument donné avant, l'ordre de $b\cdot(1+p)+p^2\mathbb{Z}$ est soit $(p-1)$, soit $p(p-1)$. Mais par le lemme $(1+p)^p\equiv 1 \mod p^2$, donc si $(b(1+p))^{p-1}\equiv 1 \mod p^2$ on aurait

$$(1+p)\equiv(b(1+p))^{p-1}(1+p)\equiv b^{p-1}(1+p)^p\equiv 1\cdot 1\equiv 1 \mod p^2,$$

ce qui est une contradiction. Donc en remplaçant b par $b(1+p)$ si nécessaire, on peut supposer que

$$p||(b^{p-1}-1)$$

et la classe de b est un générateur de $(\mathbb{Z}/p^2\mathbb{Z})^\times$.

Nous montrons par induction sur k que $b+p^k\mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^k\mathbb{Z})^\times$. Par construction, c'est déjà le cas si $k=1,2$. Soit d l'ordre de $b+p^k\mathbb{Z}$ dans $(\mathbb{Z}/p^k\mathbb{Z})^\times$, alors

$$b^d\equiv 1 \mod p^k\Rightarrow b^d\equiv 1 \mod p^{k-1}.$$

Il suit que d est divisible par l'ordre de $b+p^{k-1}\mathbb{Z}$ dans $(\mathbb{Z}/p^{k-1}\mathbb{Z})^\times$, ce qui est $p^{k-2}(p-1)$, par l'hypothèse d'induction. Donc on a soit $d=p^{k-1}(p-1)$ (et donc $b+p^k\mathbb{Z}$ est un générateur), soit $d=p^{k-2}(p-1)$. Mais le deuxième cas est impossible, car cela implique que $p^k|(b^{p^{k-2}(p-1)}-1)$, ce qui est en contradiction avec le lemme, qui dit que $p^{k-1}||(b^{p^{k-2}(p-1)}-1)$. □

Remarque. On montre de façon analogue que 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 $k \geq 3$. Est-ce que vous êtes capable de montrer ça en utilisant le (iii) du lemme ?

Et 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