TD Théorie des groupes

Mercedes Haiech

23 novembre 2020

Table des matières

1 TD1

1.1 Exo 1

Exercice 1.1. Pour chacun des couples suivants (ensemble, loi de composition), justifier s'il s'agit ou non d'un groupe.

1. $(\mathbf{Q}, *)$ avec $a * b = a + b + \alpha ab$ et $\alpha \in \mathbf{Q}$.
2. $(\{A \in \mathcal{M}_2(\mathbf{Z}) \mid \det(A) \neq 0\}, \cdot)$, où $\cdot$ est la multiplication usuelle pour les matrices.
3. $(\mathbf{Z}[X], +)$ (addition usuelle des polynômes).

Démonstration.

1. Si $\alpha = 0$ c'est un groupe, mais si $\alpha \neq 0$, alors l'élément $a = \frac{-1}{\alpha}$ n'a pas d'inverse.
2. C'est le groupe des inversibles que l'on note $\mathrm{Gl_n}(\mathbf{C})$. On vérifie les divers axiomes de groupe.
   (a) La loi est interne, car si $\det(A) \neq 0$ et $\det(B) \neq 0$ alors $\det(AB) \neq 0$.
   (b) La loi est associative.
   (c) L'élément neutre est la matrice identité.
   (d) Tout élément est inversible.

   On remarquera par contre que le groupe n'est pas commutatif.
3. C'est un groupe, il s'agit à nouveau de vérifier les divers axiomes.
   (a) La loi $+$ est une loi de composition interne.
   (b) La loi $+$ est associative (cela découle du fait que $+$ sur $\mathbf{Z}$ est associative).
   (c) L'élément neutre est l'application $0 : E \to \mathbf{Z}, x \mapsto 0$, et l'on vérifie que $f + 0 = 0 + f = f$.
   (d) L'inverse de f est donné par $g \colon E \to \mathbf{Z}, x \mapsto -f(x)$.
   (e) Le groupe est de plus abélien, cela découle du fait que $(\mathbf{Z}, +)$ est abélien.

□

1.2 Exo 2

Exercice 1.2. Soit $(G, *)$ un ensemble muni d'une loi de composition interne associative. On suppose de plus que :

1. $*$ admet un élément neutre à droite (il existe $e \in G$ tel que pour tout $x \in G$, on ait $x * e = x$)
2. tout élément $x \in G$ admet un symétrique à droite (i.e pour tout $x \in G$, il existe $x' \in G$ tel que $x * x' = e$).

Montrer que G est un groupe (on pourra commencer par montrer que l'inverse à droite est aussi un inverse à gauche).

Démonstration. Soit $x \in G$, il existe $x' \in G$ tel que $x * x' = e$. On va montrer que x' est aussi l'inverse à gauche de x. De plus, il existe $x'' \in G$ tel que $x' * x'' = e$. Par associativité $x = x * e = x * (x' * x'') = (x * x') * x'' = e * x''$. On a donc $x' * x = x' * (e * x'') = (x' * e) * x'' = x' * x'' = e$. On a bien montré que pour tout $x \in G$ il existe $x' \in G$ tel que $x * x' = x' * x = e$.

Montrons maintenant que $x*e = e*x = x$. Or $e*x = (x*x')*x = x*(x'*x) = x*e = x$.

Contre exemple : $(\mathbf{N}, *)$ où $a * b = a^b$. Alors $*$ est bien une loi de composition interne non associative, qui vérifie 1) et 2) puisque $a * 1 = a^1 = a$ et $a * 0 = a^0 = 1$ pour tout $a \in \mathbf{N}$ avec la convention $0^0 = 1$. □

1.3 Exo 3

Exercice 1.3. Soit X un ensemble de cardinal $|X| = 4$. Décrire toutes les lois de composition sur X qui en font un groupe.

1.4 Exo 4

Exercice 1.4. Soit $(G, *)$ un groupe dont tous les éléments vérifient $g^2 = e$.

1. Montrer que G est abélien et donner un exemple d'un tel groupe (non réduit à un élément).
2. Montrer que si G est fini, alors le cardinal de G est une puissance de 2 (*Indication : Montrer que G est muni d'une structure de $\mathbf{Z}/2\mathbf{Z}$ espace vectoriel.*)

Démonstration.

1. La condition $g^2 = e$ peut aussi se réécrire $g^{-1} = g$. Si l'on se donne $g, h \in G$, alors $gh = g^{-1}h^{-1} = (hg)^{-1} = hg$. Donc G est commutatif.
2. Le groupe quotient $\mathbf{Z}/2\mathbf{Z}$ et plus généralement les groupes $(\mathbf{Z}/2\mathbf{Z})^n$ sont de tels exemples. En fait, on peut montrer grâce au théorème de structure des groupes abéliens et de la question suivante que ce sont les seuls.
3. On munit G d'une structure de $Z/2Z$-espace vectoriel de la manière suivante : $\mathbf{Z}/2\mathbf{Z} \times G \to G, (a, g) \mapsto g^a$. On vérifie que les axiomes d'espace vectoriels sont vérifiés, en particulier, si $a, b \in \mathbf{Z}/2\mathbf{Z}$ et $g, h \in G$ que :
   (a) $1.g = g^1 = g$
   (b) $a(g * h) = (g * h)^a = g^a * h^a = (a.g) * (a.h)$
   (c) $(ab).g = g^{ab} = (g^a)^b = a.(b.g)$
   (d) $(a+b).g = a.g * b.g$. Dans ce dernier point, il faut être attentif car $1+1 = 0$ dans $\mathbf{Z}/2\mathbf{Z}$. On vérifie donc que l'égalité est vérifiée pour toutes les valeurs possibles de a et b et en particulier que $g^0 = e = g^{1+1[2]} = g^1 * g^1 = g^2$. Ce qui n'est vérifié que parce que $g^2 = e$ pour tout élément $g \in G$.

   Par ailleurs G est fini, donc en particulier de dimension finie n (il possède une famille génératrice finie constituée de tous les éléments de G). On en déduit que G est isomorphe en tant que $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel à $(\mathbf{Z}/2\mathbf{Z})^n$, ce qui prouve que le cardinal de G est une puissance de 2.

□

1.5 Exo 4 bis

Exercice 1.5. Soient G un groupe et $g \in G$. On définit une nouvelle loi par $x * y = xg^{-1}y$. Montrer que $(G, *)$ est encore un groupe et préciser le neutre et l'inverse d'un élément de G.

Démonstration. Vérifions que $*$ vérifie les propriétés d'une loi de groupe.

1. Puisque G est un groupe $*$ est bien une loi de composition interne.
2. La loi $*$ est associative. Soient $x, y, z \in G$:
$$x * (y * z) = x * yg^{-1}y = xg^{-1}yg^{-1}z = (x * y) * z$$
3. La loi $*$ admet un élément neutre qui est g.
$$x * g = xg^{-1}g = x$$
$$g * x = gg^{-1}x = x.$$
4. Tout élément x admet un inverse pour la loi $*$ qui est $gx^{-1}g$.
$$x * gx^{-1}g = xg^{-1}gx^{-1}g = g$$
$$gx^{-1}g * x = gx^{-1}gg^{-1}x = g$$

Donc $(G, *)$ est un groupe. □

1.6 Exo 5

Exercice 1.6. Soit $(G, *)$ un groupe.

1. Si pour tous $g, h \in G$ on a $(gh)^{-1} = g^{-1}h^{-1}$. Montrer que G est abélien
2. Si pour tous $g, h \in G$ on a $(gh)^2 = g^2h^2$. Peut-on conclure que G est abélien ?
3. On considère le groupe $G < \mathrm{GL}_3(\mathbf{Z}/3\mathbf{Z})$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale. Montrer que pour tous $g \in G$ on a $g^3 = 1$ (en particulier $(gh)^3 = g^3h^3$ pour tout $(g, h) \in G^2$). Le groupe G est-il abélien ?

Démonstration. 1. La formule nous donne en particulier $((gh)^{-1})^{-1} = (g^{-1}h^{-1})^{-1}$, d'où $gh = (h^{-1})^{-1}(g^{-1})^{-1} = hg$. Ainsi G est commutatif.

2. En développant l'égalité on obtient $ghgh = (gh)^2 = g^2h^2$. On multiplie a gauche par g^{-1} et à droite par h^{-1} pour obtenir $hg = gh$. Donc G est commutatif.

3. On peut trouver des groupes G non commutatifs vérifiant cette hypothèse. Soit G l'ensemble des matrices triangulaires supérieures de $\mathrm{Gl}_3(\mathbf{Z}/3\mathbf{Z})$ dont la diagonale est unitaire.

$$\text{Si } \; g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ alors } \; g^3 = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{Id}_3$$

Donc tout élément de G vérifie $g^3 = Id$ donc en particulier $(gh)^3 = g^3h^3$. Cependant G n'est pas commutatif, en effet :

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

alors que

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

□

1.7 Exo 6

Exercice 1.7. 1. L'ensemble $\{-1, 0, 1\}$ est-il un sous-groupe de $(\mathbf{Z}, +)$?

2. Soit $n \geqslant 1$. Montrer que $U_n := \{e^{\frac{2ik\pi}{n}} \mid k \in \mathbf{N}\}$ est un sous-groupe fini de $(\mathbf{C}^\times, \cdot)$. Montrer que la réunion des U_n forme un sous-groupe de $\mathbf{C}^\times$ qui est infini mais dont tous les éléments sont d'ordre fini.
3. Soit p un nombre premier. Montrer que $\{a + ib\sqrt{p} \mid (a, b) \in \mathbf{Z}\}$ est un sous-groupe de $(\mathbf{C}, +)$ et que $\{a + ib\sqrt{p} \mid (a, b) \in \mathbf{Q}^\times\}$ est un sous-groupe de $(\mathbf{C}^\times, \cdot)$

Démonstration. 1. $\{-1, 0, 1\}$ n'est pas un sous-groupe de $(\mathbf{Z}, +)$ car il ne contient pas $1 + 1 = 2$. Par contre, il s'agit bien d'un sous-groupe de $(\mathbf{Q}^\times, \cdot)$ (les axiomes sont facile à vérifier).

2. Les axiomes de sous-groupes sont faciles à vérifier. Soit $x = e^{\frac{2ik\pi}{n}} \in U_n$. On note $m \geqslant 1$ l'ordre de x. Puisque $x^m = 1$, cela implique $\frac{km}{n} \in \mathbf{N}$. Puisqu'il s'agit de l'ordre de x c'est le plus petit entier m non nul tel que $\frac{km}{n} \in \mathbf{N}$. On note $d = \mathrm{pgcd}(n, k)$. Ainsi, si $\frac{km}{n} \in \mathbf{N}$, il existe $a \in \mathbf{N}^\times$ tel que $mk = an$, soit encore $m\frac{k}{d} = a\frac{n}{d}$. En particulier $\frac{n}{d}$ divise $m\frac{k}{d}$ et est premier avec $\frac{k}{d}$. Donc $\frac{n}{d}$ divise m. Puisque m est le plus petit entier tel que $\frac{km}{n} \in \mathbf{N}$, la condition précédente impose que $m = \frac{n}{d}$. Donc l'ordre de x est $\frac{n}{\mathrm{pgcd}(n,k)}$.
Le groupe $U = \cup_{n \geqslant 1} U_n$ est un groupe infini dont chaque élément est d'ordre fini. Il peut aussi être interprété comme le quotient $\mathbf{Q}/\mathbf{Z}$.

3. Il faut vérifier les axiomes un par un de manière pédestre. Pour le deuxième exemple, on pourra utiliser le fait que $(\mathbf{C}, \cdot)$ est un groupe. On attire cependant l'attention sur le fait qu'il faut bien vérifier que l'inverse de $a + ib\sqrt{p}$ où $a, b \in \mathbf{Q}^\times$ est $\frac{a}{a^2+pb^2} - i\frac{b}{a^2+pb^2}\sqrt{p}$ qui est bien défini et un élément de $\{a + ib\sqrt{p} \mid (a, b) \in \mathbf{Q}, ab \neq 0\}$.

□

1.8 Exo 6 bis

Exercice 1.8. On considère l'ensemble $H = \{x + y\sqrt{3} \mid \ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$.

1. Montrer que H est un sous-ensemble de $\mathbb{R}_+^*$.
2. Soient u, v deux éléments de H. Montrer que leur produit uv (au sens du produit usuel sur $\mathbf{R}$) est dans H.
3. Soit u un élément de H, montrer que $\frac{1}{u}$ est dans H.
4. En déduire que H est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Démonstration.

1. Il s'agit de montrer que pour tout $x, y \in \mathbf{R}$, on a $x + y\sqrt{3} \in \mathbb{R}_+^*$. Soit encore que $x > -y\sqrt{3}$. Comme $x^2 - 3y^2 = 1$ alors $x^2 > 3y^2$, ce qui implique que $x > -\sqrt{3}y$.
2. On constate que le produit uv s'écrit bien sous la forme $x + y\sqrt{3}$. Si l'on note $z = x + y\sqrt{3}$ et $\bar{z} = x - y\sqrt{3}$, on constate que la condition $x^2 - 3y^2 = 1$ se réécrit $z\bar{z} = 1$. Ainsi $uv\overline{uv} = uv\bar{u}\bar{v} = u\bar{u}v\bar{v} = 1^2 = 1$. (Il faut néanmoins vérifier que $\overline{uv} = \bar{u}\bar{v}$.
3. Remarquons que $1/u = \frac{\bar{u}}{u\bar{u}} = \bar{u}$ puisque $u\bar{u} = 1$. Or $\bar{u} \in H$ puisque $\bar{\bar{u}} = u$.
4. On vérifie encore que $1 \in H$, et on a alors vérifié que H est un sous-groupe de $\mathbb{R}_+^*$.

□

1.9 Exo 7

Exercice 1.9. Soit H une partie non vide d'un groupe G qui est stable par la loi de groupe $(g, h \in H \Rightarrow gh \in H)$. Montrer que, si H est finie, H est alors un sous-groupe de G. Donner un exemple de couple (G, H) avec H multiplicativement stable mais où H n'est pas un sous-groupe de G.

Démonstration. La loi sur H déduite de la loi de groupe sur G est une loi de composition interne associative. Si l'on note e l'élément neutre de G, on va montrer que c'est un élément de H. Soit $h \in H$, et soit $f_h \colon \mathbf{N}^\times \to H, n \mapsto h^n$. Puisque l'ensemble H est fini, la fonction f_h n'est pas injective. En particulier, il existe deux entiers $n < m$ tels que $h^n = h^m$. Puisque $h \in G$ qui est un groupe, il admet un inverse h^{-1}. En multipliant l'égalité précédente par h^{-n}, on obtient $h^{m-n} = e$ où $m - n \geqslant 1$. Ainsi $e \in H$ et tout élément h de H possède un inverse qui est h^{m-n-1}.

Finalement H est un sous-groupe de G.

Contre-exemple : $\mathbf{N}$ est une partie de $(\mathbf{Z}, +)$ stable par addition mais n'est pas un sous-groupe de $\mathbf{Z}$. □

1.10 Exo 8

Exercice 1.10. Montrer en exhibant un exemple que la réunion de deux sous-groupes n'est en général pas un sous-groupe (on peut aussi montrer que si H et K sont deux sous-groupes d'un groupe G, alors $H \cup K$ est un sous-groupe si et seulement si $K \subset H$ ou $H \subset K$).

Démonstration.

1. Sans perdre de généralité, on peut supposer que $H \subset K$. Alors $H \cup K = K$ qui est bien un sous groupe de G.

Réciproquement, supposons que $K \not\subset H$ et $H \not\subset K$. Alors il existe $x \in H$ mais $x \notin K$ et $y \in K$ mais $y \notin H$. En particulier $x, y \in H \cup K$ mais $xy \notin H \cup K$. En effet, si tel était le cas, alors on aurait par exemple $xy \in H$, ce qui impliquerait $y \in H$ puisque $x \in H$, ce qui est absurde. Donc $H \cup K$ n'est pas un groupe.

2. Soit G un groupe et H, K deux sous-groupes de G tels que $G = H \cup K$, alors par la question précédente, on a $H \subset K$ ou $K \subset H$. Sans perte de généralité, on peut supposer $H \subset K$. Alors $G = K \cup H = K$. Donc G ne peut pas être la réunion de deux sous-groupes propres.
3. On prend $G = \mathbf{Z}$, $H = 2\mathbf{Z}$ et $K = 3\mathbf{Z}$, alors $2\mathbf{Z} \cup 3\mathbf{Z}$ n'est pas un sous-groupe de $\mathbf{Z}$ puisque 2 et 3 sont dans $\in 2\mathbf{Z} \cup 3\mathbf{Z}$ mais pas 2+3=5.

□

1.11 Exo 9

Exercice 1.11. En considérant les matrices

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

montrer que le produit de deux éléments d'ordres finis ne l'est pas nécessairement.

Démonstration. On constate que $A^4 = \mathrm{id}$ et que $B^6 = \mathrm{id}$. Cependant

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \text{ et } AB^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

□

1.12 Exo 10

Exercice 1.12. On considère G un groupe fini.

1. Montrer que si $|G|$ est pair, alors G contient un élément $g \neq 1$ avec $g^2 = 1$.
2. Montrer que, si G contient un élément d'ordre 2, alors il est d'ordre $|G|$ pair

Démonstration. 1. On apparie les éléments de G. À un élément $g \in G$, on associe la paire $E_g = \{g, g^{-1}\}$. L'ensemble E_g est de cardinal 2, sauf si $g = 1$ ou si $g^2 = 1$, de plus $G = \cup_{g \in G} E_g$. Soient $g_1, \cdots, g_r \in G$ tels que pour tout entiers i, j on ait $E_{g_i} \cap E_{g_j} = \varnothing$ et $G = \cup_{i=1}^{r} E_{g_i}$. Sans perdre de généralité, on peut supposer que $g_1 = 1$. Ainsi

$$|G| = 2n = \sum_{i=1}^{r} |E_{g_i}| = 1 + \sum_{i=2}^{r} |E_{g_i}|$$

Donc il existe un $j \neq 1$ tel que $|E_{g_j}| = 1$. En particulier $g_j^2 = 1$.

2. Si le théorème de Lagrange est vu, c'est une application directe.

   Démonstration sans Lagrange : On note h un élément non trivial tel que $h^2 = 1$. Pour $g \in G$, on pose $E_g = \{g, hg\}$. On constate que $G = \cup_{g \in G} E_g$ et que $E_g \cap E_{g'} \neq \varnothing$ si et seulement si $E_g = E_{g'}$. On choisit donc $g_1, \cdots, g_n \in G$ tels que

$$G = \cup_{i=1}^{n} E_{g_i}$$

   et $E_{g_i} \cap E_{g_j} \neq \varnothing$. Ainsi

$$|G| = \sum_{i=1}^{n} |E_{g_i}|$$

   Puisque tous les E_{g_i} sont de cardinal 2, on obtient bien que le cardinal de G est pair.

□

1.13 Exo 11

Exercice 1.13. Quel est le sous-groupe de $\mathbf{R}^\times$ engendré par l'ensemble des nombres premiers ? Montrer que $(\mathbf{Q}^\times, \cdot)$ n'est pas de type fini.

Démonstration. Montrons que le sous-groupe de $\mathbf{R}^\times$ engendré par l'ensemble des nombres premiers noté P est $\mathbf{Q}^\times$. En effet, tout élément de $\mathbf{Z}\backslash\{0\}$ s'écrit comme produit de nombres premiers, donc ensemblistement $\mathbf{Z}\backslash\{0\} \subset P$. Puisque P est un sous-groupe de $\mathbf{R}^\times$, il faut que tous les éléments de $\mathbf{Z}\backslash\{0\}$ aient un inverse. On obtient alors $\mathbf{Q}^\times \subset P$. Et comme $\mathbf{Q}^\times$ est un groupe, on a égalité puisque P est le plus petit sous-groupe de $\mathbf{R}^\times$ engendré par l'ensemble des nombres premiers.

Montrons que $(\mathbf{Q}^\times, \cdot)$ n'est pas de type fini. Supposons par l'absurde que

$$\mathbf{Q}^\times = \langle g_1, \cdots, g_n \rangle = \langle E \rangle.$$

Quitte à rajouter à E les dénominateurs des g_i, on peut supposer que $g_i \in \mathbf{Z}$. Quitte à rajouter au système de générateurs E les diviseurs premiers des g_i on peut supposer que les g_i sont premiers. Choisissons alors un nombre premier p qui n'apparait pas dans E. Alors ce nombre dans dans $\mathbf{Q}^\times$ mais ne peut pas s'écrire comme produit des éléments de E (qui sont premiers et différents de p). □

1.14 Exo 12

Exercice 1.14 (Groupe des quaternions)**.**

Soit les éléments de $\mathrm{GL}(2, \mathbf{C})$ suivants :

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Nous notons 1 la matrice identité de $\mathrm{GL}(2, \mathbf{C})$.

1. Montrer que : $I^2 = J^2 = K^2 = IJK = -1$.
2. En déduire que $\{\mathrm{id} = 1, -\mathrm{id} = -1, I, -I, J, -J, K, -K\}$ est le groupe d'ordre 8 engendré par I, J et K. Vérifier qu'il n'est pas abélien. Ce groupe est appelé **groupe des quaternions** et on le note Q_8.
3. Donner la liste des sous-groupes de Q_8.

Démonstration.

1. Les calculs sont immédiats.
2. À l'aide de la question 1. on vérifie que tout élément admet un inverse dans cet ensemble (par exemple $I^{-1} = -I$) et que l'ensemble est stable par produits : $IJ = K$, $JI = -K$, $IK = -J$, $KI = J$, $JK = I$, $KJ = -I$. Cela prouve aussi qu'il n'est pas abélien.
3. Par le théorème de Lagrange, on ne pourra trouver que des sous-groupes d'ordre 1, 2, 4 ou 8 (le sous-groupe d'ordre 8 étant Q_8).

   Le sous-groupe d'ordre 1 est l'identité.

   Celui d'ordre 2 est $\{\mathrm{id}, -\mathrm{id}\}$.

   Il y a plusieurs sous-groupes d'ordre 4 qui sont ceux engendrés par id et n'importe quel autre élément différent de $-\mathrm{id}$ à savoir : $\{\mathrm{id}, -\mathrm{id}, I, -I\}$, $\{\mathrm{id}, -\mathrm{id}, J, -J\}$, $\{\mathrm{id}, -\mathrm{id}, K, -K\}$.

□

1.15 Exo 13

Exercice 1.15 (Groupe libre)**.** Soit X un ensemble. À tout élément x de X, on associe un symbole x^{-1}. Et l'on note X^{-1} l'ensemble des x^{-1} pour x parcourant x. On va construire un ensemble $G(X)$ de la manière suivante : un élément de $G(X)$ est un mot, c'est-à-dire

une suite finie d'éléments de $X \cup X^{-1}$ne comprenant aucune séquence de deux termes consécutifs de la forme xx^{-1} ou $x^{-1}x$ pour $x \in X$. On va ajouter une loi de composition interne sur $G(X)$. On multiplie deux éléments (ou mots) de $G(X)$ en les concaténant puis en le réduisant, c'est-à-dire en éliminant les séquences xx^{-1} ou $x^{-1}x$ que l'on rencontre. On va définir l'élément neutre de $G(X)$ comme étant le mot vide.

1. Montrer que $G(X)$ avec la loi ainsi définie est un groupe.
2. Soit $f : X \to G$ une application ensembliste, montrez que l'on peut définir un morphisme de groupe $\tilde{f} : G(X) \to G$ qui vérifie $\tilde{f}(x) = f(x)$ pour tout $x \in X$.

1.16 Exo 14

Exercice 1.16. Soit G un groupe. On appelle centre du groupe et l'on note $\mathcal{Z}(G) := \{x \in G \mid \forall y \in G, xy = yx\}$. Montrer que $\mathcal{Z}(G)$ est un sous-groupe abélien de G et que si G possède un unique élément d'ordre deux, alors cet élément est dans $\mathcal{Z}(G)$.

Démonstration. On va montrer que $\mathcal{Z}(G)$ vérifie les axiomes des sous-groupes.

1. Si l'on note e l'élément neutre de G, il appartient à $\mathcal{Z}(G)$ car le neutre commute, par définition, à tout élément de G.
2. Soit $x \in \mathcal{Z}(G)$ et $y \in G$, alors $xy = yx$, donc en multipliant à gauche et à droite par x^{-1} on obtient $yx^{-1} = x^{-1}y$. Ce qui prouve que $x^{-1} \in \mathcal{Z}(G)$.
3. Soit maintenant $z \in \mathcal{Z}(G)$ et $y \in G$. Alors $zx^{-1}y = zyx^{-1} = yzx^{-1}$, ce qui prouve que $zx^{-1} \in \mathcal{Z}(G)$.

Ainsi $\mathcal{Z}(G)$ est bien un sous-groupe de G.

On suppose de plus que G possède un unique élément d'ordre 2 noté x. Soit $y \in G$, alors :

$$(y^{-1}xy)^2 = y^{-1}xyy^{-1}xy = y^{-1}x^2y = y^{-1}y = e.$$

Comme x est l'unique élément d'ordre deux, on a alors $y^{-1}xy = e$ ou $y^{-1}xy = x$. Le premier cas est impossible puisqu'il implique que $x = e$. Le deuxième cas implique $xy = yx$. Donc $x \in \mathcal{Z}(G)$. □

1.17 Exo 15

Exercice 1.17. Soit

$$\Gamma := \{\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbf{R}^\times\}.$$

Montrer que Γ muni de la loi de multiplication pour les matrices est un groupe mais que ce n'est pas un sous-groupe de $\mathrm{Gl}_2(\mathbf{R})$. Vérifier que Γ est isomorphe au groupe $(\mathbf{R}^\times, \cdot)$.

Démonstration. Soient $x, y \in \mathbf{R}^\times$.

$$\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} y & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xy & xy \\ 0 & 0 \end{pmatrix}$$

La multiplication est une loi de composition interne dont l'associativité découle de l'associativité de la multiplication sur $\mathbf{R}^\times$. L'élément neutre est donné par

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

et l'inverse de

$$\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}$$

est

$$\begin{pmatrix} \frac{1}{x} & \frac{1}{x} \\ 0 & 0 \end{pmatrix}.$$

Donc $(\Gamma, \cdot)$ est muni d'une structure de groupe mais ce n'est pas un sous-groupe de $\mathrm{Gl}_2(\mathbf{R})$ car ils n'ont pas le même élément neutre.

On considère le morphisme de groupe :

$$\begin{array}{rccc} \varphi\colon & \mathbf{R}^\times & \to & \Gamma \\ & x & \mapsto & \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}. \end{array}$$

Par définition de Γ, le morphisme φ est surjectif. Il est injectif car si l'on prend $x \in \mathrm{Ker}(\varphi)$, on a $\varphi(x) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ si $x = 1$. Donc φ est un isomorphisme de groupe. □

2 TD2

2.1 Exo 1

Exercice 2.1. Étant donnée une matrice a nous notons ${}^t a$ sa transposée. Pour chacune des applications suivantes, décider si elle est un morphisme et, dans le cas où c'est un morphisme, décider si celui-ci est injectif, surjectif et s'il est un isomorphisme. $n \geqslant 2$

1. $f\colon (\mathcal{M}_n(\mathbf{R}), +) \to (\mathcal{M}_n(\mathbf{R}), +)$, $a \mapsto a + {}^t a$.
2. $f\colon \mathrm{GL}_n(\mathbf{R}) \to \mathrm{GL}_n(\mathbf{R})$, $a \mapsto {}^t a$.
3. $f\colon \mathrm{GL}_n(\mathbf{R}) \to \mathrm{GL}_n(\mathbf{R})$, $a \mapsto {}^t a^{-1}$.
4. $f\colon \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^*$, $a \mapsto \det(a)$.
5. $f\colon \mathbf{C}^* \to \mathbf{R}^*$, $z \mapsto |z|$.

Démonstration.

1. Soient $A, B \in \mathcal{M}_n(\mathbf{R})$, alors $f(A+B) = (A+B) + (A+B)^t = f(A) + f(B)$. L'application f est donc un morphisme de groupe. Le morphisme f n'est pas injectif car n'importe quelle matrice antisymétrique est dans le noyau. Le morphisme f n'est pas surjectif car son image est incluse dans l'ensemble des matrices symétriques.
2. L'application n'est pas un morphisme de groupe. Si l'on choisit A et B deux matrices qui ne commutent pas entre elles $f(A^t B^t) = BA \neq AB = f(A^t) f(B^t)$. Par exemple dans $\mathrm{GL}_2(\mathbf{R})$ on peut choisir
$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, AB = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, BA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$
3. C'est un morphisme de groupe. En effet,
$$f(AB) = {}^t(AB)^{-1} = {}^t A^{-1 t} B^{-1} = f(A) f(B)$$
C'est un isomorphisme car $f^2 = \mathrm{id}$.
4. Soient $A, B \in \mathrm{GL}_n(\mathbf{R})$. Puisque le déterminant vérifie $\det(AB) = \det(A)\det(B)$, alors f est un morphisme de groupe Le morphisme est surjectif car si $x \in \mathbf{R}^*$ et si $A = \mathrm{Diag}(x, 1, \cdots, 1)$, alors $\det(A) = x$. Par contre, le morphisme n'est pas injectif car $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ont le même déterminant (égal à 1). En dimension supérieure à deux, on effectue une variation de cet exemple en complétant la matrice par l'identité.
5. Soient $x, y \in \mathbf{C}^*$, alors $|xy| = |x||y|$. L'application f est donc un morphisme de groupe. Le morphisme n'est pas surjectif car $-1 \notin f(\mathbf{C}^*)$ et il n'est pas injectif car $|-1| = |1|$.

□

2.2 Exo 2

Exercice 2.2. Soit $\varphi\colon G_1 \to G_2$ un morphisme de groupes.

1. Si g est un élément d'ordre fini de G_1, montrer que l'ordre de $\varphi(g)$ divise l'ordre de g.
2. On suppose que G_1 est engendré par l'ensemble de ses éléments d'ordre 2 et que G_2 est fini, d'ordre impair. Montrer que φ est trivial.

Démonstration.

1. Notons n l'ordre de g. Alors $\varphi(g)^n = \varphi(g^n) = \varphi(1) = 1$. Ainsi, l'ordre de $\varphi(g)$ divise n.

2. Puisque φ est un morphisme de groupe, il suffit de le déterminer sur une partie génératrice de G_1. Soit $g \in G_1$ un élément d'ordre deux. D'après la question précédente, $\varphi(g)$ divise l'ordre de g à savoir 2. Donc l'ordre de $\varphi(g)$ est 1 ou 2. Or cet ordre ne peut pas être 2 puisque cela impliquerait que G_2 est d'ordre pair. Donc $\varphi(g) = 1$. Finalement le morphisme φ est trivial.

□

2.3 Exo 3.a

Exercice 2.3. 1. Soit G un groupe à 4 éléments. Montrer que G est isomorphe soit au groupe cyclique $\mathbf{Z}/4\mathbf{Z}$, soit au groupe de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

2. Soit E un ensemble à 4 éléments. Déterminer toutes les lois de composition sur E qui en font un groupe (il y en a 16).

Démonstration. 1. Il faut faire la table du groupe. On note $\{1, a, b, c\}$ les éléments de G. Soit $a = b^{-1}$ (ou $a = c^{-1}$ mais à ce stade b et c sont interchangeables).
Si $a = b^{-1}$, alors $c^{-1} = c$. On vérifie alors que $a^2 = c$ car $a^2 = a$ est impossible ainsi que $a^2 = a^{-1}$ (car on aurait $a^3 = 1$ ce qui est impossible car l'ordre d'un élément doit diviser l'ordre du groupe). On en déduit alors que $a^3 = a^{-1}$.

	1	a	a^2	a^{-1}
1	1	a	a^2	a^{-1}
a	a	a^2	a^{-1}	1
a^2	a^2	a^{-1}	1	a
a^{-1}	a^{-1}	1	a	a^2

Ce qui est la table du groupe $\mathbf{Z}/4\mathbf{Z}$
Si $a = a^{-1}$, alors soit $b = c^{-1}$ ce qui nous ramène au cas précédent, soit $b = b^{-1}$ auquel cas $c = c^{-1}$. Alors $ab = c$ car le cas $ab = a$ implique $b = 1$, le cas $ab = b$ implique $a = 1$ et le cas $ab = 1$ implique $a = b^{-1} = a$, ce qui sont tous des cas absurdes. On montre de la même manière que $ba = c, ac = ca = b, bc = cb = a$.

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Ce qui est la table du groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

2. Notons $\{e_1, e_2, e_3, e_4\}$ les éléments de E. Il y a deux types de tables de groupe, ce sont celles ci-dessus. Il s'agit déjà de choisir parmi les éléments de E, un élément pour jouer le rôle de l'élément neutre ce qui donne 4 possibilités. Ensuite dans le cas isomorphe à $\mathbf{Z}/4\mathbf{Z}$, il faut choisir un autre élément de E pour jouer le rôle de a, ce qui donne 3 possibilités. Il y a donc 12 possibilités de loi de composition qui donnent un groupe isomorphe à $\mathbf{Z}/4\mathbf{Z}$.
Dans le cas $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, il n'y a aucun autre choix à faire que le choix de l'élément neutre. Ce qui donne 4 possibilités.
On a donc 16 possibilités en tout.

□

2.4 Exo 3

Exercice 2.4. Soient g et h deux éléments d'un groupe G.

(a) Montrer que les éléments g, g^{-1}, hgh^{-1} ont le même ordre. Plus généralement, si $\varphi \in \mathrm{Aut}(G)$, montrer que $\varphi(g)$ et g ont même ordre.

(b) Montrer que gh et hg ont le même ordre.
(c) Soit n un entier. Exprimer l'ordre de g^n en fonction de celui de g.
(d) On suppose que $gh = hg$, que $\langle g\rangle \cap \langle h\rangle = \{1\}$ et que g et h sont d'ordre fini n et m respectivement. Exprimer l'ordre de gh en fonction de n et de m.

Démonstration. (a) Soit $g \in G$ d'ordre n. On note m l'ordre de g^{-1} et k celui de hgh^{-1}. Alors $(g^{-1})^n = (g^n)^{-1} = 1$, donc $m|n$. On peut inverser les rôles de g et g^{-1}. Ainsi $g^m = ((g^{-1})^m)^{-1} = 1$. Donc $n|m$. Finalement g et g^{-1} ont le même ordre.
Par ailleurs $(hgh^{-1})^n = hg^nh^{-1} = 1$. Donc $k|n$. Et $g^k = h^{-1}(hgh^{-1})^k h = 1$. Donc $n|k$ et les éléments g et hgh^{-1} ont le même ordre.
Plus généralement, soit $\varphi \in \mathrm{Aut}(G)$. On note m l'ordre de $\varphi(g)$ Alors $\varphi(g)^n = \varphi(g^n) = 1$. Donc $m|n$. Et $g^m = \varphi^{-1}(\varphi(g)^m) = 1$. Donc $n|m$. Ainsi g et $\varphi(g)$ ont le même ordre.

(b) On note n l'ordre de hg et m l'ordre de gh. Puisque $(hg)^n = 1$ en multipliant à gauche par g et à droite par h on obtient $(gh)^{n+1} = gh$. Soit encore $(gh)^n = 1$. Ainsi $m|n$. De la même manière, on montre que $n|m$, ce qui prouve que gh et hg ont le même ordre.

(c) On note k l'ordre de g. Montrons que $o(g^n) = \frac{k}{\mathrm{pgcd}(n,k)}$. Puisque $\frac{nk}{\mathrm{pgcd}(n,k)}|k$, alors on a bien $(g^n)^{\frac{k}{\mathrm{pgcd}(n,k)}} = 1$, soit encore $o(g^n)|\frac{k}{\mathrm{pgcd}(n,k)}$. Soit maintenant un entier $m > 0$ tel que $(g^n)^m = 1$. Puisque k est l'ordre de g l'on a $k|nm$, soit encore, il existe $a \in \mathbf{N}^*$ tel que $mn = ak$. On a même $m\frac{n}{\mathrm{pgcd}(n,k)} = a\frac{k}{\mathrm{pgcd}(n,k)}$. Ainsi puisque $\frac{n}{\mathrm{pgcd}(n,k)}$ et $\frac{k}{\mathrm{pgcd}(n,k)}$ sont premier entre eux, on en déduit que $\frac{k}{\mathrm{pgcd}(n,k)}|m$. Ceci vaut en particulier si $m = o(g^n)$. Finalement, l'on a bien montré que $o(g^n) = \frac{k}{\mathrm{pgcd}(n,k)}$.

(d) On va montrer que $o(gh) = \mathrm{ppcm}(n,m)$. On remarque que

$$(gh)^{\mathrm{ppcm}(n,m)} = h^{\mathrm{ppcm}(n,m)}g^{\mathrm{ppcm}(n,m)} = 1$$

(puisque g et h commutent. Ainsi $o(gh)|\mathrm{ppcm}(n,m)$. Par ailleurs soit $k > 0$ tel que $(gh)^k = 1$. En particulier $g^kh^k = 1$ donc $g^k = h^{-k}$. Ainsi $g^k \in \langle g\rangle \cap \langle h\rangle$ et donc $g^k = 1$. De même $h^k = 1$. Ainsi $n|k$ et $m|k$ ce qui implique que $\mathrm{ppcm}(n,m)|k$. Finalement on a bien montré que $o(gh) = \mathrm{ppcm}(n,m)$

□

2.5 Exo 4

Exercice 2.5. Soit φ un morphisme d'un groupe fini $(G, *)$ vers $(\mathbb{C}^*, \times)$. On suppose que φ n'est pas une application constante. Calculer

$$\sum_{x\in G} \varphi(x)$$

Démonstration. Puisque φ n'est pas une application constante il existe $y \in G$ tel que $\varphi(y) \neq 1$.

$$\sum_{x\in G} \varphi(x) = \sum_{xy\in G} \varphi(xy) = \sum_{x\in G} \varphi(xy) = \varphi(y)\sum_{x\in G} \varphi(x)$$

On en déduit donc, puisque $\varphi(y) \neq 1$ que $\sum\limits_{x\in G} \varphi(x) = 0$. □

2.6 Exo 5

Exercice 2.6. Soit G un groupe tel que $\mathrm{Aut}(G) = \{1\}$. On veut montrer que G est d'ordre au plus deux.

1. Montrer que G est abélien.
2. En déduire que $g \mapsto g^{-1}$ est un automorphisme de G.

3. En déduire que G a une structure d'espace vectoriel V sur le corps $\mathbf{Z}/2\mathbf{Z}$ à deux éléments.
4. Montrer qu'une application $\mathbf{Z}/2\mathbf{Z}$-linéaire inversible de V est un automorphisme de G. En déduire que G est un espace vectoriel de dimension 0 ou 1.

Démonstration. 1. Soit $y \in G$, alors $g\colon G \to G, x \mapsto y^{-1}xy$ est un automorphisme de G. Ainsi $y^{-1}xy = x$ ce qui implique que G est abélien.

2. Soit $x, y \in G$, alors $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$ car G est abélien. Donc $g \mapsto g^{-1}$ est un automorphisme de G.
3. Une façon de le voir est de remarquer que si $g \mapsto g^{-1}$ est un automorphisme de G alors pour tout élément $x \in G$, on a $x = x^{-1}$ et reprendre un exercice du TD1.
4. Soit φ une application $\mathbf{Z}/2\mathbf{Z}$-linéaire inversible de V. Puisque c'est une application linéaire, alors elle vérifie pour tous $x, y \in G$, $\varphi(xy) = \varphi(x)\varphi(y)$. Puisque l'application est $\mathbf{Z}/2\mathbf{Z}$-linéaire alors $\varphi^{-1}(x) = \varphi(x^{-1})$. Donc φ est bien un automorphisme de G.
   Finalement, si G est un espace vectoriel de dimension supérieure ou égale à 2, on peut construire une application $\mathbf{Z}/2\mathbf{Z}$-linéaire en effectuant un changement de coordonnés. Ce qui est absurde puisque $\mathrm{Aut}(G) = \{1\}$. Donc G est espace vectoriel de dimension 0 ou 1.

□

2.7 Exo 6

Exercice 2.7. Soient G un groupe et H un sous-groupe. On définit les *classes à droite* de H dans G comme les classes d'équivalence de la relation $x \sim_R y \Leftrightarrow xy^{-1} \in H$ et les *classes à gauche* comme étant celles de la relation $x \sim_L y \Leftrightarrow y^{-1}x \in H$.

1. Montrer que les classes à gauche sont de la forme gH avec $g \in G$ et que les classes à droite s'écrivent Hg.
2. Montrer que l'application $gH \mapsto Hg^{-1}$ est une bijection de l'ensemble des classes à gauche sur celui des classes à droites.
3. En déduire que les ensembles quotients de ces deux relations ont même cardinal.

Démonstration. 1. Soit $g \in G$, montrons que éléments dans la classe à gauche de G sont exactement les éléments de gH. Si $x \in gH$, alors il existe $h \in H$ tel que $x = gh$, soit encore $g^{-1}x = h \in H$. Donc $x \sim_L g$. Réciproquement, si $x \sim_L g$ alors il existe $h \in H$ tel que $g^{-1}x = h$, soit encore $x = gh \in gH$. Ce qui prouve que les classes à gauche sont de la forme gH avec $g \in G$.
   La preuve pour les classes à droite est la même.

2. On note f l'application d'ensemble qui envoie gH sur Hg^{-1}. Montrons que f est injective. Si $Hg^{-1} = Hx^{-1}$ alors g^{-1} et x^{-1} représentent la même classe à droite. Donc $g^{-1} \sim_R x^{-1}$. On peut encore le réécrire sous la forme $g^{-1}x \in H$. Puisque H est un sous-groupe de G ceci est équivalent à $xg^{-1} \in H$, soit encore $x \sim_R g$. Donc f est injective.
   Par ailleurs f est surjective. En effet si $g \in G$ alors $f(g^{-1}H) = Hg$.
3. Par définition $G/\sim_R$ est l'ensemble des classes à droite de G. Or par la question précédente, l'ensemble des classes à droite de G est en bijection avec l'ensemble des classes à gauche de G. En particulier ces deux ensembles ont le même cardinal.

□

2.8 Exo 7

Exercice 2.8. On considère une décomposition d'un entier n de la forme $n = n_1 + \cdots + n_k$ avec $n_i > 0$. Montrer que $\prod_{i=1}^{k}(n_i!)$ divise $n!$ (on pourra appliquer le théorème de Lagrange à un sous-groupe bien choisi de S_n).

Démonstration. On se donne une décomposition d'un entier n de la forme $n = n_1 + \cdots + n_k$ avec $n_i > 0$. On pose $n_0 = 0$. On considère la partition de $[\![1, n]\!]$ donnée par

$$\bigsqcup_{i=0}^{k-1} [\![\sum_{j=0}^{i} n_i + 1, \sum_{j=0}^{i+1} n_i]\!]$$

On considère le sous-groupe H de $\mathfrak{S}_n$ qui stabilise cette partition. Cela revient à se donner un élément dans $\prod_{i=1}^{k} \mathfrak{S}_i$. Donc l'ordre de H vaut $\prod_{i=1}^{k}(n_i!)$. Ce qui prouve que $\prod_{i=1}^{k}(n_i!)$ divise $n!$. □

2.9 Exo 8

Exercice 2.9. Soit G un groupe qui possède exactement deux sous-groupes distincts de G et 1.

1. Montrer que G est un groupe fini en montrant d'abord que tous ses éléments sont d'ordre finis.
2. Montrer que G est cyclique.
3. En déduire que G est d'ordre pq ou p^3 avec $p \neq q$ deux nombres premiers.

Démonstration.

1. Montrons que tout élément de G est d'ordre fini. Soit $x \in G$. Supposons par l'absurde que x soit d'ordre infini. Alors le sous-groupe de G engendré par x est infini et isomorphe à $\mathbf{Z}$. Or $\mathbf{Z}$ possède une infinité de sous-groupes (les $n\mathbf{Z}$), donc G possède aussi une infinité de sous-groupes, ce qui est absurde. Donc x est d'ordre fini.

   Montrons maintenant que G est d'ordre fini. Supposons par l'absurde que G soit infini. Soit $x \neq 1$, on note $H = \langle x \rangle$. Alors H est fini, donc il n'est pas égal à G. Soit $y \notin H$. Alors $K = \langle y \rangle$ est un sous-groupe fini de G différent de G, H et 1. Comme G est infini, on peut trouver un élément $z \notin H \cup K$. Le sous-groupe engendré par z est alors différent de G, H, K et 1. Or c'est absurde car G possède exactement deux sous-groupes distincts de G et 1. Donc G est fini.
2. Soit $x \neq 1$ un élément de G. On note H le sous-groupe engendré par x. On sait que $H \neq 1$. Si $H = G$ alors on aura prouve que G est cyclique. Sinon $H \neq G$ et il existe $y \in G \backslash H$. On note K le sous-groupe engendré par y. Comme précédemment $K \neq 1$. De plus $K \neq H$. Si $K = G$ alors G est cyclique. Supposons que que $K \neq G$. Alors il existe $z \notin H \cup K$. Le sous-groupe engendré par z n'est ni 1, ni H ni K. C'est donc nécessairement G. Donc G est cyclique.
3. Comme G est un groupe cyclique, il est donc isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un certain entier $n > 1$. Or le groupe $\mathbf{Z}/n\mathbf{Z}$ possède un sous-groupe d'ordre d pour tout d diviseur de n. Puisque le groupe G possède exactement deux sous-groupes distincts de G et 1, alors G est d'ordre pq ou p^3 avec $p \neq q$ deux nombres premiers.

□

2.10 Exo 9

Exercice 2.10. Soient G et G' deux groupes. Soit morphisme de groupe $f \colon G \to G'$.

(a) On dit que f est un monomorphisme si pour tout groupe Γ, la propriété suivante est vérifiée : pour tous morphismes de groupes $u, v \colon \Gamma \to G$, si $f \circ u = f \circ v$ alors $u = v$.

(b) On dit que f est un épimorphisme si pour tout groupe Γ, la propriété suivante est vérifiée : pour tous morphismes de groupes $u, v \colon G' \to \Gamma$, si $u \circ f = v \circ f$ alors $u = v$.

Montrer les résultats suivant :

1. f est un morphisme injectif si et seulement si f est un monomorphisme

2. f est un morphisme surjectif si et seulement si f est un épimorphisme

Démonstration. 1. Supposons que f soit injective, soient alors Γ un groupe et $u, v\colon \Gamma \to G$ deux morphismes de groupes tels que $f \circ u = f \circ v$. Soit $x \in Gamma$, alors par hypothèse $f(u(x)) = f(v(x))$, donc $u(x) = v(x)$ car f est injective. Donc $u = v$ et f est un monomorphisme.

Réciproquement, si f est un monomorphisme, prenons $x, y \in G$ tels que $f(x) = f(y)$ et considérons les morphismes de groupes $u\colon \mathbf{Z} \to G, n \mapsto x^n$ et $v\colon \mathbf{Z} \to G, n \mapsto y^n$. Alors il est clair que $f \circ u = f \circ v$, donc $u = v$ puisque f est un monomorphisme. En particulier, cela implique que $x = y$ et donc f est injective.

2. Supposons que f soit surjective, et soit un groupe Γ ainsi que $u, v\colon G' \to \Gamma$ deux morphismes de groupes tels que $u \circ f = v \circ f$. Soit $z \in G'$, alors comme f est surjective, il existe $x \in G$ tel que $f(x) = z$. Alors $u(z) = u(f(x)) = v(f(x)) = v(z)$, donc $u = v$.

Réciproquement, supposons que f soit un épimorphisme. Supposons par l'absurde que f ne soit pas surjective, alors $f(G) = H \neq G'$. On pose $E = G'/f(G) \cup \{\infty\}$ l'ensemble quotient de G' par $f(G)$ union un point. Pour $g \in G'$ on définit

$$\begin{array}{rccc} \sigma_g\colon & E & \to & E \\ & x'H & \mapsto & gx'G \\ & \infty & \mapsto & \infty \end{array}$$

Soit τ la transposition de E qui échange H et ∞. Alors soit $u\colon E \to E, g \mapsto \sigma_g$ et $v\colon E \to E, g \mapsto \tau \circ \sigma_g \circ \tau$. On vérifie que $u \circ f = v \circ f$. Puisque f est un épimorphisme alors cela implique que $u = v$. Soit $z \notin H$, alors $\sigma_z(\infty) = \infty$ et

$$\tau \circ \sigma_z \circ \tau(\infty) = \tau(\sigma_z(H)) = \tau(zH) = zH$$

Ce qui est absurde.

□

3 TD3

Démo à faire

Proposition 3.1. *Soit p un nombre premier, alors le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique.*

Démonstration. On note $O = \{d \mid o(x) = d, x \in (\mathbf{Z}/p\mathbf{Z})^\times\}$.

Lemme 3.1. *Il existe un élément d'ordre* $\mathrm{ppcm}(O) = r$.

Démonstration. On commence par remarquer que si $o(x) = p$ et si $o(y) = q$ avec $p \wedge q = 1$, alors $o(xy) = pq$. En effet $(xy)^{pq} = 1$, par ailleurs si $(xy)^k = 1$, alors $x^k = y^{-k}$, et donc $x^{kp} = 1 = y^{kp}$, en particulier $q \mid kp$, donc $q \mid k$ puisque $p \wedge q = 1$. De même on montre que $p \mid k$, donc $pq \mid k$.

Soit maintenant l une puissance d'un nombre premier apparaissant dans la décomposition en facteur en facteur premier de $\mathrm{ppcm}(O) = r$. Alors il existe un élément $x \in (\mathbf{Z}/p\mathbf{Z})^\times$ tel que $o(x) = lu$ avec u un certain entier. (En effet, si l n'apparaissait dans l'ordre d'aucun x, il ne pourrait pas apparaitre dans $\mathrm{ppcm}(O)$). Ainsi $o(x^u) = l$.

On note $r = \prod_{i=1}^n p_i^{m_i}$. Alors pour tout $i \in \{1, \cdots, n\}$, il existe $x_i \in (\mathbf{Z}/p\mathbf{Z})^\times$ tel que $o(x_i) = p_i^{m_i}$. Ainsi l'élément $y = \prod_{i=1}^n x_i \in (\mathbf{Z}/p\mathbf{Z})^\times$ est d'ordre r. □

On considère maintenant l'ensemble $E = \{x \in (\mathbf{Z}/p\mathbf{Z})^\times \mid x^r = 1\}$. Cet ensemble est non vide, et on a même $(\mathbf{Z}/p\mathbf{Z})^\times \subset E$, car r est le ppcm de tous les éléments de $(\mathbf{Z}/p\mathbf{Z})^\times$.

Or comme $(\mathbf{Z}/p\mathbf{Z})^\times$ est un corps, alors l'équation $x^r - 1 = 0$ possède au plus r solutions. Donc $\mathrm{Card}(E) \leqslant r$. Ainsi $p - 1 \leqslant r$, et en particulier $r = p - 1$ (puisque r divise $p - 1$ qui est l'ordre du groupe).

Ainsi $(\mathbf{Z}/p\mathbf{Z})^\times$ possède un élément d'ordre $p - 1$ donc est cyclique.

□

3.1 Exo 1

Exercice 3.1. Quel est le dernier chiffre dans l'écriture décimale de 3^{2018} ?

Démonstration. On va chercher l'ordre de 3 dans $\mathbf{Z}/10\mathbf{Z}$. On constate que $3^2 = -1[10]$ et que $3^4 = 1[10]$. Donc 3 est d'ordre 4 modulo 10. De plus $2018 = 4 \times 504 + 2$. Donc $3^{2018} = 9[10]$. □

3.2 Exo 2

Exercice 3.2. Montrer que les groupes $\mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/90\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$ et $\mathbf{Z}/100\mathbf{Z} \times \mathbf{Z}/30\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$ sont isomorphe et écrire leur décomposition canonique.

Démonstration. On a (grâce au théorème des restes chinois)

$$\mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/90\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z} = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/3^2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5^2\mathbf{Z}$$

et

$$\mathbf{Z}/100\mathbf{Z} \times \mathbf{Z}/30\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} = \mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/5^2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/3^2\mathbf{Z}.$$

À l'ordre des facteurs ces deux écritures sont les mêmes donc les deux groupes sont isomorphes. □

3.3 Exo 3

Exercice 3.3. Si n est un entier, montrer que $\sum_{d|n} \varphi(d) = n$ (on pourra regrouper les éléments selon leur ordre dans le groupe $\mathbf{Z}/n\mathbf{Z}$).

Démonstration. On remarque que

$$\mathbf{Z}/n\mathbf{Z} = \bigsqcup_{d|n} \{\text{éléments d'ordre } d\}.$$

Le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique, on note x un générateur. On va montrer le résultat suivant

Lemme 3.2. *Un élément x^m est d'ordre d si et seulement si $m = \frac{n}{d}k$ et k premier avec d.*

Démonstration. Supposons que x^m est d'ordre d, alors $x^{md} = 1$, donc $n|md$. Ainsi $m = \frac{n}{d}k$ pour un certain entier k. Par ailleurs, soit d' un diviseur strict de d. Alors $x^{\frac{n}{d}kd'} \neq 1$, ce qui implique que n ne divise pas $\frac{n}{d}kd'$. En particulier, pour tout entier v, on a $k' \neq \frac{d}{d'}v$, donc k' est premier avec d.

Réciproquement, si $m = \frac{n}{d}k$ et k premier avec d. Alors, on a bien $x^{md} = x^{nk} = 1$. Par ailleurs, soit d' est un diviseur de d. Comme d est premier avec k, il existe u, v tels que $1 = ku + dv$. Supposons que $x^{\frac{n}{d}kd'} = 1$, alors $x^{\frac{n}{d}kd'u} = 1$, donc

$$x^{\frac{n}{d}d'(1-dv)} = x^{\frac{n}{d}d'} = 1$$

L'égalité $x^{\frac{n}{d}d'} = 1$ n'est possible que si $d = d'$ car x est d'ordre n. Ce qui prouve que x^m est d'ordre d. □

On déduit du lemme qu'il existe exactement $\varphi(d)$ éléments d'ordre d.
On a donc bien $\sum_{d|n} \varphi(d) = n$. □

3.4 Exo 4

Exercice 3.4. Calculer le cardinal de $\mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})$, l'ensemble des morphismes de groupes de $\mathbf{Z}/n\mathbf{Z}$ vers $\mathbf{Z}/m\mathbf{Z}$, pour n, $m \geqslant 1$ deux entiers.

Démonstration. Soit $\psi\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ un morphisme de groupe. Soit x un générateur de $\mathbf{Z}/n\mathbf{Z}$. Alors si l'on note $\psi(x) = y$, on a $y^n = \psi(x^n) = 0$. Donc l'ordre de y divise n. Par ailleurs, l'ordre de y divise m, donc l'ordre de y divise $\mathrm{pgcd}(n, m)$.

Réciproquement, si on définit $\psi\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ par $\varphi(x) = y$ où l'ordre de y divise le $\mathrm{pgcd}(n, m)$ et $\psi(0) = 0$, il s'agit de vérifier que $\psi(x^n) = 0 = y^n$ Or comme $\mathrm{pgcd}(n, m)|n$, on a bien $y^n = 0$.

Ainsi le cardinal de $\mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})$ est le nombre d'élément de $\mathbf{Z}/m\mathbf{Z}$ dont le cardinal divise $\mathrm{pgcd}(n, m)$. En reprenant l'exercice précédent, si d est un diviseur de $\mathrm{pgcd}(n, m)$, le nombre d'éléments d'ordre d est $\varphi(d)$ où φ désigne l'indicatrice d'Euler. Donc

$$\mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z}) = \sum_{d|\mathrm{pgcd}(n,m)} \varphi(d) = \mathrm{pgcd}(n, m)$$

□

3.5 Exo 5

Exercice 3.5. Soit $p \geqslant 3$ un nombre premier.

1. Montrer que pour tout $k \geqslant 0$,

$$(1 + p)^{p^k} = 1 + \lambda_k p^{k+1}$$

où p ne divise pas λ_k.

2. En déduire que si $\alpha \geqslant 2$ alors $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.
3. On considère le morphisme naturel $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/p\mathbf{Z})^\times$. Montrer qu'il est surjectif et en déduire que $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est cyclique.

Démonstration. 1. On procède par récurrence sur k. Lorsque $k = 0$, on a $(1+p)^{p^0} = 1+p$, donc $\lambda_k = 1$. On suppose le résultat vrai jusqu'à un certain rang k.

$$(1+p)^{p^{k+1}} = (1+\lambda_k p^{k+1})^p = 1 + \lambda_{k+1}p^{k+2}$$

où $\lambda_{k+1} = \lambda_k + \sum_{i=2}^{p}\binom{p}{i}\lambda_k^i p^{(k+1)(i-1)-1}$. Et $\lambda_{k+1} = 1 \mod [p]$. Comme la propriété est héréditaire, on a bien montré le résultat souhaité par récurrence.

2. La question précédente nous prouve que $(1+p)^{p^{\alpha-1}} = 1 \mod [p]$. Donc l'ordre de $1+p$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ divise $p^{\alpha-1}$. Soit $k < \alpha - 1$. Alors $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$, mais $1 + \lambda_k p^{k+1} \neq 1 \mod [p^\alpha]$ car p ne divise pas λ_k. Donc $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.
3. Soit $\bar{k}$ un élément de $(\mathbf{Z}/p\mathbf{Z})^\times$, il se relève en un élément de $\mathbf{Z}$ noté k dont l'image modulo p^α est dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. Le morphisme naturel est donc bien surjectif.
On sait que $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique, soit x un générateur et l'on note toujours x son relèvement à $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. On considère $x' = x^{\frac{o(x)}{p-1}}$. Alors $x'^{p-1} = 1$. Alors l'élément $(1+p)x'$ est d'ordre $p^{\alpha-1}(p-1)$ (qui est le cardinal de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$).
En effet, puisque l'image de $(1+p)x'$ est x' dans $(\mathbf{Z}/p\mathbf{Z})^\times$, alors $p-1$ divise l'ordre de $(1+p)x'$. Plus précisément, on note π la projection de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ sur $(\mathbf{Z}/p\mathbf{Z})^\times$ et l l'ordre de $(1+p)x'$:

$$\pi((1+p)x')^l = \pi(x')^l\pi(1+p)^l = x^l = 1.$$

Donc l'ordre de x divise l. Soit encore $p-1$ divise l.
De plus il est clair que l'ordre de $(1+p)x$ divise $p^{\alpha-1}(p-1)$ donc est de la forme $(p-1)p^k$ (puisqu'on vient de voir que $p-1|o(x'(p+1))$). Or $((1+p)x)^{(p-1)p^k} = (1+p)^{(p-1)p^k} = 1$. Donc $p^{\alpha-1}$ divise $(p-1)p^k$, ce qui prouve que $k = \alpha - 1$.

□

3.6 Exo 6

Exercice 3.6. 1. Montrer que pour $k \geqslant 0$, $5^{2^k} = 1 + \lambda_k 2^{k+2}$ avec λ_k impair. En déduire que $\bar{5}$ est d'ordre $2^{\alpha-2}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$.
2. Montrer que le morphisme naturel $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/4\mathbf{Z})^\times = \mathbf{Z}/2\mathbf{Z}$ est surjectif et que $\bar{5}$ engendre son noyau. En déduire que

$$(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \simeq \left(\mathbf{Z}/2^{\alpha-2}\mathbf{Z}\right) \times \mathbf{Z}/2\mathbf{Z}.$$

Démonstration. 1. On procède par récurrence sur k. Pour $k = 0$ le résultat est clair, on le considère donc comme vrai jusqu'à un certain rang k.

$$5^{2^{k+1}} = (1+\lambda_k 2^{k+2})^2 = 1 + \lambda_k 2^{k+3} + \lambda_k^2 2^{2k+4} = 1 + \lambda_{k+1}2^{k+3}$$

où $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1}$. La propriété étant héréditaire, on a bien pour $k \geqslant 0$, que $5^{2^k} = 1 + \lambda_k 2^{k+2}$ avec λ_k impair.
On vérifie que $5^{2^{\alpha-2}} = 1 \mod [p^\alpha]$. Donc l'ordre de 5 divise $2^{\alpha-2}$. Si $5^{p^k} = 1$, alors $\lambda_k 2^{k+2} = 0 \mod [p^\alpha]$, ce qui implique que $k = \alpha - 2$ puisque λ_k est impair.
2. Pour les mêmes raisons que dans l'exercice précédent, le morphisme naturel est surjectif.

Il est clair que le groupe engendré par $\bar{5}$ est dans le noyau de ce morphisme. De plus, le théorème d'isomorphisme nous assure que le cardinal du noyau est $2^{\alpha-2}$. Donc $\bar{5}$ engendre le noyau.

Soit $x \in (\mathbf{Z}/2^\alpha\mathbf{Z})^\times$, on note $f\colon (\mathbf{Z}/2^\alpha\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/4\mathbf{Z})^\times$ le morphisme canonique. Si $f(x) = 1$,alors il existe un unique k tel que $x = 5^k$. Si $f(x) = 3$, alors il existe un unique k tel que $x = 3 \times 5^k$. Le morphisme qui envoie x sur $(k, f(x))$ est un isomorphisme.

• $\{1, -1\}$ est un sous-groupe de $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ et s'envoie bijectivement sur $(\mathbf{Z}/4\mathbf{Z})^\times$. Avec ça on vérifie sans peine que le morphisme $< 5 > \times\{-1, 1\} \longrightarrow (Z/2^\alpha)^\times$ donné par le produit est un isomorphisme.

□

3.7 Exo 7

Exercice 3.7. Soit p un nombre premier et $n \geqslant 1$ un entier.

1. Dénombrer (à isomorphismes près) les groupes *abéliens* de cardinal p^n et constater que ce nombre ne dépend pas de p.
2. Montrer qu'une partie H de $G := (\mathbf{Z}/p\mathbf{Z})^n$ est un sous-groupe de G si et seulement si c'est aussi un sous-espace vectoriel (sur le corps $\mathbf{Z}/p\mathbf{Z}$). En déduire le nombre de sous-groupes d'ordre p^2 de G. Nombre de sous-groupes d'ordre p^r ?

Démonstration. 1. Soit G un groupe de cardinal p^n. Le théorème de structure des groupes abéliens nous assure que G est isomorphe à un produit de la forme $\prod_{i=1}^r \mathbf{Z}/q_i\mathbf{Z}$, où q_i est une puissance d'un nombre premier. Puisque G est de cardinal p^n, alors p divise chaque q_i. Plus précisément G est isomorphe à un produit de la forme $\prod_{i=1}^r \mathbf{Z}/p^{k_i}\mathbf{Z}$, où $\sum_{i=1}^r k_i = n$. Ainsi le nombre de groupes *abéliens* de cardinal p^n est égal à nombre de partition de l'entier n.

2. Le groupe abélien $G := (\mathbf{Z}/p\mathbf{Z})^n$ est naturellement muni d'une structure de $\mathbf{Z}/p\mathbf{Z}$ espace vectoriel. Donc si H est un sous-groupe de G, on peut le munir d'une structure de $\mathbf{Z}/p\mathbf{Z}$ espace vectoriel. Réciproquement si H est muni d'une structure de $\mathbf{Z}/p\mathbf{Z}$ espace vectoriel, alors il est donc un groupe abélien qui contient l'élément neutre de G, c'est donc un sous-groupe de G.

   On en déduit que le nombre de sous-groupes d'ordre p^r est égal au nombre de sous-espaces vectoriels de G de dimension r. Or se donner un sous-espace vectoriel de dimension r de G c'est comme se donner une base de r vecteurs. Ce cardinal est égal à $(p^n - 1)(p^n - p) \cdots (p^n - p^{r-1})$. L'idée est d'abord de choisir un élément sauf 0, puis un autre élément linéairement indépendant du premier, puis un troisième qui n'est pas dans l'espace vectoriel engendré par les deux premiers, etc.

□

3.8 Exo 8

Exercice 3.8. Donner la décomposition canonique de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ en termes de $d = \mathrm{pgcd}(n, m)$ et $k = \mathrm{ppcm}(n, n)$.

Démonstration. La décomposition est simplement donnée par

$$\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}/\mathrm{pgcd}(n, m)\mathbf{Z} \times \mathbf{Z}/\mathrm{ppcm}(n, m)\mathbf{Z}$$

en effet $\mathrm{pgcd}(n, m) \mid \mathrm{ppcm}(n, m)$. □

3.9 Exo 9

Exercice 3.9. Si G est un groupe abélien fini, on note $\hat{G} := \mathrm{Hom}(G, \mathbf{C}^\times)$ l'ensemble des morphismes de G dans $\mathbf{C}^\times$. Les éléments de $\hat{G}$ sont appelés les *caractères* de G.

1. Montrer que $\hat{G}$ est également un groupe abélien fini (pour la multiplication ponctuelle des caractères). On l'appelle le *groupe dual* de G.
2. Si G est cyclique, montrer que $G \simeq \hat{G}$ (réaliser G comme le groupe des racines $n^{\text{ièmes}}$ de l'unité).
3. Si G et H sont deux groupes abéliens finis, montrer que $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$ puis en déduire que $\hat{G} \simeq G$ pour tout groupe abélien fini.

Démonstration. 1. Pour $f, g \in \mathrm{Hom}(G, \mathbf{C}^\times)$, on définit

$$\begin{array}{rccc} f \cdot g \colon & G & \to & \mathbf{C}^\times \\ & x & \mapsto & f(x)g(x) \end{array}$$

La loi $\cdot$ muni $\hat{G}$ d'une loi de composition interne associative, d'élément neutre

$$\begin{array}{rccc} 1 \colon & G & \to & \mathbf{C}^\times \\ & x & \mapsto & 1 \end{array}$$

et dont f a pour inverse

$$\begin{array}{rccc} f^{-1} \colon & G & \to & \mathbf{C}^\times \\ & x & \mapsto & \frac{1}{f(x)} \end{array}$$

Il est clair que la loi est commutative.
Il reste à vérifier que $\hat{G}$ est fini. Soit $f \in \hat{G}$ et soit $x_1, \cdots, x_r$ une famille génératrice de G (qui est finie car G est fini). Le morphisme f est prescrit par son action sur cette famille génératrice. Si on note n_i l'ordre de x_i, on a $f(x_i)^{n_i} = 1$. Donc $f(x_i)$ est une racine n_i-ième de l'unité. Il n'y a que n_i possibilités pour être l'image de x_i. Donc le cardinal de $\hat{G}$ est majoré par $\prod_{i=1}^r n_i$.

2. Soit x un générateur de G. On définit

$$\begin{array}{rccc} \psi \colon & G & \to & \mathrm{Hom}(G, \mathbf{C}^\times) \\ & x^k & \mapsto & \psi_k \colon \begin{array}{ccc} G & \to & \mathbf{C}^\times \\ x^{k'} & \mapsto & e^{\frac{2i\pi kk'}{n}} \end{array} \end{array}$$

On constate que $\psi(1) = \psi(x^0) \colon G \to \mathbf{C}^\times, x^{k'} \mapsto 1$ est bien l'élément neutre de $\mathbf{C}^\times$. Par ailleurs

$$\begin{array}{rccc} \psi(x^k x^m) \colon & G & \to & \mathbf{C}^\times \\ & x^{k'} & \mapsto & e^{\frac{2i\pi(k+m)k'}{n}} \end{array}$$

est bien égal à

$$\begin{array}{rccc} \psi(x^k)\psi(x^m) \colon & G & \to & \mathbf{C}^\times \\ & x^{k'} & \mapsto & e^{\frac{2i\pi kk'}{n}} e^{\frac{2i\pi mk'}{n}} \end{array}$$

Calculons $\mathrm{Ker}(\psi)$. C'est l'ensemble des k tels que $\psi_k = 1$, c'est-à-dire que pour tout $k' \in \mathbf{N}$, on a $e^{\frac{2i\pi kk'}{n}} = 1$. En prenant $k' = 1$, cela implique que $k \equiv 0 \mod n$. Donc $x^k = 1$. Finalement ψ est injective et comme G et $\hat{G}$ sont de cardinal fini, on a que ψ est un isomorphisme.

3. On définit

$$\begin{array}{rccc} \psi \colon & \mathrm{Hom}(G, \mathbf{C}^\times) \times \mathrm{Hom}(H, \mathbf{C}^\times) & \to & \mathrm{Hom}(G \times H, \mathbf{C}^\times) \\ & (f, g) & \mapsto & \psi(f,g) \colon \begin{array}{ccc} G \times H & \to & \mathbf{C}^\times \\ (x, y) & \mapsto & f(x)g(y) \end{array} \end{array}$$

Montrons que ψ est un isomorphisme de groupes. On a $\psi(1,1) = 1$ et $\psi(ff', gg') = \psi(f,g)\psi(f',g')$. Par ailleurs, si $(f,g) \in \mathrm{Ker}(\psi)$, alors pour tout $(x,y) \in G \times H$, on a $f(x)g(y) = 1$. En prenant $x = e$, on obtient $g = 1$ et en prenant $y = e$, on obtient

$f = 1$, donc ψ est injective. Comme les deux groupes mis en jeu sont finis, on a que ψ est un isomorphisme de groupes.

Soit G un groupe abélien fini, alors d'après le théorème de structure des groupes abéliens on a $G \simeq \prod_{i=1}^{r} \mathbf{Z}/q_i\mathbf{Z}$ où q_i est une puissance d'un nombre premier. En particulier $H_i = \mathbf{Z}/q_i\mathbf{Z}$ est cyclique, donc d'après la question précédente, $\hat{H}_i = H_i$. En particulier

$$\hat{G} = \prod_{i=1}^{r} \hat{H}_i \simeq \prod_{i=1}^{r} \hat{H}_i \simeq \prod_{i=1}^{r} H_i \simeq G$$

□

3.10 Exo 10

Exercice 3.10. On considère un sous-groupe fini G de $\mathrm{GL}_n(\mathbf{Q})$, que l'on fait agir de manière naturelle sur $\mathbf{Q}^n$. Nous allons montrer que G est conjugué à un sous-groupe de $\mathrm{GL}_n(\mathbf{Z})$.

1. Montrer qu'un sous-groupe $H < (\mathbf{Q}^n, +)$ qui est de plus de type fini est libre de rang $r \leqslant n$.
2. En déduire que le sous-groupe $M := \sum_{g \in G} g \cdot (\mathbf{Z}^n)$ est libre de rang n.
3. Montrer qu'il existe une matrice $P \in \mathrm{GL}_n(\mathbf{Q})$ telle que $PGP^{-1} < \mathrm{GL}_n(\mathbf{Z})$.

Démonstration.

1. Le groupe H est sans torsion car c'est un sous-groupe de $(\mathbf{Q}^n, +)$ qui est sans torsion. Or on sait que tout groupe abélien de type fini et sans torsion est libre d'un certain rang r.

   Vérifions que $r \leqslant n$. Soit $(x_1, \cdots, x_r)$ une base de H. Si jamais $r > n$, alors la famille $(x_1, \cdots, x_r)$ est liée sur le $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^n$. On peut donc trouver des éléments $a_i \in \mathbf{Q}$ non tous nuls, tels que

   $$\sum_{i=1}^{r} a_i x_i = 0$$

   Quitte à multiplier par un entier assez grand, on peut supposer que $a_i \in \mathbf{Z}$. Ainsi la famille $(x_1, \cdots, x_r)$ est liée sur $\mathbf{Z}$. Ce qui est impossible puisque c'est une base. Donc $r \leqslant n$.

2. Le groupe M est un sous-groupe de $(\mathbf{Q}^n, +)$ de type fini car G est fini et $\mathbf{Z}^n$ est de type fini. Par la question précédente, M est donc aussi libre, et son rang r est inférieur ou égal à n.

   De plus, si $g \in G$ le groupe $g \cdot \mathbf{Z}^n$ est un sous-groupe libre de type fini de rang n (car isomorphe à $\mathbf{Z}^n$) de M. Donc $n \leqslant r$.

   Ce qui prouve que M est de rang n.

3. Soit $(x_1, \cdots, x_n)$ une base de M et $(e_1, \cdots, e_n)$ la base canonique de $\mathbf{Z}^n$. On définit $P \colon M \to \mathbf{Z}^n, x_i \mapsto e_i$. Puisque M est libre de type fini de rang n alors P est un isomorphisme de groupe. On peut prolonger P par $\mathbf{Q}$-linéarité en un élément de $\mathrm{GL}_n(\mathbf{Q})$. Montrons que $PGP^{-1} < \mathrm{GL}_n(\mathbf{Z})$. Pour cela, il suffit de prouver que si $x \in \mathbf{Z}^n$ alors pour tout $g \in G$, on a $PgP^{-1}x \in \mathbf{Z}^n$.

   Soit $g \in G$. Constatons que par définition de P, on a $P^{-1}x \in M$. Puisque M est stable par G, on a $gP^{-1}x \in M$. Finalement, on a bien $PgP^{-1}x \in \mathbf{Z}^n$.

   Donc $PGP^{-1} < \mathrm{GL}_n(\mathbf{Z})$.

□

3.11 Exo 11+

Exercice 3.11. 1. Montrer que si le quotient $G/\mathcal{Z}(G)$ est cyclique, alors le groupe G est en fait abélien.

2. En déduire qu'un groupe d'ordre p^2 (avec p un nombre premier) est abélien. Montrer qu'à isomorphisme près un groupe d'ordre p^2 est de la forme $(\mathbf{Z}/p\mathbf{Z})^2$ ou $\mathbf{Z}/p^2\mathbf{Z}$.

Démonstration. 1. Notons a l'élément de G tel que son image engendre le quotient $G/\mathcal{Z}(G)$. Soient $x, y \in G$, alors leur image dans le quotient $G/Z(G)$ est de la forme $\bar{x} = \bar{a^r}$ et $\bar{y} = \bar{a^n}$, ce qui revient à dire que $x = a^r x'$ et $y = a^n y'$ où $x', y' \in \mathcal{Z}_G$. Alors

$$xy = a^r x' a^n y' = a^{r+n} x' y' = yx$$

Donc G est abélien.

2. Il faut montrer que $\mathcal{Z}(G)$ n'est pas réduit au neutre ce qui se fait classiquement en faisant agir G sur le lui-même par conjugaison puis en utilisant des relations orbites stabilisateurs.

On suppose alors que $\mathcal{Z}(G)$ est de cardinal p. Alors le quotient $G/Z(G)$ est d'ordre p, donc cyclique, et par la question 1. G est donc abélien.

□

3.12 Exo 12+

Exercice 3.12. Soit G un groupe tel que $\mathrm{Aut}(G)$ est cyclique.

1. Montrer que G est abélien.
2. Si G est fini, montrer que G est cyclique. On précisera alors les différentes possibilités pour l'ordre de G.

Démonstration. 1. On sait que $G/\mathcal{Z}(G)$ est isomorphe à $\mathrm{Int}(G)$ qui est un sous-groupe de $\mathrm{Aut}(G)$. Puisque $\mathrm{Aut}(G)$ est cyclique alors tel est le cas de $G/\mathcal{Z}(G)$ et l'on conclut à l'aide de l'exercice précédent.

2. On sait que G est abélien, ainsi d'après le théorème de structure des groupes abéliens il est isomorphe à un produit de la forme $\prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$, où les p_i sont des nombres premiers.

On suppose qu'un produit de la forme $\mathbf{Z}/p^\alpha\mathbf{Z} \times \mathbf{Z}/q^\beta\mathbf{Z}$ apparaît dans l'écriture précédente (on peut avoir $p = q$). On a alors les inclusions suivantes :

$$\mathrm{Aut}(\mathbf{Z}/p^\alpha\mathbf{Z}) \times \mathrm{Aut}(\mathbf{Z}/q^\beta\mathbf{Z}) \hookrightarrow \mathrm{Aut}(\mathbf{Z}/p^\alpha\mathbf{Z} \times \mathbf{Z}/q^\beta\mathbf{Z}) \hookrightarrow \mathrm{Aut}(G).$$

Or $\mathrm{Aut}(\mathbf{Z}/p^\alpha\mathbf{Z}) \simeq (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. On sait que si p est impair alors

$$(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}.$$

Par ailleurs $(\mathbf{Z}/2\mathbf{Z})^\times \simeq \{e\}$ et si $\alpha \geqslant 2$, on a $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \simeq (\mathbf{Z}/2^{\alpha-2}\mathbf{Z}) \times \mathbf{Z}/2\mathbf{Z}$.

En raisonnant au cas par cas et en utilisant le fait que dans un groupe cyclique il y a un unique élément d'ordre 2, on montre que les seules possibilités pour le groupe G sont $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/p^\alpha\mathbf{Z}$ et $\mathbf{Z}/2p^\alpha\mathbf{Z}$, où p est un nombre premier impair.

□

4 TD 4

4.1 Exo 1

Exercice 4.1. On considère le sous-groupe $\mathbb{S}^1 < \mathbf{C}^\times$ des nombres complexes de module 1.

1. Montrer que $\mathbb{S}^1$ est isomorphe à $\mathbf{R}/\mathbf{Z}$.
2. À quel groupe bien connu est isomorphe $\mathbf{C}^\times/\mathbb{S}^1$?

Démonstration. 1. On considère le morphisme de groupe $\mathbf{R} \to \mathbb{S}^1, x \mapsto e^{2i\pi x}$. Ce morphisme est surjectif. Le noyau de ce morphisme est $\mathbf{Z}$. Ainsi le premier théorème d'isomorphisme nous assure que $\mathbb{S}^1$ est isomorphe à $\mathbf{R}/\mathbf{Z}$.

2. On considère le morphisme de groupe $\mathbf{C}^\times \to \mathbf{R}_+^\times, z \mapsto |z|$. Ce morphisme est surjectif et son noyau est $\mathbb{S}^1$. Le premier théorème d'isomorphisme nous assure dès lors que $\mathbf{C}^\times/\mathbb{S}^1$ est isomorphe à $\mathbf{R}_+^\times$.

□

4.2 Exo 2

Exercice 4.2. Soit $k \geqslant 2$ un entier et considérons $\varphi_k : \mathbf{C}^\times \longrightarrow \mathbf{C}^\times$ donné par $\varphi_k(z) = z^k$. Rappeler pourquoi φ_k est un morphisme et donner son noyau et son image. En déduire un exemple de groupe G et d'un sous-groupe normal $N \lhd G$ non trivial tel que $G/N \simeq G$.

Démonstration. Soient $x, z \in \mathbf{C}^\times$. Alors $\varphi_k(xz) = (xz)^k = x^k z^k$. Donc φ_k est bien un morphisme de groupe. Ce morphisme est surjectif. En effet si $z = re^{it}$ avec $r > 0$ et $t \in \mathbf{R}$, alors $\varphi_k(r^{\frac{1}{k}} e^{i\frac{t}{k}}) = z$. Son noyau est les racines $k$ième de l'unité, noté $\mathbf{U}_k$.

Par le premier théorème d'isomorphisme $\mathbf{C}^\times/\mathbf{U}_k \simeq \mathbf{C}^\times$ □

4.3 Exo 3

Exercice 4.3. Soient G un groupe et $H \lhd G$ d'indice fini n. Montrer que pour tout $g \in G$, $g^n \in H$. Donner un exemple de sous-groupe $H < G$ d'indice n et d'un élément $g \in G$ tel que $g^n \notin H$ (on pourra chercher un exemple dans $G = S_3$).

Démonstration. Soit $g \in G$. Puisque le groupe G/H est d'indice n, alors l'image de g dans G/H vérifie $\bar{g}^n = 1$. Cela implique que $g^n \in H$.

On prend $G = \mathfrak{S}_3$ et $H = \{\mathrm{id}, (1\ 2)\}$. Le groupe H est un sous-groupe de G d'indice 3, mais $(1\ 3)^3 = (1\ 3)$ n'est pas dans H. □

4.4 Exo 4

Exercice 4.4. 1. Soit $f : G \to H$ un morphisme de groupes finis. Soit G' un sous-groupe de G. Montrer que l'ordre de $f(G')$ divise les ordres de G' et de H.

2. Soit G un groupe fini et H, K deux sous-groupes de G. On suppose que H est normal dans G, que $|H|$ et $|G/H|$ sont premiers entre eux et $|H| = |K|$. En considérant l'image de K par la projection canonique $\pi\colon G \to G/H$, montrer que $H = K$.

Démonstration. 1. Comme $f(G')$ est un sous-groupe de H alors par le théorème de Lagrange, l'ordre de $f(G')$ divise l'ordre de H.

Par ailleurs on peut considérer la restriction de f à G'. Alors d'après le premier théorème d'isomorphisme on a $f(G') \simeq G'/\mathrm{Ker}(f_{|G'})$. Donc l'ordre de $f(G')$ divise l'ordre de G'.

2. D'après la première question on déduit que l'ordre de $\pi(K)$ divise l'ordre de K (et donc l'ordre de H car $|H| = |K|$) et l'ordre de G/H. En particulier l'ordre de $\pi(K)$ divise le pgcd de $|H|$ et $|G/H|$. Donc $|\pi(K)| = 1$. Donc $K \subset H$ et puisque leur cardinaux sont égaux on a $H = K$.

□

4.5 Exo 5

Exercice 4.5 (Sous-groupes caractéristiques)**.** Soit G un groupe. Un sous-groupe H de G est dit *caractéristique* si pour tout $\alpha \in \mathrm{Aut}(G)$, on a $\alpha(H) = H$. Cela est noté $H \blacktriangleleft G$.

1. Montrer que $H \blacktriangleleft G$ implique $H \lhd G$. Donner un exemple de sous-groupe d'un groupe G qui est normal mais pas caractéristique.
2. Montrer que $K \blacktriangleleft H \blacktriangleleft G$ implique $K \blacktriangleleft G$.
3. Montrer que $K \blacktriangleleft H \lhd G$ implique $K \lhd G$.
4. Montrer que le centre et le groupe dérivé d'un groupe G sont caractéristiques dans G.

Démonstration.

1. Être un groupe normal est équivalent à être stable par tous les automorphismes intérieur. Or $\mathrm{Int}(G) < \mathrm{Aut}(G)$. Donc être caractéristique implique d'être normal.

   On considère le sous-groupe $\{0\}\times\mathbf{Z}/2\mathbf{Z}$ de $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. L'automorphisme $\alpha\colon (x,y) \mapsto (y,x)$ ne stabilise pas $\{0\} \times \mathbf{Z}/2\mathbf{Z}$ car $\alpha(\{0\} \times \mathbf{Z}/2\mathbf{Z}) = \mathbf{Z}/2\mathbf{Z} \times \{0\}$.
2. Soit $\alpha \in \mathrm{Aut}(G)$, puisque $H \blacktriangleleft G$, alors $\alpha(H) = H$ et $\alpha \in \mathrm{Aut}(H)$. Or $K \blacktriangleleft H$, donc $\alpha(K) = K$, ce qui prouve que $K \blacktriangleleft G$.
3. Soit $\alpha \in \mathrm{Int}(G)$, puisque $H \lhd G$, alors $\alpha(H) = H$ et donc $\alpha \in \mathrm{Aut}(H)$. Puisque $K \blacktriangleleft H$, on a donc $\alpha(K) = K$, et donc $K \lhd G$.
4. Soit $x \in \mathcal{Z}(G)$ et $y \in G$. Soit $\alpha \in \mathrm{Aut}(G)$. Alors il existe $y' \in G$ tel que $\alpha(y') = y$. On va montrer que $\alpha(\mathcal{Z}(G)) \subset \mathcal{Z}(G)$ ce qui permettra de conclure sur l'égalité puisque α est un automorphisme.

   $$\alpha(x)y = \alpha(x)\alpha(y') = \alpha(xy') = \alpha(y'x) = y\alpha(x)$$

   Donc $\alpha(x) \in \mathcal{Z}(G)$ ce qui prouve que le centre de G est caractéristique.

   On rappelle que le groupe dérivé $\mathcal{D}(G) := \langle\{[x : y] \mid x, y \in G\}\rangle$, où $[x : y] = xyx^{-1}y^{-1}$. Soit $\alpha \in \mathrm{Aut}(G)$. On va vérifier que α d'un commutateur est un commutateur. Comme α est un morphisme de groupe, la linéarité permettra de déduire que $\alpha(\mathcal{D}(G)) \subset \mathcal{D}(G)$.

   $$\alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1}$$

   Ce qui prouve que $\mathcal{D}(G)$ est un sous-groupe caractéristique de G.

□

4.6 Exo 6

Exercice 4.6. Donner la liste des sous-groupes normaux de D_3 et D_4. Généraliser à D_n.

Démonstration. Nous traiterons tout de suite le cas général. Comme le suggère l'exercice, il y a une différence entre le cas où n est pair et celui où il est impair. On rappelle qu'une présentation de D_n est donnée par :

$$D_n = \{r, s \mid r^n = e, s^2 = e, srs = r^{-1}\}.$$

On constate dans un premier temps que le sous-groupe $\langle r\rangle$ est distingué dans D_n. En effet on remarque qu'il est d'ordre n donc d'indice 2 dans D_n ce qui en fait un sous-groupe distingué.

De plus, tout sous-groupe de $\langle r\rangle$ est caractéristique dans $\langle r\rangle$ (car il est cyclique) donc distingué dans D_n. Or il y a exactement un sous-groupe de $\langle r\rangle$ par diviseur de n.

• Supposons que $n = 2k$. Montrons que les seuls sous-groupes distingués non triviaux de D_n sont $\langle r^d\rangle$ (où d divise n), $\langle r^2, s\rangle$ et $\langle sr, r^2\rangle$. Soit maintenant un sous-groupe non trivial et distingué N de D_n. On suppose que N est distinct de $\langle r^d\rangle$, pour tout d divisant

n. Cela implique qu'il existe un élément $j \in \mathbf{N}$ tel que $sr^j \in N$. Par ailleurs, puisque N est distingué, on a que $r(sr^j)r^{-1} = sr^{j-2} \in N$. Soit encore que :

$$sr^j(sr^{j-2})^{-1} = sr^j r^{2-j}s = sr^2 s = r^{-2} \in N$$

Si j est pair, cela implique que $s \in N$ et que $r^{-2} \in N$. Donc que $\langle r^2, s\rangle < N$. Or $\langle r^2, s\rangle$ est d'ordre n donc d'indice 2 donc distingué dans D_n. Et si l'on rajoute un élément à $\langle r^2, s\rangle$ on obtient D_n. Donc $N = \langle r^2, s\rangle$. Si j est impair, cela implique que $sr \in N$, alors $\langle sr, r^2\rangle < N$. On peut vérifier que $\langle sr, r^2\rangle$ est d'ordre n donc d'indice 2, ainsi il est distingué.

• Supposons que $n = 2k + 1$. Montrons que les seuls sous-groupes distingués non triviaux de D_n sont $\langle r^d\rangle$ (où d divise n). Comme précédemment soit N un un sous-groupe non trivial et distingué de D_n. Supposons que N ne soit pas un sous-groupe de $\langle r\rangle$. Alors $sr^j \in N$ pour un certain $j \in \mathbf{N}$. De même que précédemment, on montre alors que $r^{-2} \in N$, donc $r^{-2k} = r \in N$. Donc $s \in N$. Ainsi $\langle r, s\rangle < N$. Donc $N = D_n$. Or N n'est pas un sous-groupe trivial de D_n, donc il est inclus dans $\langle r\rangle$. □

4.7 Exo 7

Exercice 4.7. Trouver (par exemple dans $G = D_4$) un exemple de sous-groupes $K \lhd H$ et $H \lhd G$ mais où pour autant K n'est pas normal dans G.

Démonstration. Soit $V = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Le groupe V est un sous-groupe distingué de $\mathfrak{S}_4$. En effet, $\mathfrak{A}_4$ est engendré par les cycles qui laissent stable les éléments de V. Soit $H = \{\mathrm{id}, (1\ 2)(3\ 4)\}$. C'est un sous-groupe distingué de V car V est commutatif Cependant H n'est pas un sous-groupe normal de $\mathfrak{S}_4$ car il n'est pas stable par la transposition (1 3) □

4.8 Exo 8

Exercice 4.8. Soit G un groupe *non abélien* d'ordre 8.

1. Montrer que G contient un élément x d'ordre 4 et que le groupe qu'il engendre est normal dans G.
2. Soit alors $y \in G\backslash\langle x\rangle$; montrer que $y^2 = 1$ ou $y^2 = x^2$.
3. Si $y^2 = 1$, montrer que $yxy = x^{-1}$ et en déduire que G est isomorphe à D_4.
4. Dans le cas restant, écrire la table de G est conclure que G est isomorphe à Q_8.
5. Donner la liste des groupes d'ordre 8 à isomorphisme près.

Démonstration.

1. L'ordre des éléments dans G est soit 8, soit 4, soit 2. Il n'y a pas d'élément d'ordre 8 sinon le groupe serait abélien. De même si tous les éléments de G étaient d'ordre 2, alors le groupe serait abélien. Donc il existe un élément x d'ordre 4.

   Le groupe qu'engendre x est d'indice 2 dans G, donc il est normal.

2. Soit $y \in G\backslash\langle x\rangle$. Alors l'image de y dans le quotient $G/\langle x\rangle$ n'est pas le neutre. Mais comme le cardinale de $G/\langle x\rangle$ est 2, alors $\bar{y}^2 = 1$. Donc $y^2 \in \langle x\rangle$. Si $y^2 \neq 1$, alors y^2 est d'ordre 2. Or le seul élément d'ordre 2 dans $\langle x\rangle$ est x^2. Donc $y^2 = x^2$.

3. Si $y^2 = 1$, alors puisque $\langle x\rangle$ est normal, on a que $yxy \in \langle x\rangle$. Par ailleurs yxy est d'ordre 4, il ne peut donc être égal qu'à x ou x^{-1}. Or si $yxy = x$, alors x et y commutent. Comme $G = \langle x\rangle \sqcup y\langle x\rangle$, alors cela impliquerait que G est commutatif. Donc $yxy = x^{-1}$.

   A cause des relations sur ses éléments (qui est une présentation de D_4), le groupe G s'identifie à un quotient de D_4. Comme G et D_4 ont le même ordre, alors ils sont isomorphes.

4. Les éléments de G sont $\{1, x, y, x^2, x^{-1}, y^{-1}, xy, (xy)^{-1}\}$. Avec les relations $x^4 = 1$ et $x^2 = y^2$, on peut en déduire la table du groupe.

	1	x	y	x^2	x^{-1}	y^{-1}	xy	$(xy)^{-1}$
1	1	x	y	x^2	x^{-1}	y^{-1}	xy	$(xy)^{-1}$
x	x	x^2	xy	x^{-1}	1	$(xy)^{-1}$	y^{-1}	y
y	y	$(xy)^{-1}$	x^2	y^{-1}	xy	1	x	x^{-1}
x^2	x^2	x^{-1}	y^{-1}	1	x	y	$(xy)^{-1}$	xy
x^{-1}	x^{-1}	1	$(xy)^{-1}$	x	x^2	xy	y	y^{-1}
y^{-1}	y^{-1}	xy	1	y	$(xy)^{-1}$	x^2	x^{-1}	x
xy	xy	y	x^{-1}	$(xy)^{-1}$	y^{-1}	x	x^2	1
$(xy)^{-1}$	$(xy)^{-1}$	y^{-1}	x	xy	y	x^{-1}	1	x^2

On compare cette table à la table de $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ avec les relations $i^2 = j^2 = k^2 = ijk = -1$ et $ij = k$, $ji = -k$, $ik = -j$, $jk = i$.

	1	i	j	-1	$-i$	$-j$	k	$-k$
1	1	i	j	-1	$-i$	$-j$	k	$-k$
i	i	-1	k	$-i$	1	$-k$	$-j$	j
j	j	$-k$	-1	$-j$	k	1	i	$-i$
-1	-1	$-i$	$-j$	1	i	j	$-k$	k
$-i$	$-i$	1	$-k$	i	-1	k	j	$-j$
$-j$	$-j$	k	1	j	$-k$	-1	$-i$	i
k	k	j	$-i$	$-k$	j	i	-1	1
$-k$	$-k$	$-j$	i	k	$-j$	$-i$	1	-1

5. On a classifié les groupes d'ordre 8 non abéliens. Les groupes abéliens d'ordre 8 sont $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z})^3$.

□

4.9 Exo 9

Exercice 4.9. Calculer $\mathrm{Aut}(G)$ pour $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $G = S_3$. Dans le deuxième cas, on pourra s'intéresser à l'image des deux transpositions $(1\,2)$ et $(1\,3)$.

Démonstration. 1. On va montrer que $\mathrm{Aut}(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}) = \mathrm{GL}_2(\mathbf{F}_2)$. Pour cela remarquons que $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ est naturellement muni d'une structure de $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel. De plus, un élément de $\mathrm{GL}_2(\mathbf{F}_2)$ est bien un automorphisme de $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. Réciproquement, un automorphisme f de $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. Pour que ce soit un élément de $\mathrm{GL}_2(\mathbf{F}_2)$ il faut vérifier que f est $\mathbf{Z}/2\mathbf{Z}$-linéaire. Soit $x \in \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

$$f((1+1)x) = f(0) = 0 = f(x) + f(x)$$

La linéarité découle du fait qu'il s'agit d'un automorphisme de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
Finalement $\mathrm{Aut}(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) = \mathrm{GL}_2(\mathbf{F}_2)$

2. Les transpositions $(1\,2)$ et $(1\,3)$ engendrent $\mathfrak{S}_3$. Plus précisément un automorphisme est entièrement déterminé par l'image de $(1\,2)$ et $(1\,3)$. On remarque que les transpositions sont d'ordre 2 donc leur image par un automorphisme est aussi d'ordre 2 donc une transposition de $\mathfrak{S}_3$. Il faut vérifier que si l'on choisit deux transpositions comme image de $(1\,2)$ et $(1\,3)$ on obtient un automorphisme, ce qui est le cas puisque les groupes engendrés par respectivement $(1\,2)$ et $(1\,3)$ n'ont en commun que le neutre. Donc $\mathrm{Card}(\mathrm{Aut}(\mathfrak{S}_3)) = 6$.
De plus, on a une injection $\mathfrak{S}_3/\mathcal{Z}(\mathfrak{S}_3) \simeq \mathrm{Int}(\mathfrak{S}_3) \hookrightarrow \mathrm{Aut}(\mathfrak{S}_3)$. Or $\mathcal{Z}(\mathfrak{S}_3) = \{e\}$. Et $\mathrm{Card}(\mathfrak{S}_3) = 6$, donc l'inclusion et l'égalité des cardinaux prouve que $\mathfrak{S}_3 \simeq \mathrm{Aut}(\mathfrak{S}_3)$.

□

4.10 Exo 10

Exercice 4.10. On se propose de calculer $\mathrm{Aut}(G)$ avec $G = \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On note x un générateur de $\mathbf{Z}/4\mathbf{Z}$ et y un générateur de $\mathbf{Z}/2\mathbf{Z}$. Tout élément de G s'écrit donc $nx + my$ avec $0 \leqslant n \leqslant 3$ et $m = 0$ ou 1.

1. Montrer que pour tout $\varphi \in \mathrm{Aut}(G)$, $\varphi(2x) = 2x$.
2. En envisageant les choix possibles pour $\varphi(x)$ et $\varphi(y)$, justifier que $\mathrm{Aut}(G)$ est d'ordre 8.
3. On pose $\varphi(x) = 3x + y$ et $\varphi(y) = 2x + y$. Montrer que φ s'étend en un automorphisme d'ordre 4. De même, montrer que $\psi(x) = 3x + y$ et $\psi(y) = y$ définit un automorphisme d'ordre 2.
4. Vérifier que $\psi \circ \varphi \circ \psi = \varphi^{-1}$ et en déduire que $\mathrm{Aut}(G) \simeq D_4$.

Démonstration.

1. Soit $\varphi \in \mathrm{Aut}(G)$, on note $\varphi(x) = nx + my$ avec $0 \leqslant n \leqslant 3$ et $m = 0$ ou 1. Alors $\varphi(2x) = n2x + m2y = n2x$. Donc $0 \leqslant 2n \leqslant 3$, ce qui implique $n = 0$ ou $n = 1$ ou $n = 3$. Mais $n \neq 0$, sinon φ ne serait pas un automorphisme. Donc $\varphi(2x) = 2x$.
2. D'après la question précédente, on a $\varphi(x) = x$ ou $\varphi(x) = x + y$ ou $\varphi(x) = 3x$ ou $\varphi(x) = 3x + y$. Par ailleurs, si $\varphi(y) = nx + my$, puisque $2y = 0$, alors $n2x = 0$, soit encore $n = 0$ ou $n = 2$. Donc $\varphi(y) = y$ ou $\varphi(y) = 2x + y$.

   Il faut vérifier (calculs à faire) que chaque choix pour $\varphi(x)$ et $\varphi(y)$ permet de prolonger φ en un automorphisme.

   Comme c'est le cas, on en déduit que $\mathrm{Aut}(G)$ est d'ordre 8.
3. Par définition on a $\varphi(nx+my) = n(3x+y)+m(2x+y) = (3n+2m)x+(n+m)y$. La linéarité est claire. Si $\varphi(nx + my) = 0$, alors 2 divise $n + m$ et 4 divise $3n + 2m$. En particulier 2 divise n, donc 2 divise m et puisque 4 divise $3n + 2m$ alors $4|n$. Ainsi $nx + my = 0$. Donc φ est injective. C'est donc un automorphisme, car le groupe G est fini.

   Par ailleurs $\varphi^2(nx+my) = 3nx+my$ et $\varphi^4(nx+my) = nx+my = \mathrm{id}$. Donc l'ordre de φ divise 4 mais ce n'est ni 1, ni 2, donc φ est d'ordre 4.

   De même $\psi(nx + my) = 3nx + (m + n)y$ définit un automorphisme de G. (Les mêmes vérifications sont à faire). De plus $\psi(nx + my)^2 = 9nx + (m + 3n + n)y = nx + my = \mathrm{id}$. Ainsi ψ est un élément d'ordre 2.
4. Calculons :

$$\begin{aligned} \psi \circ \varphi \circ \psi \circ \varphi(nx + my) &= \psi \circ \varphi \circ \psi((3n + 2m)x + (n + m)y) \\ &= \psi \circ \varphi((n + 2m)x + my) \\ &= \psi(3nx + (n + m)y) \\ &= nx + my \end{aligned}$$

   On a bien montré que $\psi \circ \varphi \circ \psi = \varphi^{-1}$. Finalement $\mathrm{Aut}(G)$ est un groupe à 8 éléments qui admet les mêmes relations que D_4, c'est donc D_4.

□

4.11 Exo 11

Exercice 4.11. Montrer que le groupe $\mathrm{Aut}(D_4)$ est isomorphe à D_4 (on pourra étudier les choix possibles pour les images de r et s par un automorphisme). Préciser à quel sous-groupe correspond $\mathrm{Int}(D_4)$ dans cette description.

Démonstration. Soit $\varphi \in \mathrm{Aut}(D_4)$. On pourra remarquer que $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ et que les seuls élément d'ordre 4 sont r et r^3. Puisque $\varphi(r)$ est d'ordre 4 (comme r), alors $\varphi(r) = r$ ou $\varphi(r) = r^3$. Par ailleurs, $\varphi(s)$ est d'ordre 2. Cependant si $\varphi(s) = r^2$, alors $\varphi(rs) = \varphi(sr)$ ce qui impliquerait $rs = sr$. Donc $\varphi(s) \in \{s, sr, sr^2, sr^3\}$.

On vérifie (par des calculs) que dans chacun des cas, la donnée de φ sur r et s se prolonge en un unique automorphisme de D_4. On en déduit que $\mathrm{Card}(\mathrm{Aut}(D_4)) = 8$.

On considère le morphisme φ définit par $\varphi(r) = r$ et $\varphi(s) = sr$. Alors on montre que φ est d'ordre 4 car $\varphi^2(r) = r$, $\varphi^2(s) = sr^2$ alors $\varphi^4 = \mathrm{id}$.

Par ailleurs le morphisme définit par $\psi(r) = r^3$ et $\psi(s) = s$ est d'ordre 2 et vérifie

$$\begin{aligned} \psi \circ \varphi \circ \psi \circ \varphi(r) &= \psi \circ \varphi \circ \psi(r) \\ &= \psi \circ \varphi(r^3) \\ &= \psi(r^3) \\ &= r^9 \\ &= r \end{aligned}$$

$$\begin{aligned} \psi \circ \varphi \circ \psi \circ \varphi(s) &= \psi \circ \varphi \circ \psi(sr) \\ &= \psi \circ \varphi(sr^3) \\ &= \psi(s) \\ &= s \end{aligned}$$

On a montré que que $\psi \circ \varphi \circ \psi = \varphi^{-1}$. Finalement $\mathrm{Aut}(D_4)$ est un groupe à 8 éléments qui admet les mêmes relations que D_4, c'est donc D_4. □

5 TD 5

5.1 Exo 1

Exercice 5.1. On considère l'application suivante :

$$\begin{cases} \mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_m(\mathbf{R}) \times \mathcal{M}_{n,m}(\mathbf{R}) & \longrightarrow & \mathcal{M}_{n,m}(\mathbf{R}) \\ ((P,Q),M) & \mapsto & PMQ^{-1} \end{cases}$$

Montrer qu'il s'agit d'une action de $\mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_m(\mathbf{R})$ sur $\mathcal{M}_{n,m}(\mathbf{R})$ et décrire les classes d'équivalence.

Démonstration. On vérifie que

1. Pour $M \in \mathcal{M}_{n,m}$, on a $((I_n, I_m), M) \mapsto M$
2. Pour tous $(P_1, Q_1) \in \mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_m(\mathbf{R})$ et $(P_2, Q_2) \in \mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_m(\mathbf{R})$, on a
$$((P_2, Q_2), P_1 M Q_1^{-1}) = P_2 P_1 M Q_1^{-1} Q_2^{-1} = ((P_2 P_1, Q_2 Q_1), M).$$

On veut calculer l'orbite de $M \in \mathcal{M}_{n,m}$.

$$\mathrm{Orb}(M) = \left\{ PMQ^{-1} \mid (P,Q) \in \mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_m(\mathbf{R}) \right\}$$

C'est l'ensemble des matrices de rang M. Pour cela on montre que tout matrice de rang M est équivalente à la matrice bloc constituée que de 0 et de I_r, où $r = \mathrm{rg}(M)$.
Pour le montrer on prend une base du noyau de M que l'on complète en une base de $\mathbf{R}^n$ disons $\mathcal{B}$. La matrice Q est la matrice qui envoie la base canonique sur $\mathcal{B}$.
L'ensemble $M\mathcal{B}$ est constitué de vecteurs nuls et d'une famille de vecteurs libres que l'on complète en une base $\mathcal{C}$ de $\mathbf{R}^m$. La matrice P est la matrice qui envoie la base $\mathcal{C}$ vers la base canonique.
La composition PMQ est donc matrice bloc constituée que de 0 et de I_r, où $r = \mathrm{rg}(M)$.

□

5.2 Exo 2

Exercice 5.2. Soit G un groupe agissant sur un ensemble X. On considère

$$X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$$

l'ensemble des points fixes de G dans X.

1. Si $X^G = \varnothing$, $|G| = 15$ et $|X| = 17$, calculer le nombre d'orbites de l'action et le cardinal de chacune d'entre elles.
2. Montrer que si $|G| = 33$ et $|X| = 19$, alors $X^G \neq \varnothing$.

Démonstration.

1. L'hypothèse $X^G = \varnothing$ impose que pour tout $x \in X$, on ait $\mathrm{Stab}(x) := \{g \in G \mid g \cdot x = x\} \neq G$. La formule des classes nous donne la relation :
$$|X| = \sum_{i=1}^{r} |\mathrm{Orb}(x_i)| = \sum_{i=1}^{r} |G|/\mathrm{Stab}(x_i).$$
On souhaite trouver une partition de 17 ne contenant que des 15, des 5 et des 3. On remarque $17 = 15 + 2$, $17 = 2 \times 5 + 7$ et $17 = 3 \times 5 + 2$ ne donnent pas de partition valable. Donc nécessairement, on a $17 = 5 + 3 + 3 + 3 + 3$.
On en déduit qu'il y a 5 orbites de cardinal respectivement 5,3,3,3 et 3.
2. Supposons par l'absurde que $X^G = \varnothing$. Comme précédemment, cela implique que $\mathrm{Stab}(x) \neq G$. La formule des classes implique donc qu'on peut écrire 19 sous la forme $19 = 33a + 11b + 3c$ avec $a, b, c \in \mathbf{N}$. Necessairement $a = 0$, $b = 1$ ou $b = 0$. Si $b = 1$ alors $8 = 3c$ ce qui est impossible et si $b = 0$ alors $19 = 3c$ ce qui est également impossible.
Donc $X^G \neq \varnothing$.

□

5.3 Exo 3

Exercice 5.3. Soit G un groupe et H un sous-groupe de G. On fait agir G sur G/H par translation à gauche et on a donc une action

$$\rho : G \longrightarrow \mathfrak{S}_{G/H}\,.$$

1. Montrer que le noyau de cette action est $\ker(\rho) = \bigcap_{g\in G} gHg^{-1} < H$.
2. Si G est fini et $[G : H] = p$ avec p le plus petit diviseur premier de $|G|$, montrer que $H = \ker(\rho)$ et en déduire que H est distingué dans G.
3. Si G est infini et H d'indice fini, montrer que G contient un sous-groupe normal N dont l'indice vérifie $[G : N] \leqslant [G : H]!$ (en particulier, N est d'indice fini).

Démonstration. 1. On a les équivalences suivantes :

$$\begin{array}{rcl} g \in \mathrm{Ker}(\rho) & \Leftrightarrow & \forall k \in G, gkH = kH \\ & \Leftrightarrow & \forall k \in G, k^{-1}gkH = H \\ & \Leftrightarrow & \forall k \in G, k^{-1}gk \in H \\ & \Leftrightarrow & g \in \bigcap_{g\in G} gHg^{-1} \end{array}$$

2. Par le premier théorème d'isomorphisme le quotient $G/\mathrm{Ker}(\rho)$ s'identifie à un sous-groupe de $\mathfrak{S}_{G/H}$. Donc $\mathrm{Card}(G/\mathrm{Ker}(\rho))$ divise $\mathrm{Card}(\mathfrak{S}_{G/H}) = p!$. Soit q un diviseur premier de $\mathrm{Card}(G/\mathrm{Ker}(\rho))$, alors $q \leqslant p$. Si $q < p$ et $q \neq 1$, alors q divise $\mathrm{Card}(G/\mathrm{Ker}(\rho))$, donc divise $\mathrm{Card}(G)$, ce qui est impossible puisque p est le plus petit diviseur premier de $\mathrm{Card}(G)$.

   Si $q = 1$ alors $\mathrm{Ker}(\rho) = G$, ce qui est impossible car par 1, on a $\mathrm{Ker}(\rho) \lhd H$.

   Donc $q = p$, et ainsi $\mathrm{Ker}(\rho)$ est d'indice p dans G. Comme il est inclus dans H, alors $\mathrm{Ker}(\rho) = H$, ce qui prouve que H est distingué dans G car un noyau est toujours distingué.
3. On considère l'action de G par translation sur G/H noté ρ comme précédemment. Alors si l'on pose $\mathrm{Ker}(\rho) = N$, on a trouvé un sous-groupe normal tel que $G/N \hookrightarrow \mathfrak{S}_{G/H}$, donc qui vérifie $[G : N] \leqslant [G : H]!$.

□

5.4 Exo 4

Exercice 5.4. Soit G un groupe fini et $H \lhd G$ un sous-groupe d'ordre p avec p le plus petit diviseur premier de $|G|$. Montrer que $H < Z(G)$.

Démonstration. On considère l'action de G sur H par conjugaison :

$$\begin{array}{ccc} G \times H & \longrightarrow & H \\ (g, h) & \mapsto & ghg^{-1} \end{array}$$

Soit $h \in H$, on déduit de la relation stabilisateur orbite que $\mathrm{Stab}(h) = \mathrm{Card}(G)/\mathrm{Orb}(h)$. Puisque $\mathrm{Orb}(h) \subset H$, alors $\mathrm{Card}(\mathrm{Orb}(h)) \leqslant p$. Or p est le plus petit diviseur premier de $\mathrm{Card}(G)$, donc on a $\mathrm{Card}(\mathrm{Orb}(h)) = 1$ ou p.

Mais si $\mathrm{Card}(\mathrm{Orb}(h)) = p$ alors il existe $g \in G$ tel que $ghg^{-1} = e$, soit encore $h = e$. Mais $\mathrm{Orb}(e) = 1$. Donc $\mathrm{Card}(\mathrm{Orb}(h)) = 1$ pour tout $h \in H$. En particulier, cela implique que pour tout $g \in G$ et $h \in H$ on ait $ghg^{-1} = h$, soit $H < Z(G)$. □

5.5 Exo 5

Exercice 5.5. Soit G un groupe d'ordre n et p un diviseur premier de n. On va montrer que G contient un élément d'ordre p (lemme de Cauchy) en utilisant une action bien choisie. On note

$$X := \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdot g_2 \cdots g_p = 1\}\,.$$

1. Justifier soigneusement que le groupe $\mathbf{Z}/p\mathbf{Z}$ agit sur X *via* la formule :
$$\bar{1} \cdot (g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1}).$$
2. Décrire explicitement l'ensemble $X^{\mathbf{Z}/p\mathbf{Z}}$ des points fixes.
3. Calculer le cardinal de X et montrer que $X^{\mathbf{Z}/p\mathbf{Z}}$ n'est pas réduit à un singleton. Conclure.

Démonstration. 1. Vérifions déjà que si $(g_1, \ldots, g_p) \in X$, alors $(g_p, g_1, \ldots, g_{p-1}) \in X$.
$$g_p \cdot g_1 \cdots g_{p-1} = g_p \cdot g_1 \cdots g_{p-1} \cdot g_p \cdot g_p^{-1} = e$$
Si $\bar{k}$ est un élément de $\mathbf{Z}/p\mathbf{Z}$, puisque $\bar{1}$ engendre $\mathbf{Z}/p\mathbf{Z}$, alors on a
$$\bar{k} \cdot (g_1, \ldots, g_p) = (g_{1-k}, g_{2-k}, \ldots, g_{p-k}).$$
On vérifie alors facilement que $\bar{0}\cdot(g_1, \ldots, g_p) = (g_1, \ldots, g_p)$ et que $\overline{k+l}\cdot(g_1, \ldots, g_p) = \bar{k} \cdot (\bar{l} \cdot (g_1, \ldots, g_p))$.

2. Par définition $X^{\mathbf{Z}/p\mathbf{Z}} = \{(g_1, \ldots, g_p) \in X \mid \forall \bar{k} \in \mathbf{Z}/p\mathbf{Z}, \bar{k}\cdot(g_1, \ldots, g_p) = (g_1, \ldots, g_p)\}$. En particulier, l'on a $(g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$, d'où $g_i = g_{i-1}$. On en déduit donc que $(g_1, \ldots, g_p) = (g, g, \ldots, g)$ pour un certain $g \in G$. Réciproquement tout élément de la forme $(g, g, \ldots, g)$ est dans $X^{\mathbf{Z}/p\mathbf{Z}}$.

3. Pour qu'un élément $(g_1, \ldots, g_p)$ soit dans X on peut prendre des éléments $g_1, \ldots, g_{p-1}$ quelconque dans G, et dans ce cas g_p est uniquement déterminé par $g_p^{-1} = g_1 \cdots g_{p-1}$. Donc $\mathrm{Card}(X) = n^{p-1}$.
La formule des classes nous permet d'affirmer que
$$|X| = |X^{\mathbf{Z}/p\mathbf{Z}}| + \sum_{\substack{i=0 \\ \mathrm{Orb(x_i)} \neq 1}}^{r} |\mathrm{Orb}(x_i)|.$$
Or $|\mathrm{Orb}(x_i)| = \frac{p}{|\mathrm{Stab(x_i)}|}$. Puisque $|\mathrm{Orb}(x_i)| \neq 1$, alors $|\mathrm{Orb}(x_i)| = p$. Donc $|X| \equiv |X^{\mathbf{Z}/p\mathbf{Z}}| \mod (p)$. Puisque $X^{\mathbf{Z}/p\mathbf{Z}}$ contient au moins un élément qui est $(e, e, \cdots, e)$, alors la congruence nous permet d'affirmer qu'il contient au moins un autre élément de la forme $(g, \cdots, g)$ où $g \neq e$. Ainsi $g \neq e$ vérifie $g^p = e$. On a bien trouvé un élément d'ordre p dans G.

□

5.6 Exo 6

Exercice 5.6. Soit G un groupe fini non trivial (i.e non réduit à un élément) agissant sur un ensemble fini X. On suppose que pour tout $g \in G$, $g \neq 1$, il existe un unique $x \in X$ tel que $g.x = x$. On voudrait montrer que l'action de G sur X admet un unique point fixe.

On notera G_x (resp. $G.x$) le stabilisateur (resp.l'orbite) d'un élément $x \in X$ pour cette action.

On note $Y := \{x \in X : G_x \neq \{1\}\}$.

1. Montrer que Y est non vide.
2. Montrer que Y est stable sous l'action de G : pour tout $x \in Y$, $G.x \subset Y$ (en particulier on a une action induite de G sur Y).
3. On note $Z = \{(g, x) \in (G\backslash\{1\}) \times Y : g.x = x\}$. En dénombrant Z de deux manières différentes, montrer que
$$|Z| = |G| - 1$$
et que
$$|Z| = \sum_{y \in Y} (|G_y| - 1).$$

4. On note $y_1, ..., y_n$ un système de représentants des orbites pour l'action de G sur Y et pour tout i, on pose $m_i = |G_{y_i}|$. Montrer que

$$\sum_{y \in Y} (|G_y| - 1) = \sum_{i=1}^{n} |G.y_i|(|G_{y_i}| - 1)$$

5. À l'aide des deux question précédentes, montrer que

$$1 - \frac{1}{|G|} = \sum_{i=1}^{n} (1 - \frac{1}{m_i})$$

6. Montrer que, pour tout $1 \leqslant i \leqslant n$, on a $m_i \geqslant 2$, et en déduire que

$$\sum_{i=1}^{n} (1 - \frac{1}{m_i}) \geqslant \frac{n}{2}$$

7. En déduire que $n = 1$ et conclure.

Démonstration. 1. Soit $g_1 \in G$ tel que $g_1 \neq 1$. Par définition il existe $x_1 \in X$ tel que $g_1 \cdot x_1 = x_1$. En particulier $g_1 \in G_{x_1}$ et donc $x_1 \in Y$.

2. Soit $x \in Y$ et $g \in G$. Comme $x \in Y$ il existe $g_1 \in G$ avec $g_1 \neq 1$ tel que $g_1 \cdot x = x$. Alors

$$(gg_1g^{-1}) \cdot (g \cdot x) = (gg_1) \cdot x = g \cdot x.$$

Donc $gg_1g^{-1} \in G_{g \cdot x}$, et $gg_1g^{-1} \neq 1$ puisque $g_1 \neq 1$. Donc $g \cdot x \in Y$, donc $G.x \subset Y$.

3. On a

$$Z = \bigsqcup_{g \in G \backslash \{1\}} \{(g, x) \in (G \backslash \{1\}) \times Y : g.x = x\}$$

Or, à g fixé, il existe un unique $x \in X$ tel que $g \cdot x = x$. Donc, à g fixé,

$$|\{(g, x) \in (G \backslash \{1\}) \times Y : g.x = x\}| = 1.$$

Ainsi $|Z| = \sum_{g \in G \backslash \{1\}} 1 = |G| - 1$. De même

$$Z = \bigsqcup_{x \in Y} \{(g, x) \in (G \backslash \{1\}) \times Y : g.x = x\}.$$

Et, à $x \in Y$ fixé, on a

$$\{(g \in (G \backslash \{1\}) : g.x = x\} = G_x \backslash \{1\}.$$

Ainsi $|Z| = \sum_{y \in Y} |G_y| - 1$.

4.

$$\begin{aligned} \sum_{y \in Y} (|G_y| - 1) &= \sum_{i=1}^{n} \sum_{y \in G \cdot y_i} (|G_y| - 1) \\ &= \sum_{i=1}^{n} \sum_{y \in G \cdot y_i} (|G_{y_i}| - 1) \\ &= \sum_{i=1}^{n} |G.y_i|(|G_{y_i}| - 1). \end{aligned}$$

5. D'après la relation orbite-stabilisateur, on a $|G| = |G.y_i||G_{y_i}|$. Par définition $m_i = |G_{y_i}|$. On a

$$\begin{aligned} \frac{1}{|G|}(|G| - 1) &= \frac{1}{|G|}(\sum_{i=1}^{n} |G.y_i|(|G_{y_i}| - 1)) \\ 1 - \frac{1}{|G|} &= (\sum_{i=1}^{n} (1 - \frac{|G.y_i|}{|G|})) \\ &= \sum_{i=1}^{n} (1 - \frac{1}{m_i}) \end{aligned}$$

6. Comme $m_i = |G_{y_i}|$ et que $y_i \in Y$ alors $m_i \geqslant 2$. Ainsi $1 - \frac{1}{m_i} \geqslant \frac{1}{2}$ et donc

$$\sum_{i=1}^{n}(1 - \frac{1}{m_i}) \geqslant \frac{n}{2}.$$

7. Comme $|G| \geqslant 2$ car G est non trivial alors $1 - \frac{1}{|G|} \leqslant \frac{1}{2}$. Donc

$$\frac{1}{2} \geqslant 1 - \frac{1}{|G|} = \sum_{i=1}^{n}(1 - \frac{1}{m_i}) \geqslant n/2.$$

En particulier $n \leqslant 1$. Donc $n = 1$ car il y a au moins une orbite (Y n'est pas vide). En particulier, d'après l'équation précédente, on en déduit que $|G| = m_1$ et donc $G_{y_1} = G$, donc que y_1 est un point fixe sous l'action de G. Par ailleurs il est unique puisqu'il n'y qu'une seule orbite.

□

5.7 Exo 7

Exercice 5.7. On veut montrer que le groupe $G := \mathrm{SL}_2(\mathbf{Z})$ des matrices entières de déterminant ± 1 est engendré par deux matrices :

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

Pour cela, nous introduisons le demi-plan de Poincaré $\mathbb{H} := \{z \in \mathbf{C} \mid \Im(z) > 0\}$ et notons $\Gamma := \langle S, T \rangle$ le sous-groupe de G engendré par S et T.

1. Montrer que la formule
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}$$
définit bien une action de $\mathrm{SL}_2(\mathbf{R})$ sur $\mathbb{H}$. Quel est le noyau de cette action ?
2. Exprimer l'action de S, T, ST et TS sur $\mathbb{H}$ et préciser les ordres des transformations correspondantes.
3. On note $\mathcal{D}$ la partie de $\mathbb{H}$ suivante :
$$\mathcal{D} := \left\{ z \in \mathbb{H} \mid |\Re(z)| \leqslant \frac{1}{2} \text{ et } |z| \geqslant 1 \right\}.$$
Faire un dessin. Montrer que pour $z \in \mathbb{H}$ il existe $\boldsymbol{g} \in \boldsymbol{\Gamma}$ tel que $g \cdot z \in \mathcal{D}$.
4. Soient $z \in \mathcal{D}$ et $g \in G$. Montrer que si $g \cdot z \in \mathcal{D}$ alors z est sur le bord de $\mathcal{D}$ et préciser la valeur de g (suivant la position de z).
5. Calculer les stabilisateurs de l'action de G pour un point de $\mathcal{D}$ (on prêtera une attention particulière aux cas $z = i$, $z = j$ et $z = -\bar{j}$).
6. Soit $z_0 = 2i$. Pour $g \in G$, on considère $z := g \cdot z_0$. D'après la question 3, il existe un élément $\gamma \in \Gamma$ tel que $\gamma \cdot z \in \mathcal{D}$. En utilisant la question précédente, montrer que $g = \gamma^{-1}$ et conclure.

Démonstration. 1. Vérifions dans un premier temps que $\frac{az+b}{cz+d} \in \mathbb{H}$.

$$\Im((az + b)(c\bar{z} + d)) = \Im(ac|z|^2 + adz + bc\bar{z} + bd) = (ad - bc)\Im(z).$$

Or puisque $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R})$, alors $ad - bc = 1$ et finalement $\frac{az+b}{cz+d} \in \mathbb{H}$. On vérifie par ailleurs que $I_2 \cdot z = z$ et

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) \cdot z = \begin{pmatrix} aa' + bc' & ab' + bd' \\ a'c + dc' & cb' + dd' \end{pmatrix} \cdot z$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot z \right) = \begin{pmatrix} aa' + bc' & ab' + bd' \\ a'c + dc' & cb' + dd' \end{pmatrix} \cdot z$$

Donc la formule donnée définit bien une action.

2. On a
$$S \cdot z = \frac{-1}{z}$$
$$T \cdot z = z + 1$$
$$ST \cdot z = \frac{-1}{z+1}$$
$$TS \cdot z = \frac{z-1}{z}$$
De plus $S^2 = I_2$, $T^n \cdot z = z + n$, $(ST)^3 = -I_2$ (donc $(ST)^6 = I_2$) et $(TS)^6 = I_2$.

3. On remarque que $\Im(g \cdot z) = \frac{\Im(z)}{|cz+d|^2}$. Puisque c et d sont des entiers, on peut choisir g tel que $\Im(gz)$ soit maximale. Par ailleurs, on suppose que $\Re(g \cdot z) = x \in \mathbf{R}$. Alors si l'on pose k la partie entière de x, on a $\Re(T^{-k} \cdot g \cdot z) = \Re(g \cdot z) - k$, qui est bien dans l'intervalle $[-1/2, 1/2]$. On note $z' = T^{-k} \cdot g \cdot z$. Il suffit de prouver que $|z'| \geqslant 1$. Si ce n'est pas le cas, alors $|S \cdot z'| \geqslant 1$. Mais $\Im(-1/z') > \Im(z')$ ce qui est absurde. Donc $|z'| \geqslant 1$. On a donc bien trouvé $g' \in \Gamma$ tel que $g' \cdot z \in \mathcal{D}$.

4. Posons $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On remarque que $\Im(g \cdot z) = \frac{\Im(z)}{|cz+d|^2}$. Quitte à considérer $(g \cdot z, g^{-1})$, on peut supposer que $\Im(g \cdot z) \geqslant \Im(z)$ (i.e $|cz + d|^2 \leqslant 1$). Ce n'est possible que si $|c| < 2$, on va donc distinguer les cas.

   • Si $c = 0$, alors $d = \pm 1$ et g est la translation par $\pm b$. Puisque $\Re(z)$ et $\Re(g \cdot z)$ sont dans $[-1/2, 1/2]$ alors $b = 0$ et $g = \mathrm{id}$ ou $b = \pm 1$ et $\Re(z), \Re(g \cdot z) \in \{-1/2, 1/2\}$.

   • Si $c = 1$, alors $|z + d| \leqslant 1$ donc $d = 0$ sauf si $z = \rho := \exp(2i\pi/3)$ (resp. $z = -\bar{\rho}$) auquel cas $d = 0, 1$ (resp. $d = 0, -1$). Le cas $d = 0$ donne $|z| \leqslant 1$ et donc $|z| = 1$. De plus $ad - bc = 1$, donc $b = \pm 1$ et $g \cdot z = a - \frac{1}{z}$, et par un argumentaire similaire à celui du cas $c = 0$, on en déduit que $a = 0$ sauf si $\Re(z) = \pm 1/2$ auquel cas $z = \rho$ ou $z = -\bar{\rho}$ (et dans ce cas $a = 0, -1$ resp $a = 0, 1$).

   Si $z = \rho$ et $d = 1$, alors $a - b = 1$ et $g \cdot \rho = \frac{a-1}{1+\rho} = a + \rho$ donc $a = 0, 1$. Idem si $z = -\bar{\rho}$ et $d = -1$.

   • Si $c = -1$, la discussion est la même que dans le cas $c = 1$ en inversant les signes de a, b, c et d.

   Dans tous les cas, on constate que z est sur le bord de D.

5. Si $g \neq \mathrm{id}$ est dans le stabilisateur de $z \in D$, on a en particulier que z est sur le bord de D.

   Tout élément qui n'est pas sur le bord de D possède un stabilisateur trivial.

   En reprenant la discussion de la question précédente, si $z \in D$ est tel que que $z \neq \rho, -\bar{\rho}$ et $\Re(z) = \pm 1/2$, alors $g \cdot z \in D$ si et seulement si g est une translation. En particulier g ne stabilise pas D. Donc le stabilisateur de z est réduit à l'identité.

   Si $|z| = 1$ et $g \cdot z \in D$, le point précédent prouve que $c = 1$ et d=0. Si l'on suppose $z \neq \rho, -\bar{\rho}$, on en déduit que $g \cdot z = -1/z$. Le seul z stabilisé par un tel g est $z = i$. Donc $\mathrm{Stab}(i) = \{1, S\}$.

   Il ne reste qu'à traiter le cas où $z = \rho$ ou $z = -\bar{\rho}$. Dans ces cas, (à l'aide la discussion précédente, et en testant les divers cas) on montre que $\mathrm{Stab}(\rho) = \langle ST \rangle$ et $\mathrm{Stab}(\rho) = \langle TS \rangle$.

6. On a $(\gamma g) \cdot z_0 = \gamma \cdot z \in \mathcal{D}$. Puisque $z_0 \in \mathcal{D}$ et que z_0 n'est pas sur le bord de $\mathcal{D}$, alors nécessairement $\gamma g = \mathrm{id}$. Donc $g \in \Gamma$.

□

5.8 Exo 8+

Exercice 5.8. Soit $k < n$ deux entiers. On note E_k l'ensemble des parties à k éléments de $\{0, \cdots, n-1\}$. On rappelle que $\mathrm{Card}(E_k) = \mathrm{C}_n^k = \frac{n!}{k!(n-k)!}$.

Dans toute la suite on suppose que k et n sont premiers entre eux.

1. On fait agir $\mathbf{Z}/n\mathbf{Z}$ sur E_k par $m * (a_1, \cdots, a_k) = (\overline{a_1 + m}, \cdots, \overline{a_k + m})$. Montrer que cela définit bien une action.
2. Montrer que le stabilisateur de tout élément est trivial.
3. En déduire que n divise C_n^k.

Démonstration.

1. On remarque que $0 * (a_1, \cdots, a_k) = (a_1, \cdots, a_k)$ et que $(m+l) * (a_1, \cdots, a_k) = m * (l * (a_1, \cdots, a_k))$.
2. Il faut faire attention que l'ordre des éléments dans les k-uplet de E_k n'a pas d'importance.

   Soit $m \in \mathrm{Stab}((a_1, \cdots, a_k))$. Soit σ une permutation de $\{1, \cdots, k\}$. Alors

   $$(a_\sigma(1), \cdots, a_\sigma(k)) = (\overline{a_1 + m}, \cdots, \overline{a_k + m}).$$

   Comme $\sigma^k = \mathrm{id}$, on en déduit que $a_1 = \overline{a_1 + mk}$. Soit encore $mk = 0$ dans $\mathbf{Z}/n\mathbf{Z}$, et comme k et n sont premiers entre eux, cela implique que $m = 0$ dans $\mathbf{Z}/n\mathbf{Z}$. Donc le stabilisateur de tout élément est trivial.
3. On déduit de la formule des classes que

   $$|E_k| = \sum_{i=1}^{r} |\mathrm{Orb}(x_i)| = \sum_{i=1}^{r} \frac{n}{|\mathrm{Stab}(x_i)|} = nr.$$

   Donc n divise C_n^k.

□

5.9 Exo 9+

Exercice 5.9. Soit G un groupe fini qui agit sur un ensemble fini X de manière transitive. (C'est-à-dire que pour tous $x, y \in X$, il existe $g \in G$ tel que $g \cdot x = y$). On note $n = \mathrm{Card}(X)$.

1. Pour $k \leqslant n$, on note $X^{[k]} = \{(x_1, \cdots, x_k) \mid \forall i \neq j, x_i \neq x_j\}$. Montrer que G agit naturellement sur $X^{[k]}$.
2. On dit que l'action de G sur X est k-transitive si l'action de G sur $X^{[k]}$ est transitive. Quel est le degré de transitivité de $\mathfrak{S}_n$ sur $X = \{1, \cdots, n\}$? Quel est celui de $\mathfrak{A}_n$?
3. Montrer que si G est k-transitif alors $|G| = n(n-1)\cdots(n-k+1)|\mathrm{Stab}(x_1, \cdots, x_k)|$.
4. On note $\chi(g) = \mathrm{Card}(\{x \in X \mid g \cdot x = x\})$ l'ensemble des points fixes de g dans son action dans X. Montrer que G est k-transitive si et seulement si

   $$\frac{1}{|G|} \sum_{g \in G} \chi(g)(\chi(g) - 1) \cdots (\chi(g) - k + 1) = 1$$

5. On suppose G transitif sur X. Montrer que G est 2-transitif si et seulement si $2 = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2$.

Démonstration.

1. On fait agir G sur $X^{[k]}$ par $g \cdot (x_1, \cdots, x_k) = (g \cdot x_1, \cdots, g \cdot x_k)$. On vérifie que si $x_i \neq x_j$ alors $g \cdot x_i \neq g \cdot x_j$ (vrai par définition d'une action).
2. Le degré de transitivité de $\mathfrak{S}_n$ sur X est n (envoyer n points sur n autres définit une permutation).

   Le degré de transitivité de $\mathfrak{A}_n$ sur X est $n-2$. On ne peut pas envoyer $(1, 2, 3, \cdots, n)$ sur $(2, 1, 3, \cdots, n)$ par un élément du groupe alterné. De même si l'on fixe l'image

de $n-1$ éléments, l'image du dernier élément est aussi fixée. La $n-2$ transitivité est claire : si l'on fixe $n-2$ éléments envoyé sur $n-2$ autres, on définit une permutation de de $\mathfrak{S}_{n-2}$. Si sa signature est impaire, on peut encore la multiplier par une transposition.

3. De manière plus générale, lorsqu'un groupe fini H agit de manière transitive sur un ensemble fini E, on sait que $\mathrm{Orb}(x)$ est en bijection (ensembliste) avec $H/\mathrm{Stab(x)}$. Or dans le cas d'une action transitive $\mathrm{Orb}(x) = E$. En considérant les cardinaux, on en déduit que $|E||\mathrm{Stab}(x)| = |G|$.
   Puisque G agit transitivement sur $X^{[k]}$, l'on en déduit que

$$|G| = |X^{[k]}||\mathrm{Stab}(x_1, \cdots, x_k)| = n(n-1)\cdots(n-k+1)|\mathrm{Stab}(x_1, \cdots, x_k)|$$

4. La formule de Burnside nous assure que :

$$\text{Nombre d'orbites} = \frac{1}{|G|}\sum_{g\in G} \mathrm{Fix}_g,$$

   où Fix_g est l'ensemble des points fixes dans $X^{[k]}$ sous l'action de G. Par définition $\mathrm{Fix}_g = \{(x_1, \cdots, x_n) \in X^{[k]} \mid g \cdot (x_1, \cdots, x_n) = (x_1, \cdots, x_n)\}$. On peut dénombrer cet ensemble en remarquant qu'on peut choisir pour x_1 un élément fixé par g dans X puis pour x_2 un élément fixé par g dans X sauf x_1, etc. Donc $|\mathrm{Fix}_g| = \chi(g)(\chi(g)-1)\cdots(\chi(g)-k+1)$. On a alors :

$$\text{Nombre d'orbites} = \frac{1}{|G|}\sum_{g\in G} \chi(g)(\chi(g)-1)\cdots(\chi(g)-k+1)$$

   Or l'action est transitive si et seulement si le nombre d'orbite vaut 1.
   Donc G est k-transitive si et seulement si

$$\frac{1}{|G|}\sum_{g\in G} \chi(g)(\chi(g)-1)\cdots(\chi(g)-k+1) = 1$$

5. D'après la question précédente G est 2-transitif si et seulement si

$$\frac{1}{|G|}\sum_{g\in G} \chi(g)(\chi(g)-1) = 1$$

   Or

$$\sum_{g\in G} \chi(g)(\chi(g)-1) = \sum_{g\in G} \chi(g)^2 - \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(g)^2 - 1$$

   car l'action de G est transitive. Finalement, cela prouve bien que G est 2-transitive si et seulement si $2 = \frac{1}{|G|}\sum_{g\in G} \chi(g)^2$.

□

5.10 Exo 10+ Burnside

Exercice 5.10 (Théorème de Burnside)**.** Soit G un groupe et X un ensemble. On suppose que G agit sur X. On note Ω l'ensemble des orbites de l'action de G sur X. Alors

$$\text{Nombre d'orbites de l'action} = |\Omega| = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}_g|$$

où $\mathrm{Fix}_g = \{x \in X \| \ g \cdot x = x\}$.

Indication : Dénombrer l'ensemble $A = \{(g, x) \in G \times X | g \cdot x = x\}$ par deux méthodes distinctes.

Démonstration. La preuve passe par un double dénombrement de l'ensemble $A = \{(g, x) \in G \times X | g \cdot x = x\}$. On peut écrire A comme union disjointe :

$$A = \bigsqcup_{g \in G} \{x \in X \mid g \cdot x = x\} = \bigsqcup_{g \in G} \mathrm{Fix}_g$$

$$A = \bigsqcup_{x \in X} \{g \in G \mid g \cdot x = x\} = \bigsqcup_{x \in X} \mathrm{Stab}(x).$$

On déduit de la première écriture de A que :

$$|A| = \sum_{g \in G} |\mathrm{Fix}_g|.$$

Et de la seconde écriture que :

$$\begin{aligned} |A| &= \sum_{x \in X} |\mathrm{Stab}(x)| \\ &= \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}(x)|} \\ &= \sum_{\omega \in \Omega} \sum_{x \in \Omega} \frac{|G|}{|\mathrm{Orb}(x)|} \\ &= \sum_{\omega \in \Omega} \frac{1}{|\mathrm{Orb}(\omega)|} \sum_{x \in \Omega} |G| \\ &= \sum_{\omega \in \Omega} |G| \\ &= |\Omega||G| \end{aligned}$$

En combinant les deux égalités, on montre bien que $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_g|$. □

5.11 Exo 11+

Exercice 5.11. On garde les notations de l'exercice précédent.

1. Montrer en appliquant la formule de Burnside, que si $|X| \geqslant 2$, on a

$$\sum_{g \in G} \chi(g)^2 \geqslant 2|G|.$$

2. On suppose désormais également que G agit transitivement sur X, et on note G_0 l'ensemble des éléments de G ne fixant aucun point de X. Prouver l'encadrement

$$|G| \leqslant \sum_{g \in G} (\chi(g) - 1)(\chi(g) - |X|) \leqslant |X||G_0|$$

et en déduire que $|G_0| \geqslant |G|/|X|$.

Démonstration. 1. On applique le théorème de Burnside en considérant l'action de G sur $X^{[2]}$. On a alors

$$|G||\Omega| = \sum_{g \in G} \chi(g)(\chi(g) - 1).$$

2. On applique la formule de Burnside. On a alors $|G| = \sum_{g \in G} \chi(g)$. On doit vérifier que $\chi(g) \leqslant (\chi(g)-1)(\chi(g)-|X|)$. On calcule donc par rapport à $\chi(g)$ les racines du polynôme $\chi(g)^2 - \chi(g)(|X| + 2) + |X|$ et on se rend compte qu'elles sont négatives. Donc lorsque $\chi(g) \geqslant 0$ (ce qui est toujours le cas), on a bien $\chi(g) \leqslant (\chi(g)-1)(\chi(g)-|X|)$. En en déduit la première inégalité

$$|G| \leqslant \sum_{g \in G} (\chi(g) - 1)(\chi(g) - |X|)$$

Pour la seconde, on constate que

$$\sum_{g\in G}(\chi(g)-1)(\chi(g)-|X|)=|G|\leqslant\sum_{g\in G\setminus G_0}(\chi(g)-1)(\chi(g)-|X|)+\sum_{g\in G_0}|X|$$

Or $\sum_{g\in G\setminus G_0}(\chi(g)-1)(\chi(g)-|X|)\leqslant 0$, car pour $g\notin G_0$, on a $\chi(g)-1\geqslant 0$ et $\chi(g)-|X|\leqslant 0$. On a donc bien

$$\sum_{g\in G}(\chi(g)-1)(\chi(g)-|X|)\leqslant|X||G_0|.$$

□

5.12 Exo 12+

Exercice 5.12. 1. Montrer que si le quotient $G/Z(G)$ est cyclique, alors le groupe G est en fait abélien.

2. En déduire qu'un groupe d'ordre p^2 (avec p un nombre premier) est abélien. Montrer qu'à isomorphisme près un groupe d'ordre p^2 est de la forme $(\mathbf{Z}/p\mathbf{Z})^2$ ou $\mathbf{Z}/p^2\mathbf{Z}$.

Démonstration. 1. Notons a l'élément de G tel que son image engendre le quotient $G/\mathcal{Z}(G)$. Soient $x,y\in G$, alors leur image dans le quotient $G/Z(G)$ est de la forme $\bar{x}=\bar{a^r}$ et $\bar{y}=\bar{a^n}$, ce qui revient à dire que $x=a^rx'$ et $y=a^ny'$ où $x',y'\in\mathcal{Z}_G$. Alors

$$xy=a^rx'a^ny'=a^{r+n}x'y'=yx$$

Donc G est abélien.

2. Il faut montrer que $\mathcal{Z}(G)$ n'est pas réduit au neutre ce qui se fait classiquement en faisant agir G sur le lui-même par conjugaison puis en utilisant des relations orbites stabilisateurs.

On suppose alors que $\mathcal{Z}(G)$ est de cardinal p. Alors le quotient $G/Z(G)$ est d'ordre p, donc cyclique, et par la question 1. G est donc abélien.

Le théorème de structure des groupes abélien permet de conclure.

□

5.13 Exo 12+

Exercice 5.13. 1. Soit G un groupe fini et $H<G$ un sous-groupe propre. Montrer que

$$\bigcup_{g\in G}gHg^{-1}\subsetneq G.$$

2. Si $G=\mathrm{GL}_n(\mathbf{C})$, montrer qu'il existe un sous-groupe propre H qui intersecte toutes les classes de conjugaison.

Démonstration avec Burnside. 1. On va commencer par un lemme un peu général

Lemme 5.1. *Soit G un groupe fini et X un ensemble de cardinal au moins 2. On suppose de plus que G agit transitivement sur X. Alors il existe un élément $g\in G$ qui agit sans point fixe.*

Démonstration. On rappelle la formule de Burnside

$$\text{Nombre d'orbites de l'action}=\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_g|$$

Puisque l'action de G sur X est transitive, alors le nombre d'orbites de l'action vaut 1. Supposons, par l'absurde, que pour tout $g \in G$, on ait $|\mathrm{Fix}_g| \geqslant 1$. Or $|\mathrm{Fix}_e| \geqslant 2$, on a alors

$$1 = \frac{1}{|G|}(|\mathrm{Fix}_e| + \sum_{e \neq g \in G} |\mathrm{Fix}_g|) \geqslant \frac{|G|+1}{|G|}$$

Ce qui est absurde. Donc il existe un élément g tel que $|\mathrm{Fix}_g| = 0$. □

Continuons désormais la preuve. On considère l'action de G sur l'ensemble G/H donnée par $(k, gH) \mapsto (kgH)$. Cette action est transitive. De plus puisque H est supposé propre, l'on a que $|G/H| \geqslant 2$. Puisque nous sommes dans le cadre des hypothèses du lemme, alors il existe un élément $k \in G$ tel que pour tout $g \in G$ l'on ait $kgH \neq gH$. En particulier, pour tout $g \in G$, l'on a $k \notin gHg^{-1}$. Ce qui prouve que G n'est pas égal à l'union des conjugués du sous-groupe propre H.

2. Soit H l'ensemble des matrices triangulaires supérieures. C'est un sous-groupe strict de G. Cependant chaque matrice de G est trigonalisable, donc H intersecte toutes les classes de conjugaisons.

□

Démonstration sans Burnside. On note $[G : H] = k$ l'indice de H dans G. On va montrer que $|\{gHg^{-1} \mid g \in G\}| \leqslant k$. Cela revient à montrer que si g_1 et g_2 sont dans la même classe d'équivalence dans l'ensemble quotient alors $g_1Hg - 1^{-1} = g_2Hg_2^{-1}$. Si g_1 et g_2 sont dans la même classe d'équivalence alors il existe $h \in H$ tel que $g_2 = g_1h$, et donc

$$g_2Hg_2^{-1} = g_1hHh^{-1}g_1^{-1} = g_1Hg_1^{-1}.$$

De plus, pour tout $g \in G$, $|H| = |gHg^{-1}|$, car le morphisme $x \mapsto gxg^{-1}$ de H dans gHg^{-1} est un morphisme de groupe. On note $g_1, \cdots, g_k$ des représentants de chaque classe d'équivalence de G/H.

$$|\cup_{g\in G} gHg^{-1}| = |\cup_{i=1}^{k} g_iHg_i^{-1}| \leqslant \sum_{i=1}^{k} |g_iHg_i^{-1}| - 1$$

On peut retirer 1 dans l'inégalité précédente car dans notre majoration on compte le neutre au moins deux fois (puisque $k \geqslant 2$). En conclusion, on trouve que

$$|\bigcup_{g\in G} gHg^{-1}| \leqslant [G : H]|H| - 1 \leqslant |G| - 1.$$

Pour des questions de cardinalité, on en déduit que $\bigcup_{g\in G} gHg^{-1}$ ne peut pas être G en entier. □

6 TD6

6.1 Exo 1

Exercice 6.1. Écrire les décompositions en cycles des permutations suivantes :

1. $(3\,1\,4)(1\,5\,9\,2\,6)(5\,3)$;
2. σ^{-1} avec $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$;
3. σ^{-1} avec $\sigma = (5\,6\,2)(1\,3)$.

Démonstration. 1. La permutation est donnée par

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

la décomposition en cycle disjoint est donnée par $\sigma := (1\ 5)(5\ 6\ 4\ 3\ 9)$

2. Puisque $\sigma := (1\ 2\ 5\ 4\ 3)$ alors $\sigma^{-1} := (3\ 4\ 5\ 2\ 1)$.
3. $\sigma^{-1} := (2\ 6\ 5)(1\ 3)$.

□

6.2 Exo 2

Exercice 6.2. Calculer σ^{2020} avec

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}.$$

Démonstration. On peut écrire σ en cycle disjoints $\sigma := (1\ 10\ 5\ 7\ 2\ 9\ 12)(3\ 8\ 6)(4\ 11)$. Or $2020 = 7 \times 288 + 4 = 673 \times 3 + 1 = 2 * 1010$. Donc $\sigma^{2020} = (1\ 2\ 10\ 9\ 5\ 12\ 7)(3\ 8\ 6)$. □

6.3 Exo 3

Exercice 6.3. Soit

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 8 & 7 & 3 & 1 & 6 \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 4 & 8 & 1 & 2 & 3 & 7 \end{pmatrix}$$

deux éléments de $\mathfrak{S}_8$.

Les permutations σ_1 et σ_2 sont-elles conjuguées dans $\mathfrak{S}_8$?

Démonstration.

$$\sigma_1 = (1\ 2\ 5\ 7)(3\ 4\ 8\ 6)$$

$$\sigma_2 = (1\ 5)(2\ 6)(3\ 4\ 8\ 7)$$

Deux permutations sont conjugués si et seulement si les cycles disjoints qui apparaissent dans leur décomposition sont de même longueur. Ainsi σ_1 et σ_2 ne sont pas conjugés. □

6.4 Exo 4

Exercice 6.4. Soit $n > 2$. Pour $1 \leqslant i \leqslant n-1$, on considère les transpositions $\tau_i = (i\,i+1)$ de $\mathfrak{S}_n$.

1. Montrer que $\tau_i\tau_j = \tau_j\tau_i$ si et seulement si $|i-j| \neq 1$.
2. Montrer que $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$.

Démonstration. 1. Si $|i-j| \geqslant 2$, alors τ_i et τ_j sont à support disjoints donc commutent.
Si $i = j$, alors τ_i commute avec lui-même.
Si $|i-j| = 1$, on peut supposer, sans perte de généralité que $j = i+1$. Alors

$$(i\ i+1)(i+1\ i+2) = (i\ i+1\ i+2)$$

$$(i+1\ i+2)(i\ i+1) = (i\ i+2\ i+1)$$

Donc τ_i et τ_{i+1} ne commutent pas.
! Ne marche pas si $i = i+2$, c'est-à-dire dans $\mathfrak{S}_2$.

2. On calcule

$$(i\ i+1)(i+1\ i+2)(i\ i+1) = (i\ i+1\ i+2)(i\ i+1) = (i\ i+2)$$

$$(i+1\ i+2)(i\ i+1)(i+1\ i+2) = (i\ i+2\ i+1)(i+1\ i+2) = (i\ i+2)$$

□

6.5 Exo 5

Exercice 6.5. Montrer que $\mathfrak{S}_n$ est engendré par les parties suivantes :

1. $\{(i\,i+1),\ i = 1 \dots n-1\}$;
2. $\{(1\,i),\ i = 2 \dots n\}$;
3. $\{(1\,2),\ (1\,2\ \dots\ n)\}$.

Démonstration. 1. On sait que $\mathfrak{S}_n$ est engendré par les cycles. De plus

$$(a_1\ \cdots\ a_r) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{r-1}\ a_r).$$

Donc $\mathfrak{S}_n$ est engendré par les permutations. Soit une permutation $(a\ a+k)$ avec $k > 0$. Alors $(a\ a+k) = (a\ a+1)(a+1\ a+k)(a\ a+1)$. Par récurrence on montre alors que $\{(i\,i+1),\ i = 1 \dots n-1\}$ engendre $\mathfrak{S}_n$.

2. En utilisant la question précédente, il suffit de remarquer que $(i\ i+1) = (1\ i)(1\ i+1)(1\ i)$.

3. On va encore une fois utiliser la première question. On note $c = (1\,2\ \dots\ n)$, $r \leqslant n-2$ un entier et l'on constate que $c^{-r}(1\,2)c^r = (1{+}r\ 2{+}r)$. On parvient donc à engendrer tous les éléments $(i\ i+1)$.

□

6.6 Exo 6

Exercice 6.6. Soit $n > 2$. Montrer que $\mathfrak{A}_n$ est engendré par les cycles $(i\,i+1\,i+2)$ pour $1 \leqslant i \leqslant n-2$.

Démonstration. On sait *(cours)* que $\mathfrak{A}_n$ est engendré par les 3-cycles. On peut raisonnablement supposé qu'un 3-cycles est de la forme $(i\ j\ k)$, où $i < j$ et $i < k$ avec $j \neq k$. Remarquons que $(i\ i+2\ i+1)$ est $(i\ i+1\ i+2)^2$. De plus

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

Par ailleurs si $k \geqslant 3$ et $i+k \leqslant n$, on a

$$(i+k-1\ i+k\ i+k+1)(i\ i+1\ i+k)(i+1\ i+2\ i+3) = (i\ i+1\ i+k+1)$$

On veut montrer qu'on veut avoir tous les 3-cyles de la forme $(i\ i+1\ k)$ où $k \neq i, i+1$. On l'a déjà si $k = i-1$ et si $k \geqslant i+2$.

Par ailleurs

$$(i+1\ i-2\ i-1)(i\ i-1\ i+1)(i+1\ i-2\ i-1)^{-1} = (i\ i+1\ i-2)$$

De plus si $k \geqslant 2$

$$(i-k+1\ i-k\ i-k-1)(i\ i+1\ i-k)(i-k+1\ i-k\ i-k-1)^{-1} = (i\ i+1\ i-k-1)$$

Soit maintenant $(i\ i+j\ k)$ un trois-cycle. Sans perte de généralité, on peut suppose que $j > 1$ (si $j = 1$ on sait faire). On suppose $n \geqslant 5$ (sinon on sait faire aussi). Si $j = 2$, (on suppose $k \neq i+3$ sinon on sait faire aussi) on calcule

$$(i+1\ i+2\ i+3)(i\ i+1\ k)(i+1\ i+2\ i+3)^{-1} = (i\ i+2\ k)$$

Si $j \geqslant 3$, alors

$$(i+j-1\ i+1\ i+j)(i\ i+1\ k)(i+j-1\ i+1\ i+j)^{-1} = (i\ i+j\ k)$$

On sait donc engendrer tous les 3 cycles. □

6.7 Exo 7

Exercice 6.7. On considère un cycle c de longueur k dans $\mathfrak{S}_n$.

1. Calculer le cardinal de la classe de conjugaison de c dans $\mathfrak{S}_n$ et en déduire celui du centralisateur de c (c'est le stabilisateur de c pour l'action par conjugaison).
2. Si $k = n$, en déduire que $\langle c \rangle$ est un sous-groupe abélien maximal de $\mathfrak{S}_n$: si $\langle c \rangle \subset H < \mathfrak{S}_n$ avec H abélien, alors $H = \langle c \rangle$.

Démonstration.

1. On constate qu'un le conjugué d'un cycle de longueur k est un cycle de longueur k.

   On note $c = (a_1\ \cdots\ a_k)$, et soit $c' = (b_1\ \cdots\ b_k)$. On considère la permutation σ qui envoie a_i sur b_i pour tout i (et qu'on complète de manière quelconque de sorte à avoir une permutation). Alors $\sigma c \sigma^{-1} = c'$.

   Donc tout cycle de longueur k est un conjugué de c.

   Il ne reste plus qu'à dénombrer les cycles de longueur k. Il s'agit de choisir k éléments parmi n. Un tel support donne $k!$ permutations (en choisissant la place de chaque élément). Cependant toutes ces permutations ne sont pas distinctes, on peut effectuer une rotation des éléments. Chaque élément précédemment construit est donc compté en k exemplaires.

   Finalement $\mathrm{Card}(\mathrm{Orb}(c)) = (k-1)!\binom{n}{k}$.

   Par la relation orbite stabilisateur on a $\mathrm{Card}(\mathrm{Stab}(c) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(\mathrm{Orb}(c))} = k(n-k)!$
2. Soit H un sous-groupe abélien tel que $\langle c \rangle \subset H$. Soit $\sigma \in H$. Comme H est abélien, on a donc $\sigma c = c\sigma$. En particulier $\sigma \in \mathrm{Stab}(c)$. Or $\langle c \rangle \subset \mathrm{Stab}(c)$, or il y a égalité des cardinaux de ces sous-groupes, donc $\langle c \rangle = \mathrm{Stab}(c)$, en particulier $\sigma \in \langle c \rangle$. Donc $H = \langle c \rangle$

□

6.8 Exo 8

Exercice 6.8.

1. Dans $\mathfrak{S}_3$, donner la liste des éléments (avec leurs centralisateurs et leurs classes de conjugaison) ainsi que la liste des sous-groupes (avec normalisateurs et classes de conjugaison). Préciser les sous-groupes normaux.
2. Dans $\mathfrak{S}_4$, donner la liste des éléments (avec centralisateurs et classes de conjugaison). Montrer que pour tout diviseur d de 24, $\mathfrak{S}_4$ admet des sous-groupes d'ordre d et préciser quels groupes apparaissent à isomorphisme près.

Démonstration. Les éléments de $\mathfrak{S}_3$ sont

$$\mathfrak{S}_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

Soit $(a\ b)$ une transposition, soit c différent de a et b. Alors $(a\ c)(a\ b)(a\ c) = (c\ b)$ et $(b\ c)(a\ b)(b\ c) = (a\ c)$. Donc la classe de conjugaison d'une transposition est l'ensemble de toutes les transpositions. De plus $\mathrm{Stab}((a\ b)) = \langle (a\ b) \rangle$.

Soit $(a\ b\ c)$ un 3-cycle. Alors $(b\ c)(a\ b\ c)(b\ c) = (a\ c\ b)$. Donc la classe de conjugaison d'un 3-cycle est l'ensemble de tous les 3-cycles. De plus $\mathrm{Stab}((a\ b\ c)) = \langle (a\ b\ c) \rangle$.

Comme $6 = 2 \times 3$, on peut avoir que des sous-groupes d'ordre $1, 2, 3$ ou 6. Les sous-groupes d'ordre 1 et 6 sont $\{\mathrm{id}\}$ et $\mathfrak{S}_3$. Les sous-groupes d'ordre 2 sont ceux engendré par une transposition. Les sous-groupes d'ordre 3 sont ceux engendré par un 3-cycle.

Un sous-groupe est normal s'il est l'union de classes de conjugaisons. Pour des raisons de cardinalité, les seuls sous-groupes distingués sont $\{\mathrm{id}\}$ et $\mathfrak{S}_3$.

Pour $\mathfrak{S}_4$ voir Ortiz, Exercice d'Algèbre, p26

□

6.9 Exo 9

Exercice 6.9. Énumérer les sous-groupes de $\mathfrak{A}_4$. Parmi ceux-ci, lesquels sont normaux ? Constater également que $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6.

Démonstration. On sait que $\mathrm{Card}(\mathfrak{A}_n) = 12$. De plus

$$\mathfrak{A}_4 = \left\{ \begin{array}{c} id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(3\ 2), (1\ 2\ 3), (1\ 3\ 2), \\ (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3) \end{array} \right\}.$$

D'après le théorème de Lagrange, l'ordre d'un sous-groupe non trivial de $\mathfrak{A}_4$ est 2,3,4 ou 6.

• $\mathfrak{A}_4$ admet 3 sous-groupes d'ordre 2 chacun engendré par une double transposition.

• Tout sous-groupe d'ordre 3 est engendré par un trois-cycle et il en existe 4 (un par point de $\{1, 2, 3, 4\}$ fixé par le sous-groupe).

• Le groupe engendré par toutes les doubles transpositions est d'ordre 4, et comme un tel sous-groupe ne peut pas contenir d'élément d'ordre 3 il n'y en a pas d'autre.

• Si $\mathfrak{A}_4$ admet un sous-groupe H d'ordre 6, alors H est d'indice 2 et donc distingué dans $\mathfrak{A}_4$. Alors H est réunion de classes de conjugaison distinctes, ce qui est absurde puisqu'elles sont de cardinal 1,3,4 et 4. On constate bien que $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6.

Les sous-groupe distingués de $\mathfrak{A}_4$ sont réunion de classe de conjugaisons distinctes. Or les classes de conjugaison sont d'ordre 1,3,4 et 4. Donc les cardinaux possible pour un sous-groupe distingué (par le théorème de Lagrange) sont $1, 4, 12$. Et on vérifie que le groupe engendré par les doubles transpositions est bien distingué dans $\mathfrak{A}_4$.

Autre preuve qu'il n'existe pas de sous-groupe d'ordre 6 : Soit H un sous-groupe de $\mathfrak{A}_n$ d'ordre 6. Il est donc distingué car d'indice 2. Alors il contient un élément d'ordre 2, disons t et un élément d'ordre 3 c. Alors la conjugaison $c^{-1}tc$ et ctc^{-1} donne deux autres éléments d'ordre 2 distincts, tous contenus dans H. Donc le groupe contenant toutes les doubles transpositions que l'on note K est contenu dans H, or 4 ne divise pas 6. C'est absurde. Il n'y a donc pas de groupe d'ordre 6.

□

7 TD7

7.1 Exo 1

Exercice 7.1. Soit $\tau \in \mathfrak{S}_n$ une permutation impaire et considérons l'automorphisme $\varphi : \mathfrak{A}_n \to \mathfrak{A}_n$ défini par $\varphi(\sigma) = \tau\sigma\tau^{-1}$. Montrer que φ n'est pas un automorphisme intérieur de $\mathfrak{A}_n$.

Démonstration. On va faire la prouve si $n > 2$, les cas $n = 1$ et $n = 2$ sont triviaux. Supposons que φ soit un automorphisme intérieur. Alors il existe $c \in \mathfrak{A}_n$ tel que pour tout $\sigma \in \mathfrak{A}_n$, l'on ait $\tau\sigma\tau^{-1} = c\sigma c^{-1}$. Autrement dit, $c^{-1}\tau$ appartient à l'ensemble des éléments de $\mathfrak{S}_n$ qui commute avec tous les éléments de $\mathfrak{A}_n$.

De plus $c^{-1}\tau$ est de signature -1 et commute avec lui-même, donc le groupe engendré par $\langle \mathfrak{A}_n, c^{-1}\tau \rangle$ commute avec $c^{-1}\tau$ et ce groupe n'est autre que $\mathfrak{S}_n$. Donc $c^{-1}\tau \in \mathcal{Z}(\mathfrak{S}_n) = \{\mathrm{id}\}$ (si $n > 2$). Ce qui implique que $c = \tau$, ce qui est absurde.

Ainsi, φ n'est pas un automorphisme intérieur de $\mathfrak{A}_n$ pour $n \geqslant 4$. □

7.2 Exo 2

Exercice 7.2. On se place dans le groupe $\mathfrak{S}_6$.

1. Résoudre l'équation $\sigma^2 = (1\,2)(3\,4)$ dans $\mathfrak{S}_6$.
2. En déduire que l'on ne peut pas plonger Q_8 dans $\mathfrak{S}_6$ (indication : dans Q_8, -1 a 6 racines carrées).

Démonstration.

1. Si $\sigma^2 = (1\,2)(3\,4)$, alors l'ordre de σ vaut 4. On écrit la décomposition en cycle disjoint de sigma, et on regarde les diverses partitions de 6 (on omet les partitions comportant qu'un cycle de longueur qui ne divise pas 4), à savoir les cycles de longueur $3, 5$ et 6. On remarque également que σ ne peut pas être composé uniquement de transposition, sinon σ serait d'ordre 2. Il reste donc : $6 = 4+1+1 = 4+2$. Pour que σ soit d'ordre 4, les seules possibilités sont que σ soit un produit de 2-cycles et de 4-cycles. Le 4-cycle faisant nécessairement intervenir les entiers $1, 2, 3$ et 4.

   On trouve donc 4 possibilités. A savoir $\sigma = (1\ 3\ 2\ 4)$, $\sigma = (1\ 4\ 2\ 3)$, et $\sigma = (1\ 3\ 2\ 4)(5\ 6)$ ou $\sigma = (1\ 4\ 2\ 3)(5\ 6)$.

2. On suppose qu'il existe un plongement $\varphi\colon Q_8 \hookrightarrow \mathfrak{S}_6$. Alors $\varphi(-1)$ est une double transposition. En effet, puisque -1 possède au moins une racine dans Q_8 et est d'ordre 2 alors $\varphi(-1)$ possède au moins une racine dans $\mathfrak{S}_6$ et est d'ordre 2. Or les transpositions ne possèdent pas de racine dans $\mathfrak{S}_6$ (s'ils en avait une, ce serait un 4-cycle, mais le carré d'un 4-cycle est une double transposition). De même le produit de 3 transpositions n'ont pas de racines dans $\mathfrak{S}_6$. Ainsi $\varphi(-1)$ est une double transposition.

   Mais -1 possède 6 racines dans Q_8 alors qu'une double transposition ne possède que 4 racines dans $\mathfrak{S}_6$. Finalement on ne peut pas plonger Q_8 dans $\mathfrak{S}_6$.

   On prouve aussi que l'on ne peut pas plonger Q_8 dans $\mathfrak{S}_7$. En effet, les éléments d'ordre 4 dans $\mathfrak{S}_7$ sont les produits de 4-cycles et de transposition (à support disjoints). De plus, une double transposition est la seule à avoir des racines, et elle en possède 8 distinctes. Par exemple si $\sigma^2 = (1\ 2)(3\ 4)$, alors

$$\sigma \in \left\{ \begin{array}{l} (1\ 3\ 2\ 4), (1\ 3\ 2\ 4)(5\ 6), (1\ 3\ 2\ 4)(5\ 7), (1\ 3\ 2\ 4)(6\ 7), \\ (1\ 4\ 2\ 3), (1\ 4\ 2\ 3)(5\ 6), (1\ 4\ 2\ 3)(5\ 7), (1\ 4\ 2\ 3)(6\ 7) \end{array} \right\}.$$

   De plus, si $\varphi\colon Q_8 \hookrightarrow \mathfrak{S}_7$ est un plongement alors $\varphi(-1)$ est une double transposition. Pour plus de simplicité on peut supposer que $\varphi(-1) = (1\ 2)(3\ 4)$, alors $\varphi(i), \varphi(j)$ et $\varphi(k)$ sont dans l'ensemble

$$\left\{ \begin{array}{l} (1\ 3\ 2\ 4), (1\ 3\ 2\ 4)(5\ 6), (1\ 3\ 2\ 4)(5\ 7), (1\ 3\ 2\ 4)(6\ 7), \\ (1\ 4\ 2\ 3), (1\ 4\ 2\ 3)(5\ 6), (1\ 4\ 2\ 3)(5\ 7), (1\ 4\ 2\ 3)(6\ 7) \end{array} \right\}.$$

Mais $(1\ 3\ 2\ 4)(1\ 3\ 2\ 4) = (1\ 2)(3\ 4)$ et $(1\ 3\ 2\ 4)(1\ 4\ 2\ 3) = \mathrm{id}$. Donc on peut peut pas vérifier la relation $\varphi(i)\varphi(j) = \varphi(k)$.
Donc Q_8 ne se plonge pas dans $\mathfrak{S}_7$.

□

7.3 Exo 3

Exercice 7.3. Déterminer tous les morphismes de $\mathfrak{S}_4$ vers $\mathfrak{S}_3$.

Démonstration. Soit $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ un morphisme de groupe. Comme $4! > 3!$ ce morphisme a un noyau non trivial. De plus $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué de $\mathfrak{S}_4$. Ainsi $\mathrm{Ker}(\varphi) \in \{\mathfrak{S}_4, \mathfrak{A}_4, K\}$ où K est le sous-groupe de $\mathfrak{S}_4$ engendré par les doubles transpositions.

• Si $\mathrm{Ker}(\varphi) = \mathfrak{S}_4$, alors φ est le morphisme trivial.

• Si $\mathrm{Ker}(\varphi) = \mathfrak{A}_4$, alors trouver φ revient à trouver un morphisme injectif $\psi\colon \mathfrak{S}_4/\mathfrak{A}_4 \to \mathfrak{S}_3$. Or $\mathfrak{S}_4/\mathfrak{A}_4 \simeq \mathbf{Z}/2\mathbf{Z}$. On cherche donc tous les morphismes de groupe de $\mathbf{Z}/2\mathbf{Z} \to \mathfrak{S}_3$. Or un tel morphisme est uniquement déterminé par l'image de 1 qui s'envoie nécessairement sur une double transposition (car 1 est d'ordre 2 dans $\mathbf{Z}/2\mathbf{Z}$). On trouve donc 3 tels morphismes.

• Si $\mathrm{Ker}(\varphi) = K$ alors trouver φ revient à trouver un morphisme injectif $\psi\colon \mathfrak{S}_4/K \to \mathfrak{S}_3$.

On va montrer que $\mathfrak{S}_4/K$ est isomorphe à $\mathfrak{S}_3$. On note K^* le sous-ensemble de K constitué seulement des trois doubles transpositions. On peut l'identifier à l'ensemble $\{1,2,3\}$. On considère alors l'action :

$$\begin{array}{rccc} f\colon & \mathfrak{S}_4 \times K^* & \to & K^* \\ & (\sigma,\tau) & \mapsto & \sigma\tau\sigma^{-1} \end{array}$$

Cette action induit un morphisme de groupe de $\psi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$. Ce morphisme est surjectif puisque qu'on peut engendrer toutes les transpositions de la forme $(1,i)$ de $\mathfrak{S}_3$. En effet si on note $1 = (1\ 2)(3\ 4)$, $2 = (1\ 3)(2\ 4)$ et $3 = (1\ 4)(2\ 3)$, alors $\psi(2\ 3)) = (1\ 2)$ et $\psi(2\ 4) = (1\ 3)$. Par ailleurs le noyau de ψ est l'ensemble des éléments de $\mathfrak{S}_4$ qui commutent avec toutes les doubles transpositions, et c'est précisément K. Donc le premier théorème d'isomorphisme nous assure que $\mathfrak{S}_4/K$ est isomorphe à $\mathfrak{S}_3$.

L'ensemble des morphismes $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ tels que $\mathrm{Ker}(\varphi) = K$ sont en bijection avec l'ensemble des morphismes injectifs (donc bijectif) de $\mathfrak{S}_3 \to \mathfrak{S}_3$. Or $\mathrm{Aut}(\mathfrak{S}_3) = \mathfrak{S}_3$.

Finalement, on a trouvé 10 morphismes de $\mathfrak{S}_4$ vers $\mathfrak{S}_3$. □

7.4 Exo 4

Exercice 7.4. Soit $n \geqslant 4$ un entier.

1. Soit $\varphi\colon S_{n+1} \to S_n$ un morphisme non trivial. Montrer que $\mathrm{Ker}(\varphi) = A_{n+1}$.
2. Montrer que l'ensemble de tels morphismes est en bijection avec l'ensemble des éléments d'ordre 2 de S_n.
3. Soit $k \geqslant 1$ un entier. Montrer que dans S_n, le nombre de produits de k transpositions à supports disjoints vaut
$$\frac{\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}$$
4. En déduire que que le nombre de morphismes de S_{n+1} dans S_n ($n \geqslant 4$) vaut exactement
$$1 + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}.$$

Démonstration. 1. Le noyau d'un morphisme est distingué. Or pour $n \geqslant 5$ les seuls sous-groupes distingués de S_n sont $\{\mathrm{id}\}$, S_n et A_n. Pour des raisons de cardinalité, le morphisme ne peut pas être injectif, donc $\mathrm{Ker}(\varphi) \neq \mathrm{id}$. Comme le morphisme n'est pas trivial, alors $\mathrm{Ker}(\varphi) \neq S_n$, donc nécessairement $\mathrm{Ker}(\varphi) = A_n$.

2. D'après le 1er théorème d'isomorphisme (et comme $S_n/A_n = \mathbf{Z}/2\mathbf{Z}$), φ induit un isomorphisme
$$\psi_\varphi \colon \mathbf{Z}/2\mathbf{Z} \to S_n.$$
Par ailleurs l'application $\varphi \mapsto \psi_\varphi$ est une bijection. Enfin ψ_φ est entièrement déterminé par l'image de 1 et $\psi_\varphi(1)$ est un élément d'ordre 2. Réciproquement, la donné d'un élément d'ordre 2 de S_n détermine de manière unique un morphisme $\mathbf{Z}/2\mathbf{Z} \to S_n$. Donc les morphismes $\varphi \colon S_{n+1} \to S_n$ non triviaux sont en bijection avec l'ensemble des éléments d'ordre 2 de S_n.

3. Un produit de k transposition revient à se fixer les transpositions les uns après les autres. Pour la première transposition on choisit 2 nombres parmi n sans tenir compte de l'ordre, ce qui donne $\binom{n}{2}$ choix. Pour la deuxième, on choisit 2 éléments parmi $n-2$ (puisqu'on ne peut plus choisir les éléments déjà choisit pour la première transposition) ce qui donne $\binom{n-2}{2}$ choix. On continue ainsi, et on se retrouve avec $\prod_{i=0}^{k-1} \binom{n-2i}{2}$ possibilités (si l'on considère que l'ordre dans lequel on a choisit les transpositions est importants). cependant, on peut encore mélanger les transpositions entre elles (car $(1\ 2)(3\ 4)$ est la même chose que $(3\ 4)(1\ 2)$). On considère une transposition comme un point qu'on peut permuter, et il faut donc diviser par $k!$ qui est le nombre de permutation d'un ensemble à k éléments. On obtient donc
$$\frac{\displaystyle\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}$$
produit de k transpositions à support disjoint.

4. Il s'agit de constater que les morphismes de S_{n+1} dans S_n sont le morphisme trivial et les morphismes non triviaux. Les morphismes non triviaux sont en bijection avec les éléments d'order 2 de S_n qui sont les produits de k transpositions pour k variant entre 1 et $\lfloor \frac{n}{2} \rfloor$. On en déduit donc que le nombre de morphismes de S_{n+1} dans S_n vaut
$$1 + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}.$$

□

7.5 Exo 5

Exercice 7.5. Nous allons montrer que $\mathrm{Aut}(\mathfrak{S}_4) \simeq \mathfrak{S}_4$.

1. Justifier rapidement l'égalité $\mathrm{Int}(\mathfrak{S}_4) = \mathfrak{S}_4$ et en déduire que $|\mathrm{Aut}(\mathfrak{S}_4)| \geqslant 24$.
2. Montrer que si $\sigma \in \mathfrak{S}_4$ et $\varphi \in \mathrm{Aut}(\mathfrak{S}_4)$ alors les classes de conjugaison de σ et $\varphi(\sigma)$ ont même cardinal (c'est un fait général). En déduire qu'il y a au plus 6 possibilités pour $\varphi((1\,2))$ et au plus 4 pour $\varphi((1\,2\,3\,4))$.
3. Montrer que $|\mathrm{Aut}(\mathfrak{S}_4)| \leqslant 24$ et conclure.

Démonstration. 1. On sait que $\mathfrak{S}_4/\mathcal{Z}(\mathfrak{S}_4) \simeq \mathrm{Int}(\mathfrak{S}_4)$. Or $\mathcal{Z}(\mathfrak{S}_4) = \{\mathrm{id}\}$. Donc on a bien $\mathrm{Int}(\mathfrak{S}_4) = \mathfrak{S}_4$. De plus, comme $\mathrm{Int}(\mathfrak{S}_4)$ s'injecte dans $\mathrm{Aut}(\mathfrak{S}_4)$, alors $|\mathrm{Aut}(\mathfrak{S}_4)| \geqslant 24$.(

2. Par définition $\mathrm{Orb}(\sigma) = \{\tau\sigma\tau^{-1} \mid \tau \in \mathfrak{S}_4\}$ et
$$\mathrm{Orb}(\varphi(\sigma)) = \{\tau\varphi(\sigma)\tau^{-1} \mid \tau \in \mathfrak{S}_4\} = \{\varphi(\tau\sigma\tau^{-1}) \mid \tau \in \mathfrak{S}_4\} = \varphi(\mathrm{Orb}(\sigma)).$$

Donc les classes de conjugaison de σ et $\varphi(\sigma)$ ont même cardinal.

On liste le cardinal des classes de conjugaison de $\mathfrak{S}_4$.

Représentant	cardinal de la classe de conjugaison
id	1
$(a\ b)$	6
$(a\ b)(c)$	3
$(a\ b\ c)$	8
$(a\ b\ c\ d)$	6

Ainsi $\varphi((1\ 2))$ ne peut s'envoyer que sur une transposition ou un 4-cycle, mais pour des questions d'ordres $\varphi((1\ 2))$ ne peut s'envoyer que sur une transposition, ce qui laisse 6 possibilités.

Pour des raisons similaires $\varphi((1\ 2\ 3\ 4))$ ne peut s'envoyer que sur un 4-cycles. Mais puisque $(1\ 2)$ et $(1\ 2\ 3\ 4)$ engendrent $\mathfrak{S}_4$, il faut que $\varphi((1\ 2))$ et $\varphi((1\ 2\ 3\ 4))$ engendrent $\mathfrak{S}_4$, ce qui ne laisse que 4 possibilités à $\varphi((1\ 2\ 3\ 4))$ (une fois $\varphi((1\ 2))$ fixé).

3. La question précédente prouve donc que $|\operatorname{Aut}(\mathfrak{S}_4)| \leqslant 24$. Or $\mathfrak{S}_4$ s'injecte dans $\operatorname{Aut}(\mathfrak{S}_4)$, donc on peut conclure quant à l'égalité $\operatorname{Aut}(\mathfrak{S}_4) = \mathfrak{S}_4$.

□

7.6 Exo 6

Exercice 7.6. Soit G un groupe fini d'ordre $|G| = 2m$ avec m impair. Montrer que G admet un sous-groupe H d'indice 2 (en particulier $N \lhd G$ et G n'est pas simple). On pourra s'intéresser à l'image de G dans son plongement de Cayley.

Démonstration. On note $\varphi\colon G \hookrightarrow \mathfrak{S}_{2m}$ le plongement de Cayley de G. On note $\epsilon\colon \mathfrak{S}_{2m} \to \mathbf{Z}/2\mathbf{Z}$ la signature. Et on considère le morphisme $\bar{\varphi} = \epsilon \circ \varphi\colon G \to \mathbf{Z}/2\mathbf{Z}$. Comme G est d'ordre $2m$ alors G possède un élément d'ordre 2 dont l'image par φ est le produit de m transpositions, et dont l'image par $\bar{\varphi}$ est 1. Donc le morphisme $\bar{\varphi}$ est surjectif.

On note $N = \operatorname{Ker}(\bar{\varphi})$ qui est distingué, alors par le premier théorème d'isomorphisme G/N est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. On a donc bien trouvé un sous-groupe N d'indice 2. □

7.7 Exo 7

Exercice 7.7. Soit $\sigma \in \mathfrak{A}_n$ et notons $\sigma^{\mathfrak{A}_n}$ (*resp.* $\sigma^{\mathfrak{S}_n}$) sa classe de conjugaison dans $\mathfrak{A}_n$ (*resp.* dans $\mathfrak{S}_n$).

1. Montrer que s'il existe $\tau \in \mathfrak{S}_n$ impaire avec $\tau\sigma = \sigma\tau$ alors $\sigma^{\mathfrak{A}_n} = \sigma^{\mathfrak{S}_n}$.
2. Dans le cas contraire, en déduire que $C_{\mathfrak{A}_n}(\sigma) = C_{\mathfrak{S}_n}(\sigma)$ et que $|\sigma^{\mathfrak{A}_n}| = \dfrac{1}{2}|\sigma^{\mathfrak{S}_n}|$.

Démonstration.

1. Il est clair que $\sigma^{\mathfrak{A}_n} \subset \sigma^{\mathfrak{S}_n}$. Soit $c\sigma c^{-1} \in \sigma^{\mathfrak{S}_n}$ avec c impaire, alors $c\tau \in \mathfrak{A}_n$ et $c\sigma c^{-1} = c\tau\sigma\tau^{-1}c^{-1} \in \sigma^{\mathfrak{A}_n}$. On a bien $\sigma^{\mathfrak{A}_n} = \sigma^{\mathfrak{S}_n}$.
2. Dans le cas contraire, il n'existe pas (par hypothèse) de permutation impaire dans le stabilisateur de σ, donc $C_{\mathfrak{A}_n}(\sigma) = C_{\mathfrak{S}_n}(\sigma)$. La relation orbite-stabilisateur nous assure alors que $|\sigma^{\mathfrak{A}_n}| = \dfrac{1}{2}|\sigma^{\mathfrak{S}_n}|$.

□

7.8 Exo 8

Exercice 7.8. En utilisant l'exercice précédent (et votre connaissance des classes de conjugaison dans $\mathfrak{S}_5$), décrire les classes de conjugaison de $\mathfrak{A}_5$. En déduire une nouvelle démonstration du fait que $\mathfrak{A}_5$ est simple.

Démonstration. On note $G = \mathfrak{S}_5$

représentant	ordre du rep	card. de la classe de conj.	centralisateur
id	1	1	G
(1 2)	2	10	$\langle(1\ 2)\rangle\mathfrak{S}(\{3,4,5\})$
(1 2)(3 4)	2	15	$\langle(1\ 2),(1\ 3\ 2\ 4)\rangle$
(1 2 3)	3	20	$\langle(1\ 2\ 3)(4\ 5)\rangle$
(1 2 3 4)	4	30	$\langle(1\ 2\ 3\ 4)\rangle$
(1 2 3 4 5)	5	24	$\langle(1\ 2\ 3\ 4\ 5)\rangle$
(1 2 3)(4 5)	6	20	$\langle(1\ 2\ 3)(4\ 5)\rangle$

Par l'exercice précédent, la classe de (1 2 3 4 5) est la seule qui se coupe en deux.

représentant	ordre du rep	card. de la classe de conj.	centralisateur
id	1	1	$\mathfrak{A}_5$
(1 2)(3 4)	2	15	$\langle(1\ 2)(3\ 4),(1\ 3)(2\ 4)\rangle$
(1 2 3)	3	20	$\langle(1\ 2\ 3)(4\ 5)\rangle$
(1 2 3 4 5)	5	12	$\langle(1\ 2\ 3\ 4\ 5)\rangle$
(2 1 3 4 5)	5	12	$\langle(2\ 1\ 3\ 4\ 5)\rangle$

Tout sous-groupe distingué de H de G est une réunion disjointe de classes de conjugaison dont une est {id} et H est d'ordre un diviseur de 60. L'équation aux classes $(60 = 1 + 15 + 20 + 12 + 12)$ montre alors que G n'admet aucun sous-groupe distingué non trivial.

□

7.9 Exo 9

Exercice 7.9. Montrer que les sous-groupes d'indice n de $\mathfrak{S}_n$ sont isomorphes à $\mathfrak{S}_{n-1}$. On pourra (dans le cas $n \geqslant 5$) faire agir $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ si H est un tel sous-groupe. En déduire, les ordres possibles pour les sous-groupes de $\mathfrak{S}_5$.

Démonstration. On se contentera du cas $n \geqslant 5$. Soit H un sous-groupe de $\mathfrak{S}_n$ d'indice n. On considère l'action de $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ par translation. On en déduit un morphisme de groupe $\psi\colon \mathfrak{S}_n \to \mathfrak{S}_{\mathfrak{S}_n/H} \simeq \mathfrak{S}_n$. Le morphisme ψ est non trivial donc son noyau est soit $\mathfrak{A}_n$ soit 1.

Mais dire que $\mathrm{Ker}(\psi) = \mathfrak{A}_n$ implique par définition que pour $c \in \mathfrak{A}_n$ et pour tout $\sigma \in \mathfrak{S}_n$ on ait $c\sigma H = \sigma H$. En particulier cela implique que $\mathfrak{A}_n \subset H$, ce qui est absurde (pour des questions d'indices). Donc ψ est injective.

On considère la restriction de ce morphisme à H que l'on notera encore ψ. Alors $\psi\colon H \to \mathfrak{S}_n$ est un morphisme de groupe injectif. De plus par définition ce morphisme laisse fixe l'image de H (vu comme point de $\mathfrak{S}_n/H$), donc $\mathrm{Im}(\psi) \subset \mathfrak{S}_{n-1}$. Puisque ψ et injective, et par égalité des cardinaux entre H et $\mathfrak{S}_{n-1}$ on en déduit que ψ est un isomorphisme. □

7.10 Exo 10

Exercice 7.10. Si $n \geqslant 5$, montrer que $\mathfrak{S}_n$ n'admet pas de sous-groupes d'indice k avec $2 < k < n$. Si $H < \mathfrak{S}_n$ est un sous-groupe avec $[\mathfrak{S}_n, H] = k$, on fera agir $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ et on s'intéressera au noyau de $\mathfrak{S}_n \to \mathfrak{S}_{\mathfrak{S}_n/H} \simeq \mathfrak{S}_k$.

Démonstration. On fait agir $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ par translation. On en déduit un morphisme de groupe $\rho\colon \mathfrak{S}_n \to \mathfrak{S}_{\mathfrak{S}_n/H} \simeq \mathfrak{S}_k$. Comme $\mathrm{Ker}(\rho)$ est un sous-groupe distingué alors est soit trivial soit égal à $\mathfrak{A}_n$ (qui sont les seuls sous-groupes distingués de $\mathfrak{S}_n$).

• Si $\mathrm{Ker}(\rho) = \{\mathrm{id}\}$, alors ρ est injective, ce qui est impossible puisque $k < n$.

• Si $\mathrm{Ker}(\rho) = \mathfrak{S}_n$ cela implique que pour tous $g, x \in \mathfrak{S}_n$ on ait $gxH = xH$, soit encore $x^{-1}gx \in H$. Ce qui est impossible si $H \neq \mathfrak{S}_n$ (on prend $x = g \notin H$).

• Si $\mathrm{Ker}(\rho) = \mathfrak{A}_n$, on sait aussi que $\mathrm{Ker}(\rho) \subset H$, ce qui implique que $2 = [G : \mathrm{Ker}(\rho)] \geqslant [G : H] = k$, ce qui est impossible puisque $k > 2$.

Finalement un tel sous-groupe H n'existe pas. □

7.11 Exo 11

Exercice 7.11. Montrer qu'il existe un morphisme injectif $\mathfrak{S}_n \hookrightarrow \mathfrak{A}_{n+2}$. Peut-on plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+1}$?

Démonstration. On considère l'application $\psi\colon \mathfrak{S}_n \to \mathfrak{A}_{n+2}$ définie par $\psi(\sigma) = \sigma$ si σ est une permutation paire et $\psi(\sigma) = \sigma \circ (n+1\ n+2)$ si σ est une permutation impaire. L'application ψ est injective par unicité de l'écriture en produit de cycle disjoints. On vérifie de plus que ψ est un morphisme de groupe.

On va montrer que $\mathfrak{S}_n$ ne se plonge pas dans $\mathfrak{A}_{n+1}$. Pour des raisons de divisibilité on constate déjà que n doit être impair.

Supposons que ce soit le cas alors $\mathfrak{S}_n$ peut être vu comme un sous-groupe de $\mathfrak{A}_{n+1}$. On peut alors considérer l'action de $\mathfrak{A}_{n+1}$ sur $\mathfrak{A}_{n+1}/\mathfrak{S}_n$ par translations. Cette action induit un morphisme de groupe ψ de $\mathfrak{A}_{n+1}$ dans $\mathfrak{S}_{\mathfrak{A}_{n+1}/\mathfrak{S}_n} \simeq \mathfrak{S}_{\frac{n+1}{2}}$. Or $\frac{(n+1)!}{2} > (\frac{n+1}{2})!$, donc ψ n'est pas injectif. Alors $\mathrm{Ker}(\psi)$ est un sous-groupe distingué de $\mathfrak{A}_n$ non réduit au neutre. Pour $n \geqslant 4$ on sait que $\mathfrak{A}_{n+1}$ est simple, donc $\mathrm{Ker}(\psi) = \mathfrak{A}_{n+1}$. Mais l'action de $\mathfrak{A}_{n+1}$ sur $\mathfrak{A}_{n+1}/\mathfrak{S}_n$ par translations n'est pas triviale.

Il reste à traiter le cas $n = 3$, alors on a $\psi\colon \mathfrak{A}_4 \to \mathfrak{S}_2 \simeq \mathbf{Z}/2\mathbf{Z}$. Comme précédemment, $Ker(\psi)$ n'est ni réduit au neutre, ni $\mathfrak{A}_4$. C'est donc un sous-groupe normal de $\mathfrak{A}_4$ à savoir V_4. Mais $\mathfrak{A}_4/V_4$ est de cardinal 3, donc pas en bijection avec $\mathbf{Z}/2\mathbf{Z}$. □

8 TD8

8.1 Exo 1

Exercice 8.1. Montrer que $\mathfrak{S}_3$ s'écrit comme un produit semi-direct de $\mathbf{Z}/3\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$. Ce produit est-il direct ?

Démonstration. On constate que $H = \mathfrak{A}_3 \lhd \mathfrak{S}_3$. On pose $K = \{\mathrm{id}, (1\ 2)\} < \mathfrak{S}_3$. On a $H \cap K = \{\mathrm{id}\}$ et $HK = \mathfrak{S}_3$. Alors $\mathfrak{S}_3$ est le produit semi direct de H et de K où $\alpha : K \to \mathrm{Aut}(H), k \mapsto k \bullet k^{-1}$.

Puisque $\mathfrak{A}_3 \simeq \mathbf{Z}/3\mathbf{Z}$ et que $K \simeq \mathbf{Z}/2\mathbf{Z}$, on a bien que $\mathfrak{S}_3$ s'écrit comme un produit semi-direct de $\mathbf{Z}/3\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$.

Ce n'est pas un produit direct, car le produit direct de $\mathbf{Z}/3\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$ est abélien. □

8.2 Exo 2

Exercice 8.2. On considère le groupe $\mathrm{T}_n(\mathbf{R})$ des matrices triangulaires supérieures inversibles. Montrer que $\mathrm{T}_n(\mathbf{R})$ est le produit semi-direct de $\mathrm{U}_n(\mathbf{R})$ (matrices triangulaires supérieures avec des 1 sur la diagonale) par $\mathrm{D}_n(\mathbf{R})$ (matrices diagonales inversibles).

Démonstration. On doit vérifier que :

1. $\mathrm{U}_n(\mathbf{R})$ est distingué dans $\mathrm{T}_n(\mathbf{R})$
2. $\mathrm{D}_n(\mathbf{R})\mathrm{U}_n(\mathbf{R}) = \mathrm{T}_n(\mathbf{R})$
3. $\mathrm{D}_n(\mathbf{R}) \cap \mathrm{U}_n(\mathbf{R}) = \{\mathrm{id}\}$

Or il se trouve que, si l'on note

$$A = \begin{pmatrix} a_1 & & & \\ 0 & a_2 & (*) & \\ & & \ddots & \\ 0 & 0 & & \\ 0 & \dots & \dots & a_n \end{pmatrix}$$

Et $D = \mathrm{Diag}(a_1, \cdots, a_n)$, alors $D^{-1}A \in \mathrm{U}_n(\mathbf{R})$. Donc (2) est vérifié.

Si on considère le morphisme

$$\begin{array}{rccc} f: & \mathrm{T}_n(\mathbf{R}) & \to & \mathrm{D}_n(\mathbf{R}) \\ & A & \mapsto & \mathrm{Diag}(a_1, \cdots, a_n) \end{array}$$

alors f est un morphisme de groupes et $\mathrm{Ker}(f) = \mathrm{U}_n(\mathbf{R})$. Donc (1) est vérifié.

De plus (3) est immédiat.

Donc $\mathrm{T}_n(\mathbf{R})$ est le produit semi-direct de $\mathrm{U}_n(\mathbf{R})$ par $\mathrm{D}_n(\mathbf{R})$ □

8.3 Exo 3

Exercice 8.3. Soit G un groupe d'ordre mn avec m et n deux entiers premiers entre eux. On suppose de plus que G admet un unique sous-groupe d'ordre m noté M et, de même, un unique sous-groupe d'ordre n noté N. Montrer que $G \simeq M \times N$.

Démonstration. On va utiliser la caractérisation du produit direct. On a que $M \lhd G$ car pour tout $g \in G$, le groupe gMg^{-1} est d'ordre m, donc par unicité du sous-groupe de G d'ordre m, on a $M = gMg^{-1}$. De même on montre que $N \lhd G$.

De plus $M \cap N = \{e\}$. En effet si $a \in M \cap N$ et si k désigne l'ordre de a. Alors k divise n et k divise m (par le théorème de Lagrange). Alors k divise $\mathrm{pgcd}(m, n) = 1$.

Si $a \in M$ et $b \in N$ alors $b^{-1}aba^{-1} \in M \cap N$. Donc $ab = ba$. En particulier $MN = NM$.

De plus, comme $MN < G$, $M < MN$ et $N < MN$, alors le cardinal de M et de N divise celui de MN. Donc $|MN| = |G|$, d'où $MN = G$.

Donc par caractérisation du produit direct, on a que $G \simeq M \times N$. □

8.4 Exo 4

Exercice 8.4. Considérons $\mathrm{Aff}(\mathbf{R}) := \{f : \mathbf{R} \to \mathbf{R} \mid f(x) = ax + b,\ a \neq 0\}$ l'ensemble des transformations affines de $\mathbf{R}$. Montrer que $\mathrm{Aff}(\mathbf{R})$ est un groupe et l'écrire comme un produit semi-direct.

Démonstration. On munit $\mathrm{Aff}(\mathbf{R})$ d'une structure de groupe à l'aide de la composition. Alors $f(x) = x$ est l'élément neutre et la composée de deux applications affines est une application affine. Si $f(x) = ax+b$ et $g(x) = a'x+b'$ on vérifie que $f \circ g(x) = aa'x+ab'+b$.

Par ailleurs $\varphi\colon \mathrm{Aff}(\mathbf{R}) \to \mathbf{R}^*, ax + b \mapsto a$ est un morphisme de groupe. Donc $\mathrm{Ker}(\varphi) = \mathcal{T}(\mathbf{R})$ (l'ensemble des translations) est un sous-groupe distingué de $\mathrm{Aff}(\mathbf{R})$.

On note $\mathcal{H}(\mathbf{R})$ les homothéties. Alors $\mathcal{H}(\mathbf{R}) \cap \mathcal{T}(\mathbf{R}) = \{\mathrm{id}\}$. De plus, $\mathcal{T} \circ \mathcal{H} = \mathrm{Aff}(\mathbf{R})$. Donc $\mathrm{Aff}(\mathbf{R})$ est un produit semi-direct des translations par les homothéties. □

8.5 Exo 5

Exercice 8.5. Montrer que le groupe Q_8 ne s'écrit pas comme un produit semi-direct.

Démonstration. Si Q_8 est un produit semi-direct, alors il possède deux sous-groupes Q et N tels que $Q \cap N = \{1\}$. Or pour tous sous-groupes Q et N non réduit au neutre, on a $Q \cap N = \{1, -1\}$.

Donc Q_8 ne peut pas s'écrire comme produit semi-direct. □

8.6 Exo 6

Exercice 8.6. On considère un produit direct $G = N \rtimes Q$ fini et $g = nq$ un élément de G.

1. Montrer que l'ordre de g est de la forme $\mathrm{Ord}(g) = k\,\mathrm{Ord}(q)$ avec k qui divise $|N|$.
2. Que vaut $\mathrm{Ord}(g)$ si Q agit trivialement sur N ?
3. Si $N = \mathfrak{A}_5$, $Q = \langle (1\,2) \rangle$ et $G = \mathfrak{S}_5$, calculer $\mathrm{Ord}(g)$ pour $n = (1\,4\,3\,2\,5)$ et $q = (1\,2)$.
4. Si $G = (\mathbf{Z}/p\mathbf{Z})^p \rtimes \mathbf{Z}/p\mathbf{Z}$ est défini par l'action $1 \cdot (a_1, \dots, a_p) = (a_p, a_1 \dots, a_{p-1})$, $n = (1, 0, \dots, 0)$ et $q = 1$, montrer que
$$\forall\, 1 \leqslant i \leqslant p,\ (n, q)^i = ((\underbrace{1, \dots, 1}_{i \text{ fois}}, 0 \dots, 0), i)$$
et en déduire l'ordre de (n, q).
5. Si N est abélien et $Q = \mathbf{Z}/2\mathbf{Z}$ agit par $n \mapsto -n$, montrer que $(n, 1)$ est d'ordre 2 pour tout $n \in N$.

Démonstration.

1. On va plutôt écrire $g = (n, q)$. Par définition du produit semi direct, on a que $(n, q)^{\mathrm{Ord}(g)} = (n', q^{\mathrm{Ord}(g)}) = e$, où $n' \in N$. En particulier, cela implique que $\mathrm{Ord}(q)$ divise $\mathrm{Ord}(g)$. On pose $\mathrm{Ord}(g) = k\,\mathrm{Ord}(q)$. On peut alors remarquer que $n' = (n\alpha_q(n)\alpha_{q^2}(n) \cdots \alpha_{q^{\mathrm{Ord}(q)-1}})^k$. Or $n'^k = e$, et $n\alpha_q(n)\alpha_{q^2}(n) \cdots \alpha_{q^{\mathrm{Ord}(q)-1}} \in N$, donc k divise $|N|$.
2. Si Q agit trivialement sur N, alors G est un produit direct, donc $\mathrm{Ord}(g) = \mathrm{ppcm}(\mathrm{Ord}(n), \mathrm{Ord}(q))$.
3. $nq = (1\ 5)(2\ 4\ 3)$ qui est d'ordre 6.
4. On procède par récurrence. On note $n_i = (\underbrace{1, \dots, 1}_{i \text{ fois}}, 0 \dots, 0)$.
$$(n, q)^{i+1} = (n, q)^i (n, q) = (n_i, i)(n, q) = (n_i + \alpha_i(n), i + 1) = (n_{i+1}, i + 1)$$
En effet, $\alpha_i(n) = (\underbrace{0, \dots, 0}_{i \text{ fois}}, 1, 0 \dots, 0)$.
La question 1) nous permet de voir que l'ordre de (n, q) est une puissance de p mais que ce n'est pas p. De plus $(n, q)^{p^2})(0, 0)$. Donc l'ordre de (n, q) est p^2.

5. $(n,1)^2 = (n+\alpha_1(n), 1+1) = (n-n, 0) = (0,0)$. Donc $(n,1)$ est d'ordre 2 pour tout $n \in N$.

□

9 TD9

9.1 Exo 1

Exercice 9.1. Soient H et N deux groupes et $\alpha : H \to \mathrm{Aut}(N)$ un morphisme.

1. Si $\varphi \in \mathrm{Aut}(H)$, on pose $\beta := \alpha \circ \varphi : H \to \mathrm{Aut}(N)$. Montrer que les deux groupes $N \rtimes_\alpha H$ et $N \rtimes_\beta H$ sont isomorphes.
2. Si $u \in \mathrm{Aut}(N)$, on définit $\gamma : H \to \mathrm{Aut}(N)$ par $\gamma(h) = u\alpha(h)u^{-1}$. Montrer que les deux groupes $N \rtimes_\alpha H$ et $N \rtimes_\gamma H$ sont isomorphes.

Démonstration. fait en cours

1. On définit
$$\begin{array}{rccc} \psi\colon & N \rtimes_\alpha H & \to & N \rtimes_\beta H \\ & (n,h) & \mapsto & (n, \varphi^{-1}(h)) \end{array}$$
On vérifie que ψ définit bien un morphisme de groupe.
$$\begin{array}{rcccc} \psi((n,h)\cdot_\alpha (n',h')) & = & (n\alpha_h(n'), \varphi^{-1}(hh')) & & \\ & = & (n,\varphi^{-1}(h))\cdot_\beta (n',\varphi^{-1}(h')) & = & (n\beta_{\varphi^{-1}(h)}(n'), h) \end{array}$$
car $\beta_{\varphi^{-1}(h')} = \alpha_{h'}$. De plus ce morphisme est clairement bijectif puisque φ est un automorphisme.
2. On définit
$$\begin{array}{rccc} \psi\colon & N \rtimes_\alpha H & \to & N \rtimes_\gamma H \\ & (n,h) & \mapsto & (u(n), h) \end{array}$$
On vérifie que ψ définit bien un morphisme de groupe.
$$\begin{array}{rcccc} \psi((n,h)\cdot_\alpha (n',h')) & = & (u(n)u(\alpha_h(n')), hh') & & \\ & = & (u(n),h)\cdot_\gamma (u(n'),h') & = & (u(n)u\circ\alpha(h)\circ u^{-1}\circ u(n'), hh') \end{array}$$
De plus ce morphisme est clairement bijectif puisque u est un automorphisme.

□

9.2 Exo 2

Exercice 9.2. On rappelle que $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ a pour groupe d'automorphismes $\mathrm{Aut}(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}) \simeq \mathfrak{S}_3$. Montrer que le groupe $\mathfrak{S}_4$ est le produit semi-direct de $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ par $\mathfrak{S}_3$.

Démonstration. fait en cours Notons $V_4 = \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. On sait que $V_4 \rhd \mathfrak{S}_4$. De plus le groupe $\mathfrak{S}_3$ est un sous-groupe de $\mathfrak{S}_4$ (par un morphisme d'injection).

Comme $\mathfrak{S}_3$ ne contient pas de doubles transpositions, on a $V_4 \cap \mathfrak{S}_3 = \{e\}$. Il ne reste qu'à vérifier que $V_4\,\mathfrak{S}_3 = \mathfrak{S}_4$, ce qui est le cas car on a un isomorphisme entre $\mathfrak{S}_4/V_4$ et $\mathfrak{S}_3$.

Ainsi (théorème de cours) $\mathfrak{S}_4$ est le produit semi-direct de $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ par $\mathfrak{S}_3$.

Preuve que $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$. On considère l'action par conjugaison :
$$\begin{array}{rccc} & \mathfrak{S}_4 \times V_4 & \to & V_4 \\ & (\sigma,\tau) & \mapsto & \sigma\tau\sigma^{-1} \end{array}$$
Cette action induit un morphisme de groupe $\rho\colon \mathfrak{S}_4 \to \mathrm{Aut}(V_4) \simeq \mathfrak{S}_3$. Ce morphisme de groupe est surjectif car $\mathrm{Int}(\mathfrak{S}_3) = \mathfrak{S}_3$, donc a fortiori tous les éléments de $\mathfrak{S}_3$ peuvent être vus comme des éléments de $\mathrm{Int}(\mathfrak{S}_4)$. Donc $\mathrm{Ker}(\rho)$ est un sous-groupe distingué de $\mathfrak{S}_4$ de cardinal 4, c'est donc V_4. Le premier théorème d'isomorphisme nous permet de conclure quant à l'isomorphisme $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$. □

9.3 Exo 3

Exercice 9.3. On sait (*cf* cours) qu'il y a un unique produit semi-direct non trivial de $\mathfrak{S}_3$ par $\mathbf{Z}/2\mathbf{Z}$; préciser lequel. Montrer que les deux groupes $\mathfrak{S}_3 \rtimes \mathbf{Z}/2\mathbf{Z}$ et $\mathfrak{S}_3 \times \mathbf{Z}/2\mathbf{Z}$ sont cependant isomorphes.

Démonstration. Se donner un produit semi-direct, c'est se donner un morphisme de groupe

$$\alpha \colon \mathbf{Z}/2\mathbf{Z} \to \mathrm{Aut}(\mathfrak{S}_3) \simeq \mathfrak{S}_3 .$$

Or l'image de 1 par α est une permutation (ou l'identité, mais ce choix donne le produit direct). Or toutes les transpositions sont conjuguées dans $\mathfrak{S}_3$, donc la question 2 de l'exercice précédent nous assure que tous les produits semi-directs sont isomorphes.

On va noter τ la transposition qui correspond au morphisme $\alpha \colon \mathbf{Z}/2\mathbf{Z} \to \mathrm{Aut}(\mathfrak{S}_3)$. On pose $H = \mathfrak{S}_3$. Comme H est d'indice 2, il est donc distingué dans $\mathfrak{S}_3 \rtimes \mathbf{Z}/2\mathbf{Z}$. (Il est aussi distingué comme la partie distinguée du produit semi-direct).

On pose aussi $Q = \langle(\tau, 1)\rangle$. On vérifie que $(\tau, 1)^2 = (\mathrm{id}, 1)$. De plus, soit $(\sigma, x) \in \mathfrak{S}_3 \rtimes \mathbf{Z}/2\mathbf{Z}$. Si $x = 0$, alors

$$(\sigma, 0) \times_\alpha (\tau, 1) = (\tau, 1) \times_\alpha (\sigma, 0) = (\sigma\tau, 1).$$

Si $x = 1$, alors

$$(\sigma, 1) \times_\alpha (\tau, 1) = (\tau, 1) \times_\alpha (\sigma, 1) = (\sigma\tau, 0).$$

Donc Q est central et donc distingué dans $\mathfrak{S}_3$.

De plus il est clair que $Q \cap H = \{(\mathrm{id}, 0)\}$ et que $QH = \mathfrak{S}_3 \rtimes \mathbf{Z}/2\mathbf{Z}$. Donc $\mathfrak{S}_3 \rtimes \mathbf{Z}/2\mathbf{Z}$ est le produit direct de Q par H. □

9.4 Exo 4

Exercice 9.4. On se propose de montrer que $\mathrm{Aut}(Q_8) \simeq \mathfrak{S}_4$.

1. Montrer que $\mathrm{Aut}(Q_8)$ agit sur l'ensemble des sous-groupes d'ordre 4 de Q_8 et en déduire un morphisme $\pi : \mathrm{Aut}(Q_8) \longrightarrow \mathfrak{S}_3$.
2. Montrer que le noyau de $\mathrm{Aut}(Q_8) \longrightarrow \mathfrak{S}_3$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
3. Exhiber 2 éléments de $\mathrm{Aut}(Q_8)$ engendrant un sous-groupe $Q < \mathrm{Aut}(Q_8)$ avec $\pi(Q) = \mathfrak{S}_3$ et $\ker(\pi) \cap Q = 1$ et en déduire que $\mathrm{Aut}(Q_8) \simeq \mathfrak{S}_4$.

Démonstration.

1. Il y a 3 sous-groupes d'ordre 4 dans Q_8 qui sont de la forme $\langle\alpha\rangle$ où $\alpha \in \{i, j, k\}$. On note S l'ensemble des sous-groupes d'ordre 4 de Q_8. Un automorphisme φ de Q_8 envoie un élément d'ordre 4 sur un élément d'ordre 4, donc envoie un élément de S sur un élément de S par $\varphi(\langle\alpha\rangle) = \langle\varphi(\alpha)\rangle$.

   Cette action définit un morphisme de groupe $\pi \colon \mathrm{Aut}(Q_8) \longrightarrow \mathfrak{S}_3$. On vérifie que l'image de ρ contient les transpositions (1 2) et (1 3) qui engendrent $\mathfrak{S}_3$. En effet, si l'on pose $\varphi(i) = j$ et $\varphi(j) = i$, cela définit un automorphisme de Q_8 qui correspond à la permutation (1 2) (calculs de vérification à effectuer). De même si l'on pose $\varphi(i) = k$ et $\varphi(j) = j$, cela définit un automorphisme de Q_8 qui correspond à la permutation (1 3).

   Donc π est surjectif.

2. Un élément $\varphi \in \mathrm{Aut}(Q_8)$, si pour tout $\alpha \in \{i, j, k\}$, on a $\langle\varphi(\alpha)\rangle = \langle\alpha\rangle$. Cela implique nécessairement que $\alpha \in \{i, j, k\}$ on ait $\varphi(\alpha) = \pm\alpha$. Or φ est entièrement déterminé par la donnée de l'image de i et j. On constate que cela ne donne que 4 possibilités pour φ qui sont $\varphi \in \{\mathrm{id}, -id, \psi, -\psi\}$, où $\psi(i) = i$ et $\psi(j) = -j$. Il faut vérifier que la donnée de ψ définit bien un automorphisme de Q_8. (C'est un calcul).

   Donc $\mathrm{Ker}(\pi) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

3. On pose $\varphi_1(i) = j$ et $\varphi_1(j) = i$, cela définit un automorphisme de Q_8 qui correspond à la permutation (1 2), comme vu dans la question 1. De même si l'on pose $\varphi_2(i) = k$ et $\varphi_2(j) = j$, cela définit un automorphisme de Q_8 qui correspond à la permutation (1 3). Si l'on pose $Q = \langle \varphi_1, \varphi_2 \rangle$, on a exhibé deux éléments de $\mathrm{Aut}(Q_8)$ tels que $\pi(Q) = \mathfrak{S}_3$ (cf question 1). De plus, on a vu que $\mathrm{Ker}(\pi) = \{\mathrm{id}, -id, \psi, -\psi\}$, on a bien $\ker(\pi) \cap Q = 1$.

   On peut considérer la restriction de π à Q. Le premier théorème d'isomorphisme prouve alors que $Q \simeq \mathfrak{S}_3$. De plus $\mathrm{Ker}(\pi)Q = \mathrm{Aut}(Q_8)$ (car $\mathrm{Aut}(Q_8)/\mathrm{Ker}(\pi) \simeq Q$). De plus comme $\mathrm{Ker}(\pi)$ est distingué dans $\mathrm{Aut}(Q_8)$, on en déduit que $\mathrm{Aut}(Q_8)$ est le produit semi-direct $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \rtimes \mathfrak{S}_3 \simeq \mathfrak{S}_4$.

□

9.5 Exo 5

Exercice 9.5. On considère le groupe d'ordre p^3 (avec p premier)

$$G := \left\{ \begin{pmatrix} 1 & \star & \star \\ 0 & 1 & \star \\ 0 & 0 & 1 \end{pmatrix} \right\} < \mathrm{GL}_3(\mathbf{Z}/p\mathbf{Z}).$$

1. Déterminer $Z(G)$ et $G/Z(G)$. Vérifier que $Z(G) = D(G)$.
2. Montrer que G ne contient aucun sous-groupe Q tel que $G = Z(G) \rtimes Q$ (on pourra remarquer qu'un sous-groupe d'ordre p^2 de G est automatiquement normal et qu'il contient le centre).
3. Montrer que le groupe G peut cependant s'écrire un produit semi-direct (considérer pour cela un sous-groupe engendré par un élément du centre et par un élément non central).

Démonstration. 1. Soit A une matrice de $Z(G)$.

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

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

Pour que A soit une matrice du centre, on peut que pour tout $a', b' \in \mathbf{Z}/p\mathbf{Z}$ on ait $ab' = a'b$. Prendre $a' = 0$ et $b' = 1$ implique $a = 0$ et prendre $a' = 1$ et $b' = 0$ implique $b = 0$. On vérifie réciproquement que toute matrice de la forme

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

est dans le centre.

Puisque le centre est d'ordre p, alors $G/Z(G)$ est d'ordre p^2. Un groupe d'ordre p^2 est abélien donc isomorphe à $\mathbf{Z}/p^2\mathbf{Z}$ ou $(\mathbf{Z}/p\mathbf{Z})^2$. On peut alors vérifier que $G/Z(G)$ ne contient pas d'élément d'ordre p^2. Donc $G/Z(G) = (\mathbf{Z}/p\mathbf{Z})^2$.

Comme $G/Z(G)$ est abélien alors $D(G) \subset Z(G)$. Par ailleurs l'ordre de $D(G)$ divise l'ordre de $Z(G)$, donc c'est soit 1 soit p. Or l'ordre de $D(G)$ ne peut pas être 1 car G n'est pas abélien, donc l'ordre de $D(G)$ vaut p et donc $D(G) = Z(G)$.

2. Si G s'écrit sous la forme $G = Z(G) \rtimes Q$, alors Q est d'ordre p^2. Par un exercice de la feuille 4 (exercice 3 qui dit que si H d'indice p avec p le plus petit diviseur premier de G alors H est distingué), on sait que Q est distingué. De plus, comme Q est d'ordre p^2, il est abélien. Si l'intersection de Q avec le centre était réduite au neutre, cela signifierait que G serait produit semi-direct (qui serait en fait un produit direct) de deux groupes abéliens et serait donc abélien. Comme ce n'est pas le cas l'intersection de Q avec le centre n'est pas réduite au neutre. Comme $Z(G)$ est cyclique d'ordre premier, et que Q contient un élément de $Z(G)$ qui n'est pas le neutre, alors Q contient $Z(G)$.

3. On pose
$$Q = \langle Z(G), \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rangle$$
Alors Q est d'ordre p^2 (car la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre p), donc Q est distingué. On pose aussi
$$H = \langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \rangle$$
Alors H est d'ordre p. On a bien $H \cap Q = \{\mathrm{id}\}$, et $HQ = G$, car $G/Q \simeq H$. D'après la caractérisation des produits semi-directs, on en déduit que $G \simeq Q \rtimes H$.

□

10 TD10

Théorème 10.1 (Théorème de Sylow (rappel))**.** *Soit G un groupe de cardinal $|G| = p^\alpha m$ avec p premier qui ne divise pas m.*

1. *Si H est un p-sous-groupe de G, alors il existe un p-Sylow S tel que $H \subset S$.*
2. *Les p-Sylow sont tous conjugués et leur nombre n_p divise n.*
3. *On a $n_p \equiv 1 \mod (p)$, donc n_p divise m.*

10.1 Exo1

Exercice 10.1. Décrire les sous-groupes de Sylow de $\mathfrak{A}_4$ et $\mathfrak{A}_5$ (structures, cardinal et éventuellement structure du normalisateur).

Si X est une partie de G, le normalisateur de X dans G est donné par

$$N_G(X) = \{g \in G \mid gXg^{-1} = X\}.$$

Démonstration. On sait que $\operatorname{Ord} \mathfrak{A}_4 = 12 = 4 \times 3$. Les p-Sylow sont donc d'ordre 4 ou 3. On sait que $\mathfrak{A}_4$ possède un sous-groupe distingué d'ordre 4 qui est V_4 (groupe engendré par les doubles transpositions). On sait que V_4 est distingué dans G donc son normalisateur est $\mathfrak{A}_4$.

Les 3-Sylow de $\mathfrak{A}_4$ sont les sous-groupes engendrés par un 3-cycle. Soit c un 3-cycle. Les sous-groupes de $\mathfrak{A}_4$ contenant c sont $\langle x \rangle$ et $\mathfrak{A}_4$. Et $N_G(\langle c \rangle)$ est un sous-groupe de $\mathfrak{A}_4$ contenant c, mais ce n'est pas $\mathfrak{A}_4$ car $\langle c \rangle$ n'est pas distingué. Donc $N_G(\langle c \rangle) = \langle c \rangle$.

On sait que $\operatorname{Ord} \mathfrak{A}_5 = 60 = 5 \times 4 \times 3$.

Les 5-Sylow sont les sous-groupes engendrés par un 5-cycle.

Les 3-Sylow sont les sous-groupes engendrés par un 3-cycle.

Les 4-Sylow sont les sous-groupes engendrés par 2 doubles transpositions (les 2 doubles transpositions font intervenir les mêmes éléments a, b, c, d), ils sont alors isomorphes à V_4.

Par une relation orbite stabilisateur, on sait que si P est un p-Sylow $|N_G(P)| = |G|/n_p$

On montre $N_G((1\ 2\ 3)) = \langle (1\ 2\ 3), (1\ 2)(4\ 5) \rangle$.

$N_G((1\ 2)(3\ 4))) = \mathfrak{A}_4$.

$N_G((1\ 2\ 3\ 4\ 5)) = \langle (1\ 2\ 3\ 4\ 5), (2\ 5)(3\ 4) \rangle$ □

10.2 Exo2

Exercice 10.2. Soit G un groupe et H un sous-groupe de G.

1. On se donne p un diviseur de l'ordre de H et P un p-Sylow de H. Montrer qu'il existe P_1 un p-Sylow de G tel que $P = P_1 \cap H$.
2. Réciproquement, montrer que si $H \lhd G$, alors $P_1 \cap H$ est un p-Sylow de H pour tout P_1 p-Sylow de G.
3. En considérant $G = \mathfrak{A}_5$ et $H = \mathfrak{A}_4 < G$, montrer que si P est un p-Sylow de G alors $H \cap K$ n'est pas nécessairement un p-Sylow de H (prendre $p = 2$).

Démonstration.

1. P est un p-sous-groupe de G donc d'après le premier théorème de Sylow, il existe P_1 un p-Sylow de G tel que $P \subset P_1$. Par ailleurs $P_1 \cap H \supset P \cap H = P$. Donc $P_1 \cap H = P$.
2. Soit P_1 un p-Sylow de G. Alors $P_1 \cap H$ est un sous-groupe de P_1 donc un p-groupe. C'est donc un p-sous-groupe de H. Il existe donc un p-Sylow P de H tel que $P_1 \cap H \subset P$. Par la question 1), il existe un p-Sylow P_2 de G tel que $P = P_2 \cap H$. Comme tous les p-Sylow de G sont conjugués, il existe $g \in G$ tel que $P_1 = xP_2x^{-1}$. Ainsi, comme H est distingué, on a $H = xHx^{-1}$ et donc

$$P_1 \cap H = xP_2x^{-1} \cap xHx^{-1} = x(P_2 \cap H)x^{-1} = xPx^{-1}$$

Comme xPx^{-1} est un p-Sylow de H alors $P_1 \cap H$ est un p-Sylow de H.

3. On prend $P = \langle (1\ 2)(3\ 5), (1\ 3)(2\ 5) \rangle$ qui est un 2-Sylow de G. Mais $H = \mathfrak{A}_4$ est tel que $P \cap H = \{\mathrm{id}\}$, or $\{\mathrm{id}\}$ n'est pas 2-Sylow de H.

□

10.3 Exo3

Exercice 10.3. Décrire les structures possibles pour les groupes d'ordre $1225 = 5^2 7^2$ (pour cela, montrer que les Sylow sont distingués).
On constate que tous les groupes d'ordre 225 sont abéliens ; peut-on conclure la même chose pour les groupes d'ordre $441 = 3^2 7^2$?

Démonstration. 1. D'après le théorème de Sylow, on a $n_5 \mid 7^2$, donc $n_5 \in \{1, 7, 49\}$. De plus $n_5 \equiv 1 \mod 5$, donc $n_5 = 1$. Il y a un unique 5-Sylow. Comme tous les 5-Sylow sont conjugués alors l'unique 5-Sylow est distingué.

D'après le théorème de Sylow, on a $n_7 \mid 5^2$, donc $n_7 \in \{1, 5, 25\}$. De plus $n_7 \equiv 1 \mod 7$, donc $n_7 = 1$. Donc le 7-Sylow de G est distingué.

G possède un unique sous groupe N d'ordre 49 et un unique sous-groupe Q d'ordre 25, or $\gcd(49, 25) = 1$, donc d'après TD8 exercice 3, G est le produit direct de N et Q. En particulier G est abélien.

2. D'après le théorème de Sylow, on a $n_7 \mid 3^2$, donc $n_7 \in \{1, 3, 9\}$. De plus $n_7 \equiv 1 \mod 7$, donc $n_7 = 1$. Donc le 7-Sylow de G est distingué.

Par contre $n_3 \mid 49$ et $n_3 \equiv 1 \mod 3$, donc $n_3 \in \{1, 7, 49\}$.

En particulier, soit $N = \mathbf{Z}/49\mathbf{Z}$, $H = (\mathbf{Z}/3\mathbf{Z})^2$, et

$$\begin{array}{rccc} \alpha : & (\mathbf{Z}/3\mathbf{Z})^2 & \to & \mathrm{Aut}(\mathbf{Z}/49\mathbf{Z}) \\ & (0,1) & \mapsto & x \mapsto 0 \\ & (1,0) & \mapsto & x \mapsto 18 * x \end{array}$$

C'est bien un morphisme de groupes car $18^3 \equiv 1 \mod 49$.

Par ailleurs $18^2 \equiv 30 \mod 49$.

On vérifie de plus que le groupe $N \rtimes_\alpha H$ est non abélien

$$(1, [0,1]) \cdot_\alpha (1, [0,2]) = (1 + \alpha(0,1)(1), [0,0]) = (19, [0,0])$$

$$(1, [0,2]) \cdot_\alpha (1, [0,1]) = (1 + \alpha(0,2)(1), [0,0]) = (31, [0,0])$$

Ce n'est donc pas un produit direct.

□

10.4 Exo4

Exercice 10.4. Soient $n \geqslant 2$ et p un entier premier.

1. Montrer que $|GL_n(\mathbf{Z}/p\mathbf{Z})| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.
2. Montrer que le sous-groupes des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$.

Démonstration. 1. Une matrice de $GL_n(\mathbf{Z}/p\mathbf{Z})$ est une matrice dont les colonnes forment une famille libre. Pour la première colonne on a $p^n - 1$ possibilités (tout sauf la colonne nulle). Pour la seconde, elle ne doit pas être dans l'espace vectoriel engendrée par la première, on a donc $p^n - p$ possibilité. Pour la $i$ème colonne, elle ne doit pas être dans l'espace vectoriel engendré par les $i - 1$ème précédente. Il y a donc $p^n - p^{i-1}$.

Finalement on trouve bien $|GL_n(\mathbf{Z}/p\mathbf{Z})| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

2. On vérifie facilement que l'ensemble T des matrices triangulaires supérieures avec des 1 sur la diagonale est un sous-groupe de $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$. De plus en les dénombrant, on remarque que $|(|T) = \prod_{i=1}^{n-1} p^i$.
On vérifie que $|GL_n(\mathbf{Z}/p\mathbf{Z})|/|(|T) = \prod_{i=0}^{n-1}(p^{n-i}-1)$ qui est premier avec p. Donc T est un p-Sylow de $GL_n(\mathbf{Z}/p\mathbf{Z})$.

□

10.5 Exo5

Exercice 10.5. On va donner une autre démonstration du premier théorème de Sylow (existence d'un p-Sylow).

1. Soient G un groupe admettant un p-Sylow P et $H < G$ un sous-groupe de G. Montrer qu'il existe $g \in G$ tel que $gPg^{-1} \cap H$ est un p-Sylow de H. Pour cela, on fera agir H sur G/P et on s'intéressera aux cardinaux des orbites.
2. Soit maintenant G d'ordre $|G| = n$ et p un diviseur de n. Montrer qu'il existe un plongement de G dans $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ et, en utilisant l'exercice précédent, montrer que G admet un p-Sylow.

Démonstration. 1. On définit l'action de H sur G/P par

$$\begin{array}{ccc} H \times G/P & \to & G/P \\ (h, xP) & \mapsto & hxP \end{array}$$

On montre que

$$\mathrm{Stab}(xP) = \{h \in H \mid hxP = xP\} = x^{-1}Px \cap H$$

De plus on a la relation suivante :

$$|G/P| = \sum_{i=1}^{r} \mathrm{Orb}(x_iP) = \sum_{i=1}^{r} \frac{|H|}{|\mathrm{Stab}(x_iP)|}$$

Or, puisque P est un p-Sylow, alors $|G/P|$ n'est pas divisible par P. Donc il existe j tel que $|\mathrm{Stab}(x_jP)| = |x_j^{-1}Hx_j|$ ne soit pas divisible par p. Ce qui prouve que $x_j^{-1}Px_j \cap H$ est un p-Sylow de H.

2. Par le théorème de Cayley, il existe un plongement de G dans $\mathfrak{S}_n$. De plus, il existe un plongement de $\mathfrak{S}_n$ dans $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$: à chaque permutation, on lui associe sa matrice de permutation. On identifie alors G à un sous-groupe de $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$. Or par l'exercice précédent $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ possède un p-Sylow, donc d'après la question 1), G possède aussi un p-Sylow.

□

11 TD11

Théorème 11.1 (Théorème de Sylow (rappel))**.** *Soit G un groupe de cardinal $|G| = p^\alpha m$ avec p premier qui ne divise pas m.*

1. *Si H est un p-sous-groupe de G, alors il existe un p-Sylow S tel que $H \subset S$.*
2. *Les p-Sylow sont tous conjugués et leur nombre n_p divise n.*
3. *On a $n_p \equiv 1 \mod (p)$, donc k divise m.*

11.1 Exo 1

Exercice 11.1. Montrer qu'un groupe d'ordre pq (avec p et q deux entiers premiers distincts) n'est pas simple.

Démonstration. On suppose que $p > q$. D'après le théorème de Sylow, il existe un p-Sylow disons S et le nombre de p-Sylow divise q et est congru à 1 modulo p. En particulier $n_p \leqslant q < p$, et $n_p \equiv 1 \mod (p)$. Finalement le seul choix possible est $n_p = 1$.

Comme tous les p-Sylow sont conjugués et qu'il n'y en a qu'un, on en déduit que S est distingué, donc que le groupe n'est pas simple. □

11.2 Exo 2

Exercice 11.2. Montrer qu'un groupe d'ordre p^2q n'est pas simple (attention au cas $p = 2$ et $q = 3$).

Démonstration. On va traiter deux cas selon que $p > q$ ou que $q > p$.

• Si $p > q$, alors il existe un p-Sylow et le nombre n_p de p-Sylow vérifie $n_p|q$ et $n_p \equiv 1 \mod (p)$. En particulier $n_p \leqslant q < p$, donc $n_p = 1$. Comme tous les p-Sylow sont conjugués, alors S est un sous-groupe distingué.

• Si $q > p$, alors il existe un q-Sylow S, et le nombre n_q de q-Sylow vérifie $n_q|p^2$ et $n_q \equiv 1 \mod (q)$. En particulier $n_q \in \{1, p, p^2\}$.

Si $n_q = p$ alors comme $q > p$, on aurait $p \equiv 1 \mod (q)$, ce qui est impossible. Si $n_q = p^2$, alors $p^2 \equiv 1 \mod (q)$, et donc $p \equiv 1 \mod (q)$ ou $p \equiv -1 \mod (q)$. Comme le premier cas est impossible, on a nécessairement $p \equiv -1 \mod (q)$, ce qui implique $p = q-1$. Or q étant impair, alors p est pair, ce qui n'est possible que si $p = 2$ et $q = 3$. Dans tous les autres cas, on a alors $n_q = 1$, et donc S est distingué.

Si jamais $p = 2$ et $q = 3$. Supposons que $n_3 \neq 1$, alors comme $n_3|4$ et $n_3 \equiv 1 \mod (3)$, on a $n_3 = 4$. Ainsi le groupe contient quatre 3-Sylow et leur union contient 8 éléments d'ordre 3 (et l'identité). Il ne reste alors de la place que pour un 2-Sylow, qui est alors unique et donc distingué. □

11.3 Exo 3

Exercice 11.3. Montrer qu'un groupe d'ordre p^2q^2 n'est jamais simple (attention au cas $p = 2$ et $q = 3$).

Démonstration. Par symétrie, on peut supposer sans perte de généralité que $p > q$. Il existe un p-Sylow, disons S et le nombre n_p de p-Sylow vérifie $n_p|q^2$ et $n_p \equiv 1 \mod (p)$. En particulier $n_q \in \{1, q, q^2\}$.

Si $n_p = q$ alors comme $p > q$, on aurait $q \equiv 1 \mod (p)$, ce qui est impossible.

Si $n_p = q^2$, alors $q^2 \equiv 1 \mod (p)$, et donc $q \equiv 1 \mod (p)$ ou $q \equiv -1 \mod (p)$. Comme le premier cas est impossible, on a nécessairement $q \equiv -1 \mod (p)$, ce qui implique $q = p - 1$. Or p étant impair, alors q est pair, ce qui n'est possible que si $q = 2$ et $p = 3$. Dans tous les autres cas, on a alors $n_p = 1$, et donc S est distingué.

Si jamais $p = 2$ et $q = 3$. Comme tous les 3-Sylow sont conjugués on peut définir une action de G sur l'ensemble de ses 3-Sylow. On sait que $n_3|4$ et $n_3 \equiv 1 \mod (3)$, alors

$n_3 = 1$ ou 4. Supposons que $n_3 = 4$. Cela induit un morphisme de groupe $\varphi\colon G \to \mathfrak{S}_4$. Or $4! = 24$ et $24 < 36$, donc φ ne peut pas être injectif et son noyau est un sous-groupe distingué non trivial. □

11.4 Exo 4

Exercice 11.4. Montrer qu'un groupe d'ordre pqr (avec $p > q > r$ trois entiers premiers) n'est jamais simple.

Démonstration. Puisque $n_p | qr$ on a que $n_p \in \{1, q, r, qr\}$. Puisque $n_p \equiv 1 \mod (p)$, on ne peut pas avoir $n_p \in \{q, r\}$. Supposons que $n_p = qr$. Alors deux p-Sylow ont une intersection triviale (car engendrés par élément d'ordre p, et si leur intersection est non triviale alors ils sont égaux). Le groupe G contient alors $qr(p-1)$ éléments d'ordre p. Si en outre $n_r, n_q \neq 1$, alors comme $n_r | pq$ et $n_q | pr$, alors $n_r \geqslant q$ et $n_q \geqslant r$ et G contient au moins $q(r-1)+r(q-1)$ éléments d'ordre r ou q. Ainsi, en comptant le neutre pour G, on a :

$$qr(p-1) + q(r-1) + r(q-1) + 1 \leqslant |G| = pqr$$

En particulier, on a $q(r-1) + r(q-1) + 1 \leqslant qr$, soit encore $q + r \geqslant qr + 1$. Puisque $2 \leqslant r < q$, on a en particulier $2q + 1 \leqslant 2q$, ce qui est absurde.

Donc $n_p = qr$ donne $n_q = 1$ ou $n_r = 1$, dans tous les cas G possède un sous-groupe distingué. □

11.5 Exo 5

Exercice 11.5.

1. Montrer que si $|G| \in \{24, 40, 48, 56\}$ alors G n'est pas simple (si besoin, faire agir G sur un ensembles de Sylows).
2. Déduire de la question précédente et des exercices 11.1, 11.2, 11.3 et 11.4 qu'un groupe G d'ordre $|G| < 60$ simple est alors cyclique d'ordre p premier.

Démonstration.

1. Si $|G| = 24$, on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2 | 3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 24$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué de G non trivial.
2. Si $|G| = 40 = 2^3 \times 5$. Alors $n_5 | 8$ et $n_5 \equiv 1 \mod (5)$. Donc $n_5 \in \{1, 2, 4, 8\}$. Or le seul élément de cet ensemble qui vérifie $n_5 \equiv 1 \mod (5)$ est 1. Donc $n_5 = 1$.
3. Si $|G| = 48 = 2^4 \times 3$ on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2 | 3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 48$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué de G non trivial.
4. Si $|G| = 56$ alors $n_7 | 8$ et $n_7 \equiv 1 \mod (7)$. Alors $n_7 \in \{1, 8\}$. Supposons que $n_7 = 8$. Alors deux 7-Sylow disjoints ont une intersection triviale et G possède $8 \times 6 = 48$ éléments d'ordre 7. Il reste donc $56 - 48 = 8$ autres éléments, soit juste assez de place pour un 2-Sylow qui est donc unique et distingué. Dans tous les cas, G n'est pas simple.
5. Soit G un groupe d'ordre < 60 non banal (pas un $\mathbf{F}_p$). Si p est premier et $\alpha > 1$, alors un groupe d'ordre p^α n'est pas simple car son centre n'est pas réduit au neutre (et tout sous-groupe du centre est distingué). Les exercices 11.1, 11.2, 11.3 et 11.4 nous assurent que tout groupe d'ordre pq, p^2q, p^2q^2 et pqr ne sont pas simple. Si jamais un groupe G a un facteur de type p^3q. Comme $3^3 \times 5 > 60$, les seules possibilités sont $|G| \in \{2^3 \times 3, 2^3 \times 5, 2^3 \times 7, 3^3 \times 2\}$. Mais $3^3 \times 2 = 54$ n'est pas simple (on fait comme dans l'exercice 11.1 en considérant les 3-Sylow) et on a vu que dans les autres possibilités G n'est pas simple. Si G a un facteur de type p^4q, alors comme $3^4 = 81 > 60$, et que $2^4 \times 5 = 80 > 60$, la seule possibilité est $|G| = 2^4 \times 3 = 48$. On

a vu qu'un tel groupe n'était pas simple. Comme $2^5 = 32$, on n'aura pas de groupe avec un facteur du type $p^5 q$.

On a couvert toutes les possibilités, donc un groupe G d'ordre $|G| < 60$ simple est alors cyclique d'ordre p premier.

□

11.6 Exo 6

Exercice 11.6. Soit G un groupe simple d'ordre $60 = 2^2 \cdot 3 \cdot 5$.

1. Montrer que les nombres de sous-groupes de Sylow vérifient
$$\text{ﾑ}_5 = 6, \quad \text{ﾑ}_3 \in \{4, 10\} \quad \text{et} \quad \text{ﾑ}_2 \in \{3, 5, 15\}.$$
2. En faisant agir G sur l'ensemble des 3-Sylows, montrer que $\text{ﾑ}_3 = 4$ est exclue. De même, montrer que $\text{ﾑ}_2 = 3$ ne peut survenir.
3. Si $\text{ﾑ}_2 = 5$, faire agir G sur les 2-Sylows et montrer que $G \simeq \mathfrak{A}_5$ (on vérifiera que $\mathfrak{A}_5$ a bien les caractéristiques suivantes : $\text{ﾑ}_2(\mathfrak{A}_5) = 5$, $\text{ﾑ}_3(\mathfrak{A}_5) = 10$ et $\text{ﾑ}_5(\mathfrak{A}_5) = 6$).
4. Par un argument de comptage, montrer que, si $\text{ﾑ}_2 = 15$, alors il existe S_1 et S_2 des 2-Sylows vérifiant $S_1 \cap S_2 = \{1, g\}$. Montrer que le centralisateur de g a pour ordre $|C_G(g)| = 12$ ou 20 et aboutir à une contradiction.

Démonstration. On n'a jamais $\text{ﾑ}_k = 1$ sinon G ne serait pas distingué.

1. D'après le théorème de Sylow, on sait que $\text{ﾑ}_5 \in \{2, 3, 4, 6, 12\}$ et que $\text{ﾑ}_5 \equiv 1 \mod (5)$. Donc nécessairement $\text{ﾑ}_5 = 6$.

   De même $\text{ﾑ}_3 \in \{2, 4, 5, 10, 20\}$ et $\text{ﾑ}_3 \equiv 1 \mod (3)$, donc nécessairement $\text{ﾑ}_3 \in \{4, 10\}$.

   De même $\text{ﾑ}_2 \in \{3, 5, 15\}$ et $\text{ﾑ}_3 \equiv 1 \mod (2)$, ce qui n'apporte aucune information supplémentaire.
2. Supposons par l'absurde que $\text{ﾑ}_3 = 4$, alors l'action de G sur ses 3-Sylow par conjugaison induit un morphisme $\rho \colon G \to \mathfrak{S}_4$. Pour des raisons de cardinalité, ce morphisme n'est pas injectif. Il n'est pas non plus trivial car tous les 3-Sylow sont conjugués. Cela implique que $\mathrm{Ker}(\rho)$ est un sous-groupe distingué non trivial de G, ce qui est impossible puisque G est simple.

   Les mêmes arguments en faisant agir G sur ses 2-Sylow prouve que $\text{ﾑ}_2 = 3$ est exclu.
3. Si $\text{ﾑ}_2 = 5$, alors l'action de G sur ses 2-Sylow induit un morphisme de groupe $\rho \colon G \to \mathfrak{S}_5$. Puisque G est simple et que ρ n'est pas trivial, alors ce morphisme est nécessairement injectif. Donc G s'identifie à un sous-groupe d'ordre 60 de $\mathfrak{S}_5$. Un tel groupe G étant distingué dans $\mathfrak{S}_5$ c'est nécessairement $\mathfrak{A}_5$.
4. On suppose que $\text{ﾑ}_2 = 15$. Soient S_1 et S_2 deux 2-Sylow distincts. Alors $S_1 \cap S_2$ est un sous-groupe de S_2 donc est d'ordre 1 ou 2 (pas 4 puisque c'est un sous-groupe propre). Supposons que tous les 2-Sylow soient d'intersection triviale. Alors $|\cup_{i=1}^{15} S_i| = 3 \times 15 + 1 = 46$. Il existe donc 45 éléments d'ordre 2 ou 4 dans G, mais puisque $\text{ﾑ}_3 = 10$, il y a aussi $2 \times 10 = 20$ éléments d'ordre 3. C'est impossible puisque $45 + 20 > 60$.

   Donc il existe S_1 et S_2 des 2-Sylows vérifiant $S_1 \cap S_2 = \{1, g\}$.

   Par définition $C_G(g) = \{x \in G \mid xg = gx\}$. Puisque $C_G(g)$ est un sous-groupe de G alors $|C_G(g)||60$. De plus, tout groupe d'ordre 4 est abélien, donc $S_1 \subset C_G(g)$, donc $4||C_G(g)|$. Finalement on a $|C_G(g)| \in \{12, 20, 60\}$. Or $|C_G(g)| \neq 60$ puisque sinon on aurait $g \in Z(G)$, ce qui est impossible puisque $Z(G) = \{e\}$ par simplicité de G.

   • Supposons que $|C_G(g)| = 20$. On considère l'action de G sur $G/C_G(g)$ (qui est de cardinal 3). Elle induit un morphisme de groupe $\rho \colon G \to \mathfrak{S}_3$. Pour des raisons de cardinalité, ce morphisme n'est pas injectif. Il n'est pas non plus égal à G. Donc son

noyau est un sous-groupe distingué non trivial de G. Ce qui est absurde puisque G est simple.

• Supposons que $|C_G(g)| = 12$. Comme précédemment, on considère l'action de G sur $G/C_G(g)$ (qui est de cardinal 5). Elle induit un morphisme de groupe $\rho\colon G \to \mathfrak{S}_5$. Le noyau de ce morphisme n'est pas tout G. Donc ρ est injectif (sinon G aurait un sous-groupe distingué non trivial) et G s'identifie à un sous-groupe d'ordre 60 de $\mathfrak{S}_5$. Or il n'y en a qu'un et c'est $\mathfrak{A}_5$. Cependant $\mathfrak{A}_5$ ne possède que cinq 2-Sylow. C'est absurde.

Donc $s_2 = 5$.

□

12 TD12

12.1 Exo 1

Exercice 12.1. Montrer qu'un groupe G d'ordre $|G| < 60$ est nécessairement résoluble (on pourra utiliser les résultats de la feuille 11).

Démonstration. On va procéder par récurrence en utilisant la feuille de 11) exercice 5, qui affirme que tout groupe, qui n'est pas un p-groupe, d'ordre < 60 n'est pas simple.

1. Si $|G| = p^\alpha$. On se référera au résultat de l'exercice 2.
2. Dans le cas général, on procédera par récurrence. Un groupe d'ordre 2 est résoluble. On suppose savoir démontrer que tout groupe d'ordre $2 \leqslant k < n$ est résoluble.

   D'après la feuille 7) tout groupe d'ordre < 60 qui n'est pas un p-groupe n'est pas simple. Soit G un groupe d'ordre $n < 60$. Si c'est un p-groupe il est résoluble, sinon il possède un sous-groupe H distingué non trivial. Alors H est d'ordre $< n$ donc est résoluble par hypothèse de récurrence. Alors G/H est d'ordre $< n$ donc est résoluble par hypothèse de récurrence. Finalement on en déduit que G est résoluble.

   Dans tous les cas, G est résoluble.

□

Démonstration. On va montrer que si p et q sont deux nombres premiers alors un groupe d'ordre dans l'ensemble $\{p^\alpha, pq, p^2q, p^2q^2pqr\}$ est toujours résoluble. Pour couvrir l'ensemble des groupes de cardinal inférieur à 60, il restera à prouver que les groupes d'ordre $\{24, 36, 40, 48, 54, 56\}$ sont résolubles.

1. Si $|G| = p^\alpha$. On se référera au résultat de l'exercice 2.
2. Si $|G| = pq$. Sans perdre de généralité on peut suppose que $p > q$, alors soit S un p-Sylow de G. On a vu (feuille 7, mais c'est corollaire du théorème de Sylow) que S est distingué. De plus $G/S \simeq \mathbf{Z}/q\mathbf{Z}$ est cyclique donc abélien, et S est d'ordre p donc abélien. Ainsi $\{e\} \lhd S \lhd G$, donc G est résoluble.
3. Si $|G| = p^2q$.

   Si $p > q$, alors (feuille 7) l'unique p-Sylow S est distingué et G/S est cyclique donc abélien. De plus S est d'ordre p^2 donc abélien. Ainsi $\{e\} \lhd S \lhd G$, donc G est résoluble.

   Si $q > p$ et $p \neq 2, q \neq 3$, alors (feuille 7) il existe un unique q-Sylow qui est distingué. De plus G/S est d'ordre p^2 donc abélien et S est d'ordre q donc cyclique donc abélien. Ainsi $\{e\} \lhd S \lhd G$, donc G est résoluble.

   Si $p = 2, q = 3$, alors on a vu que soit un 2-Sylow S est unique et donc distingué , c'est c'est le cas pour les 3-Sylow. Dans tous les cas, on peut avoir une suite du type $\{e\} \lhd S \lhd G$ donc G est résoluble.
4. Si $|G| = pqr$ alors (feuille 7), G admet au moins un Sylow distingué H qu'on peut supposer être d'ordre p sans perte de généralité. Alors H est résoluble et G/H est résoluble (car d'ordre qr), donc G est résoluble.
5. Si $|G| = 24$, on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2|3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 24$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué H de G non trivial. En étudiant les cas selon l'image de φ on trouve que $|H| \in \{4, 8, 12\}$. Dans tous les cas H et G/H sont résolubles, donc G est résoluble.
6. Si $|G| = 36$, comme tous les 3-Sylow sont conjugués on peut définir une action de G sur l'ensemble de ses 3-Sylow. On sait que $n_3|4$ et $n_3 \equiv 1 \mod (3)$, alors $n_3 = 1$ ou 4. Supposons que $n_3 = 4$. Cela induit un morphisme de groupe $\varphi\colon G \to \mathfrak{S}_4$. Or

$4! = 24$ et $24 < 36$, donc φ ne peut pas être injectif et son noyau H est un sous-groupe distingué non trivial. En examinant l'image de G les différentes possibilités sont $|H| \in \{18, 12, 9, 6, 3\}$. Dans tous les cas H et G/H sont résolubles sont G est résoluble.

7. Si $|G| = 40$, alors (feuille 7) il n'y a qu'un unique 5-Sylow S qui est donc distingué. De plus G/S est de cardinal 8 donc résoluble, et S est résoluble, donc G est résoluble.
8. Si $|G| = 48$, on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2|3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 48$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué H de G non trivial. En étudiant les cardinaux, les seules possibilités pour H sont $\{8, 16, 24\}$. Ainsi H est résoluble et G/H est résoluble, donc G est résoluble.
9. Si $|G| = 54 = 3^3 \times 2$, alors $\lambda_3 = 1$ donc le 3-Sylow S est distingué d'ordre 9 donc résoluble et G/S est d'ordre 2 donc résoluble. Donc G est résoluble.
10. Si $|G| = 56 = 2^3 \times 3$, alors (c.f feuille 7) soit il possède un 2-Sylow S distingué et alors S et G/S sont résolubles, soit il possède un 7-Sylow S' distingué et alors S' et G/S' sont résolubles. Dans tous les cas, G est résoluble.

□

12.2 Exo 2

Exercice 12.2. Montrer qu'un p-groupe est résoluble.

Démonstration. Si $|G| = p^\alpha$. On va procéder par récurrence sur α. Le résultat est évident si $\alpha = 1$. Sinon le centre d'un p-groupe n'est pas réduit au neutre alors $G/Z(G)$ est d'ordre p^β avec $\beta < \alpha$. Par hypothèse de récurrence, $G/Z(G)$ est résoluble et $Z(G)$ est résoluble, donc G est résoluble. □

12.3 Exo 3

Exercice 12.3. Montrer que le sous-groupe $B_n(\mathbf{R}) < \mathrm{GL}_n(\mathbf{R})$ formé des matrices triangulaires supérieures (et inversibles) est résoluble. On pourra considérer le sous-groupe $N < B_n(\mathbf{R})$ des matrices avec des 1 sur la diagonale. On vérifiera que $N \lhd B_n(\mathbf{R})$ et que N et $B_n(\mathbf{R})$ sont résolubles.

Démonstration.

1. Montrons que N est distingué et que $B_n(\mathbf{R})/N$ est résoluble. Par le morphisme
$$\begin{array}{rccc} \varphi\colon & B_n(\mathbf{R}) & \to & (\mathbf{R}^\times)^n \\ & (a_{i,j})_{1\leqslant i,j\leqslant n} & \mapsto & (a_{i,i})_{1\leqslant i\leqslant n} \end{array}$$
On vérifie que φ est un morphisme de groupe, et que son noyau $\mathrm{Ker}\varphi = N$. Puisque le morphisme φ est surjectif, on en déduit du premier théorème d'isomorphisme que $B_n(\mathbf{R})/N$ est isomorphe à $(\mathbf{R}^\times)^n$ qui est résoluble car abélien.
2. Montrons que N est résoluble. L'idée est de montrer qu'à chaque fois qu'on calcule un commutateur, on fait "remonter" la diagonale de 0.
Pour tout entier $m \geqslant 1$ (tant que ça a du sens), on pose
$$N_m = \{A \in N \mid a_{i,j} = 0 \text{ si } \ 0 < j - i < m\}.$$
On va voir que $D^(m)(G) < N_m$.
On considère
$$\begin{array}{rccc} \varphi_{m+1}\colon & N_m & \to & N \\ & (a_{i,j}) & \mapsto & (a'_{i,j}) \end{array}$$

où $a'_{i,j} = a_{i,j}$ si $j-i=k$ et $a'_{i,j}=0$ sinon. Alors φ_{m+1} est un morphisme de groupe. En effet soit $A=(a_{i,j})$ et $B=(b_{i,j})$ deux éléments de N_m. On note $AB=(c_{i,j})$. Alors

$$\begin{aligned} c_{i,i+k} &= \sum_{u=0}^{n} a_{i,u}b_{u,i+k} \\ &= \sum_{u=i+1}^{n} a_{i,u}b_{u,i+k} + b_{i,i+k} \\ &= \sum_{u=i+k}^{n} a_{i,u}b_{u,i+k} + b_{i,i+k} \\ &= a_{i,i+k} + b_{i,i+k} \end{aligned}$$

De plus $\mathrm{Ker}(\varphi_{m+1}) = N_{m+1}$. (Se lit facilement sur l'écriture matricielle). On vient donc de construire une suite de groupe $N = N_1 \geqslant N_2 \geqslant \cdots \geqslant N_m \geqslant \cdots$ telle que $N_{m+1} \lhd N_m$, et on vérifie que N_m/N_{m+1} est abélien (c'est isomorphe à l'image de $\varphi_{m+1}(N_m)$ dont le calcul déjà effectué justifie que c'est un groupe abélien).

Or puisque N_m/N_{m+1} est abélien, on en déduit que $D(N_m) < N_{m+1}$. En particulier $D(G) < N_1$, et par récurrence on montre que $D^(m)(G) < N_m$.

Finalement comme $N_n = \{\mathrm{id}\}$, on a montré que $D^(n)(G) = \{\mathrm{id}\}$, donc N est résoluble.

Comme N et $B_n(\mathbf{R})/N$ sont résolubles alors $B_n(\mathbf{R})$ est résoluble. □

12.4 Exo 4

Exercice 12.4. Décrire les suites dérivées des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$, Q_8 et D_n.

Démonstration. Pour les groupes $\mathfrak{A}_4, \mathfrak{S}_4, Q_8$, on a vu dans l'exercice 1 qu'ils sont résolubles, donc on sait que $D(G) \neq G$ pour $G \in \{\mathfrak{A}_4, \mathfrak{S}_4, Q_8\}$. De plus on sait que $D(G)$ est distingué dans G et $D(G) = \{e\}$ si et seulement si G est abélien.

1. Le seul sous-groupe distingué non trivial de $\mathfrak{A}_4$ est V (engendré par les doubles transpositions), puisque $\mathfrak{A}_4$ est résoluble non abélien, alors $D(\mathfrak{A}_4) = V$. Par contre V est abélien, donc la suite dérivée est $\{e\} \lhd V \lhd \mathfrak{A}_4$.
2. On a vu que $\mathfrak{S}_4/V \simeq \mathfrak{S}_3$ n'est pas abélien, donc la suite dérivée de $\mathfrak{S}_4$ est $\{e\} \lhd V \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$.
3. Dans Q_8 on remarque que $[i:j] = -1$. En faisant tous les calculs, on constate que $D(Q_8) = \{1, -1\}$.
4. Soient $\alpha, \beta, \alpha', \beta'$ des entiers. On peut supposer $\alpha \geqslant \alpha'$

$$\begin{aligned} \left[s^\alpha r^\beta : s^{\alpha'} r^{\beta'}\right] &= s^\alpha r^\beta s^{\alpha'} r^{\beta'} r^{-\beta} s^{-\alpha} r^{-\beta'} s^{-\alpha'} \\ &= s^{\alpha-\alpha'} s^{\alpha'} r^\beta s^{\alpha'} r^{\beta'-\beta} s^{\alpha-\alpha'} s^{\alpha'} r^{-\beta'} s^{\alpha'} \\ &= s^{\alpha-\alpha'} r^{(-1)^{\alpha'}\beta} r^{\beta'-\beta} s^{\alpha-\alpha'} r^{(-1)^{\alpha'+1}\beta'} \\ &= r^{(-1)^{(\alpha-\alpha')}[(-1)^{\alpha'}\beta+\beta'-\beta]} r^{(-1)^{(\alpha'+1)}\beta'} \\ &= r^{[((-1)^\alpha-(-1)^{(\alpha-\alpha')})\beta+((-1)^{(\alpha-\alpha')}-(-1)^{\alpha'})\beta']} \end{aligned}$$

Puisque $((-1)^\alpha - (-1)^{(\alpha-\alpha')})$ ne peut valoir que $-2, 0, 2$ alors on a $D(D_n) = \langle r^2 \rangle$.

- Si n est impair alors $D(D_n) = \langle r \rangle$. On a donc $\{e\} \lhd \langle r \rangle \lhd D_n$.
- Si n est pair, alors$D(D_n) = \langle r^2 \rangle$. On a donc $\{e\} \lhd \langle r^2 \rangle \lhd D_n$.

5. (méthode 2 pour 4) On sait que $D_n/D(D_n)$ est abélien. Alors $r^{-1}s = sr = rs$ dans $D_n/D(D_n)$ (car abélien). Ceci arrive si et seulement si $r = r^{-1}$ dans $D_n/D(D_n)$, soit encore si et seulement si $r^2 \in D(D_n)$. Donc $\langle r^2 \rangle < D(D_n)$.

• Si n est impair alors $\langle r^2\rangle = \langle r\rangle$. De plus $D_n/\langle r\rangle$ est de cardinal 2 donc abélien. Donc $D(D_n) < \langle r\rangle$, soit encore l'égalité : $\langle r\rangle = D(D_n)$. On a donc la suite dérivée $\{e\} \lhd \langle r\rangle \lhd D_n$.
• Si n est pair, alors$D(D_n) = \langle r^2\rangle$. En effet $D_n/\langle r\rangle$ est de cardinal 4 donc abélien. On a donc la suite dérivée $\{e\} \lhd \langle r^2\rangle \lhd D_n$.

□

12.5 Exo 5

Exercice 12.5. Donner un exemple de groupes G et H non isomorphes mais pour lesquels $D(G) \simeq D(H)$ et $G/D(G) \simeq H/D(H)$.

Démonstration. On considère $G = D_4$ et $H = Q_8$. D'après l'exercice précédent, $D(D_4) = \langle r^2\rangle \simeq \mathbf{Z}/2\mathbf{Z}$, et $D(Q_8) = \{-1, 1\} \simeq \mathbf{Z}/2\mathbf{Z}$. De plus $D_4/D(D_4)$ est un groupe d'ordre 4 qui contient au moins deux éléments d'ordre 2, à savoir r et s, c'est donc $V_4 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Par ailleurs $Q_8/D(D_4)$ est un groupe d'ordre 4 qui contient aussi au moins deux éléments d'ordre 2, à savoir i et j, c'est donc $V_4 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. □

12.6 Exo 6

Exercice 12.6. On se place dans le groupe $\mathrm{GL}_2(\mathbf{R})$.

1. Montrer que les matrices de la formes
$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}, \quad \text{avec } (\lambda, \mu) \in \mathbf{R}^2$$
engendrent $\mathrm{SL}_2(\mathbf{R})$.
2. Montrer que les matrices $\begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ sont conjugués **dans** $\mathrm{SL}_2(\mathbf{R})$. On pourra chercher à conjuguer par une matrice diagonale.
3. Déduire des questions précédentes la suite dérivée de $\mathrm{GL}_2(\mathbf{R})$. Ce groupe est-il résoluble ?

Démonstration. 1.
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+\lambda b \\ c & d+\lambda c \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} = \begin{pmatrix} a+\mu b & b \\ c+\mu d & d \end{pmatrix}$$
On part d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Si $b = 0$, on multiplie par $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ de sorte que leur produit ait le coefficient en haut à droite non nul.
On peut donc supposer sans perdre de généralité que $b \neq 0$. On pose alors $\mu = \frac{1-a}{b}$, alors
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \frac{1-a}{b} & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ \frac{d-1}{b} & d \end{pmatrix}$$
Puis $\lambda = -b$,
$$\begin{pmatrix} 1 & b \\ \frac{d-1}{b} & d \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{d-1}{b} & 1 \end{pmatrix}$$
Donc les matrices engendrent bien $\mathrm{SL}_2(\mathbf{R})$.

2. Conjuguons par $P = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$, alors
$$P\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}P^{-1} = \begin{pmatrix} 1 & a^2\lambda \\ 0 & 1 \end{pmatrix}$$
Prendre $a = \sqrt{2}$ convient.

3. On remarque que $D(\mathrm{GL}_2(\mathbf{R})) \subset \mathrm{SL}_2(\mathbf{R})$. De plus avec P comme précédemment et $a = \sqrt{2}$, on a
$$P \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} P^{-1} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$
De même,
$$P \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} P^{-1} \begin{pmatrix} 1 & 0 \\ -\mu & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$
Donc $D(\mathrm{GL}_2(\mathbf{R})) = \mathrm{SL}_2(\mathbf{R})$, et de même $D(\mathrm{SL}_2(\mathbf{R})) = \mathrm{SL}_2(\mathbf{R})$. En particulier, $\mathrm{GL}_2(\mathbf{R})$ n'est pas résoluble.

□

12.7 Exo 7

Exercice 12.7. On considère le groupe formé des matrices :
$$G := \left\{ \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix} \mid f \in \mathbf{R}[x],\, g \in \mathbf{R}[y],\, h \in \mathbf{R}[x,y] \right\}.$$

1. Montrer que G est un groupe.
2. Calculer le commutateur $[\alpha, \beta]$ de deux éléments α, $\beta \in G$ et montrer que
$$D(G) = \left\{ \begin{pmatrix} 1 & 0 & h(x,y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid h \in \mathbf{R}[x,y] \right\}.$$
3. Montrer cependant que la matrice
$$\begin{pmatrix} 1 & 0 & x^2+xy+y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
n'est pas un commutateur.

Démonstration. 1. On a
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & c+c'+b'a \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & c+c'+a'b \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$
Donc G est stable par la loi du groupe et l'inverse
$$\begin{pmatrix} 1 & -a & ba-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in G$$
Donc G est un groupe.

2.
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ba-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a' & b'a'-c' \\ 0 & 1 & -b' \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & a+a' & c+c'+b'a \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a-a' & -c+-c'+b'a+ba+b'a' \\ 0 & 1 & -b-b' \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & b'a-a'b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Donc un commutateur vérifie $f'(x) = 0, g'(y) = 0$ et $h'(x,y) = f(x)v(y) - u(x)g(y)$. En particulier

$$D(G) = \left\{ \begin{pmatrix} 1 & 0 & h(x,y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid h \in \mathbf{R}[x,y] \right\}.$$

puisque le produit de plusieurs commutateurs vérifie $f'(x) = g'(y) = 0$ et $h'(x,y) = \sum_i u_i(x)v_i(y)$.

3. Si la matrice

$$\begin{pmatrix} 1 & 0 & x^2+xy+y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

est un commutateur, alors $x^2 + xy + y^2 = f(x)v(y) - u(x)g(y)$.

Posons $v(y) = \sum v_i y^i$ et $g(y) = \sum g_i y^i$. Alors, en identifiant les coefficients (en voyant ce polynôme en deux variables comme un polynôme en y à coefficients dans $\mathbf{R}(x)$), on obtient

$$\begin{aligned} x^2 &= v_0 f(x) + u(x) g_0 \\ x &= v_1 f(x) + u(x) g_1 \\ 1 &= v_2 f(x) + u(x) g_2 \end{aligned}$$

Donc les polynômes $1, x, x^2$ qui sont linéaires indépendants dans $\mathbf{R}[x]$, sont combinaisons linéaires de seulement deux polynômes. C'est absurde.

Donc ce n'est pas un commutateur.

□

12.8 Exo 8+

Exercice 12.8. Soit G un groupe dont on suppose que le centre $Z(G)$ est d'indice fini $[G : Z(G)] = n < +\infty$.

1. Considérons $(g_i)_{i=1\dots n}$ une famille de représentants de $G/Z(G)$. Montrer que tout commutateur est de la forme $[g_i, g_j]$ pour certains indices $1 \leqslant i,\ j \leqslant n$. Il y a donc au plus n^2 commutateurs.
2. Montrer que pour tout $(x,y) \in G^2$: $[x,y]^{n+1} = [x, y^2] \cdot [yxy^{-1}, y]^{n-1}$.
3. Soit $x \in D(G)$ et écrivons x comme un produit de commutateurs $x = c_1 \cdots c_k$. Montrer que si un commutateur c apparaît au moins $n+1$ fois dans le produit, alors $x = c^{n+1} c'_1 \cdots c'_l$ où les c'_i sont des commutateurs. En déduire (avec la question précédente) que $D(G)$ est fini avec la majoration :

$$|D(G)| \leqslant n^{2n^3}.$$

Démonstration. 1. Soit $[x,y] = xyx^{-1}y^{-1}$ un commutateur. Alors il existe $i, j \in \{1, \cdots, n\}$ et $a, b \in Z(G)$ tels que $x = g_i a$ et $y = g_j b$.

$$[x,y] = g_i a g_j b a^{-1} g_i^{-1} b^{-1} g_j^{-1} = g_i g_j g_i^{-1} g_j^{-1} = [g_i, g_j]$$

car $a, b \in Z(G)$. Il y a donc au plus n^2 commutateurs.

2. On constate que

$$a[x,y]a^{-1} = axyx^{-1}y^{-1}a^{-1} = [axa^{-1}, aya^{-1}]$$

En particulier $y[x,y]^k y^{-1} = [yxy^{-1},y]^k$. Comme $Z(G)$ est distingué dans G et d'ordre n alors $[x,y]^n = e$ dans le quotient. Donc $[x,y]^n \in Z(G)$.

$$\begin{aligned}[x,y]^{n+1} &= xyx^{-1}[x,y]^n y^{-1} \\ &= xyx^{-1}xyx^{-1}y^{-1}[x,y]^{n-1}y^{-1} \\ &= xy^2x^{-1}y^{-2}y[x,y]^{n-1}y^{-1} \\ &= [x,y^2][yxy^{-1},y]^{n-1}\end{aligned}$$

3. On suppose que c apparaît dans l'écriture de x. Montrons que l'on peut faire "avancer" c dans cette écriture. Or $c_1 c = cc^{-1}c_1 c = cc_1'$ où $c_1' = c^{-1}c_1 c$ est un commutateur. Donc on peut faire avancer n'importe quel c de sorte que x puisse s'écrire sous la forme $x = c^{n+1}c_1' \cdots c_l'$ où les c_i' sont des commutateurs.
Mais c^{n+1} peut s'écrire comme produit de n commutateurs, et il y a au plus n^2 commutateurs possibles. Donc x est produit d'au plus n^3 commutateurs et il y a au plus n^2 commutateurs. Donc $|D(G)| \leqslant (n^2)^{n^3}$.

□

12.9 Exo 9+

Exercice 12.9. Dans $\mathrm{GL}_2(\mathbf{R})$, on considère le sous-groupe

$$G := \left\langle x = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

1. Montrer que G est résoluble (on pourra utiliser l'exercice précédent).
2. Montrer que $xyx^{-1} = y^2$ et en déduire que le sous-groupe engendré par tous les conjugués de y est abélien. On note $\langle\langle y \rangle\rangle$ ce sous-groupe.
3. Le groupe $\langle\langle y \rangle\rangle$ est-il de type fini ?

Démonstration. 1. G est un sous-groupe d'un groupe résoluble (cf exercice précédent) donc est résoluble.

2. On a

$$xy = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

$$y^2 x = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

Donc $xyx^{-1} = y^2$.
Le groupe engendré par les commutateurs de y est engendré par$y$, xyx^{-1} et $x^{-1}yx$. Pour montrer que le groupe engendré par les conjugués de y est abélien, il suffit de vérifier que y commute avec xyx^{-1} et $x^{-1}yx$ et que xyx^{-1} et $x^{-1}yx$ commutent entre eux.

$$y \cdot xyx^{-1} = y^3 = xyx^{-1} \cdot y$$

$$y \cdot x^{-1}yx = x^{-1}xyx^{-1}yx = x^{-1}y^2yx = x^{-1}yxx^{-1}y^2x = x^{-1}yx \cdot y$$

$$xyx^{-1} \cdot x^{-1}yx = y^2 \cdot x^{-1}yx = x^{-1}yx \cdot y^2 = x^{-1}yx \cdot xyx^{-1}$$

Donc $\langle\langle y \rangle\rangle$ est abélien.

3. On remarque que

$$x^{-1}yx = \begin{pmatrix} 2 & 1 \\ 0 & \frac{1}{2} \end{pmatrix}$$

Soit encore

$$x^{-n}yx^n = \begin{pmatrix} 2^n & 1 \\ 0 & \frac{1}{2^n} \end{pmatrix}$$

Comme $x^{-n}yx^n$ n'est pas engendré par $x^{-k}yx^k$, pour $k < n$, alors $\langle\langle y \rangle\rangle$ n'est pas de type fini.

□