TD2 : Actions de groupes et théorèmes de Sylow

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soit p un nombre premier.

a) Montrer qu'un groupe de cardinal p^2 est commutatif.

b) Combien d'éléments d'ordre p y a-t-il dans un groupe de cardinal p ? Et dans un groupe de cardinal p^2 ?

Solution de l'exercice 1.

a) Soit G un groupe d'ordre p^2. L'équation aux classes pour l'action de G sur lui-même par conjugaison assure que le centre Z de G n'est pas réduit à l'élément neutre. Donc G/Z est de cardinal 1 ou p. Dans le second cas, le groupe G/Z est donc cyclique, ce qui assure que G est commutatif (voir la feuille de TD1, exercice 9). En outre, si G admet un élément d'ordre p^2, alors G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Si G n'admet pas de tel élément, alors tous ses éléments autres que le neutre sont d'ordre p. En choisissant $x \in G \setminus \{e\}$ et $y \in G \setminus \langle x \rangle$, on voit que $G = \langle x, y \rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

b) Dans un groupe de cardinal p, tout élément autre que le neutre est d'ordre p (1 et p sont les seuls diviseurs positifs de p). Donc un tel groupe admet $p-1$ éléments d'ordre p.
Soit G un groupe d'ordre p^2. Si G est cyclique engendré par x, on voit que x^n est d'ordre p si et seulement si p divise n et p^2 ne divise pas n. Cela assure que les éléments d'ordre p sont exactement les x^{pr}, avec $r = 1, \ldots, p-1$. Ils sont donc en nombre de $p-1$. Si G n'est pas cyclique, tous les éléments autres que le neutre sont d'ordre p, donc G contient $p^2 - 1$ éléments d'ordre p.

Exercice 2 : ⋆
Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble

$$E := \{(g, x) \in G \times X : g \cdot x = x\},$$

calculer le nombre moyen de point fixes d'un élément de G.
Que dire en particulier si l'action est transitive ? Que dire de la moyenne du nombre de points fixes d'une permutation aléatoire ?

Solution de l'exercice 2. On calcule le cardinal de E de deux façons différentes :

$$|E| = \sum_{g \in G} |\mathrm{Fix}(g)|$$

et

$$\begin{aligned} |E| &= \textstyle\sum_{x \in X} |\mathrm{Stab}_G(x)| \\ &= \textstyle\sum_{\overline{x} \in X/G} \sum_{y \in \overline{x}} |\mathrm{Stab}_G(y)| \\ &= \textstyle\sum_{\overline{x} \in X/G} |\overline{x}|.|\mathrm{Stab}_G(\overline{x})| = |G|.|X/G|, \end{aligned}$$

où on note $\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\}$ l'ensemble des points fixes de g dans X. On en déduit donc l'égalité

$$\sum_{g \in G} |\mathrm{Fix}(g) = |G|.|X/G|,$$

i.e.

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = |X/G|\,.$$

Cela signifie que le nombre moyen de points fixes d'un élément de G est exactement $|X/G|$, i.e. le nombre d'orbites de l'action.
En particulier, si l'action est transitive, ce nombre vaut 1.
Par exemple, si $G = \mathfrak{S}_n$ agit (via l'action évidente) sur $X = \{1, \dots, n\}$, alors on voit que le nombre moyen de points fixes d'une permutation est exactement 1.

Exercice 3 : (Lemme de Cauchy) ⋆
Soit G un groupe fini et soit p un nombre premier divisant le cardinal de G. En utilisant une action convenable de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble

$$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

prouver que G admet un élément d'ordre p (sans utiliser les théorèmes de Sylow !).

Solution de l'exercice 3. On peut indicer un élément de X (qui est un p-uplets d'éléments de G) par les éléments de $\mathbb{Z}/p\mathbb{Z}$.
On considère l'action de $H = \mathbb{Z}/p\mathbb{Z}$ sur l'ensemble X définie, pour $k \in H$ et $x = (g_1, \dots, g_p) \in X$, par

$$h \cdot x := (g_{1+k}, \dots, g_{p+k})\,,$$

où les indices des g_i sont pris dans le groupe $H = \mathbb{Z}/p\mathbb{Z}$.
Vérifions que pour tout $k \in H$ et $x \in X$, $h \cdot x \in X$. Pour cela, on doit vérifier que si $g_1 \dots g_p = 1$ implique que $g_{1+k} \dots g_{p+k} = 1$. Ceci est clair via le calcul suivant : si $g_1 \dots g_p = 1$, on a $g_2 \dots g_p = g_1^{-1}$, donc $g_2 \dots g_p g_1 = 1$, et donc par récurrence, on a $g_{k+1} \dots g_p g_1 \dots g_k = 1$.
Donc la formule précédente définit bien une action de H sur X.
Léquation aux classes s'écrit alors

$$|X| = |X^H| + \sum_{\overline{x}\in X/H x\notin X^H} [H : H_x]\,.$$

Or H est de cardinal p, donc H_x est nécessairement le groupe trivial si $x \notin X^H$. D'où

$$|X| = |X^H| + p|X/H \setminus X^H|\,.$$

Or il est clair que $|X| = |G|^{p-1}$, donc $|X|$ est divisible par p.
L'équation aux classes assure donc que p divise $|X^H|$. Or $X^H \neq \emptyset$ car $(1, \dots, 1) \in X^H$, donc il existe un élément de X^H distinct de $(1, \dots, 1)$. Un tel élément est de la forme $(g, \dots, g) \in G^p$ pour un certain $g \in G \setminus \{1\}$. Par définition de X, on a donc $g^p = 1$ et $g \neq 1$, ce qui assure que g est d'ordre p dans G.

Exercice 4 : ⋆
Combien y a-t-il de colliers différents formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges ?

Solution de l'exercice 4. On représente un collier par un cercle du plan euclidien orienté $\mathbb{R}^2$ (de centre 0 et rayon 1) muni de neuf points $A_1, \dots, A_9$ disposés à intervalles réguliers.
On choisit de dire que deux colliers sont équivalents (ce sont les "mêmes" colliers) si et seulement si on peut obtenir l'un à partir de l'autre en effectuant une rotation plane du collier ou en le retournant (comme une crêpe) dans l'espace de dimension 3.
Autrement dit, l'ensemble X de tous les colliers possibles à 9 perles dont 4 bleues, 3 blanches et 2 rouges, est muni d'une action du groupe diédral $G = \mathrm{D}_9$ des isométries d'un polygône régulier à neuf côtés. Ce groupe G est donc un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$, il est de cardinal 18 et ses éléments sont les suivants :

$$G = \{\mathrm{id}, r, r^2, r^3, r^4, r^5, r^6, r^7, r^8, s, r\circ s, r^2\circ s, r^3\circ s, r^4\circ s, r^5\circ s, r^6\circ s, r^7\circ s, r^8\circ s\}\,,$$

où r est la rotation de centre O et d'angle $\frac{2\pi}{9}$ et s est la symétrie orthogonale d'axe $\Delta = (OA_1)$. En particulier, G contient 9 rotations et 9 symétries orthogonales.
Au vu de la discussion précédente, le nombre de colliers différents est exactement le nombre d'orbites dans l'action de G sur X, i.e. $|X/G|$.
On calcule ce nombre grâce à la formule démontrée à l'exercice 2 :

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \,.$$

Calculons maintenant $\mathrm{Fix}(g)$ pour tout $g \in G$: soit $g \in G$.
- Si $g = \mathrm{id}$, il est clair que $\mathrm{Fix}(g) = X$.
- Si $g = r, r^2, r^4, r^5, r^7, r^8$, alors le sous-groupe de G engendré par g est constitué des 9 rotations (r^k engendre ce sous-groupe si et seulement si k est premier avec 9). Donc un collier fixe par g est fixe par r, ce qui implique que toutes les perles sont de la même couleur. Ceci n'est pas possible, donc $\mathrm{Fix}(g) = \emptyset$.
- Si $g = r^3, r^6$, alors dans un collier fixe par g, le nombre de perles d'une couleur donnée doit être un multiple de 3, ce qui n'est pas le cas dans l'ensemble X, donc $\mathrm{Fix}(g) = \emptyset$.
- Si g est une symétrie, on peut supposer $g = s$, les autres cas étant identiques. Puisque l'axe Δ de g ne contient qu'une perle (A_1 en l'occurence), dans un collier fixe par g, les perles A_i, $i \neq 1$ vont par paire de même couleur. Cela assure que la perle A_1 est nécessairement blanche. Se donner un collier fixe par g revient alors à se donner les couleurs des perles A_2, A_3, A_4, A_5 de sorte que 2 soient bleues, 1 blanche et 1 rouge. Il est clair que le nombre de tels colliers vaut

$$|\mathrm{Fix}(g)| = \binom{4}{2}.\binom{2}{1} = 6.2 = 12 \,.$$

Enfin, le cardinal de X se calcule simplement via la formule suivante

$$|X| = \binom{9}{4}.\binom{5}{3} = 126.10 = 1260 \,.$$

Donc on en déduit que

$$|X/G| = \frac{1}{18}\,(1260 + 9.12) = 76 \,.$$

Il y a donc exactement 76 colliers distincts (à équivalence près) satisfaisant les contraintes de l'énoncé.

Exercice 5 : $\star\star$
Soit G un groupe.

a) On suppose que G est fini et on note p le plus petit nombre premier divisant le cardinal de G. Montrer que tout sous-groupe de G d'indice p est distingué.

b) On suppose que G est infini et qu'il admet un sous-groupe strict H d'indice fini. Montrer que G n'est pas un groupe simple.

Solution de l'exercice 5.

a) Soit H un sous-groupe de G d'indice p. On note $X := G/H$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi : G \to \mathfrak{S}(X)$. On s'intéresse à la restriction de cette action au sous-groupe H, i.e. au morphisme

$$\varphi : H \to \mathfrak{S}(X) \,.$$

Puisque H agit trivialement sur la classe x_0 de H dans $X = G/H$, l'action de H sur X induit une action de H sur $X' := X \setminus \{x_0\}$, c'est-à-dire un morphisme de groupes

$$\psi : H \to \mathfrak{S}(X') \,.$$

Or X' est de cardinal $p-1$, donc tous les facteurs premiers du cardinal de $\mathfrak{S}(X')$ sont strictement inférieur à p. Or les facteurs premiers du cardinal de H sont par hypothèse tous supérieurs ou égaux à p. Par conséquent, les cardinaux de H et $\mathfrak{S}(X')$ sont premiers entre eux, ce qui implique que le morphisme ψ est le morphisme trivial. Donc H agit trivialement sur X', donc aussi sur X.

Montrons que cela implique que H est distingué dans G. Soit $h \in H$ et $g \in G$. Puisque H agit trivialement sur X, on sait que $h \cdot (gH) = gH$, donc $(g^{-1}hg)H = H$, donc $g^{-1}hg \in H$, donc H est distingué dans G.

b) Comme en a), on considère l'action de G sur l'ensemble fini $X := G/H$, i.e. le morphisme de groupes induit

$$\varphi : G \to \mathfrak{S}(X)\,.$$

Comme l'action de G sur X est transitive et comme $H \neq G$, le morphisme φ est non trivial. Son noyau $\mathrm{Ker}(\varphi)$ est donc un sous-groupe distingué de G distinct de G. En outre, G est infini et $\mathfrak{S}(X)$ est fini, donc le morphisme φ n'est pas injectif, donc $\mathrm{Ker}(\varphi)$ n'est pas le groupe trivial. Donc $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué non trivial de G, donc G n'est pas un groupe simple.

Exercice 6 :

a) Montrer que si G est un groupe fini et H un sous-groupe strict de G, alors la réunion des conjugués de H n'est pas égale à G tout entier. Que dire si le groupe G est infini et si H est d'indice fini dans G ? Et si on ne suppose plus H d'indice fini ?

b) Soit G un groupe fini agissant transitivement sur un ensemble fini X tel que $|X| \geq 2$. Montrer qu'il existe $g \in G$ ne fixant aucun point de X.

Solution de l'exercice 6.

a) Puisque pour tout $g \in G$ et $h \in H$, on a $gHg^{-1} = (gh)H(gh)^{-1}$ et $|gHg^{-1}| = |gHG^{-1}|$, on estime le cardinal de $\bigcup_{g\in G} gHg^{-1}$ de la façon suivante :

$$\begin{aligned} |\textstyle\bigcup_{g\in G} gHg^{-1} \setminus \{e\}| &= |\textstyle\bigcup_{\overline{g}\in G/H} gHg^{-1} \setminus \{e\}| \\ &\leq \textstyle\sum_{\overline{g}\in G/H} |gHg^{-1} \setminus \{e\}| \\ &\leq \textstyle\sum_{\overline{g}\in G/H} |H \setminus \{e\}| \\ &\leq |G/H|.\,(|H|-1) \\ &\leq |G| - \tfrac{|G|}{|H|}\,. \end{aligned}$$

Or on a $|G \setminus \{e\}| = |G| - 1$, donc comme $H \neq G$, on a bien

$$|\bigcup_{g\in G} gHg^{-1} \setminus \{e\}| < |G \setminus \{e\}|$$

donc

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

Si l'on suppose désormais le groupe G infini et le sous-groupe H d'indice fini, alors on a une action naturelle transitive de G sur l'ensemble fini $X := G/H$ par multiplication à droite, induisant un morphisme non trivial

$$\varphi : G \to \mathfrak{S}(X)\,.$$

Or $\mathfrak{S}(X)$ est un groupe fini, $\varphi(H)$ est contenu dans le sous-groupe de $\mathfrak{S}(X)$ fixant la classe de H, et la transitivité de l'action de G sur X assure que $\varphi(G)$ n'est pas contenu dans ce sous-groupe. Donc $\varphi(H)$ est un sous-groupe strict du groupe fini $\varphi(G)$. Donc la preuve précédente assure que

$$\bigcup_{g\in G} \varphi(g)\varphi(H)\varphi(g)^{-1} \neq \varphi(G)\,.$$

On en déduit immédiatement que

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

Enfin, si le sous-groupe H n'est plus supposé d'indice fini, la conclusion n'est plus vérifiée en général : par exemple, si $G := \mathrm{SO}_3(\mathbb{R})$ est le groupe des rotations vectorielles de $\mathbb{R}^3$ (matrices réelles 3×3 orthogonales de déterminant 1) et si $H := \mathrm{SO}_2(\mathbb{R})$ est le sous-groupe des rotations d'axe fixé Δ (par exemple $\Delta = \mathbb{R}(1,0,0)$), alors H est clairement un sous-groupe stricit de G (d'indice infini) et pourtant on a

$$\bigcup_{g\in G} gHg^{-1} = G\,,$$

puisque toute rotation de $\mathbb{R}^3$ est conjuguée dans $\mathrm{SO}_3(\mathbb{R})$ à une rotation d'axe Δ.

Un autre tel exemple est donné par le groupe $G = \mathrm{GL}_n(\mathbb{C})$ ($n \geq 2$) et le sous-groupe strict $H := \mathrm{T}_n(\mathbb{C}) \cap \mathrm{GL}_n(\mathbb{C})$ des matrices triangulaires supérieures inversibles : un résultat classique d'algèbre linéaire assure que tout élément de g est trigonalisable, i.e. conjugué dans G à un élément de H, ce qui assure que

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

b) On choisit un point $x_0 \in X$ et on note $H := \mathrm{Stab}_G(x_0)$. Alors H est un sous-groupe de G, et $H \neq G$ (sinon on aurait $X = \{x_0\}$). Donc la question a) assure qu'il existe $g_0 \in G$ tel que $g_0 \notin \bigcup_{g\in G} gHg^{-1}$. Soit alors $x \in X$. On sait qu'il existe $g \in G$ tel que $x = g\cdot x_0$. Alors $\mathrm{Stab}_G(x) = gHg^{-1}$, donc par construction on sait que $g_0 \notin \mathrm{Stab}_G(x)$, ce qui signifie que $g_0\cdot x \neq x$. Cela conclut la preuve.

Exercice 7 :
Soit G un groupe fini non trivial agissant sur un ensemble fini X. On suppose que pour tout $g \neq e \in G$, il existe un unique $x \in X$ tel que $g\cdot x = x$. On souhaite montrer que X admet un point fixe sous G (nécessairement unique).

a) On note $Y := \{x \in X : \mathrm{Stab}_G(x) \neq \{e\}\}$. Montrer que Y est stable par G.

b) On note $n = |Y/G|$ et $y_1, \ldots, y_n$ un système de représentants de Y/G. Pour tout i, on note m_i le cardinal de $\mathrm{Stab}_G(y_i)$. En considérant l'ensemble $Z := \{(g,x) \in (G\setminus\{e\}) \times X : g\cdot x = x\}$, montrer que

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

c) En déduire que $n = 1$.

d) Conclure.

Solution de l'exercice 7.

a) Soit $x \in Y$ et $g \in G$. On sait que $\mathrm{Stab}_G(g\cdot x) = g\mathrm{Stab}_G(x)g^{-1}$, donc comme $\mathrm{Stab}_G(x) \neq \{e\}$, on a $\mathrm{Stab}_G(g\cdot x) \neq \{e\}$, donc $g\cdot x \in Y$. Donc Y est stable par G.

b) On calcule le cardinal de Z de deux façons différents comme dans l'exercice 2 et on obtient, puisque pour tout $x \in X\setminus Y$, $\mathrm{Stab}_G(x)\setminus\{e\} = \emptyset$:

$$|G| - 1 = \sum_{y\in Y}\left(|\mathrm{Stab}_G(y)| - 1\right)\,.$$

On peut alors regrouper les éléments de Y par orbites, et on obtient

$$|G| - 1 = \sum_{i=1}^{n}|O_{y_i}|\left(|\mathrm{Stab}_G(y_i)| - 1\right) = \sum_{i=1}^{n}|G|\left(1 - \frac{1}{m_i}\right)\,.$$

On divise par $|G|$ et on obtient le résultat.

c) Par définition, on a pour tout i, $m_i \geq 2$. Donc on en déduit que

$$1 > 1 - \frac{1}{|G|} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right) \geq \frac{n}{2},$$

donc $n < 2$, donc $n = 1$ (le cas $n = 0$ est impossible car G est non trivial).

d) On choisit donc $y_1 \in Y$. Alors par les questions b) et c), on a $|\mathrm{Stab}_G(y_1)| = |G|$, donc $\mathrm{Stab}_G(y_1) = G$, donc y_1 est fixe par G.

Exercice 8 : $\star\star$

a) Soit G un p-groupe fini agissant sur un ensemble fini X. On note X^G l'ensemble des points fixes de X sous G. Montrer que

$$|X^G| \equiv |X| \pmod{p}.$$

b) Soit G un p-groupe agissant sur un ensemble fini X dont le cardinal n'est pas divisible par p. Montrer que X admet un point fixe sous G.

c) Soit G un p-groupe fini et $H \neq \{e\}$ un sous-groupe distingué de G. Montrer que l'intersection de H avec le centre de G n'est pas réduite à l'élément neutre.

d) Montrer qu'un groupe d'ordre p^n admet des sous-groupes d'ordre p^i pour tout $0 \leq i \leq n$.

e) Soit p un nombre premier congru à 1 modulo 4. On souhaite montrer que p est somme de deux carrés d'entiers. On note

$$X := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}.$$

i) On définit $i : X \to X$ par les formules suivantes

$$i : (x, y, z) \mapsto \begin{array}{l} (x + 2z, z, y - x - z) \text{ si } x < y - z, \\ (2y - x, y, x - y + z) \text{ si } y - z < x < 2y, \\ (x - 2y, x - y + z, y) \text{ si } x > 2y. \end{array}$$

Vérifier que i est bien définie.

ii) Montrer que i est une involution.

iii) Montrer que i a un unique point fixe.

iv) Montrer que $|X|$ est impair.

v) Montrer que l'application $j : X \to X$ définie par $j(x, y, z) := (x, z, y)$ admet un point fixe.

vi) Conclure.

Solution de l'exercice 8.

a) On note p^n le cardinal de G. On écrit l'équation aux classes :

$$|X| = \sum_{\overline{x} \in X/G} |O_x| = \sum_{x \in X^G} 1 + \sum_{\overline{x} \in X/G,\, x \notin X^G} \frac{|G|}{|\mathrm{Stab}_G(x)|} = |X^G| + \sum_{\overline{x} \in X/G,\, x \notin X^G} \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Or, pour tout $x \notin X^G$, $\mathrm{Stab}_G(x)$ est un sous-groupe strict de G, son cardinal est donc de la forme p^i, avec $0 \leq i < n$. Donc $\frac{|G|}{|\mathrm{Stab}_G(x)|} = p^{n-i}$ est divisible par p, donc la formule précédente assure que

$$|X^G| \equiv |X| \pmod{p}.$$

b) Par hypothèse, on a $|X| \not\equiv 0 \pmod{p}$, donc par la question a), on a $|X^G| \not\equiv 0 \pmod{p}$, donc en particulier $|X^G| \neq 0$, donc $X^G \neq \emptyset$.

c) On considère l'ensemble $X := H$ et l'action de G sur X par conjugaison. Alors la question a) assure que l'on a $|H^G| \equiv |H| \equiv 0 \pmod{p}$. Or $e \in H^G$, donc $|H^G| \neq 0$, donc $|H^G| \geq p$, donc H^G n'est pas réduit à l'élement neutre. Enfin, il est clair que H^G est l'intersection de H avec le centre de G.

d) On raisonne par récurrence sur n. Pour $n = 0$, la propriété est évidente. Supposons la propriété connue pour un entier n et montrons-la pour l'entier $n+1$. Soit G un groupe d'ordre p^{n+1}. Si $i = 0$, la réponse est évidente. On peut donc supposer $i \geq 1$. La question c) assure que le centre de G est non trivial, et comme ce centre est un p-groupe, il admet un élément d'ordre p, donc un sous-groupe Z d'ordre p. Comme Z est central dans G, il est distingué. On note $\pi : G \to G/Z$ le morphisme quotient. Par hypothèse de récurrence, comme G/Z est de cardinal p^n, il existe un sous-groupe H' de G/Z de cardinal p^{i-1}. Alors il est clair que $H := \pi^{-1}(H')$ est un sous-groupe de G de cardinal p^i. Cela conclut la preuve.

e) i) Il suffit de vérifier que pour tout $(x, y, z) \in X$, on a $x \neq y - z$, $x \neq 2y$ et $i(x, y, z) \in X$. Tout cela est évident (les deux premières vérifications utilisent le fait que p est premier).

ii) Il s'agit de vérifier que pour tout $(x, y, z) \in X$, on a $i(i(x, y, z)) = (x, y, z)$. Pour cela, il y a trois cas à considérer :
- Si $x < y - z$: alors $i(x, y, z) = (x', y', z')$ avec $x' = x + 2z$, $y' = z$ et $z' = y - x - z$. On voit immédiatemment que $x' > 2y'$, ce qui assure que $i(x', y', z') = (x' - 2y', x' - y' + z', y') = (x, y, z)$.
- Si $y - z < x < 2y$: alors $i(x, y, z) = (x', y', z')$ avec $x' = 2y - x$, $y' = y$ et $z' = x - y + z$. On voit immédiatemment que $y' - z' < x' < 2y'$, ce qui assure que $i(x', y', z') = (2y' - x', y', x' - y' + z') = (x, y, z)$.
- Si $x > 2y$: alors $i(x, y, z) = (x', y', z')$ avec $x' = x - 2y$, $y' = x - y + z$ et $z' = y$. On voit immédiatemment que $x' < y' - z'$, ce qui assure que $i(x', y', z') = (x' + 2z', z', y' - x' - z') = (x, y, z)$.

Donc $i \circ i = \mathrm{id}_X$.

Enfin, il est clair que cela définit une action de $G = \mathbb{Z}/2\mathbb{Z}$ sur X via la formule $g \cdot x := i^g(x)$ pour $g \in G$ et $x \in X$.

iii) Soit $(x, y, z) \in X$. La question e)ii) assure que $i(x, y, z) = (x, y, z)$ si et seulement si $y - z < x < 2y$, $x = 2y - x$, $y = y$ et $z = x - y + z$ si et seulement si $x = y$. En outre, pour tout $(x, z) \in \mathbb{N}^2$, on a $(x, x, z) \in X$ si et seulement si $x^2 + 4xz = p$ si et seulement si $x(x + 4z) = p$ si et seulement si $x = 1$ et $p = 4z + 1$ (car p est premier). Or par hypothèse, p est congru à 1 modulo 4, donc il existe un unique $k \in \mathbb{N}$ tel que $p = 4k + 1$. Finalement, on a montré que i admettait le point $(1, 1, k)$ comme unique point fixe.

iv) Comme G est un 2-groupe, la question a) assure que l'on a

$$|X^G| \equiv |X| \ (\text{mod. } 2)\,.$$

Or $|X^G| = 1$, donc $|X| \equiv 1 (\text{mod. } 2)$, i.e. $|X|$ est impair.

v) L'application j est clairement une involution de X, donc elle définit une nouvelle action de G sur X. Par la question a), le nombre de points fixes pour cette action (qui est le nombre de points fixes de j) est congru à $|X|$ modulo 2. Or la question e)iv) assure que $|X|$ est impair, donc j a un nombre impair de points fixes, donc j a (au moins) un point fixe.

vi) Notons (x_0, y_0, y_0) un point fixe de j (qui existe par la question précédente). Alors on a $x_0^2 + 4y_0^2 = p$, i.e.

$$p = x_0^2 + (2y_0)^2\,,$$

ce qui conclut la preuve.

Exercice 9 :
Soit $n \geq 1$ un entier. Montrer qu'il n'existe qu'un nombre fini de classes d'isomorphisme de groupes finis admettant exactement n classes de conjugaison.

Solution de l'exercice 9. Soit G un tel groupe. On considère l'action de G sur lui-même par conjugaison : si $g \in G$ et $x \in G$, on pose $g \cdot x := gxg^{-1}$. Les classes de conjugaison dans G sont exactement les orbites pour cette action, donc on sait que cette action admet exactement n orbites. Si on note

$g_1, \dots, g_n$ un ensemble de représentants dans G pour l'action par conjugaison, et si $m_i := |\mathrm{Stab}_G(g_i)|$, alors l'équation aux classes assure que

$$\sum_{i=1}^{n} \frac{1}{m_i} = 1\,. \tag{1}$$

Comme il est clair que les m_i déterminent le cardinal de G (le plus grand des m_i est égal à $|G|$, puisque l'élément neutre commute à tous les éléments de G), il suffit de montrer que l'équation (1) d'inconnues $(m_1, \dots, m_n)$ admet un nombre fini de solutions dans $\mathbb{N}^n$.
Pour cela, on peut raisonner comme suit : pour $A \in \mathbb{Q}$, on note $N(n, A)$ le nombre de solutions (éventuellement infini) dans $\mathbb{N}^n$ de l'équation

$$\sum_{i=1}^{n} \frac{1}{m_i} = A\,. \tag{2}$$

Soit $n \geq 2$. Il est clair que si $(m_1, \dots, m_n)$ est solution de (2), si on choisit $1 \leq j \leq n$ tel que $m_j = \min_i m_i$, alors $\frac{1}{A} < m_j \leq \frac{n}{A}$ et $(m_i)_{i \neq j}$ est solution de l'équation

$$\sum_{i \neq j} \frac{1}{m_i} = A - \frac{1}{m_j}\,. \tag{3}$$

Donc on en déduit que

$$N(n, A) \leq n \sum_{\frac{1}{A} < k \leq \frac{n}{A}} N\left(n-1, A - \frac{1}{k}\right)\,.$$

Comme $N(1, A) \leq 1$ pour tout $A \in \mathbb{Q}$, une récurrence simple assure que $N(n, A)$ est fini pour tout $A \in \mathbb{Q}$.
Cela assure que $N(n, 1)$ est fini pour tout n, et donc que si G a exactement n classes de conjugaison, son cardinal est borné par une constante ne dépendant que de n. Comme il n'y a qu'un nombre fini de (classes d'isomorphisme de) groupes de cardinal donné, cela assure qu'il n'y a qu'un nombre fini de (classes d'isomorphisme de) groupes finis ayant n classes de conjugaison.

Exercice 10 : $\star\star$
On suppose qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente-six 5-Sylow.

b) Montrer que G contient dix 3-Sylow, puis que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_G$. (Indication : on pourra considérer les ordres possibles pour le centralisateur de g ; on observera qu'un groupe d'ordre 18 admet un unique 3-Sylow.)

c) Conclure.

Solution de l'exercice 10.

a) Pour tout p premier divisant $|G|$, on note n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_5 divise 36 et $n_5 \equiv 1$ [5]. Cela implique que $n_5 = 1, 6, \text{ou } 36$. Comme G est simple, le cas $n_5 = 1$ est impossible (sinon le 5-Sylow serait distingué dans G), donc $n_5 = 6$ ou $n_5 = 36$. Supposons $n_5 = 6$, alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $G \to \mathfrak{S}_6$. Comme G est simple, ce morphisme est injectif. Comme le morphisme $G \to \mathbb{Z}/2\mathbb{Z}$ donné par la signature a nécessairement un noyau trivial, on voit que G est un sous-groupe de $\mathfrak{A}_6$. En calculant les cardinaux, on voit que G est un sous-groupe d'indice 2 dans $\mathfrak{A}_6$, il est donc distingué et non trivial, ce qui contredit la simplicité de $\mathfrak{A}_6$. Cela assure donc que $n_5 = 36$.

b) Comme auparavant, on sait que n_3 divise 20 et que $n_3 \equiv 1$ [3]. Cela implique, comme G est simple, que $n_3 = 4$ ou $n_3 = 10$. Si on avait $n_3 = 4$, on en déduirait comme en a) un morphisme injectif de G dans $\mathfrak{S}_4$, ce qui est impossible car le cardinal de G est strictement supérieur à celui de $\mathfrak{S}_4$. Donc $n_3 = 10$.

Soient S et T deux 3-Sylow de G distincts, et soit $g \in S \cap T$. On suppose $g \neq e_G$ et on note $Z := \{x \in G : xg = g = x\}$ le centralisateur de g dans G. Puisqu'un groupe d'ordre 9 est abélien, on voit que Z contient S et T. Donc nécessairement, on a $|Z| \in \{18, 36, 45, 90\}$. Or l'action (transitive) de G sur G/Z induit un morphisme injectif de G vers $\mathfrak{S}(G/Z)$, donc par cardinalité, on a nécessairement $|Z| = 18$. Alors S et T sont des 3-Sylow de Z, et un groupe d'ordre 18 admet un unique 3-Sylow, donc $S = T$, ce qui est contradictoire. Donc finalement $S \cap T = \{e_G\}$.

Finalement, G admet dix 3-Sylow dont les intersections deux-à-deux sont triviales. Par conséquent, il y a dans G exactement $10.8 = 80$ éléments $\neq e_G$ d'ordre divisant 9.

c) La question a) assure que G contient exactement $36.4 = 144$ éléments d'ordre 5. Donc G possède au moins $144 + 80$ éléments, ce qui est contradictoire.

Donc il n'existe pas de groupe simple d'ordre 180.

Exercice 11 : ⋆⋆

Soient p et q deux nombres premiers distincts.

a) Montrer qu'un groupe d'ordre pq n'est pas simple.

b) Montrer que si $p < q$ et p ne divise pas $q - 1$, alors tout groupe d'ordre pq est cyclique.

c) Soit G un groupe simple d'ordre $p^\alpha m$, avec $\alpha \geq 1$ et m non divisible par p. On note n_p le nombre de p-Sylow de G. Montrer que $|G|$ divise $n_p!$.

d) Montrer qu'un groupe d'ordre $p^m q^n$, avec $p < q$, $1 \leq m \leq 2$ et $n \geq 1$, n'est pas simple.

e) Montrer qu'un groupe d'ordre $p^2 q$ ou $p^3 q$ n'est pas simple.

Solution de l'exercice 11.

a) Soit G un groupe d'ordre pq. On peut supposer $p < q$. On sait que le nombre de q-Sylow n_q divise p et est congru à 1 modulo q. Comme $p < q$, cela assure que $n_q = 1$, donc l'unique q-Sylow de G est distingué dans G, donc G n'est pas simple.

b) La question précédente assure que G admet un sous-groupe distingué H d'ordre q, engendré par un élément x. Le quotient G/H est cyclique d'ordre p. L'action de G par conjugaison sur H induit une action de G/H sur H, i.e. un morphisme de groupes $G/H \to \mathrm{Aut}(H) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Par hypothèse, comme p ne divise pas $q - 1$, ce morphisme est nécessairement trivial. Donc le sous-groupe H est contenu dans le centre de G. Or G admet un élément y d'ordre p, qui commute donc avec x. Donc l'élément $xy \in G$ est d'ordre pq, donc G est cyclique.

c) On regarde l'action transitive de G par conjugaison sur l'ensemble S_p de ses p-Sylow. Comme G est simple, $n_p > 1$, donc cela fournit un morphisme de groupes non trivial $G \to \mathfrak{S}(S_p) \cong \mathfrak{S}_{n_p}$. Par simplicité de G, ce morphisme est injectif, donc $|G|$ divise $|\mathfrak{S}_{n_p}| = n_p!$.

d) Par la question a), on peut supposer $m = 2$. Soit G un tel groupe, que l'on suppose simple. On sait que $n_q \equiv 1 \ [q]$ et n_q divise p^2. Donc $n_q = p^2$ et q divise $p^2 - 1 = (p-1)(p+1)$, donc $q \leq p + 1$, donc $q = p + 1$, donc $p = 2$ et $q = 3$, donc $|G| = 4.3^n$. La question c) assure alors que 4.3^n divise $4!$, donc 3^n divise 6, donc $n = 1$ et G est de cardinal 12. Alors $n_2 = 3$, et donc $|G|$ divise $3! = 6$, ce qui est contradictoire. Cela conclut la preuve.

e) On suppose G simple. La question d) assure que l'on peut supposer $|G| = p^3 q$, avec $p < q$. Alors nécessairement $n_q \equiv 1 \ [q]$ et $n_q = p$, p^2 ou p^3. Comme $p < q$, on a $n_q = p^2$ ou p^3. Comptons les éléments d'ordre q dans G : il y en a exactement $n_q(q-1)$.

Si $n_q = p^3$, alors G contient exactement $|G| - p^3$ éléments d'ordre q. Le complémentaire de l'ensemble de ces éléments d'ordre q est donc un ensemble de cardinal p^3. Or tout p-Sylow de G est de cardinal p^3 et ne contient aucun élément d'ordre q, donc il coïncide avec le complémentaire de l'ensemble des éléments d'ordre q. Cela assure que G admet unique p-Sylow, qui est donc distingué, donc G n'est pas simple, ce qui est une contradiction.

Si $n_q = p^2$, alors la condition $n_q \equiv 1 \ [q]$ assure que q divise $p^2 - 1$, donc $q = p + 1$, donc $p = 2$ et $q = 3$ et $|G| = 24$. Alors $n_2 = 3$, donc $|G| = 24$ divise $3! = 6$, ce qui est contradictoire.

Cela conclut la preuve.

Exercice 12 : $\star$

Montrer qu'un groupe non commutatif d'ordre < 60 n'est pas simple.

Solution de l'exercice 12. On utilise les exercices 8 et 11 pour réduire le problème : il reste à traiter le cas des groupes de cardinal 30, 42 et 48.

- Soit G un groupe d'ordre $30 = 2.3.5$. Supposons G simple. Alors les théorèmes de Sylow assurent que $n_3 = 10$ et $n_5 = 6$. Or l'intersection de deux 3-Sylow (resp. de deux 5-Sylow) distincts de G est réduite à l'élément neutre, donc G admet $10.2 = 20$ éléments d'ordre 3 et $6.4 = 24$ éléments d'ordre 5. Comme $20 + 24 > 30$, on a une contradiction.
- Soit G un groupe d'ordre $42 = 2.3.7$. Les théorèmes de Sylow assurent que $n_7 = 1$, donc G admet un unique 7-Sylow, qui est donc distingué dans G, donc G n'est pas simple.
- Soit G un groupe d'ordre $38 = 2^4.3$. Supposons G simple. Alors les théorèmes de Sylow assurent que $n_2 = 3$. Par conséquent, l'exercice 11, question c), assure que le cardinal de G divise $n_2! = 6$, ce qui est une contradiction.

Cela termine la preuve.

Exercice 13 : $\star\star$

On cherche à montrer que $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathfrak{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathfrak{A}_5$.

b) Montrer que $\mathfrak{A}_5$ est simple.

c) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

d) En déduire que G contient un sous-groupe d'ordre 12.

e) Conclure.

Solution de l'exercice 13.

a) Les 60 éléments de $\mathfrak{A}_5$ sont les suivants :
   - l'identité, d'ordre 1, qui forme une classe de conjugaison.
   - les bitranspositions $(ab)(cd)$, avec $\{a, b, c, d\}$ de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2, et elles forment une classe de conjugaison.
   - les 3-cycles (abc), avec $\{a, b, c\}$ de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3, et forment une classe de conjugaison.
   - les 5-cycles $(abcde)$, avec $\{a, b, c, d, e\}$ de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5, et ils forment exactement deux classes de conjugaison : celle de (12345) et celle de (21345) (voir par exemple la feuille de TD1, exercice 18).

   On vérifie que l'on a bien énuméré tous les éléments en calculant $1 + 15 + 20 + 24 = 60$.

b) Soit $H \neq \{e\}$ un sous-groupe distingué de $G = \mathfrak{A}_5$. Comme H est distingué, H est réunion de classes de conjugaison dans G. Puisque $1 + 15 = 16$, $1 + 12 = 13$, $1 + 24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 2015 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$, et qu'aucun des ces entiers ne divise 60, le théorème de Lagrange assure que H contient nécessairement toutes les classes de conjugaison dans G, donc $H = G$.

c) Les théorèmes de Sylow assure que n_2 est impair et divise 15, ce qui assure que $n_2 = 1$, 3, 5 ou 15. Comme G est simple, on a $n_2 \neq 1$. Si $n_2 = 3$, alors l'exercice 11, question c), assure que 60 divise $3! = 6$, ce qui est contradictoire. Donc $n_2 = 5$ ou 15.

d) – Supposons d'abord $n_2 = 5$. Alors le normalisateur d'un 2-Sylow de G est de cardinal $60/5 = 12$ d'où le résultat.
   – Supposons maintenant $n_2 = 15$. Montrons qu'il existe deux 2-Sylow distincts S et T tels que $|S \cap T| = 2$. Dans le cas contraire, on aurait exactement $15.3+1 = 46$ éléments d'ordre divisant 4 ; les théorèmes de Sylow assurent que $n_5 = 6$, donc G contient $6.4 = 24$ éléments d'ordre 5. Mais ceci est contradictoire car $46 + 24 = 70 > |G|$. On dispose donc de deux 2-Sylow distincts S et T tels que $S \cap T = \{e, x\}$, avec x d'ordre 2. Notons H le centralisateur de x

dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6, donc $|H| = 12$, 20 ou 60. Dans le deuxième cas, l'action transitive de G sur G/H induit un morphisme injectif $G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_3$, ce qui est contradictoire. Dans le troisième cas, x est dans le centre de G, ce qui assure $Z(G)$ est non trivial, ce qui contredit le fait que G soit simple. Donc finalement on a bien $|H| = 12$.

– On note $H \subset G$ le sous-groupe d'ordre 12 construit en d). L'action transitive de G sur G/H induit un morphisme injectif $\varphi : G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_5$. Alors $\varphi(G) \cap \mathfrak{A}_5$ est un sous-groupe distingué de $\varphi(G)$ (qui est simple), donc $\varphi(G) \cap \mathfrak{A}_5 = \{\mathrm{id}\}$ ou $\mathfrak{A}_5$. Dans le premier cas, on en déduit que $|\varphi(G)| \leq 2$ (en composant avec la signature), ce qui est contradictoire. Donc $\varphi(G)$ contient $\mathfrak{A}_5$, donc par cardinalité, φ induit bien un isomorphisme $G \cong \mathfrak{A}_5$.

Exercice 14 : $\star\star\star$

Soit G un groupe fini.

a) Soit H un sous-groupe de G d'indice n. On note $x_1, \ldots, x_n \in G$ un ensemble de représentants de G modulo H. L'action de G sur G/H induit une action de G sur $\{1, \ldots, n\}$, et pour tout $g \in G$ et $1 \leq i \leq n$, il existe $h_{i,g\cdot i} \in H$ tel que $gx_i = x_{g\cdot i} h_{i,g\cdot i}$. On note enfin $\pi : H \to H/D(H)$ la projection canonique. Montrer que la formule

$$V(g) := \pi\left(\prod_{i=1}^{n} h_{i,g\cdot i}\right)$$

définit un morphisme de groupes $G \to H/D(H)$ indépendant du choix des x_i.

b) Avec les notations précédentes, soit $h \in H$. On considère l'action de $\langle h \rangle$ sur $X = G/H$ et on note $g_1, \ldots, g_r$ des éléments de G tels que les classes $[g_i]$ des g_i dans X forment un ensemble de représentants pour cette action. Pour tout i, on note n_i l'entier minimal non nul tel que $h^{n_i} \cdot [g_i] = [g_i]$. Montrer que

$$V(h) = \pi\left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i\right).$$

c) Soient S un p-Sylow de G et $A, B \subset S$ des parties stables par conjugaison dans S. Montrer que si A et B sont conjuguées dans G, alors elles le sont dans $N_G(S)$ (on pourra considérer deux p-Sylow de $N_G(A)$).

d) Soit S un p-Sylow de G tel que $S \subset Z(N_G(S))$. Montrer que le morphisme $V : G \to S$ défini à la question a) est surjectif. En déduire qu'il existe un sous-groupe distingué H de G tel que S soit isomorphe à G/H.

e) En déduire que si G est simple non cyclique, alors le cardinal de G est divisible par 12 ou son plus petit facteur premier apparaît au moins au cube dans sa décomposition en facteurs premiers.

Solution de l'exercice 14.

a) On rappelle que le groupe $H/D(H)$ est commutatif, donc l'ordre des produits effectués dans ce groupe n'importe pas. Soient $g, g' \in G$. On a par définition

$$V(gg') = \pi\left(\prod_{i=1}^{n} h_{i,(gg')\cdot i}\right),$$

où les $h_{i,(gg')\cdot i} \in H$ sont définis par la formule

$$(gg')x_i = x_{(gg')\cdot i} h_{i,(gg')\cdot i}\,.$$

Or on a

$$(gg')x_i = g(g'x_i) = g(x_{g'\cdot i} h_{i,g'\cdot i}) = x_{g\cdot(g'\cdot i)} h_{g'\cdot i, g\cdot(g'\cdot i)} h_{i,g'\cdot i}\,,$$

donc

$$h_{i,(gg')\cdot i} = h_{g'\cdot i, g\cdot(g'\cdot i)} h_{i,g'\cdot i}\,.$$

Donc, puisque $H/D(H)$ est commutatif, on a

$$V(gg') = \pi\left(\prod_{i=1}^{n} h_{g'\cdot i, g\cdot(g'\cdot i)}\right)\pi\left(\prod_{i=1}^{n} h_{i,g'\cdot i}\right) = V(g)V(g')\,,$$

car l'application de $\{1,\dots,n\}$ dans lui-même donnée par $i \mapsto g'\cdot i$ est une bijection.
En outre, il est clair que $V(1) = 1$, donc cela assure que V est un morphisme de groupes.
Montrons maintenant que V est indépendant du choix des x_i : la commutativité de $H/D(H)$ assure que V reste le même si l'on permute les x_i. Si x_i' est un autre ensemble de représentants de G modulo H (définissant un morphisme $V' : G \to H/D(H)$), alors quitte à permuter les x_i', on peut supposer que x_i' est congru à x_i modulo H, i.e. qu'il existe $k_i \in H$ tel que $x_i' = x_i k_i$. Par conséquent, on voit (avec les notations naturelles) que l'on a

$$h_{i,g\cdot i} = k_{g\cdot i} h'_{i,g\cdot i} k_i^{-1}\,.$$

Donc, en utilisant à nouveau la commutativité de $H/D(H)$, on voit que pour tout $g \in G$,

$$V(g) = \pi\left(\prod_i h_{i,g\cdot i}\right) = \pi\left(\prod_i k_{g\cdot i} h'_{i,g\cdot i} k_i^{-1}\right) = \pi\left(\prod_i h'_{i,g\cdot i}\right) = V'(g)\,,$$

donc $V = V'$, ce qui assure que V ne dépend pas du choix des x_i.

b) Il est clair qu'un ensemble de représentants de G modulo H est donné par

$$g_1, hg_1, \dots, h^{n_1-1}g_1, g_2, hg_2, \dots, h^{n_2-1}g_2, g_3, \dots, g_r, hg_r, \dots h^{n_r-1}g_r\,.$$

Avec ce choix pour les x_i, on voit facilement que l'on a

$$V(h) = \pi\left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i\right)\,.$$

c) On suppose qu'il existe $g \in G$ tel que $B = gAg^{-1}$. Alors les hypothèses assurent que l'on a les inclusions suivantes :

$$S \subset N_G(A) \text{ et } g^{-1}Sg \subset N_G(A)\,.$$

Or S et $g^{-1}Sg$ sont deux p-Sylow du groupe $N_G(A)$, donc ils sont conjugués dans $N_G(A)$: il existe donc $h \in N_G(A)$ tel que

$$g^{-1}Sg = hSh^{-1}\,,$$

donc $gh \in N_G(S)$. Enfin, on a

$$(gh)A(gh)^{-1} = g(hAh^{-1})g^{-1} = gAg^{-1} = B$$

car h normalise A. Cela conclut la preuve.

d) Soit $s \in S$. En conservant les mêmes notations, la question b) assure que

$$V(s) = \pi\left(\prod_{i=1}^{r} g_i^{-1} s^{n_i} g_i\right)\,.$$

On pose alors $A = \{g_i^{-1}s^{n_i}g_i\}$ et $B = \{s^{n_i}\}$. Comme S est commutatif, A et B sont deux parties de S stables par conjugaison dans S, et conjuguées par l'élément g_i de G. Alors la question c) assure qu'il existe $y_i \in N_G(S)$ tel que $g_i^{-1}s^{n_i}g_i = y_i s^{n_i} y_i^{-1}$. Or par hypothèse S est contenu dans le centre de $N_G(S)$, ce qui assure que

$$g_i^{-1}s^{n_i}g_i = y_i s^{n_i} y_i^{-1} = s^{n_i}\,,$$

donc

$$V(s) = \prod_i s^{n_i} = s^{\sum_i n_i} = s^{[G:S]}\,.$$

Enfin, S est un p-Sylow de G, donc $[G : S]$ est premier au cardinal de S (qui est un groupe commutatif), ce qui assure que le morphisme $S \to S$ défini par $s \mapsto s^{[G:S]}$ est un isomorphisme (Lagrange assure que ce morphisme est injectif, donc bijectif. On peut aussi utiliser une relation de Bézout).

On a donc montré que la restriction de V à S était un isomorphisme, ce qui assure que $V : G \to S$ est surjectif. Donc $H = \mathrm{Ker}(V)$ est un sous-groupe distingué de G tel que S soit isomorphe à G/H via V.

e) Soit G un groupe non cyclique. On note p le plus petit facteur premier de $|G|$, et on suppose que p^3 ne divise pas $|G|$. Soit S un p-Sylow de G. Alors S est de cardinal p ou p^2, donc S est commutatif et comme plus haut, l'action par conjugaison induit un morphisme de groupes

$$\overline{\phi} : N_G(S)/S \to \mathrm{Aut}(S)\,,$$

dont la trivialité équivaut au fait que $S \subset Z(N_G(S))$.

Or tous les facteurs premiers du cardinal de $N_G(S)/S$ sont $> p$, alors que $\mathrm{Aut}(S)$ est l'un des trois groupes suivants : $\mathbb{Z}/p-1\mathbb{Z}$ (si S est d'ordre p), $\mathbb{Z}/p(p-1)\mathbb{Z}$ (si S est cyclique d'ordre p^2), $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (si S est non cyclique d'ordre p^2). Les cardinaux de ces trois groupes sont respectivement $p-1$, $p(p-1)$ et $(p^2-1)(p^2-p) = (p-1)^2p(p+1)$. Par conséquent, dans les trois cas, les facteurs premiers du cardinal de $\mathrm{Aut}(S)$ sont tous $\leq p+1$. On a donc deux cas :

– si $p > 2$, alors $p+1$ n'est pas premier, donc le morphisme $\overline{\phi}$ est trivial dans tous les cas.
– si $p = 2$, alors $p+1 = 3$ est premier, et le morphisme $\overline{\phi}$ trivial, sauf éventuellement si $p^2 = 4$ et $p+1 = 3$ divisent le cardinal de G.

Finalement, on a $S \subset Z(N_G(S))$ dans tous les cas, sauf si $p = 2$ et $|G|$ est multiple de 12. Donc la question d) assure que G admet un sous-groupe distingué d'indice $|S|$, sauf si 12 divise $|G|$.

On en déduit immédiatemment que G n'est pas simple, sauf si éventuellement 12 divise $|G|$.

Cela conclut la preuve.

Exercice 15 : $\star\star\star$

a) Montrer qu'un groupe d'ordre $60 < n < 168$ avec n non premier n'est jamais simple.

b) Montrer que $\mathrm{SL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$ sont d'ordre 168.

c) Montrer que $\mathrm{SL}_3(\mathbb{F}_2)$ est simple.

d) Soit G simple d'ordre 168. Montrer que G est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$.

e) Montrer que l'on a un isomorphisme entre $\mathrm{SL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$.

Solution de l'exercice 15.

a) On fait les listes des entiers entre 61 et 167, et on utilise les exercices 8, 11 et 14 pour voir que les seuls cardinaux possibles pour un groupe simple dans cet intervalle sont

$$72 = 2^3.3^2, 80 = 2^4.5, 88 = 2^3.11, 96 = 2^5.3, 104 = 2^3.13, 112 = 2^4.7, 120 = 2^3.3.5, 135 = 3^3.5,$$
$$136 = 2^3.17, 144 = 2^4.3^2, 152 = 2^3.19, 156 = 2^2.3.13, 160 = 2^5.5\,.$$

Puis on étudie séparément les cas restants en utilisant les théorèmes de Sylow.

b) Le calcul du cardinal de $\mathrm{GL}_n(\mathbb{F})$, où $\mathbb{F}$ est un corps fini de cardinal q, est classique. On trouve $|\mathrm{GL}_n(\mathbb{F})| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$. Donc ici, comme $\mathrm{SL}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2)$, on obtient $|\mathrm{SL}_3(\mathbb{F}_2)| = 7.6.4 = 168$.

c) Les éléments de $\mathrm{SL}_2(\mathbb{F}_3)$ ont un polynôme minimal dans la liste suivante : $X+1$, X^2+1, X^2+X+1, X^3+1, X^3+X+1, X^3+X^2+1, X^3+X^2+X+1. Montrons que le polynôme minimal d'une matrice de $\mathrm{SL}_3(\mathbb{F}_2)$ caractérise sa classe de conjugaison, que presque tous ces polynômes apparaissent effectivement et comptons au passage le nombre d'éléments dans chaque classe de conjugaison et l'ordre de ces éléments.

– La seule matrice de polynôme minimal $X+1$ est la matrice I_3.

– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Le polynôme minimal de A est $X^2+1=(X+1)^2$ si et seulement si $A \neq I_3$ et $\mathrm{Im}\,(A-I_3) \subset \mathrm{Ker}(A-I_3)$, si et seulement si $\mathrm{Ker}(A-I_3)$ est un plan contenant la droite $\mathrm{Im}\,(A-I_3)$. Donc se donner une telle matrice équivaut à se donner un plan P et une droite $D \subset P$ dans $\mathbb{F}_2^3$, et il y a exactement 7 choix pour P et 3 pour $D \subset P$, donc 21 matrices de polynôme minimal X^2+1. Ces matrices sont clairement d'ordre 2 et deux-à-deux conjuguées).
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Si le polynôme minimal de A est X^2+X+1, son polynôme caractéristique est nécessairement X^3+1 (car A est inversible), donc 1 est valeur propre de A, mais 1 n'est pas racine de X^2+X+1, ce qui est contradictoire. Donc le polynôme X^2+X+1 n'apparaît pas comme polynôme minimal d'une matrice de $\mathrm{SL}_3(\mathbb{F}_2)$.
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. On voit que le polynôme minimal de A est $X^3+1=(X+1)(X^2+X+1)$ si et seulement si $\mathbb{F}_2^3$ est somme directe de la droite $\mathrm{Ker}(A+1)$ et du plan $\mathrm{Ker}(A^2+A+1)$. Une telle matrice est complétement caractérisée par la donnée d'une droite et d'un plan supplémentaire, ainsi que celle d'un vecteur quelconque du plan dont l'image par A n'est pas colinéaire à lui-même. Il y a donc exactement $7.4.2 = 56$ telles matrices, qui sont toutes d'ordre 3, et bien deux-à-deux conjuguées.
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Le polynôme minimal de A est irréductible de degré 3 si et seulement si pour tout vecteur non nul x, (x, Ax, A^2x) est une base de $\mathbb{F}_2^3$. Comme X^3+X+1 et X^3+X^2+1 sont les seuls polynômes irréductibles de degré 3, on en déduit facilement qu'il y a exactement $6.4 = 24$ matrices de polynôme minimal X^3+X+1 et 24 matrices de polynôme minimal X^3+X^2+1. Toutes ces matrices sont clairement d'ordre 7 et deux telles matrices de même polynôme minimal sont bien conjuguées. Notons enfin que si A a pour polynôme minimal X^3+X+1, alors A^{-1} a pour polynôme minimal X^3+X^2+1 (et vice-versa).
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Le polynôme minimal de A est $X^3+X^2+X+1=(X+1)^3$ si et seulement si $\mathrm{Ker}(A+I_3)$ est une droite contenue dans le plan $\mathrm{Ker}((A+I_3)^2)$ et pour tout vecteur hors de ce plan, son image est dans le plan mais pas dans la droite. On voit donc qu'il y a exactement $7.3.2 = 42$ telles matrices, que leur ordre est 4 et qu'elles sont bien toutes conjuguées.

Finalement, on vérifie que l'on a bien $1+21+56+24+24+42=168$. On a donc ainsi décrit les 6 classes de conjugaison dans $\mathrm{SL}_3(\mathbb{F}_2)$.

Soit maintenant $H \lhd \mathrm{SL}_3(\mathbb{F}_2)$ un sous-groupe distingué $\neq \{I_3\}$. Supposons que H ne contienne aucun élément d'ordre 3 ou 7. Alors le cardinal de H est un diviseur de 8, donc H contient un élément d'ordre 2, donc H contient les 21 éléments d'ordre 2 (on a vu qu'ils étaient tous conjugués), donc H contient au moins 22 éléments, ce qui est contradictoire. Donc H contient soit un élément d'ordre 3 soit un d'ordre 7. Dans le premier cas, H contient 56 éléments d'ordre 7, donc $|H| \geq 57$, donc $|H| = 84$ ou 168, donc H contient un élément d'ordre 2 et un élément d'ordre 7, donc au moins 21 éléments d'ordre 2 et 24 d'ordre 7, donc $|H| \geq 57+21+24 = 102$, donc $|H| = 168$. Dans le second cas, H contient au moins 24 éléments d'ordre 7, et en fait H contient tous les 48 éléments d'ordre 7, car les deux classes de conjugaison sont échangées par l'inversion. Donc $|H| \geq 49$, donc $|H| = 56$, 84 ou 168. Donc H a un élément d'ordre 7 et on conclut par le premier cas que $|H| = 168$.

Finalement, on a $H = \mathrm{SL}_3(\mathbb{F}_2)$, ce qui assure la simplicité de $\mathrm{SL}_3(\mathbb{F}_2)$.

d) Les théorèmes de Sylow assurent que G admet exactement huit 7-Sylow. Si on note X l'ensemble des 7-Sylow de G, l'action transitive par conjugaison de G sur X induit un morphisme de groupes injectif

$$\varphi : G \hookrightarrow \mathfrak{S}(X) \cong \mathfrak{S}_8 .$$

Or les éléments de $\mathfrak{S}_8$ sont d'ordre 1, 2, 3, 4, 5, 6, 7, 8, 10, 12 et 15. Or G n'admet aucun élément d'ordre 15, donc tous les éléments de G sont d'ordre ≤ 12.

En outre, on voit que pour tout 7-Sylow S de G, $|N_G(S)| = \frac{|G|}{|X|} = 21$. Donc en particulier, le groupe $N_G(S)$ n'est pas cyclique.

Montrons que $N_G(S)$ agit transitivement sur $X' := X \setminus \{S\}$. Comme $N_G(S)$ agit trivialement sur S, on voit que la restriction de φ à S induit un morphisme

$$\widetilde{\varphi} : S \to \mathfrak{S}(X') \cong \mathfrak{S}_7 .$$

Si $T \in X'$, alors S n'est pas contenu dans $N_G(T)$ (sinon on aurait $S = T$), donc $S \cap N_G(T) = \{e\}$ et pour tous $g, g' \in S$, on a $gTg^{-1} = g'Tg'^{-1}$ si et seulement si $g = g'$. Par conséquent, l'orbite

de T sous l'action de S dans X' est de cardinal $|S| = 7 = |X'|$, donc S agit transitivement sur X'.

Soit $T \in X'$. On a vu que le groupe $N_G(S)$ de cardinal 21 agissait transitivement sur l'ensemble X' de cardinal 7, et le stabilisateur de T pour cette action n'est autre que $N_G(S) \cap N_G(T)$. Donc en calculant les cardainaux, on voit que $|N_G(S) \cap N_G(T)| = 3$.

On a $n_3 \neq 1$, congru à 1 modulo 3 et diviseur de 56, donc $n_3 \in \{4, 7, 28\}$. Le cas $n_3 = 4$ est impossible par 168 ne divise pas $4! = 24$. Supposons que $n_3 = 7$. Le sous-groupe $N_G(S)$ est d'ordre 21, il contient donc un ou sept 3-Sylow. Comme $N_G(S)$ n'est pas cyclique et d'ordre 21, on voit que cela implique que $N_G(S)$ possède exactement sept 3-Sylow, donc que $N_G(S)$ contient tous les 3-Sylow de G. Ceci étant valable pour tout 7-Sylow S, on aurait donc pour $T \neq S$ dans X, $|N_G(S) \cap N_G(T)| \geq 7.2 + 1 = 15$, ce qui contredit un calcul précédent. Donc finalement $n_3 = 28$.

On pose $H := N_G(N_G(S) \cap N_G(T))$. Comme $N_G(S) \cap N_G(T)$ est un 3-Sylow de G, H est de cardinal $\frac{168}{28} = 6$. Si H est cyclique, alors G contient au moins un élément x d'ordre 6. Alors $\langle x^2 \rangle$ est un 3-Sylow de G, et comme les 3-Sylow de G sont conjugués, on voit que tout 3-Sylow est engendré par le carré d'un élément d'ordre 6. Donc G contient au moins $2.28 = 56$ éléments d'ordre 6. Le groupe G contiendrait donc finalement $28.2 = 56$ éléments d'ordre 3, au moins 56 éléments d'ordre 6 et $8.6 = 48$ éléments d'ordre 7. Or $56 + 56 + 48 = 160$, et G possède en outre également au moins deux 2-Sylow, donc au moins 9 éléments d'ordre divisant 8, on trouve que G contiendrait au moins 169 éléments, ce qui est contradictoire. Donc H n'est pas cyclique, donc $H \cong \mathfrak{S}_3$.

Fixons maintenant un générateur s du 7-Sylow S. Alors l'application

$$\tau : \{0, \ldots, 6\} \to X'$$

définie par $\tau(k) := s^k T s^{-k}$ est bijective (car S agit transitivement sur X'). En posant $\tau(\infty) := S$, on obtient ainsi une bijection

$$\tau : \mathbb{P}^1(\mathbb{F}_7) = \mathbb{F}_7 \cup \{\infty\} \xrightarrow{\simeq} X\,.$$

On vérifie qu'avec ces identifications, l'action de s sur $X \cong \mathbb{P}^1(\mathbb{F}_7)$ définie par la formule suivante

$$\forall x \in \mathbb{P}^1(\mathbb{F}_7)\,,\ s \cdot x = x + 1$$

avec la convention naturelle que $\infty + 1 = \infty$. Autrement dit, l'action de s sur X est donnée par l'homographie de $\mathbb{P}^1(\mathbb{F}_7)$ définie par la matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)\,.$$

Choisissons $t \in N_G(S) \cap N_G(T)$ non trivial (donc d'ordre 3). Le morphisme $c : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(S) \cong \mathbb{Z}/6/Z$ donné par la conjugaison par les puissances de t est non trivial (sinon $N_G(S)$ serait cyclique engendré par st), il est donc égal à $k \mapsto 2k$ ou $k \mapsto 4k$, ce qui signifie que tst^{-1} est égal à s^2 ou s^4. Alors quitte à remplacer t par $t^2 = t^{-1}$, on peut supposer que $tst^{-1} = s^2$. Alors on voit facilement que l'action de t sur X correspond à la bijection de $\mathbb{P}^1(\mathbb{F}_7)$ donnée par la formule

$$\forall x \in \mathbb{P}^1(\mathbb{F}_7)\,,\ t \cdot x = 2.x$$

avec la convention naturelle que $2.\infty = \infty$. Autrement dit, l'action de t sur X est donnée par l'homographie de $\mathbb{P}^1(\mathbb{F}_7)$ définie par la matrice

$$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)\,.$$

Soient maintenant $u \in H \setminus (N_G(S) \cap N_G(T))$. Comme $H \cong \mathfrak{S}_3$, on voit que u correspond à une transposition, alors que t correspond à un 3-cycle. il est donc clair que $utu^{-1} = t^{-1}$. On en déduit

que pour tout $x \in \mathbb{P}^1(\mathbb{F}_7)$, on a $u \cdot (2.x) = 4.u \cdot x$. Montrons que $G = \langle s, t, u \rangle$. Il est clair que le groupe de droite est de cardinal > 21 et divisible par 21, donc son cardinal vaut 42, 84 ou 168. S'il vaut 84, c'est un sous-groupe d'indice 2 de G, il est distingué, ce qui contredit la simplicité de G. S'il vaut 42, c'est un sous-groupe d'indice 4, ce qui permet de construire un morphisme non trivial, donc injectif $G \to \mathfrak{S}(G/\langle s, t, u, \rangle \cong \mathfrak{S}_4$, ce qui est impossible par cardinalité. Donc on a bien $G = \langle s, t, u \rangle$. Comme G agit transitivement sur X, on voit que nécessairement $u(0) = \infty$ et $u(\infty) = 0$ (on rappelle que s et t fixent 0 et ∞). Supposons maintenant que $u(1) \in \{1, 2, 4\}$. Alors la relation $u \cdot (2.x) = 4.u \cdot x$ assure que vu comme permutation d'ordre 2 de $\mathbb{P}^1(\mathbb{F}_7)$, u a au moins deux points fixes, donc u est dans le normalisateur d'un 7-Sylow de G, ce qui est exclu puisque u est d'ordre 2 et ce normalisateur est d'ordre 21. Donc $u(1) \in \{3, 5, 6\}$. Alors la formule $u \cdot (2.x) = 4.u \cdot x$ assure que si l'on note $a := u(1) \in \{3, 5, 6\}$, l'action de u sur X correspond à la bijection de $\mathbb{P}^1(\mathbb{F}_7)$ donnée par la formule

$$\forall x \in \mathbb{P}^1(\mathbb{F}_7)\,,\ u \cdot x = \frac{a}{x}$$

avec les conventions naturelles. Autrement dit, l'action de t sur X est donnée par l'homographie de $\mathbb{P}^1(\mathbb{F}_7)$ définie par la matrice

$$\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_7)\,.$$

Or $a \in \{3, 5, 6\}$, donc $\frac{-1}{a} \in \{1, 2, 4\}$ est un carré dans $\mathbb{F}_7$, donc il existe $c \in \mathbb{F}_7^*$ tel que $\frac{-1}{a} = c^2$, et alors on voit que l'action de t sur X est donnée par l'homographie définie par la matrice

$$\begin{pmatrix} 0 & ac \\ c & 0 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)\,.$$

Finalement, comme $G = \langle s, t, u \rangle$, on voit que $\varphi(G) \subset \mathfrak{S}_8$ est contenu dans le sous-groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ de $\mathfrak{S}_8$ (en identifiant X et $\mathbb{P}^1(\mathbb{F}_7)$ via l'application τ). Or ces deux groupes ont pour cardinal 168, donc φ induit un isomorphisme entre G et $\mathrm{PSL}_2(\mathbb{F}_7)$.

e) Les questions c) et d) assurent le résultat. Le lecteur curieux pourra chercher à construire un isomorphisme explcite entre ces deux groupes.