## Exercices du chapitre 4

**Exercice** 4.1. Soit $\sigma$ dans le centre de $\mathrm{S}_n$. Écrivons que $\sigma$ commute à la transposition $(i\,j)$. On a $(i\,j) = \sigma(i\,j)\sigma^{-1} = (\sigma(i)\,\sigma(j))$, *i.e.* $\sigma(\{i,j\}) = \{i,j\}$. Ainsi, si $\sigma$ préserve toutes les parties à 2 éléments de $\{1,\dots,n\}$. Comme on a $n \geqslant 3$, pour tout $i \in \{1,\dots,n\}$ on peut trouver $j,k \in \{1,\dots,n\}$ avec $i,j,k$ distincts. On a alors $\{i\} = \{i,j\} \cap \{i,k\}$ puis $\sigma(i) = i$ : $\sigma$ est l'identité.

**Exercice** 4.2. (i) Un morphisme de groupes $f : G \to G'$ *avec* $G'$ *abélien* est constant sur les classes de conjugaison de $G$ : si on a $g,x \in G$ alors $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1}f(x) = f(x)$. Comme deux transpositions sont conjuguées dans $\mathrm{S}_n$, tout morphisme $\mathrm{S}_n \to \{\pm 1\}$ prend la même valeur $\epsilon \in \{\pm 1\}$ sur chaque transposition. Comme les transpositions engendrent $\mathrm{S}_n$, il y a donc au plus deux morphismes $\mathrm{S}_n \to \{\pm 1\}$. Pour $\epsilon = 1$, le morphisme est nécessairement trivial (et existe bien !). Pour $\epsilon = -1$, il existe encore : c'est la signature.

(ii) Pour tout sous-groupe $H$ d'indice 2 d'un groupe $G$ on a vu en cours qu'il existe un morphisme $G \to \{\pm 1\}$ de noyau $H$. En effet, on sait que $H$ est distingué, et on regarde alors la composée de la projection canonique $G \to G/H$ et de l'unique isomorphisme $G/H \simeq \{\pm 1\}$. Comme il n'y a qu'un morphisme non trivial $\mathrm{S}_n \to \{\pm 1\}$ par le (i), à savoir la signature, $\mathrm{A}_n$ est le seul sous-groupe d'indice 2 de $\mathrm{S}_n$.

**Exercice** 4.5. (i) Soit $f : \mathrm{A}_n \to \{\pm 1\}$ un morphisme. On sait que $\mathrm{A}_n$ est engendré par les 3-cycles. Il suffit donc de montrer que si $c$ est un 3-cycle on a $f(c) = 1$. Mais on a $f(c^3) = f(c)^3 = 1$ et donc $f(c) = 1$ car $f(c) = \pm 1$. (Plus généralement, si on a un morphisme $f : G \to G'$ et $g \in G$ tels que l'ordre de $g$ est premier à $|G'|$, alors on a $f(g) = 1$.)

(ii) On a $|\mathrm{A}_4| = 12$. Si $\mathrm{A}_4$ admet un sous-groupe $H$ d'ordre 6, ce sous-groupe est donc d'indice 2, puis le noyau d'un morphisme surjectif $\mathrm{A}_4 \to \{\pm 1\}$. Il n'y a pas de tel morphisme par le (i). C'est le contre-exemple à la réciproque naive du théorème de Lagrange évoqué après le Corollaire 4.7 Chap. 2.

**Exercice** 4.6. Soit $H$ le sous-groupe de $\mathrm{A}_n$ engendré par les $(i\ i+1\ i+2)$ avec $1 \leqslant i < n-1$. On veut montrer $H = \mathrm{A}_n$. Il suffit de voir que tous les 3-cycles sont dans $H$, car ces derniers engendrent $\mathrm{A}_n$ par le cours. C'est clair pour $n = 1,2,3$. Noter $(i\,j\,k)^{-1} = (j\,i\,k)$. Pour $n = 4$, on a $(1\,2\,3)(3\,2\,4) = (1\,2\,4) \in H$ et $(1\,3\,4) = (2\,3\,4)(1\,2\,3)(2\,3\,4)^{-1}$. Les 8 3-cycles sont bien dans $H$. Pour $n \geqslant 4$, on déduit du cas $n = 4$ que $H$ contient toutes les permutations paires à support dans $\{i,i+1,i+2,i+3\}$, pour tout $1 \leqslant i \leqslant n-3$. Si $(i\,j\,k)$ est dans $H$, on a aussi $\sigma(i\ j\ k)\sigma^{-1} = (\sigma(i)\,\sigma(j)\,\sigma(k))$ pour tout $\sigma \in H$. On en déduit successivement que $H$ contient tous les $(i\,i+1\,k)$ avec $i+2 \leqslant k \leqslant n$, puis que $H$ contient tous les $(i,j,k)$ avec $i < j < k$.

(Pour ce type d'arguments, il est souvent plus pratique d'utiliser l'Exercice 4.23. Concrètement, on aurait d'abord pu vérifier que $H$ agit 3-transitivement sur $\{1,\dots,n\}$ pour $n \geqslant 5$ (clair par récurrence), puis conclure en disant que $H$ contient un 3-cycle, et donc tous les 3-cycles par conjugaison et 3-transitivité.)

**Exercice** 4.7. Quitte à conjuguer $c$ (i.e. à renuméroter les entiers de 1 à $n$), on peut supposer $c = (1\,2\,3\,\dots\,m)$. Pour $k$ divisant $m$, on constate alors que $c^k$ est le produit des $m/k$-cycles $(i\ i{+}k\ i{+}2k\ \cdots\ i{+}(m{-}1)/k)$ avec $i = 1,\dots,k$. (Ces cycles sont bien disjoints : les entiers dans leur support sont $\equiv i \bmod k$). Pour $k$ général on écrit $c^k = (c^d)^{k/d}$. Les cycles de $c^d$ sont de longueur $m/d$ comme on l'a vu, et on a $k/d$ premier à $d$.

On est donc ramené au cas où $k$ est premier avec $m$, et il faut voir que $c^k$ est un $m$-cycle, *i.e.* que $\langle c^k \rangle$ permute transitivement $\{1,\dots,m\}$. Mais par Bezout il existe $q \in \mathbb{Z}$

avec $kq \equiv 1 \bmod m$. On a alors $(c^k)^q = c$, et donc $\langle c^k \rangle = \langle c \rangle$ permute transitivement $\{1, \dots, m\}$.

**Exercice** 4.10. (i) L'ordre d'un élément est le ppcm des longueurs des cycles de sa décomposition en cycles. Si c'est $p$, c'est que tous ses cycles sont de longueur $p$. Comme on est dans $\mathrm{S}_p$, l'unique possibilité est que ce soit un $p$-cycle.

(ii) Il existe $1 \leqslant i < p$ tel que $\sigma^i(1) = 2$. Comme $p$ est premier, $i$ est premier à $p$, et donc $c := \sigma^i$ est un $p$-cycle par l'exercice précédent (voir le second paragraphe du corrigé). Par définition, on a $c(1) = 2$. Enfin, les $p$ éléments $\sigma^j(1)$ avec $j = 0, \dots, p-1$ sont $\{1, \dots, p\}$ car $c$ est un cycle, de sorte que l'application $\{0, 1, \dots, p-1\} \to \{1, 2, \dots, p\}$ envoyant $j$ sur $c^j(1)$ est bijective. Il y a donc un unique $j$ tel que $\sigma^j(1) = 2$.

(iii) Par les (i) et (ii), tout sous-groupe $H$ d'ordre $p$ est engendré par un unique $p$-cycle de la forme $(1\,2\,a_3\,a_4\,\dots\,a_p)$, avec $\{a_3, a_4, \dots, a_p\} = \{3, 4, \dots, p\}$. Il y a $(p-2)!$ tels éléments.

**Exercice** 4.8. (i) Soit $H$ le sous-groupe engendré par la transposition $t$ et le $p$-cycle $c$. On veut montrer $H = \mathrm{S}_p$. Quitte à conjuguer à $H$ (= renuméroter), on peut supposer $t = (1\,2)$. Par le (ii) de l'exercice précédent, il existe $1 \leqslant i < p$ tel que $c^i = (1\,2\,a_3\,\dots\,a_p) \in H$ avec $\{a_3, a_4, \dots, a_p\} = \{3, 4, \dots, p\}$. On a alors $\gamma := tc = (1\,2)(1\,2\,a_3\,\dots\,a_p) = (2\,a_3\,\dots\,a_p) \in H$, puis $\gamma^i t \gamma^{-i} = (1\,a_{i+1}) \in H$ pour $1 \leqslant i < p$, et donc $(1\,i) \in H$ pour tout $i = 2, \dots, p$. Enfin, pour $1 < i < j$ on en déduit $(i\,j) = (1\,i)(1\,j)(1\,i)^{-1} \in H$ : le groupe $H$ contient toutes les transpositions, c'est $\mathrm{S}_p$.

(ii) Pour $p = 4$, les éléments $c = (1\,2\,3\,4)$ et $t = (1\,3)$ n'engendrent pas $\mathrm{S}_4$. En effet, on a $tct^{-1} = (3\,2\,1\,4) = c^{-1}$, de sorte que tout élément de $\langle c, t \rangle$ est de la forme $t^k c^q$ avec $0 \leqslant k \leqslant 1$ et $0 \leqslant q \leqslant 3$ : il y a un plus 8 tels éléments.

**Exercice**4.3. Comme $G$ contient une transposition par hypothèse, on a $n \geqslant 2$, et de même on a $n \geqslant 3$ dans la question (ii).

(i) La condition suffisante est claire car $\mathrm{S}_n$ agit 2-transitivement sur $\{1, \dots, n\}$. Réciproquement, fixons $i < j$ avec $(i\,j) \in G$. Pour $g \in G$ on a $g(i\,j)g^{-1} = (g(i)\,g(j))$. Si $G$ agit 2-transitivement sur $\{1, \dots, n\}$, on a donc $(k\,l) \in G$ pour tout $k < l$, puis $G$ contient toutes les transpositions, et on a $G = \mathrm{S}_n$.

(ii) Le groupe $G$ agit transitivement sur $\{1, \dots, n\}$ car il contient un $n$-cyclique. Pour voir qu'il agit 2-transitivement, il suffit de voir que pour un certain $i \in \{1, \dots, n\}$ le stabilisateur $G_i$ de $i$ dans $G$ agit transitivement sur $\{1, \dots, \hat{i}, \dots, n\}$. C'est clair si on prend pour $i$ le point fixe d'un $n-1$-cycle dans $G$.

**Exercice** 4.4 Pour montrer l'indication, on raisonne par récurrence sur $r := |X|$ et on note $H(x_1, \dots, x_n) \subset S_X$ le sous-groupe engendré par les $t_i := (x_i\ x_{i+1})$. Le résultat est évident pour $r \leqslant 2$. Écrivons $X = Y \cup \{x_n\}$ avec $Y = \{x_1, \dots, x_{n-1}\}$. Par récurrence, on a $H(x_1, \dots, x_{n-1}) = \mathrm{S}_Y$. Si on a $X = Y$, on a gagné. Sinon, $x_n$ n'est pas dans $Y$ et on identifie $\mathrm{S}_Y$ au sous-groupe de $\mathrm{S}_X$ fixant $x_n$. Pour $\sigma \in \mathrm{S}_Y$ on a $\sigma\, t_r\, \sigma^{-1} = (\sigma(x_r)\,\sigma(x_{r+1}))$. On en déduit que $H(x_1, \dots, x_n)$ contient tous les $(x\,x')$ avec $x, x' \in X$, et donc $H(x_1, \dots, x_n) = \mathrm{S}_X$.

Supposons que le graphe $\mathscr{G}$ n'est pas connexe. Il existe donc une partition $S = S_1 \coprod S_2$ telle que toute arête de $\mathscr{G}$ est incluse dans $S_1$ ou dans $S_2$. Par définition de $\mathscr{G}$ on constate que toute transpositions dans $T$ préserve $S_1$ et $S_2$. On en déduit que le groupe $\langle T \rangle$ préserve aussi $S_1$ et $S_2$. Il n'agit donc pas transitivement sur $\{1, \dots, n\}$, et donc $\langle T \rangle \neq \mathrm{S}_n$.

Supposons enfin que $\mathscr{G}$ est connexe...

**Exercice** 4.9 Soit $H$ le sous-groupe de $\mathrm{S}_n$ engendré par $c := (1\,2\,\cdots\,n)$ et la transposition $(i\,j)$. Notons $d$ le pgcd de $n$ et $|j-i|$. Montrons d'abord que $H = \mathrm{S}_n$ entraîne $d = 1$. Observons pour cela que si l'on a $1 \leqslant a, b \leqslant n$ avec $a \equiv b \bmod d$, alors pour tout $\sigma \in H$ on a $\sigma(a) \equiv \sigma(b) \bmod d$. En effet, c'est vrai pour $\sigma = c, c^{-1}$ et $\sigma = (i\,j)$, et on conclut par définition de $H$. Autrement dit, les parties de $\{1, \ldots, n\}$ de la forme $P_i := (i + d\mathbb{Z}) \cap \{1, \ldots, n\}$ avec $i \in \mathbb{Z}$ sont préservées dans leur ensemble par $H$. Noter

$$\coprod_{i=1}^{d} P_i = \{1, \ldots, n\} \quad \text{et} \quad |P_i| = n/d, \ \ \forall i \in \mathbb{Z}.$$

Supposant $H = \mathrm{S}_n$, le groupe $H$ agit 2-transitivement sur $\{1, \ldots, n\}$ et on a donc soit $d = 1$ et $|P_i| = n$, soit $d = n$ et $|P_i| = 1$. Le second cas est exclus car $d$ divise $i - j$ et $|i - j| < n$.

Supposons réciproquement $d = 1$. Regardons les transpositions dans $H$ de la forme $c^k(i\,j)c^{-k} = (i + k \ \ j + k)$, avec $k \in \mathbb{Z}$, et identifions pour simplifier $\{1, \ldots, n\}$ avec $\mathbb{Z}/n\mathbb{Z}$. Posant $s = j - i$, ces transpositions contiennent notamment

$$(0\ s), \ \ (s\ 2s), \ \ \ldots, \ \ (ks\ (k+1)s), \ \ \forall k \in \mathbb{Z}.$$

Mais comme $s$ est dans $(\mathbb{Z}/n\mathbb{Z})^\times$ par hypothèse, tout élément de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $ks$ pour $k \in \mathbb{Z}$ bien choisi. Ainsi, le graphe de sommets $\mathbb{Z}/n\mathbb{Z}$ et dont les arêtes sont les $\{ks, \ (k+1)s\}$ avec $k \in \mathbb{Z}$, est connexe (tout point est relié à 0). On conclut par Exercice **??** (vi).

**Exercice** 4.12. (i) Soit $H$ le sous-groupe des permutations de $\mathrm{S}_n$ à support dans le complémentaire $T$ de $S$. L'application $H \to \mathrm{S}_T, \sigma \mapsto \sigma_{|T}$, est un isomorphisme. Les éléments de $\langle c \rangle$ sont à support dans $S$. On a donc $H \cap \langle c \rangle = 1$ et $hg = gh$ pour tout $h \in H$ et tout $g \in \langle c \rangle$. En particulier, on a $\langle c \rangle H \subset C$. Reste à voir $C = \langle c \rangle H$. Écrivons $c = (i_1, \ldots, i_k)$ et considérons $\sigma \in C$. L'identité

$$\sigma(i_1\, i_2\, \ldots\, i_k)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \ldots\, \sigma(i_k)) = (i_1\, i_2\, \ldots\, i_k)$$

montre que $\sigma$ préserve $S$ (et donc $T$), et aussi que si l'on a $\sigma(i_1) = i_1$ alors $\sigma_{|S} = \mathrm{id}_S$. Mais on a $\sigma(i_1) = c^q(i_1)$ pour un certain $q$ car $\sigma$ préserve $S$. On a donc $c^{-q}\sigma \in C$ et $c^{-q}\sigma(i_1) = i_1$, et donc $c^{-q}\sigma$ préserve $S$ et y vaut l'identité : c'est un élément de $H$. On a montré $\sigma \in \langle c \rangle H$.

(ii) D'après le (i), le centralisateur de $(1\,2)$ est $\langle (1\,2), (3\,4) \rangle = \{1, (1\,2), (3\,4), (1\,2)\,(3\,4)\}$. Il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. De même, celui de $(1\,2\,3)$ est $\langle (1\,2\,3) \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, et celui de $(1\,2\,3\,4)$ est $\langle (1\,2\,3\,4) \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Reste à déterminer le centralisateur $C$ de la double transposition $d = (1\,2)(3\,4)$. Un élément $\sigma \in \mathrm{S}_4$ est dans $C$ si, et seulement si, on a $(1\,2)(3\,4) = \sigma d \sigma^{-1} = (\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4))$. Il y a donc exactement deux cas. Soit on a $\sigma(\{1,2\}) = \{1,2\}$ et $\sigma(\{3,4\}) = \{3,4\}$, ce qui équivaut à dire que $\sigma$ est dans le sous-groupe $H := \langle (1\,2), (3\,4) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soit on a $\sigma(\{1,2\}) = \{3,4\}$ et $\sigma(\{3,4\}) = \{1,2\}$, ce qui revient aussi à dire que l'élément $(1\,3)(2\,4)\sigma$ est dans $H$. On en déduit $C = \langle (1\,2), (3\,4), (1\,3)(2\,4) \rangle$. En fait, on a $(1\,2)(1\,3)(2\,4) = (1\,3\,2\,4) \in C$, $(1\,3\,2\,4)^2 = (1\,2)(3\,4)$, et $(1\,2)(3\,4)(1\,3)(2\,4) = (1\,4)(2\,3)$. On en déduit $C = \langle (1\,4)(2\,3), (1\,3\,2\,4) \rangle$ : c'est aussi le conjugué par $(2\,3)$ du groupe diédral $\mathrm{D}_8 \subset \mathrm{S}_4$ du cours. En particulier, on a $C \simeq \mathrm{D}_8$.

**Exercice** 4.14. (i) Pour $i = j$ on a $s_i^2 = 1$. Mais si on a $s_i^2 = s_j^2 = 1$, les relations $s_i s_j s_i s_j = 1$ et $s_i s_j s_i s_j s_i s_j = 1$ s'écrivent respectivement $s_i s_j = s_j s_i$ et $s_i s_j s_i = s_j s_i s_j$.

(ii) On raisonne par récurrence sur $n$. Le cas $n = 1$ est trivial, car on a $G = \{1, s_1\}$. On suppose $n > 1$. Soit $g \in G$. Utilisant $s_n^2 = 1$ on peut écrire

$$g \ = \ h_1\, s_n\, h_2\, s_n\, \cdots\, s_n\, h_k, \tag{78}$$

pour un certain $k \geqslant 1$ et des éléments $h_1, \dots, h_k$ dans $H := \langle s_1, \dots, s_{n-1} \rangle$. Si on a $k = 1$, alors $g$ est dans $H$, et il n'y a rien à démontrer. Sinon, l'élément $h_2$ s'écrit par récurrence $h_2 = s_i\, s_{i+1} \cdots s_{n-1}\, h_2'$ avec $1 \leqslant i \leqslant n$ et $h_2' \in \langle s_1, \dots, s_{n-2} \rangle$. Supposons d'abord $k > 2$. Comme $s_n$ commute aux $s_i$ avec $i < n-1$ par hypothèse, on a donc

$$s_n\, h_2\, s_n = s_i\, s_{i+1} \cdots s_n\, s_{n-1}\, s_n\, h_2'.$$

La relation de tresse permet de remplacer $s_n\, s_{n-1}\, s_n$ par $s_{n-1}\, s_n\, s_{n-1}$. Le nombre $k$ d'occurences de $s_n$ dans l'écriture (78) de $g$ a donc chuté de 1. Par récurrence sur $k$, on peut donc supposer $k = 2$, *i.e.* $g = h_1\, s_n\, h_2$. Écrivons $h_1 = s_j\, s_{j+1} \cdots s_{n-1}\, h_1'$ avec $1 \leqslant j \leqslant n$ et $h_1' \in \langle s_1, \dots, s_{n-2} \rangle$. Comme $s_n$ commute aux $s_j$ avec $j < n-1$ on a donc

$$g = h_1\, s_n\, h_2 = s_j\, s_{j+1} \cdots s_{n-1}\, s_n\, h_1'\, h_2 = f_j\, h_1'\, h_2 \in f_j H.$$

(iii) On raisonne par récurence sur $n$. C'est évident pour $n = 1$ car alors $G = \{1, s_1\}$ est de cardinal $\leqslant 2$. Le sous-groupe $H$ de $G$ engendré par les $s_i$ avec $i < n$ satisfait l'hypothèse de récurrence, et donc vérifie $|H| \leqslant n!$. On a donc $|G| \leqslant (n+1)n! = (n+1)!$ par le (ii).

(iv) On constate que les $n$ transpositions $t_i := (i\ i+1)$ de $\mathrm{S}_{n+1}$, avec $1 \leqslant i \leqslant n$, satisfont $(t_i\, t_j)^2 = 1$ pour $i = j$ et $|i - j| > 1$, et que l'élément $t_i\, t_{i+1} = (i\ i+1\ i+2)$, pour $i < n$, vérifie aussi $(t_i\, t_{i+1})^3 = 1$. Soit $\Gamma$ le groupe de droite défini par les générateurs $s_i$ avec $1 \leqslant i \leqslant n$, et les relations $(s_i\, s_j)^{m_{i,j}} = 1$ pour tout $1 \leqslant i \leqslant j \leqslant n$. Par la propriété universelle de $\Gamma$, on a un unique morphisme de groupes

$$f : \Gamma \to \mathrm{S}_{n+1}$$

vérifiant $f(s_i) = t_i$ pour tout $i = 1, \dots, n$. Mais les $t_i$ engendrent $\mathrm{S}_{n+1}$ par le cours, donc $f$ est surjectif. On a aussi $|\Gamma| \leqslant (n+1)!$ par le (iii). Le morphisme $f$ est donc un isomorphisme.

**Exercice** 4.15. (i) Si la case vide est déplacée horizontalement pour passer de $E$ à $F$, ou plus généralement en suivant le serpent, on a $\mathrm{s}(E) = \mathrm{s}(F)$ et donc $\sigma(F) = \sigma(E)$. Sinon nous allons voir que $\sigma(E)^{-1}\sigma(F)$ est un cycle de longueur $3, 5$ ou $7$ qui ne dépend pas de $E$. En effet, supposons par exemple que la case vide se trouve à la $i$-ème case de la deuxième ligne et monte verticalement en première ligne. Écrivons $\mathrm{s}(E) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, \dots)$. Alors selon que l'on a $i = 1, 2, 3$, l'élément $\mathrm{s}(F)$ vaut $(x_2, x_3, x_4, x_5, x_6, x_7, x_1, \dots)$, $(x_1, x_3, x_4, x_5, x_6, x_2, x_7, \dots)$ et $(x_1, x_2, x_4, x_5, x_3, x_6, x_7, \dots)$ respectivement. On constate donc que l'on a $\sigma(F) = \sigma(E) \circ \sigma_i$ avec

$$\sigma_1 = (1\,2\,3\,4\,5\,6\,7),\ \sigma_2 = (2\,3\,4\,5\,6) \text{ et } \sigma_3 = (3\,4\,5).$$

En étudiant de même la montée de la case vide en partant des lignes 3 et 4, on trouve les permutations suivantes (conjuguées de celles ci-dessus par $x \mapsto x+4$ et $x \mapsto x+8$) :

$$(7\,8\,9),\ (6\,7\,8\,9\ 10),\ (5\,6\,7\,8\,9\ 10\ 11),\ (9\,10\ 11\ 12\ 13\ 14\ 15),\ (10\ 11\ 12\ 13\ 14) \text{ et } (11\ 12\ 13).$$

Bien entendu, lorsque l'on descend la case vide au lieu de la monter, on obtient les cycles inverses à ceux ci-dessus.

(ii) Soient $E = E_1, \dots, E_n = F$ une suite d'états du taquin obtenus par mouvements élémentaires successifs. On a

$$\sigma(E)^{-1}\sigma(F) = (\sigma(E_1)^{-1}\sigma(E_2))\,(\sigma(E_2)^{-1}\sigma(E_3))\,\dots\,(\sigma(E_{n-1})^{-1}\sigma(F)). \tag{79}$$

Ainsi, on constate que $\sigma(E)^{-1}\sigma(F)$ est un produit de $n-1$ éléments parmi les 9 cycles ci-dessus et leurs inverses. Comme tous ces cycles sont de longueur impaire, il est dans $\mathrm{A}_{15}$. Si le taquin A donné était dans $\mathscr{E}$ on aurait donc $\sigma(E_0)^{-1}\sigma(A) = (13\ 14) \in \mathrm{A}_{15}$, une contradiction.

(iii) La Formule (79) et le (i) montrent que l'ensemble $G$ de l'énoncé est un sous-groupe de $\mathrm{S}_{15}$ inclus dans $\mathrm{A}_{15}$. Mieux, c'est le sous-groupe de $\mathrm{A}_{15}$ engendré par les 9 cycles indiqués plus haut. On constate que $G$ agit 3-transitivement sur $\{1, \dots, 15\}$. En effet, la transitivité est claire rien que grâce aux trois 7-cycles. La transitivité du stabilisateur $G_1$

sur $\{2,\dots,15\}$ est aussi claire à cause de $(2\,3\,4\,5\,6)$, $(5\,6\,7\,8\,9\ 10\ 11)$ et $(9\,10\ 11\ 12\ 13\ 14\ 15)$. Enfin, la transitivité du stabilisateur $(G_1)_2$ sur $\{3,\dots,15\}$ est encore claire à cause de $(3\,4\,5)$, $(5\,6\,7\,8\,9\ 10\ 11)$ et $(9\,10\ 11\ 12\ 13\ 14\ 15)$. On conclut par l'Exercice 4.23. Comme $G$ contient le 3-cycle $(3\,4\,5)$, il contient par conjugaison tous les $(\sigma(3)\,\sigma(4)\,\sigma(5))$ avec $\sigma\in G$ et donc tous les 3-cycles par 3-transitivité de $G$. On a montré $G=\mathrm{A}_{15}$.

(iv) On a $\sigma(C)^{-1}\sigma(B)=(13\ \ 14)$ donc un seul de $B$ ou $C$ est un état du jeu de Taquin par le (iii). On a $\mathrm{s}(B)=(1\,2\,3\,7\,6\,5\,4\,8\,9\,10\,11\,15\,14\,13\,12)$, et donc on constate

$$\sigma(E_0)^{-1}\sigma(B)=\begin{bmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\ 10\ 11\ 12\ 13\ 14\ 15\\ 1\,2\,3\,6\,7\,8\,4\,5\,9\ 10\ 11\ 13\ 14\ 15\ 12\end{bmatrix},$$

qui vaut aussi $(4\,6\,8\,5\,7)(12\,13\,14\,15)$. Il n'est pas dans $\mathrm{A}_{15}$ : c'est le C qui est un état du taquin.

(v) Il est clair que l'on a $\mathrm{s}(F)=\mathrm{s}(F')$ si, et seulement si, $F'$ est obtenu à partir de $F$ et d'un déplacement de la case vide le long du serpent. Il y a donc exactement 16 tels $F'$ à $F$ donné. Il est équivalent de se donner $\mathrm{s}(F)$ et $\sigma(F)$, ou encore son translaté $\sigma(E_0)^{-1}\sigma(F)$. L'application $\mathscr{E}\to G, F\mapsto\sigma(E_0)^{-1}\sigma(F)$, est donc injective, et toutes ses fibres ont 16 éléments. On en déduit $|\mathscr{E}|=16|\mathrm{A}_{15}|=16!/2$.

**Exercice** 4.16. (i) L'élément $f^{-1}\circ\sigma\circ f$ est une bijection de $\{1,\dots,n\}$ (composée de 3 bijections), *i.e.* dans $\mathrm{S}_n$. Il y a donc un sens à considérer sa signature. Changer $f$ en une autre bijection $f'$ revient à écrire $f=f'\circ g$ avec $g\in\mathrm{S}_n$. On a alors $(f')^{-1}\circ\sigma\circ f'=g^{-1}(f^{-1}\circ\sigma\circ f)g$. On conclut car deux éléments conjugués de $\mathrm{S}_n$ ont même signature (voir par exemple le corrigé de la question (i) de l'Exercice 4.2).

(ii) Pour vérifier le (ii), on choisit un $f$ et on utilise simplement $f^{-1}\circ\sigma\sigma'\circ f=(f^{-1}\circ\sigma\circ f)(f^{-1}\circ\sigma'\circ f)$ et le fait que la signature est un morphisme sur $\mathrm{S}_n$. On définit bien sûr le groupe $\mathrm{A}_X$ comme le noyau de la signature.

(iii) On peut par exemple écrire $\tau=t_1t_2\dots t_r$ où les $t_i$ sont des transvections de $Y$. On constate alors que l'on a $\sigma=t_1't_2'\dots t_r'$ où $t_i'$ est l'unique transposition de $X$ à support dans $Y$ et coïncidant avec $t_i$ sur $Y$. On a bient $\epsilon(\tau)=(-1)^r=\epsilon(\sigma)$.

**Exercice** 4.17. Soit $f:G\to\mathrm{S}_G, g\mapsto\mathrm{m}_g$, le morphisme donné par l'action de Cayley. En le composant avec la signature $\epsilon:\mathrm{S}_G\to\{\pm1\}$, on en déduit un morphisme $\epsilon\circ f:G\to\{\pm1\}$. Comme $G$ est simple, ce morphisme est soit trivial, soit injectif, et ce dernier cas ne se produit que si on a $|G|\leqslant 2$. On suppose désormais $|G|>2$, et donc $\epsilon\circ f=1$.

Pour $g\in G$, regardons la décomposition en cycles de la bijection $\mathrm{m}_g:G\to G, h\mapsto gh$. Pour cela, on introduit l'ordre $d$ de $g$, ainsi que des représentants $h_1,\dots,h_n\in G$ de $\langle g\rangle\backslash G$ (classes à droite). Tout $h\in G$ s'écrit de manière unique sous la forme $g^ih_j$ avec $1\leqslant j\leqslant n$ et $0\leqslant i<d$, et on a $dn=|G|$. On en déduit que $\mathrm{m}_g$ est un produit de $n$ $d$-cycles à supports disjoints. Sa signature $\epsilon(\mathrm{m}_g)$ vaut donc $(-1)^{(d-1)n}$.

Supposons maintenant $|G|$ pair, et par Cauchy, que l'on a choisi $g\in G$ d'ordre $d=2$. On a $\epsilon(\mathrm{m}_g)=(-1)^n=1$, et donc $n=|G|/2$ est pair, et $|G|\equiv 0 \bmod 4$.

**Exercice** 4.11. (i) On pose $G=\mathrm{A}_4$ et $K=\mathrm{K}_4$. On a $K\lhd G$. Soit $H$ le sous-groupe $\langle(1\,2)(3\,4)\rangle$ de $\mathrm{K}_4$. C'est un sous-groupe d'ordre 2 et distingué dans $\mathrm{K}_4$, ce dernier étant abélien. Mais il n'est pas distingué dans $\mathrm{A}_4$, car $(1\,2\,3)(1\,2)(3\,4)(1\,2\,3)^{-1}=(2\,3)(1\,4)\notin H$.

(ii) Soit $g\in G$. Alors l'automorphisme $\alpha:=\mathrm{int}_g$ de $G$ vérifie $\alpha(K)=K$ car $K$ est distingué dans $G$, de sorte que l'on a $\alpha_{|K}\in\mathrm{Aut}(K)$. Comme $H$ est caractéristique dans $K$, on a $\alpha_{|K}(H)=H$, i.e. $gHg^{-1}=H$. On a montré que $H$ est distingué dans $G$.

**Exercice** 4.13. (i) Supposons que $\sigma$ possède un cycle $c$ de cardinal pair. Alors $\tau = c$ convient. Supposons que $\sigma$ possède deux cycles de même cardinal $m$ impair, disons $(i_1\, i_2\, \dots\, i_m)$ et $(j_1\, j_2\, \dots\, j_m)$. Alors $\tau = (i_1\, j_1)(i_2\, j_2)\dots(i_m\, j_m)$ est de signature $(-1)^m = 1$ et vérifie $\tau\sigma\tau^{-1} = \sigma$. Si $\sigma$ a deux points fixes $i$ et $j$ alors $\tau = (i\, j)$ convient aussi. Supposons enfin $\sigma = c_1c_2\cdots c_r$ avec les $c_i$ de longueur impaires distinctes, et au plus un point fixe. Soient $C$ le centralisateur de $\sigma$ dans $\mathrm{S}_n$ et $\tau \in C$. On sait que les cycles de $\tau\sigma\tau^{-1} = \sigma$ sont les $\tau c_i\tau^{-1}$. Par unicité des longueurs des cycles, on a donc $\tau c_i\tau^{-1} = c_i$ pour tout $i$. En particulier, $\tau$ préserve le support $S_i$ de chaque $c_i$, ainsi que l'éventuel point fixe de $\sigma$. Quitte à multiplier $\tau$ par un élément du sous-groupe $H = \langle c_1, c_2, \dots, c_r\rangle \subset C$, on peut supposer que $\tau$ admet un point fixe dans chacun des $S_i$. La formule $\tau c_i\tau^{-1} = c_i$ montre alors $\tau_{|S_i} = \mathrm{id}_{S_i}$, puis $\tau = 1$. On a montré $C = H$. On conclut car $\varepsilon(c_i) = 1$ pour tout $i$, et donc $\varepsilon(C) = \{1\}$.

(ii) Supposons $\sigma \in \mathrm{A}_n$ non spécial. Soit $\tau \in \mathrm{S}_n$ avec $\tau\sigma = \sigma\tau$ et $\varepsilon(\tau) = -1$. Pour tout $g \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$ on a $g\sigma g^{-1} = g\tau\sigma(g\tau)^{-1}$ avec $g\tau \in \mathrm{A}_n$. L'inclusion évidente $\mathrm{Conj}_{\mathrm{A}_n}(\sigma) \subset \mathrm{Conj}_{\mathrm{S}_n}(\sigma)$ est donc une égalité.

(iii) Supposons $\sigma \in \mathrm{A}_n$ spécial et fixons $s \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$. On a $\mathrm{S}_n = \mathrm{A}_n \coprod \mathrm{A}_n s$ car $\mathrm{A}_n$ est d'indice 2 dans $\mathrm{S}_n$. On en déduit que pour $g \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$, on a $g = hs$ pour un certain $h \in \mathrm{A}_n$, puis $g\sigma g^{-1} = hs\sigma s^{-1}h^{-1}$. Cela montre $\mathrm{Conj}_{\mathrm{S}_n}(\sigma) = \mathrm{Conj}_{\mathrm{A}_n}(\sigma) \cup \mathrm{Conj}_{\mathrm{A}_n}(s\sigma s^{-1})$. Supposons enfin que l'on a $g\sigma g^{-1} = hs\sigma s^{-1}h^{-1}$ avec $g, h$ dans $\mathrm{A}_n$. Alors l'élément $s^{-1}h^{-1}g \in \mathrm{S}_n$ commute avec $\sigma$ et il est de signature $-1$ : absurde.

(iv) Par le cours, des représentants des classes de conjugaison de $\mathrm{S}_4$ incluses dans $\mathrm{A}_4$ sont $1, (1\,2)(3\,4), (1\,2\,3)$. Les éléments 1 et $(1\,2)(3\,4)$ sont non spéciaux dans $\mathrm{S}_4$, mais $(1\,2\,3)$ y est spécial. Des représentants des classes de conjugaison de $\mathrm{A}_4$ sont donc $1, (1\,2)(3\,4), (1\,2\,3)$ et $(2\,1\,3)$ (on a pris $s = (1\,2)$). De même, des représentants des classes de conjugaison de $\mathrm{S}_5$ incluses dans $\mathrm{A}_5$ sont $1, (1\,2)(3\,4), (1\,2\,3)$ et $(1\,2\,3\,4\,5)$. Les éléments $1, (1\,2)(3\,4), (1\,2\,3)$ sont non spéciaux dans $\mathrm{S}_5$, mais $(1\,2\,3\,4\,5)$ y est spécial. Des représentants des classes de conjugaison de $\mathrm{A}_4$ sont donc $1, (1\,2)(3\,4), (1\,2\,3), (1\,2\,3\,4\,5)$ et $(2\,1\,3\,4\,5)$.

**Exercice** 4.18. On suppose que $G$ agit transitivement sur $X$, avec $|X| = n$ et $G$ fini.

(i) Soit $x \in X$. On a $\mathrm{O}_x = X$ car l'action est transitive. On a donc $|G| = |X||\mathrm{G}_x|$ par la formule orbite-stabilisateur, puis $n$ divise $|G|$.

(ii) Par hypothèse, le morphisme $\mathrm{m} : G \to \mathrm{S}_X$ associé à l'action est injectif. On a $G \simeq \mathrm{m}(G)$, $\mathrm{m}(G)$ sous-groupe de $\mathrm{S}_X$, et $\mathrm{S}_X \simeq \mathrm{S}_n$. On a donc $|G| \,|\, n!$ par Lagrange.

(iii) Soient $x_1, \dots, x_r$ des représentants des orbites de $G$ dans $X$. On a donc $|X| = \sum_{i=1}^{r} |\mathrm{O}_{x_i}|$ par l'équation aux classes. Mais on a $G_x = \{1\}$ pour tout $x \in X$ par hypothèse, et donc $|G| = |\mathrm{O}_x|$ par la formule orbite-stabilisateur, puis $|X| = r|G|$.

**Exercice** 4.19. (i) On peut supposer $G = \mu_n$. Soit $d$ un diviseur de $n$. On fait agir $G$ sur $\mu_d$ par $G \times \mu_d \to \mu_d, (g, x) \mapsto g^{n/d}x$. C'est clairement une action transitive. On aurait aussi pu utiliser le point de vue $\mathbb{Z}/n\mathbb{Z}$, et observer que $\mathbb{Z}/n\mathbb{Z}$ agit sur $\mathbb{Z}/d\mathbb{Z}$ par $(\overline{m}, \overline{x}) \mapsto \overline{m + x}$.

(ii) On sait que deux actions transitives de $G$ sont isomorphes si, et seulement si, elles ont un stabilisateur en commun. Mais on sait aussi que les sous-groupes du groupe cyclique $\mu_n$ sont les $\mu_d$ avec $d \,|\, n$. Le stabilisateur de 1 dans l'action ci-dessus est $\mu_{n/d}$. Cela conclut.

**Exercice** 4.20. Pour $n \geqslant 2$, on a une action transitive de $\mathrm{S}_n$ sur l'ensemble à 2 éléments $\{\pm 1\}$ donnée par $(\sigma, u) \mapsto \epsilon(\sigma)u$. (On peut bien sur transporter cette action en une action sur $\{1, 2\}$.) Ainsi, comme le souligne l'énoncé, on dispose d'une action transitive de $\mathrm{S}_3$ sur $1, 2, 3$ et 6 éléments. Pour voir que ce sont les seuls, il suffit de voir d'après le cours que tout sous-groupe de $\mathrm{S}_3$ est le stabilisateur d'un point dans une de ces 4 actions.

Soit donc $H$ un sous-groupe de $\mathrm{S}_3$. Si on a $H = \{1\}$, c'est le stabilisateur de n'importe quel point de l'action de Cayley (qui est libre). Si on a $H = \mathrm{S}_3$, c'est le stabilisateur de l'unique point de l'action triviale. Sinon, on a $|H| = 2$ ou $|H| = 3$ par Lagrange. Si on a $|H| = 3$, la seule possibilité est $H = \langle (1\,2\,3) \rangle = \mathrm{A}_3$ : c'est le stabilisateur d'un point quelconque dans l'action sur $\{\pm 1\}$. Enfin si on a $|H| = 2$, alors $H$ est engendré par une transposition $(i\,j)$, et si $k$ est tel que $\{1,2,3\} = \{i,j,k\}$, alors $H$ s'identifie au stabilisateur de $\{k\}$ dans l'action naturelle sur $\{1,2,3\}$.

**Exercice** 4.21. (i) L'action de Cayley étant libre et transitive, l'image de l'action de Cayley de $\mathrm{S}_3$ convient. On peut par exemple nommer respectivement $a, b, c, d, e, f$ les éléments 1, $(1\,2)$, $(2\,3)$, $(1\,3)$, $(1\,2\,3)$, $(1\,3\,2)$ de $\mathrm{S}_3$. Le morphisme de Cayley $\mathrm{S}_3 \to \mathrm{S}_X, g \mapsto \mathrm{L}_g$, avec $X = \mathrm{S}_3 = \{a,b,c,d,e,f\}$, vérifie alors

$$\mathrm{L}_1 = 1,\ \mathrm{L}_{(1\,2)} = (a\,b)(c\,e)(d\,f),\ \mathrm{L}_{(2\,3)} = (a\,c)(b\,f)(d\,e),\ \mathrm{L}_{(1\,3)} = (a\,d)(b\,e)(c\,f),$$

$$\mathrm{L}_{(1\,2\,3)} = (a\,e\,f)(b\,d\,c) \ \text{ et } \ \mathrm{L}_{(1\,3\,2)} = (a\,f\,e)(b\,c\,d).$$

(ii) On procède de même que ci-dessus pour $\mathrm{H}_8$. (iii) Supposons que $\mathrm{S}_n$ possède un sous-groupe isomorphe à $\mathrm{H}_8$, ou ce qui revient au même, que l'on dispose d'une action fidèle de $\mathrm{H}_8$ sur $X = \{1,\dots,n\}$. Soient $x \in X$ et $\mathrm{O}_x$ son orbite sous $\mathrm{H}_8$. Si le stabilisateur de $x$ est trivial, on a $|\mathrm{O}_x| = |\mathrm{H}_8| = 8$ par la formule orbite-stabilisateur, et donc $n = |X| \geqslant |\mathrm{O}_x| = 8$, ce qui conclut. On peut donc supposer que le stabilisateur de chaque $x \in X$ est non trivial dans $\mathrm{H}_8$. Mais on constate sur la description des sous-groupes de $\mathrm{H}_8$ que tout sous-groupe non trivial contient $-1$. On en déduit que $-1$ agit trivialement sur $X$, contredisant le caractère fidèle de l'action de $\mathrm{H}_8$ sur $X$.

**Exercice** 4.22. (i) En effet, $G_x$ stabilise l'ensemble $Y = X \smallsetminus \{x\}$ qui a $p-1$ éléments. Toute orbite $\mathrm{O}_y$ de $G_x$ dans $Y$ est de cardinal $1 \leqslant d \leqslant p-1$. On a $d \mid |G_x|$ par la formule orbite-stabilisateur, et donc $d \mid |G|$ (Lagrange). Cela montre $d = 1$ par hypothèse sur $p$, donc $\mathrm{O}_y = \{y\}$ : l'action est triviale.

(ii) Soit $H$ un sous-groupe d'indice $p$ dans $G$. On fait agir $G$ par translations sur $X = G/H$, qui a $p$ éléments. Le stabilisateur de $H$ est $H$ lui-même. Par le (i), il agit trivialement sur $G/H$ : on a donc $H \subset \mathrm{Stab}_G(gH) = gHg^{-1}$ pour tout $g \in G$, puis $H \lhd G$.

**Exercice** 4.23. (i) Posons $Y = X \smallsetminus \{x\}$. Alors $G_x$ agit naturellement sur $Y$. On a clairement $|X| \geqslant k+1 \iff |Y| \geqslant k$. Supposons que $G$ agit $k+1$-transitivement sur $X$. Alors $G$ agit transitivement sur $X$. Soient $(x_1,\dots,x_k)$ et $(y_1,\dots,y_k)$ deux $k$-uples d'éléments distincts de $Y$. Alors $(x,x_1,\dots,x_k)$ et $(x,y_1,\dots,y_k)$ sont des $k+1$-uples d'éléments distincts de $X$. Par $k+1$-transitivité de l'action de $G$, il existe $g \in G$ avec $g(x) = x$ et $g(x_i) = y_i$ pour $i = 1,\dots,k$. On a donc $g \in G_x$, et $G_x$ est bien $k$-transitif sur $Y$. Réciproquement supposons que $G$ agit transitivement sur $X$, et que $G_x$ agit $k$-transitivement sur $Y$. Soient $(x_1,\dots,x_{k+1})$ et $(y_1,\dots,y_{k+1})$ des $k+1$-uples d'éléments distincts dans $X$. Par transitivité de $G$ sur $X$, il existe $g,h \in G$ tels que $g(x_1) = x$ et $h(y_1) = x$. Les $k$-uples $(g(x_2),\dots,g(x_{k+1}))$ et $(h(y_2),\dots,h(x_{k+1}))$ sont bien constitués d'éléments distincts de $Y$. Par $k$-transitivité de $G_x$ sur $Y$, il existe $\sigma \in G_x$ vérifiant $\sigma(g(x_i)) = h(y_i)$ pour tout $2 \leqslant i \leqslant k+1$. Ainsi, l'élément $h^{-1}\sigma g$ envoie $x_i$ sur $y_i$ pour $2 \leqslant i \leqslant k+1$, et aussi pour $i = 1$.

(ii) On a $|G| = |X||G_x|$ car $G$ agit transitivement sur $X$, par la formule orbite stabilisateur. On raisonne par récurrence sur $k$. Le cas $k = 1$ est simplement la formule que l'on vient d'écrire. Pour $k > 1$ on sait que $G_x$ agit $k-1$ transitivement sur $Y = X \smallsetminus \{x\}$, et donc $|G_x|$ est multiple de $|Y|(|Y|-1)\cdots(|Y|-k+2)$. On conclut par $|G| = |X||G_x|$ et $|Y| = |X| - 1$.

(iii) Le fait que $\mathrm{S}_n$ et $\mathrm{A}_n$ agissent respectivement $n$-transitivement et $n-2$ transitivement sur $\{1,\dots,n\}$ est du cours. Réciproquement, si $G \subset \mathrm{S}_n$ agit $n-2$ transitivement

sur $\{1,\dots,n\}$ on a $\frac{n!}{2}$ divise $|G|$ par le (ii). On en déduit que $G$ est d'indice 1 ou 2. Mais on a vu à l'Exercice 4.2 que $\mathrm{A}_n$ est l'unique sous-groupe d'indice 2 de $\mathrm{S}_n$.

**Exercice** 4.24. (i) On pose $c = (1\,2\,3\,4\,5)$, $t = (1\,2)(3\,6)(5\,4)$. L'orbite de 6 sous l'action de $G$ contient $3 = t(6)$, puis $\{1,2,3,4,5\} = \{c^i(3) \mid i \in \mathbb{Z}\}$, ainsi bien sûr que 6 : l'action en question de $G$ est donc transitive. Pour montrer qu'elle est 2-transitive, on utilise le (i) de l'exercice précédent. Il suffit de voir que $G_6$ agit transitivement sur $\{1,2,3,4,5\}$, mais c'est clair car on a $c \in \mathrm{G}_6$. On constate enfin que l'on a

$$c\,t \;=\; (1\,2\,3\,4\,5)\,(1\,2)(3\,6)(5\,4) \;=\; (1\,3\,6\,4).$$

Mais toujours par le (i) de l'exercice précédent, l'action de $G$ est 3-transitive si, et seulement si, celle de $G_2 \cap G_5$ est transitive sur $\{1,3,4,6\}$. On conclut car on vient de voir $(1\,3\,6\,4) \in G_2 \cap G_5$.

(ii) On a donc $|G|$ divisible par $6 \cdot 5 \cdot 4 = 120$ par le (ii) de l'exercice précédent. Mais on a construit dans le cours un morphisme $f : \mathrm{S}_5 \to \mathrm{S}_X$ avec $X = \{a,b,c,d,e,f\}$ envoyant $(1\,2)$ sur $(a\,d)(b\,c)(e\,f)$ et $(1\,2\,3\,4\,5)$ sur $(b,c,d,e,f)$. Identifiant $X$ à $\{1,\dots,6\}$ en envoyant respectivement $a,b,c,d,e,f$ sur $6,1,2,3,4,5$, et donc $\mathrm{S}_X$ à $\mathrm{S}_6$, on a alors $t = f((1\,2))$ et $c = f((1\,2\,3\,4\,5))$. On a donc $G \subset f(\mathrm{S}_5)$. Mais on a à la fois $|f(\mathrm{S}_5)|\,|\ker f| = |\mathrm{S}_5| = 120$ et $|G| \geqslant 120$. Cela montre $\ker f = \{1\}$ et $G = f(\mathrm{S}_5) \simeq \mathrm{S}_5$.

**Exercice** 4.25. (i) Les égalités données se vérifie immédiatement en appliquant l'algorithme donnant la décomposition en cycle d'une permutation. Étant donné la notation pour les types discutée en cours, les éléments $a$, $b$, $b^2a$, $[a,b]$ et $aba$ sont respectivement de type 11, $1^3\,4^2$, $1^2\,3^3$, $1\,5^2$ et $1\,2\,8$.

(ii) Comme $G := \mathrm{M}_{11}$ possède un 11-cycle, il agit transitivement sur $E = \{1,2,\dots,11\}$. On va appliquer de nombreuses fois le critère de multiple transitivité de l'Exercice 4.23 (i). Observons que si $G$ possède un élément $g$ ayant un point fixe $x$ dans $E$, alors pour tout $y \in E$, il existe $h \in G$ de même type que $g$, et avec en outre $h(y) = y$. En effet, comme $G$ agit transitivement sur $E$, il existe $\sigma \in G$ avec $\sigma(x) = y$, et $h = \sigma g \sigma^{-1}$ convient. On déduit de cela que pour tout $x \in E$, le stabilisateur $G_x$ de $x$ dans $G$, qui agit naturellement sur $E' = E \smallsetminus \{x\}$, possède des éléments de type $1^2\,4^2$, $1\,3^3$, $5^2$ et $2\,8$ vus dans $\mathrm{S}_{E'}$. La présence de $2\,8$ et $5^2$ par exemple montre que $G_x$ agit transitivement sur $E'$. Rappliquant l'observation ci-dessus à $G_x$ agissant sur $E'$, on en déduit que pour tout $y \in E'$, $(G_x)_y = G_x \cap G_y$ possède des éléments de types $1\,4^2$ et $3^3$ vus comme éléments de $\mathrm{S}_{E''}$ avec $E'' = E \smallsetminus \{x,y\}$. Cela force la transitivité de $(G_x)_y$ sur $E''$. C'est assez clair ! On peut dire qu'une orbite de ce dernier doit être de cardinal à la fois multiple de 3, et égal à 1, 4, $1+4$, $4+4$ ou $1+4+4$. La seule possibilité est le cardinal 9.

(iii) On a vu que $G$ agit 3-transitivement sur $E$. En particulier, il permute transitivement les parties à 3 éléments de $E$. Soit $F$ une telle partie. Noter que $G_F$ préserve $F$ et son complémentaire $E \smallsetminus F$, mais que $G_F$ n'agit pas nécessairement trivialement sur $F$. D'après le (i), observons que $G_F$ contient des éléments de type $4^2$, $1^2\,3^2$ et 8 vus comme éléments de $\mathrm{S}_{E \smallsetminus F}$ (c'est une variante de l'observation du (ii)). Il suffit de voir que si $G$ possède un élément $g$ ayant une partie stable $S \subset E$ à 3 él'ements, alors il existe $h \in G_F$ tel que $h_{|F}$ a même type que $g_{|S}$ et $h_{|E \smallsetminus F}$ a même type que $g_{|E \smallsetminus S}$. Mais comme $G$ agit permute transitivement les parties à 3 éléments de $E$, il existe $\sigma \in G$ avec $\sigma(S) = F$, et $h = \sigma g \sigma^{-1}$ convient. Cela conclut l'observation. Comme $G_F$ possède un élément qui agit comme un 8-cycle sur $E \smallsetminus F$, il agit bien transitivement sur $E \smallsetminus F$, puis transitivement sur les parties à 4 éléments de $E$.

(iv) et (v) Comme $G$ agit transitivement sur les parties à 4 éléments de $E$, l'argument ci-dessus et le (i) montrent que $G_F$ contient des éléments de type $1\,3$ et 4 vus comme permutations de $F$. Il reste à voir qu'un sous-groupe $H$ de $\mathrm{S}_4$ engendré par un 4-cycle

et un 3 cycle est $\mathrm{S}_4$. On peut le faire à la main, ou observer que le cardinal de $H$ serait multiple de $3 \cdot 4 = 12$ par Lagrange, donc $H$ serait d'indice 1 ou 2. Mais $\mathrm{A}_4$ est l'unique sous-groupe d'ordre 12 de $\mathrm{S}_4$ (Exercice 4.2), et $H$ contient un 4-cycle, non dans $\mathrm{A}_4$, on a donc bien $H = \mathrm{S}_4$.

(vi) La seconde assertion découle de la première et du (ii) de l'Exercice 4.23. Pour la première, soient $(x_1, x_2, x_3, x_4)$ et $(y_1, y_2, y_3, y_4)$ des 4-uples d'éléments distincts de $E$. On pose $X = \{x_1, x_2, x_3, x_4\}$ et $Y = \{y_1, y_2, y_3, y_4\}$. Par le (iii), il existe $g \in \mathrm{M}_{11}$ avec $g(X) = Y$. Posons $x'_i = g(x_i)$ pour tout $1 \leqslant i \leqslant 4$. Par le (iv), il existe $h \in \mathrm{G}_Y$ avec $h(x'_i) = y_i$ pour tout $1 \leqslant i \leqslant 4$. L'élément $gh \in G$ envoie bien $x_i$ sur $y_i$ pour tout $1 \leqslant i \leqslant 4$.

**Exercice** 4.26. (i) On a $Hn = nn^{-1}Hn = nH$ pour tour $n \in N$, puis $gHn = gnH$ pour tout $g \in G$ et $n \in N$. La multiplication à droite par $n \in N$ dans $\mathrm{P}(G)$ préserve donc $G/H$. Elle est bijective d'inverse la multiplication à droite par $n^{-1}$. C'est trivialement un isomorphisme de $(G/H, \bullet)$ : on a $g' \bullet (gHn) = (g' \bullet gH)n = g'gHn$ pour tout $g, g' \in G$ (les multiplications à droite et à gauche commutent...).

(ii) L'application $N \times G/H \to G/H, (n, gH) \mapsto gHn^{-1}$, définit manifestement une action de $N$ sur $G/H$, et donc un morphisme associé $f : N \to \mathrm{S}_{G/H}$. Notons $A \subset \mathrm{S}_{G/H}$ le sous-groupe des automorphismes de $(G/H, \bullet)$. On a vérifié au (i) que l'on a $f(N) \subset A$. Remarquons que $\ker f$ est le sous-groupe des $n \in N$ vérifiant $gHn = gH$ pour tout $g \in G$, ce qui équivaut à $n \in H$, on a donc $\ker f = H$. Choisissons enfin $\varphi \in A$. On a $\varphi(gH) = g\varphi(H)$ pour tout $g \in G$. Soit $n \in G$ tel que $\varphi(H) = nH$. On a donc $nH = \varphi(H) = \varphi(hH) = h\varphi(H) = hnH$ pour tout $h \in H$. Cela implique $n^{-1}Hn \subset H$. En considérant de même $\varphi^{-1} \in A$, qui envoie $nH$ sur $H$ et donc $H$ sur $n^{-1}H$, on a l'inclusion dans l'autre sens $nHn^{-1} \subset H$, puis $nHn^{-1} = H$. On a montré $n \in N$, puis $\varphi(H) = Hn$, $\varphi(gH) = gHn$, et donc $\varphi = f(n)$. Ainsi, $f$ induit un isomorphisme $N/H \xrightarrow{\sim} A$.

**Exercice** 4.27. (i) Soit $x \in X$. On a $\mathrm{O}_x = \{g \bullet x \mid g \in G\}$. Comme on a $f(g \bullet x) = g \star f(x)$ pour $g \in G$, on a donc $f(\mathrm{O}_x) = \{g \star f(x) \mid g \in G\} = \mathrm{O}_{f(x)}$. Ainsi, $f(X_i)$ est une $G$-orbite dans $Y$ : c'est $Y_j$ pour un unique $j \in J$.

(ii) La restriction $f_i$ de $f$ à $X_i$ définit donc une bijection $X_i \to Y_j$ où $j = \varphi(i)$. On a $f_i(g \bullet x) = f(g \bullet x) = g \star f(x) = g \star f_i(x)$ pour $x \in X_i$, donc $f_i$ est un isomorphisme entre $(X_i, \bullet)$ et $(Y_j, \star)$. L'action de $G$ sur $X_i$ (resp. $Y_j$) est transitive car $X_i$ (resp. $Y_j$) est une $G$-orbite. Comme $f$ est surjective la fonction $\varphi : I \to J$ l'est aussi. Vérifions qu'elle est injective. Supposons $i, i' \in I$ distincts. On a $X_i \cap X_{i'} = \varnothing$ et donc on a $f(X_i) \cap f(X_{i'}) = \varnothing$ car $f$ est injective, cela conclut.

(iii) Réciproquement, supposons donnés une bijection $\varphi : I \to J$, et pour tout $i \in I$ un isomorphisme d'actions $f_i : X_i \xrightarrow{\sim} Y_{\varphi(i)}$. On définit $f : X \to Y$ par $f(x) = f_i(x)$ où $i$ est l'unique élément de $I$ tel que $x$ est dans $X_i$. C'est clairement un isomorphisme d'actions car les $f_i$ en sont.

**Exercice** 4.28. (i) Quitte à échanger $i$ et $j$ on peut supposer que l'on a $g^{i+1} = hg^ih^{-1}$ avec $h \in G$. On en déduit $g = g^{-i}\, h\, g^i\, h^{-1} = [g^{-j}, h]$.

(ii) Écrivons $g^i = h\, g^j\, h^{-1}$ avec $h \in G$. On a $g^{i-j} = [g^{-j}, h] \in \mathrm{D}(G)$. Soit $k \in \mathbb{Z}$ tel que $k(i-j) \equiv 1 \bmod n$. On a donc $g = (g^{i-j})^k \in \mathrm{D}(G)$.

**Exercice** 4.29. Soit $\pi : G \to G/\mathrm{D}(G)$ le morphisme canonique. Le groupe $G/\mathrm{D}(G)$ étant commutatif, tous ses sous-groupes sont distingués. Mais tout sous-groupe de $G$ contenant $\mathrm{D}(G)$ est de la forme $\pi^{-1}(H)$ avec $H$ sous-groupe de $G/\mathrm{D}(G)$, d'après le cours. On conclut car l'image inverse d'un sous-groupe distingué par un morphisme de groupes est encore distingué.

**Exercice** 4.30. Pour le (i), ce sont des vérifications triviales. Par exemple, on a $[x,yz] = xyzx^{-1}(yz)^{-1} = (xyx^{-1}y^{-1})y(xzx^{-1}z^{-1})y^{-1} = [x,y]\ {}^y[x,z]$. Pour le (ii), on a $[x,y^{n+1}] = [x,y^n y] = [x,y^n]\ {}^{y^n}[x,y]$ par le (i), et on conclut par récurrence sur $n$.

**Exercice** 4.31. (i) Le groupe $Z = \{\pm 1\}$ est central donc distingué dans $\mathrm{H}_8$. La relation $[I,J] = IJI^{-1}J^{-1} = -1$ montre $-1 \in \mathrm{D}(H_8)$, donc $Z \subset \mathrm{D}(\mathrm{H}_8)$, et aussi que $\mathrm{H}_8/Z$ est commutatif, car il est engendré par les classe de $I$ et $J$ qui commutent modulo $Z$. On a donc $\mathrm{D}(\mathrm{H}_8) \subset Z$ puis $\mathrm{D}(\mathrm{H}_8) = Z$. On en déduit $\mathrm{H}_8/\mathrm{D}(\mathrm{H}_8) = \mathrm{H}_8/\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(ii) Posons $G = \mathrm{D}_{2n}$. On a $G = \langle c,\tau\rangle$ comme dans le cours, avec $\tau c = c^{-1}\tau$. Le sous-groupe $C := \langle c\rangle$ est distingué et d'indice 2 dans $G$. On a donc $G/C \simeq \mathbb{Z}/2\mathbb{Z}$ (abélien) et donc $\mathrm{D}(G) \subset C$. D'autre part, on a aussi $\tau c\tau^{-1}c^{-1} = c^{-2} \in \mathrm{D}(G)$. Notons $C'$ le sous-groupe de $C$ engendré par $c^2$. On a montré $C' \subset \mathrm{D}(G)$. Si $n$ est impair, on a $C' = C$ et donc $C = \mathrm{D}(G)$ et $G/\mathrm{D}(G) \simeq \mathbb{Z}/2\mathbb{Z}$. Si $n$ est pair, alors $C'$ est d'ordre $n/2$ et distingué dans $G$, car $c^2$ commute avec $c$ et vérifie $\tau c^2\tau^{-1} = c^{-2} \in C'$. Ainsi, $G/C'$ est d'ordre 4, engendré par les images de $c$ et $\tau$. Mais on a $c^2 \in C'$, $\tau^2 \in C'$ et $[\tau,c] = c^{-2} \in C'$, on a donc $G/C' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Comme $G/C'$ est abélien on a $\mathrm{D}(G) \subset C'$, puis $\mathrm{D}(G) = C'$ et $G/\mathrm{D}(G) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Exercice** 4.33. C'est un fait général que pour $\dim V \geqslant 2$, le groupe $\mathrm{GL}(V)$ agit 2-transitivement sur $\mathbb{P}(V)$. En effet, on a d'abord clairement $|\mathrm{P}(V)| > 2$. De plus, soient $(D_1,D_2)$ et $(D_1',D_2')$ deux couples de droites distinctes de $V$. Fixons $e_i \in D_i$ et $f_i \in D_i'$ des vecteurs non nuls. Alors $e_1,e_2$ est libre, ainsi que $f_1',f_2'$. On peut donc les compléter en des bases respectives $\{e_i\}_{1\leqslant i\leqslant n}$ et $\{f_i\}_{1\leqslant i\leqslant n}$ de $V$, avec $n = \dim V$. Il existe un unique $g \in \mathrm{GL}(V)$ avec $g(e_i) = f_i$ pour tout $i$. Il vérifie $g(D_1) = D_1'$ et $g(D_2) = D_2'$.

Supposons maintenant $V$ de dimension 2. Fixons $\{e_1,e_2\}$ une base de $V$ et posons $L_1 = ke_1$, $L_2 = ke_2$ et $L_3 = k(e_1+e_2)$. Soit $G \subset \mathrm{GL}(V)$ le sous-groupe des éléments $g$ tels que $g(L_1) = L_1$ et $g(L_2) = L_2$. Par l'Exercice 4.23 (i), il suffit de montrer que l'action naturelle de $G$ sur $X = \mathbb{P}(V) \smallsetminus \{L_1,L_2\}$ est transitive. Mais toute droite $D$ de $V$ distincte de $L_1$ et $L_2$ est engendrée par un (unique) vecteur de la forme $e_1 + \lambda e_2$ avec $\lambda \neq 0$. Soit $g \in \mathrm{GL}(V)$ l'unique élément avec $g(e_1) = e_1$ et $g(e_2) = \lambda e_2$. On a $g \in G$ et $g(L_3) = D$. Ainsi, $X$ est l'orbite de $L_3$ sous $G$.

**Exercice** 4.34. (i) Ce sont des opérations élémentaires sur les lignes et les colonnes. Pour $i,j$ notons $\mathrm{E}_{i,j} \in \mathrm{M}_n(k)$ la matrice élémentaire d'indice $(i,j)$ égal à 1 et d'indice $(p,q)$ nul pour $(p,q) \neq (i,j)$. Pour $i < j$, on a $\mathrm{e}_{i,j}(x) = 1_n + x\mathrm{E}_{i,j}$ dans $\mathrm{M}_n(k)$. Notons que pour $i$ fixé, les $\mathrm{e}_{i,j}(x)$ avec $j > 1$ et $x \in k$ commutent deux à deux. Si $m = (m_{i,j}) \in \mathrm{U}_n(k)$, on constate que la matrice $m\prod_{j=2}^n \mathrm{e}_{1,j}(-m_{1,j})$ a sa première ligne nulle hors du coefficient diagonal (et même tous ses autres coefficients identiques à ceux de $m$). On conclut en raisonnant par récurrence dans le bloc $(n-1)\times(n-1)$.

(ii) Pour $i < j$ on a $\mathrm{e}_{i,j}(0) = 1$ et $\mathrm{e}_{i,j}(x)\mathrm{e}_{i,j}(y) = \mathrm{e}_{i,j}(x+y)$. En particulier, l'ensemble $Z \subset \mathrm{U}_n(k)$ des $\mathrm{e}_{1,n}(x)$, $x \in k$, est un sous-groupe de $\mathrm{U}_n(k)$ (isomorphe à $(k,+)$). Pour tout $t \in \mathrm{T}_n(k)$ on constate dans $\mathrm{M}_n(k)$ les égalités

$$t\,\mathrm{e}_{1,n}(x) \;=\; t \;+\; t_{1,1}x\,\mathrm{E}_{1,n} \;\text{ et }\; \mathrm{e}_{1,n}(x)\,t \;=\; t \;+\; t_{n,n}x\,\mathrm{E}_{1,n}. \tag{80}$$

En particulier, $Z$ est dans le centre de $\mathrm{U}_n(k)$. Montrons que le sous-groupe $C$ des éléments de $\mathrm{T}_n(k)$ qui commute à tous les éléments de $\mathrm{U}_n(k)$ est $k^\times Z$. On a déjà vu $C \supset k^\times Z$. Réciproquement fixons $g \in C$. Écrivons matriciellement $g\,\mathrm{e}_{i,j} = \mathrm{e}_{j,i}\,g$ pour $i < j$. On en déduit $g_{i,i} = g_{j,j}$ et $g_{k,i} = 0$ pour $1 \leqslant k < i$ et $g_{j,k} = 0$ pour $j < k \leqslant n$. Cela conclut. De $C = k^\times Z$ on déduit $\mathrm{Z}(\mathrm{U}(k)) = Z$ et par la formule (80), $\mathrm{Z}(\mathrm{T}_n(k)) = k^\times$.

**Exercice** 4.35. (i) On a $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ et donc $\mathrm{T}_n(\mathbb{Z}/2\mathbb{Z}) = \mathrm{U}_n(\mathbb{Z}/2\mathbb{Z})$. Pour $n \geqslant 1$, on a toujours un morphisme surjectif $\mathrm{U}_n(k) \to k^{n-1}$ donné par la surdiagonale, et donc $\mathrm{D}(\mathrm{U}_n(k) \subsetneq \mathrm{U}_n(k)$ pour $n > 1$. On en déduit $\mathrm{D}(\mathrm{T}_n(\mathbb{Z}/2)) \subsetneq \mathrm{U}_n(\mathbb{Z}/2\mathbb{Z})$. Supposons

maintenant $k \neq \mathbb{Z}/2\mathbb{Z}$. Soient $1 \leqslant i < j \leqslant n$ et $x \in k$. Par le (i) de l'exercice précédent, il suffit de montrer $\mathrm{e}_{i,j}(x) \in \mathrm{D}(\mathrm{T}_n(k))$. Soit $t = \mathrm{diag}(t_1, \ldots, t_n)$ une matrice diagonale. Mais on constate

$$[t, \mathrm{e}_{i,j}(x) = t\mathrm{e}_{i,j}(x)t^{-1}\mathrm{e}_{i,j}(-x) = \mathrm{e}_{i,j}(t_i t_j^{-1}x)\mathrm{e}_{i,j}(-x) = \mathrm{e}_{i,j}((t_i t_j^{-1} - 1)x) \in \mathrm{D}(\mathrm{T}_n(k))$$

Comme $k \neq \mathbb{Z}/2\mathbb{Z}$, il existe $u \in k \smallsetminus \{0, 1\}$ et donc on peut choisir $t$ avec $t_j = 1$ et $t_i = u$. On conclut car l'application $k \mapsto k, x \mapsto (u-1)x$ est bijective.

(ii) C'est un simple calcul à partir de $\mathrm{E}_{i,j}\mathrm{E}_{k,l} = \delta_{j,k}\mathrm{E}_{i,l}$ et de

$$[\mathrm{e}_{i,i+2^m}, \mathrm{e}_{i+2^m,i+2^{m+1}}] = (1 + \mathrm{E}_{i,i+2^m})(1 + \mathrm{E}_{i+2^m,i+2^{m+1}})(1 - \mathrm{E}_{i,i+2^m})(1 - \mathrm{E}_{i+2^m,i+2^{m+1}}).$$

(iii) On raisonne par récurrence sur $m \geqslant 0$ (le cas $m = 0$ est évident). On peut supposer $j = i + 2^{m+1} \leqslant n$. On a $\mathrm{e}_{i,i+2^m}$ et $\mathrm{e}_{i+2^m,i+2^{m+1}} \in \mathrm{D}^m(\mathrm{U}_n(k))$ par hypothèse de récurrence, puis $\mathrm{e}_{i,j} \in \mathrm{D}^{m+1}(\mathrm{U}_n(k))$ par le (ii).

(iv) On suppose $n \geqslant 2$. Soit $m$ le plus grand entier tel que $1 + 2^m \leqslant n$. On a $\mathrm{e}_{1,1+2^m} \in \mathrm{D}^m(\mathrm{U}_n(k))$ par le (iii), et donc $\mathrm{D}^m(\mathrm{U}_n(k)) \neq \{1\}$. On en déduit que la classe $c$ de résolubilité de $\mathrm{U}_n(k)$ est $\geqslant 1 + m$. Par définition, on a $m = \lfloor \log_2(n-1) \rfloor$. Par le cours (démonstration de la Proposition 6.13), on a aussi $c \leqslant \lceil \log_2(n) \rceil$. Pour conclure il suffit d'observer l'égalité $1 + \lfloor \log_2(n-1) \rfloor = \lceil \log_2(n) \rceil$. En effet, si on a $n = 2^k$ avec $k \geqslant 1$, alors on a $2^{k-1} < n - 1 < 2^k$ et donc l'égalité s'écrit $1 + k - 1 = k$. L'autre situation est $2^{k-1} < n < 2^k$, et donc $2^{k-1} \leqslant n - 1 < 2^k$, et l'égalité s'écrit encore $1 + k - 1 = k$.

**Exercice** 4.36. (i) L'action naturelle de $\mathrm{GL}(V)$ sur $\mathscr{F}$ sous-entendue dans l'énoncé est bien sûr $(g, (V_i)) \mapsto (g(V_i))$. Elle est bien définie car on a $\dim g(V_i) = \dim V_i$ et $V_i \subset V_j \implies g(V_i) \subset g(V_j)$. C'est manifestement une action. Montrons qu'elle est transitive. Soient $V_0 \subset V_1 \subset \cdots \subset V_n = V$ et $W_0 \subset W_1 \subset \cdots \subset W_n = V$ deux drapeaux de $V$. Par récurrence sur $i$, et par le théorème de la base incomplète, on peut trouver une base $e_1, \ldots, e_n$ de $V$ telle que $V_i = \sum_{j=1}^{i} k\, e_j$ pour tout $i = 1, \ldots, n$. De même, on peut trouver une base $f_1, \ldots, f_n$ de $V$ telle que $W_i = \sum_{j=1}^{i} k\, f_j$ pour tout $i = 1, \ldots, n$. Soit $g \in \mathrm{GL}(V)$ l'unique élément vérifiant $g(e_i) = f_i$ pour $i = 1, \ldots, n$. On a $g(V_i) = W_i$ pour tout $i$ : l'action de l'énoncé est transitive.

(ii) Le stabilisateur du drapeau standard est par définition $\mathrm{T}_n(k)$. Montrons (iii). Un sous-groupe $G \subset \mathrm{GL}(V)$ préserve un drapeau $d = (V_i)$ si, et seulement si, il est inclus dans le stabilisateur $\mathrm{Stab}_{\mathrm{GL}(V)}(d)$ de ce drapeau. Mais par le (i) tout drapeau $d$ s'écrit $d = p(s)$ où $s \in \mathscr{F}$ est le drapeau standard, et $p$ est un certain élément de $\mathrm{GL}(V)$. Mais on a $\mathrm{Stab}_{\mathrm{GL}(V)}(d) = p\,\mathrm{Stab}_{\mathrm{GL}(V)}(s)\,p^{-1} = p\,\mathrm{T}_n(k)\,p^{-1}$ par le principe de conjugaison et le (ii). Cela conclut le (iii).

**Exercice** 4.37. (i) On pose $H = \mathrm{GL}_n(\mathbb{C})$. C'est à la fois un groupe et un ouvert du $\mathbb{C}$-espace vectoriel de dimension finie $\mathrm{M}_n(\mathbb{C})$, ce qui lui confère une structure d'espace topologique. Observons que la multiplication $H \times H \to H, (x, y) \mapsto xy$, et l'inversion $H \to H, x \mapsto x^{-1}$, sont toutes les deux continues : la première est polynomiale, et pour la seconde utiliser $x^{-1} = {}^{\mathrm{t}}\mathrm{Co}(x)(\det x)^{-1}$ et la continuité et non annulation du déterminant. (On dit que $H$ est un *groupe topologique*). Il découle de ces observations que si $X$ et $Y$ sont des parties connexes de $H$, il en va de même de $X^{-1}$ (image de $X$ par l'inversion) et de $XY$ (image du connexe $X \times Y$ par la multiplication). Si en outre $X$ contient 1, alors on a $1 \in X^n$ pour tout $n \in \mathbb{Z}$ puis $X^n \cap X^m \neq \varnothing$, et donc $\langle X \rangle = \cup_{n \in \mathbb{Z}} X^n$ est connexe. On a montré que *le sous-groupe engendré par une partie connexe contenant* 1 *de* $\mathrm{GL}_n(\mathbb{C})$ est connexe. Considérons enfin $G$ comme dans l'énoncé. L'ensemble des commutateurs $C = \{[x, y] \,|\, (x, y) \in G \times G\}$ est une partie connexe de $G$, comme image du connexe $G \times G$ par l'application continue $H \times H \to H, (x, y) \mapsto xyx^{-1}y^{-1}$. Ainsi, $C$ est un connexe contenant 1, et donc $\mathrm{D}(G) = \langle C \rangle$ est connexe.

(ii) Pour $g, h \in \mathrm{GL}_n(\mathbb{C})$ on a $\det([g,h]) = [\det(g), \det(h)] = 1$ car $\mathbb{C}^\times$ est commutatif. Montrons le (iii). Si $\mathrm{D}(G)$ est constitué d'homothéties, alors ces homothéties sont de rapport $\lambda \in \mathbb{C}^\times$ avec $\lambda^n = 1$ par le (ii). Mais par le (i) $\mathrm{D}(G)$ est connexe. Le seul sous-groupe connexe de $\mathbb{C}^\times$ inclus dans $\mu_n$ est $\{1\}$. On a donc $\mathrm{D}(G) = 1$, c'est-à-dire $G$ abélien. Les éléments de $G$ sont trigonalisables et commutent : ils sont donc co-trigonalisables par un exercice classique.

(iv) Choisissons une base $e = (e_1, \dots, e_n)$ de $\mathbb{C}^n$ telle que $e_1, \dots, e_m$ est une base de $W$. Par hypothèse on a $1 \leqslant m = \dim W < n$. De plus, pour tout $g \in G$ on a

$$\mathrm{Mat}_e g = \begin{bmatrix} A(g) & B(g) \\ 0 & C(g) \end{bmatrix} \text{ avec } A(g) \in \mathrm{GL}_m(\mathbb{C}) \text{ et } B(g) \in \mathrm{GL}_{n-m}(\mathbb{C}).$$

Les applications $A : G \to \mathrm{GL}_r(\mathbb{C}), g \mapsto A(g)$, et $B : G \to \mathrm{GL}_{n-m}(\mathbb{C}), g \mapsto B(g)$, sont des morphismes de groupes, et sont manifestement continues. Ainsi, les groupes images $A(G)$ et $B(G)$ sont connexes (images continues d'un connexe) et quotients de $G$, donc résolubles et de classe respective $a, b \leqslant r$. On a $m + a < n + r$ et $m - n + b < n + r$. Par récurrence, $A(G)$ et $B(G)$ sont donc co-trigonalisables. Quitte à changer de base $e$, cela montre que l'on peut supposer que $A(G)$ et $B(G)$ sont triangulaires supérieurs dans la base $e$, ainsi donc que $G$.

(v) La classe de résolubilité de $\mathrm{D}(G)$ est $r - 1$, et $\mathrm{D}(G)$ est connexe par le (i). Par hypothèse de récurrence, $\mathrm{D}(G)$ est co-trigonalisable. En particulier, il existe une droite $D \subset V$ stable par tout élément de $\mathrm{D}(G)$. Soit $e$ une base de $D$, *i.e.* $D = \mathbb{C}e$. Pour tout $g \in \mathrm{D}(G)$, il existe un unique $\lambda_g \in \mathbb{C}^\times$ tel que $g(e) = \lambda_g e$. On a donc $\lambda_{gh} e = gh(e) = g(h(e)) = \lambda_h g(e) = \lambda_g \lambda_h e$, puis $\chi(g) := \lambda_g$ définit un caractère de $\mathrm{D}(G)$. On a $e \in V_\chi$, et donc $\chi \in S$.

(vi) Soit $X \subset S$ de cardinal non nul et minimal tel qu'il existe une relation $0 = \sum_{\chi \in X} v_\chi$ avec $v_\chi$ non nul et dans $V_\chi$ pour tout $\chi \in X$. Soient $\alpha \in X$ et $g \in G$. Appliquant $\alpha(g)\mathrm{id} - g$ à cette relation on trouve $0 = \sum_{\chi \in X} (\alpha(g) - \chi(g)) v_\chi$. Le coefficient $\alpha(g) - \chi(g)$ est nul pour $\alpha = \chi$, et donc on a $\alpha(g) = \chi(g)$ pour tout $\chi \in X$ et tout $g \in G$ par minimalité de la relation. Cela montre $X = \{\alpha\}$, puis $0 = v_\alpha$, une contradiction.

(vii) La somme des $V_\chi$ étant directe par le (vi) on a $n \geqslant \dim V = \sum_{\chi \in S} \dim V_\chi$. Mais on a $\dim V_\chi \geqslant 1$ pour $\chi \in S$ par définition de $S$. On a donc $|S| \leqslant n$.

(viii) On sait que $\mathrm{D}(G)$ est distingué dans $G$, donc pour $g \in G$ la restriction de $\mathrm{int}_g$ à $\mathrm{D}(G)$ est un automorphisme de $\mathrm{D}(G)$. Pour $\chi \in \mathscr{C}$ on constate que l'on a ${}^g\chi = \chi \circ \mathrm{int}_{g^{-1}}$ : c'est donc bien un élément de $\mathscr{C}$. De plus, on a $\chi^1 = \chi$ et ${}^g({}^h\chi)(x) = {}^h\chi(g^{-1}xg) = \chi(h^{-1}g^{-1}xgh) = \chi((gh)^{-1}x(gh)) = {}^{gh}\chi(x)$ pour $g, h \in G$ et $x \in \mathrm{D}(G)$. Ainsi, $G \times \mathscr{C} \to \mathscr{C}, (g, \chi) \mapsto {}^g\chi$, est une action de $G$ sur $\mathscr{C}$.

Si on a $v \in V_\chi$ et $g \in G$, on a $g(v) \in V_{{}^g\chi}$. En effet, pour $h \in \mathrm{D}(G)$ et $g \in G$ on a $g^{-1}hg \in \mathrm{D}(G)$ et donc $hgv = g(g^{-1}hg)v = g\chi(g^{-1}hg)v = {}^g\chi(h)gv$. On a donc montré $g(V_\chi) \subset V_{{}^g\chi}$ pour tout $g \in G$ et tout $\chi \in \mathscr{C}$. Appliquant ceci à $g^{-1}$ et ${}^g\chi$, on a l'égalité de l'énoncé.

(ix) Fixons $\chi \in S$. La dernière assertion du (viii) montre que pour $g \in G$ on a ${}^g\chi \in S$. Comme $S$ est fini, l'ensemble des ${}^g\chi$ est donc fini. En particulier, pour $h \in \mathrm{D}(G)$ donné et $v \in V_\chi$, l'application $G \to \mathbb{C}^\times, g \mapsto \chi(ghg^{-1})$, est d'image finie. Admettons temporairement que l'application $\chi : \mathrm{D}(G) \to \mathbb{C}^\times, x \mapsto \chi(x)$, est continue. Comme $G$ est connexe, l'application ci-dessus est alors constante. On en déduit ${}^g\chi = \chi$, ce qui était demandé. Vérifions enfin la continuité de $\chi$. Pour tout $v \in \mathbb{C}^n$, l'application $G \to \mathbb{C}^n$, $g \mapsto g(v)$, est continue, et si on choisit $v \in V_\chi$ non nul, elle coïncide avec $g \mapsto \chi(g)v$ sur $\mathrm{D}(G)$.

(x) Par le (v) on a $S \neq \varnothing$. Fixons donc $\chi \in S$. Soit $g \in G$. Par le (ix), on a ${}^g\chi = \chi$, et donc $g(V_\chi) = V_\chi$ par le (ii). On en déduit que $G$ stabilise $V_\chi$. Par le (iv), on conclut si $\dim V_\chi < n$. Mais si $V_\chi = V$, alors $\mathrm{D}(G)$ agit par homothéties sur $V$, et on conclut encore par le (iii).

(xi) Le sous-groupe $\mathrm{H}_8 \subset \mathrm{GL}_2(\mathbb{C})$ est résoluble mais pas co-trigonalisable. En effet, les seules droites stables de $I = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$ sont $\mathbb{C}\epsilon_1$ et $\mathbb{C}\epsilon_2$, mais aucune des deux n'est stable par $J$.

**Exercice** 4.38. Pour $m, m' \in \mathbb{Z}/n\mathbb{Z}$ et $k, k' \in \mathbb{Z}/2\mathbb{Z}$ on a dans le groupe $G_s$ la relation $(m', k')(m, k) = (m' + s^{k'}m, k' + k)$. Ainsi, $(m, k)$ est dans le centre de $G_s$ si, et seulement si, on a $sm = m$. Soit $H_s$ le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ défini par $H = \{m \in \mathbb{Z}/n\mathbb{Z} \mid sm = m\}$. On a montré $\mathrm{Z}(G_s) \simeq H_s \times \mathbb{Z}/2\mathbb{Z}$ (groupe produit).

Notons $s_p$ et $s_q \in \{\pm 1\}$ les signes tels que $s \equiv s_p \bmod p$ et $s \equiv s_q \bmod q$. L'isomorphisme chinois identifie $H_s$ au sous-groupe des $(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ vérifiant $s_p x = x$ et $s_q y = y$. Pour $l$ impair et $x \in \mathbb{Z}/l\mathbb{Z}$, on a $-x = x \iff x = 0$. On en déduit

$$H_{-1} = 0, \;\; H_1 \simeq \mathbb{Z}/pq\mathbb{Z}, \;\; H_a \simeq \mathbb{Z}/p\mathbb{Z} \;\text{ et }\; H_b \simeq \mathbb{Z}/q\mathbb{Z}.$$

Ainsi, pour $s = -1, 1, a$ et $b$ respectivement, le centre de $G_s$ est cyclique d'ordre $2, 2pq, 2p$ et $2q$ respectivement.

**Exercice** 4.39. Soit $a \in \mathrm{Aut}(G)$. Considérons le morphisme de groupes $\alpha : \mathbb{Z} \to \mathrm{Aut}(G), n \mapsto a^n$. On pose $G' = G \rtimes_\alpha \mathbb{Z}$. On a un morphisme injectif $f : G \to G', g \mapsto (g, 0)$. Soit $x = (0, 1) \in G'$. On conclut car pour $g \in G$ on a

$$xf(g)x^{-1} = (0,1) \star_\alpha (g,0) \star_\alpha (0,-1) = (a(g),1) \star_\alpha (0,-1) = (a(g),0) = f(a(g)).$$

**Exercice** 4.40. (i) Par Cauchy, $G$ possède un élément $x$ d'ordre $p$, et un élément $y$ d'ordre $q$. On pose $P = \langle x \rangle$ et $Q = \langle y \rangle$. Comme $Q$ est d'indice $p$, le plus petit facteur premier de $|G|$, alors il est distingué par le Lemme de Ore (Exercice 4.22).

(ii) Le sous-groupe $P \cap Q$ est un sous-groupe de $P$ et de $Q$, d'ordres premiers entre eux, et donc $P \cap Q = \{1\}$ par Lagrange. On a aussi $|G| = pq = |P||Q|$. On sait donc que $Q$ et $P$ sont complémentaire. Comme $Q$ est distingué, on a donc $G = Q \rtimes P$ (produit semi-direct interne) et un morphisme $\alpha : P \to \mathrm{Aut}(Q), p \mapsto \mathrm{int}_{p|Q}$. Comme $Q$ est cyclique d'ordre $q$, on sait que l'on a $\mathrm{Aut}(Q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, puis $|\mathrm{Aut}(Q)| = q - 1$ car $q$ est premier. Tout morphisme $f : G \to G'$ avec $G$ et $G'$ finis de cardinaux premiers entre eux étant trivial, on a donc $\alpha = 1$ si $p$ ne divise pas $q - 1$. Dans ce cas, on a donc $xy = yx$, et donc $xy$ est d'ordre $pq$ car $p$ et $q$ sont premiers entre eux, puis $G = \langle xy \rangle$ est cyclique d'ordre $pq$.

(iii) On suppose désormais $p \,|\, |\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q - 1$. Dans ce cas $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ possède un élément $c$ d'ordre $p$. Concrètement, il existe un élément $u \in (\mathbb{Z}/q\mathbb{Z})^\times$ d'ordre $p$ et on a $c(m) = um$ pour $m \in \mathbb{Z}/q\mathbb{Z}$. Il existe donc un morphisme injectif $\beta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ avec $\beta_{\overline{1}} = c$, i.e. $\beta_{\overline{1}}(m) = um$. Le groupe $\Gamma_{p,q} = \mathbb{Z}/q\mathbb{Z} \rtimes_\beta \mathbb{Z}/p\mathbb{Z}$ convient. En effet, il n'est pas commutatif car $c$ n'est pas l'identité : on a $(0,1) \star_\beta (m,0) \star_\beta (0,1)^{-1} = (c(m),0)$ pour tout $x \in \mathbb{Z}/q\mathbb{Z}$.

(iv) On raffine l'analyse du (ii). On a $G = Q \rtimes P$ et $\alpha : P \to \mathrm{Aut}(Q), p \mapsto \alpha_p$, le morphisme associé. Si $\alpha = 1$ on conclut $G \simeq \mathbb{Z}/pq\mathbb{Z}$ comme au (ii), donc on peut supposer $\alpha \neq 1$. On rappelle l'isomorphisme $(\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(Q), k \mapsto \varphi_k$, défini par $\varphi_k(g) = g^k$. Comme $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique d'ordre $q - 1 \equiv 0 \bmod p$, il a un unique sous-groupe d'ordre $p$, nécessairement cyclique. En particulier, si $u \in (\mathbb{Z}/q\mathbb{Z})^\times$ est l'élément d'ordre $p$ choisi au (ii), les autres sont les $u^k$ avec $k \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Comme $\alpha$ est non trivial et $P = \langle y \rangle$, l'automorphisme $\alpha_y \in \mathrm{Aut}(Q)$ est d'ordre $p$. On a donc $\alpha_y = \varphi_{u^k}$ pour un certain $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. Soit $q$ l'inverse de $k$ dans $\mathbb{Z}/p\mathbb{Z}$. On a alors $\alpha_{y^q} = \varphi_{u^{kq}} = \varphi_u$. Ainsi, quitte à remplacer le générateur $y$ de $P$ par $y^q$ (un autre générateur), on peut supposer que l'on a $\alpha_y = \varphi_u$. Suivont maintenant les isomorphismes : on a des isomorphismes $a : \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} P$, $m \mapsto x^m$, $b : \mathbb{Z}/q\mathbb{Z} \xrightarrow{\sim} Q$, $m \mapsto y^m$, et donc $G = Q \rtimes P \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\alpha'} \mathbb{Z}/2\mathbb{Z}$ d'après la Proposition 7.8, avec pour $m \in \mathbb{Z}/p\mathbb{Z}$ la formule

$$\alpha'_{\overline{1}}(m) = (a^{-1}\alpha_y a)(m) = a^{-1}(\alpha_\tau(x^m)) = a^{-1}(x^{um}) = um.$$

On a donc $\alpha' = \beta$ (notation du (iii)), et on a montré $G \simeq \Gamma_{p,q}$.

(v) On considère $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $p$ comme au (iii). Soit $Q$ le sous-groupe de $\mathrm{GL}_p(\mathbb{C})$ constitué des matrices diagonales de la forme

$$\mathrm{d}(\zeta) := \mathrm{diag}(\zeta, \zeta^u, \zeta^{u^2}, \ldots, \zeta^{u^{p-1}}) \text{ avec } \zeta \in \mu_q.$$

Il est cyclique d'ordre $q$ engendré par $\mathrm{d}(e^{2i\pi/q})$. Notons $\epsilon_1, \ldots, \epsilon_p$ la base canonique de $\mathbb{C}^p$ et $\sigma \in \mathrm{GL}_p(\mathbb{C})$ la matrice de permutation circulaire définie par $\sigma(e_i) = e_{i+1}$ pour $i < p$ et $\sigma(e_p) = e_1$. On constate que l'on a $\sigma^{-1}\mathrm{d}(\zeta)\sigma = \mathrm{d}(\zeta^u)$. Cela montre que le sous-groupe $G$ de $\mathrm{GL}_p(\mathbb{C})$ engendré par $Q$ et $P = \langle \sigma \rangle$ (cyclique d'ordre $p$) s'écrit ausi $G = QP$, et comme on a $Q \cap P = \{1\}$, qu'il est d'ordre $pq$. Il est non commutatif par la formule ci-dessus. Il est donc isomorphe à $\Gamma_{p,q}$ d'après le (iv).

**Exercice** 4.41. Si $\mathrm{D}_{2m}$ possède un sous-groupe d'ordre $2n$, on a $2n \mid 2m$ par Lagrange, puis $n \mid m$. Supposons donc réciproquement $n \mid m$. Par définition, on a $\mathrm{D}_{2m} = \langle c, \tau \rangle$ avec $c$ d'ordre $m$, $\tau$ d'ordre 2 et $\tau c \tau^{-1} = c^{-1}$. L'élément $d := c^{m/n}$ est donc d'ordre $n$, et il vérifie encore $\tau d \tau^{-1} = (\tau c \tau^{-1})^{m/n} = (c^{-1})^{m/n} = d^{-1}$. Posant $D = \langle d \rangle$ et $K = \langle \tau \langle$ on en déduit que $H := DK$ est un sous-groupe de $\mathrm{D}_{2m}$ qui est produit semi-direct interne de $K \simeq \mathbb{Z}/2\mathbb{Z}$ par $D \simeq \mathbb{Z}/n\mathbb{Z}$, et ce pour l'action d'inversion de $K \simeq \mathbb{Z}/2\mathbb{Z}$ sur $D$. Par la remarque précédent l'exercice (Exemple 4.41), on en déduit $H \simeq \mathrm{D}_{2n}$.

**Exercice** 4.42. On note $G_n$ le groupe défini par générateurs et relations dans l'énoncé.

(Cas $n = 1$) On a $G_1 = \langle s, t \rangle$ avec $st = 1$ et $s^2 = 1$, donc $s = t$, puis $G_1 = \langle s \rangle = \{1, s\}$ est de cardinal $\leqslant 2$. Par la propriété universelle de $G_1$, il existe un unique morphisme de groupes $f_1 : G_1 \to \{\pm 1\}$ vérifiant $f(s) = f(t) = -1$, car $-1 \cdot -1 = 1$. Le morphisme $f_1$ est clairement surjectif. Comme on a $|G_1| \leqslant 2 = |\{\pm 1\}|$, c'est un isomorphisme.

(Cas $n = 2$) On a $G_2 = \langle s, t \rangle$ avec $s^2 = t^2 = 1$ et $st = ts$. On en déduit $G_2 = \{1, s, t, st\}$ puis $|G_2| \leqslant 4$. Par la propriété universelle de $G_2$, il existe un unique morphisme de groupes $f_2 : G_2 \to \{\pm 1\} \times \{\pm 1\}$ vérifiant $f(s) = (-1, 1)$ et $f(t) = (1, -1)$ car $\{\pm 1\} \times \{\pm 1\}$ est commutatif d'exposant 2. Le morphisme $f_2$ est clairement surjectif. Comme on a $|G_2| \leqslant 4 = |\{\pm 1\}^2|$, c'est un isomorphisme.

(Cas $n > 2$) On a $G_2 = \langle s, t \rangle$ avec $s^2 = t^2 = 1$ et $(st)^n = 1$. On en déduit

$$G_2 = \{1, s, t, st, ts, sts, tst, ststs, tsts, \ldots, (st)^{n-1}, (ts)^{n-1}\}$$

et en particulier $|G_2| \leqslant 2n$. On rappelle que $\mathrm{D}_{2n}$ est le sous-groupe de $\mathrm{S}_n$ engendré par $\sigma = (1\,2\,\ldots\,n)$ et $\tau = (1\,n)(2\,n{-}1)\cdots$. On constate que l'on a $\sigma\tau = (2\,n)\,(3\,n{-}1)\,(4\,n{-}2)\,\ldots$. On a donc $\tau^2 = 1$, $(\sigma\tau)^2 = 1$ et $(\sigma\tau\tau)^n = 1$. Par la propriété universelle de $G_n$, il existe donc un unique morphisme de groupes $f_n : G_n \to \mathrm{D}_{2n}$ vérifiant $f(s) = \sigma\tau$ et $f(t) = \tau$. Il est surjectif par $\mathrm{Im}\, f_n$ contient $\langle \tau, \sigma \rangle = \mathrm{D}_{2n}$. On a vu $|\mathrm{D}_{2n}| = 2n$ en cours, et $|G_n| \leqslant 2n$ ci-dessus. On en déduit que $f_n$ est un isomorphisme.

**Exercice** 4.43. (i) Dans le groupe $G_n$, on a $(v, \sigma)(v', \sigma') = (v + \sigma(v'), \sigma\sigma')$, et $\sigma((v_i)) = (v_{\sigma^{-1}(i)})$. Si $(v, \sigma)$ est dans le centre de $G_n$, on constate donc que $\sigma$ est dans le centre de $\mathrm{S}_n$, *i.e.* $\sigma = 1$ d'après l'Exercice 4.1. Comme on a $(v', \sigma') = (v', 1)(0, \sigma')$, l'élément $(v, 1)$ est dans le centre de $G_n$ si, et seulement si, il commute à tous les $(v', 1)$ et les $(0, \sigma')$. Mais on

a $(v,1)(v',1) = (v+v',1) = (v',1)(v,1)$, donc la première condition est automatique. Pour la seconde, on a $(0,\sigma')(v,1)(0,\sigma'^{-1}) = (\sigma'(v),1)$. Ainsi, $(v,\sigma)$ est dans le centre de $G_n$ si, et seulement si, on a $\sigma = 1$ et toutes les coordonnées de $v$ sont égales, i.e. $v \in \langle e\rangle = \{0,e\}$. Le centre de $G_n$ est donc $\langle e\rangle \times 1 \simeq \mathbb{Z}/2\mathbb{Z}$.

(ii) Le sous-groupe $\langle e\rangle \subset (\mathbb{Z}/2\mathbb{Z})^n$ est bien stable par $\mathrm{S}_n$. Soit $V$ comme dans l'énoncé avec $V$ non inclus dans $\langle e\rangle$. Il existe $v \in V$ et $i \neq j$ tels que $v_i = 1$ et $v_j = 0$. En considérant $(i\,j)v - v \in V$. On en déduit $\epsilon_i - \epsilon_j \in V$, où $\epsilon_1, \ldots, \epsilon_n$ est la base canonique de $(\mathbb{Z}/2\mathbb{Z})^n$. Mais on a $\sigma(\epsilon_i - \epsilon_j) = \epsilon_{\sigma(i)} - \epsilon_{\sigma(j)}$, et comme $\mathrm{S}_n$ permute transitivement sur les parties à 2 éléments de $\{1,2,\ldots,n\}$ on a $\epsilon_i - \epsilon_j \in V$ pour tout $1 \leqslant i \neq j \leqslant n$. Cela montre $V \supset \mathrm{H}_n$.

(iii) Notons que $\varphi$ est un morphisme de groupes, et qu'elle vérifie $\varphi(\sigma(v)) = \varphi(v)$ pour tout $v \in (\mathbb{Z}/2\mathbb{Z})^n$ et tout $\sigma \in \mathrm{S}_n$. Soit $f(v,\sigma) := (\varphi(v),\sigma)$ l'application de l'énoncé. On a donc

$$f((v,\sigma)(v',\sigma')) = f(v+\sigma(v'),\sigma\sigma') = (\varphi(v)+\varphi(v'),\sigma\sigma') = (\varphi(v),\sigma)(\varphi(v'),\sigma').$$

(iv) Comme $f : G_n \to \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_n$ est un morphisme surjectif, on a

$$f(\mathrm{D}(G_n)) = \mathrm{D}(\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_n) = \{0\} \times \mathrm{A}_n.$$

On a utilisé $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$, et le fait immédiat $\mathrm{D}(G \times G') = \mathrm{D}(G) \times \mathrm{D}(G')$. Tout $g \in \mathrm{D}(G_n)$ s'écrit donc $(v,\sigma) = (v,1)(0,\sigma)$ avec $v \in \mathrm{H}_n$ et $\sigma \in \mathrm{A}_n$. Comme réciproquement l'injection canonique $\mathrm{S}_n \to G_n, \sigma \mapsto (0,\sigma)$, est un morphisme de groupes, on a aussi $\{0\} \times \mathrm{A}_n \subset \mathrm{D}(G_n)$. On en déduit que $(v,\sigma)$ est dans $\mathrm{D}(G_n)$ si, et seulement si, $\sigma \in \mathrm{A}_n$, $v \in \mathrm{H}_n$ et $(v,1) \in \mathrm{D}(G_n)$. Notons $V \subset \mathrm{H}_n$ le sous-ensemble des $v$ tels que $(v,1) \in \mathrm{D}(G_n)$. C'est clairement un sous-groupe, et il est stable par $\mathrm{S}_n$ car $\mathrm{D}(G_n)$ est distingué dans $G_n$ et on a $(0,\sigma)(v,1)(0,\sigma)^{-1} = (\sigma(v),1)$. D'après le (ii), on a donc soit $V \subset \langle e\rangle$, soit $V = \mathrm{H}_n$. Mais pour $v \in (\mathbb{Z}/2\mathbb{Z})^n$ et $\sigma \in \mathrm{S}_n$ on a la formule

$$[(v,1),(0,\sigma)] = (v,1)(0,\sigma)(-v,1)(0,\sigma^{-1}) = (v-\sigma(v),1).$$

Prenant $v = (1,0,\ldots,0)$ et $\sigma = (1\,2)$ on obtient $\epsilon_1 - \epsilon_2 \in V$. On a donc $V \neq \{0\}$. Pour $n = 2$ on a $\langle e\rangle = \mathrm{H}_2$, et on conclut. Pour $n > 2$ on a $\epsilon_1 - \varepsilon_2 \notin \langle e\rangle$, et donc $V = \mathrm{H}_n$.

(v) On a une suite exacte courte $1 \to (\mathbb{Z}/2\mathbb{Z})^n \to G_n \to \mathrm{S}_n \to 1$. Le groupe $(\mathbb{Z}/2\mathbb{Z})^n$ est abélien donc résoluble. D'après le cours, $G_n$ est résoluble si, et seulement si, $\mathrm{S}_n$ l'est, *i.e.* $n \leqslant 4$.

(vi) Observons d'abord que l'on a $\sigma(\mathrm{H}_n) \subset H_n$ pour tout $\sigma \in \mathrm{S}_n$. Ainsi, le groupe $G'_n := \mathrm{H}_n \rtimes_\alpha \mathrm{S}_n$ a bien un sens, et c'est un sous-groupe de $G_n$. De plus, l'application $G'_n \times H_n \to H_n, ((v,\sigma),w) \mapsto v+\sigma(w)$, est bien définie. C'est une action car on a $(v,\sigma)(v',\sigma') = (v+\sigma(v'),\sigma\sigma')$ dans $G'_n$, et on a bien $v+\sigma(v'+\sigma'(w)) = v+\sigma(v')+\sigma\sigma(w')$ dans $H_n$. Montrons que cette action est fidèle. Soit $(v,\sigma) \in G'_n$ avec $v+\sigma(w) = w$ pour tout $w \in H_n$. Pour $w = v$ on a $\sigma(v) = 0$, puis $v = \sigma^{-1}\sigma(v) = 0$, et donc $\sigma(w) = w$ pour tout $w \in H_n$. Appliquée à $w = \epsilon_i + \epsilon_j \in \mathrm{H}_n$ pour $1 \leqslant i < j \leqslant n$, on en déduit que $\sigma$ préserve $\{i,j\}$ pour tout $i \neq j$. Pour $n > 2$, cela implique $\sigma = 1$.

(vii) Soit $X = H_3$. On a $|X| = 4$ et le groupe $G'_3$ agit fidèlement sur $X$ par le (vi), le morphisme associé $G'_3 \to \mathrm{S}_X \simeq \mathrm{S}_4$ est donc injectif. Mais on a $|G'_3| = |X||\mathrm{S}_3| = 4 \cdot 6 = 24$ : c'est un isomorphisme.