UNIVERSITÉ DE RENNES 1

Théorie des Groupes et Géométrie

TD n°1 - Éléments de correction

Sous-groupes distingués

Exercice 1 (Sous-groupes d'indice 2)

Si $x \notin H$ alors $G = H \sqcup xH = H \sqcup Hx$ donc $Hx = xH$ donc $H = xHx^{-1}$ donc H est distingué.

Exercice 2 (Produit de sous-groupes)

1. On suppose S distingué dans G. On a $1 \in ST$ et $sts't' = s(ts't^{-1})tt' \in ST$ et $(st)^{-1} = t^{-1}s^{-1} = (t^{-1}s^{-1}t)t^{-1} \in ST$ donc ST est un sous-groupe. Le cas T distingué se montre de façon similaire (ou alors on se place dans $TS = (ST)^{-1}$.) Pour le contre-exemple, nécessairement il faut G non abélien, donc par exemple $\mathfrak{S}_3$. Avec $S = \langle(12)\rangle$ et $T = \langle(13)\rangle$ on a
$$ST = \{1, (12), (13), (12)(13) = (132)\},$$
qui n'est pas un sous-groupe puisque $(132)^{-1} = (123) \notin ST$. Si maintenant S et T sont distingués, alors on a $gstg^{-1} = (gsg^{-1})(gtg^{-1}) \in ST$.
2. On regarde $f : S \times T \to ST$ donnée par $f(s,t) \coloneqq st$. C'est une application surjective par définition, donc ST est fini et $|ST| \leqslant |S \times T| = |S||T|$. Maintenant $f(s,t) = f(s',t') \iff st = s't' \iff s'^{-1}s = t't^{-1} \in S \cap T$. Ainsi, les couples (s',t') qui ont la même image que (s,t) sont les $(su, u^{-1}t)$ avec $u \in S \cap T$. Si $\sim$ est la relation d'équivalence sur $S \times T$ donnée par $c \sim c' \iff f(c) = f(c')$, on a donc montré que chaque classe est de cardinal $|S \cap T|$. Puisque f est surjective, on en déduit que $|S \times T| = |S \cap T||ST|$ d'où le résultat.
On suppose maintenant S et T distingués dans G et $S \cap T = \{1\}$. On va montrer que f est un morphisme. Pour $s, s' \in S$ et $t, t' \in T$ on a $f\big((s,t)(s',t')\big) = f(s,t)f(s',t') \iff sts't' = ss'tt' \iff ts' = s't \iff t^{-1}s'^{-1}ts' = 1$. Or on a $t^{-1}s'^{-1}ts' = (t^{-1}s'^{-1}t)s' \in S$ et $t^{-1}s'^{-1}ts' = t^{-1}(s'^{-1}ts') \in T$ donc $t^{-1}s'^{-1}ts' \in S \cap T$ donc on a bien $t^{-1}s'^{-1}ts' = 1$. L'égalité d'avant montre que f est un morphisme surjectif entre deux groupes de même cardinal donc f est un isomorphisme.

Exercice 3 (Lemme de Zassenhaus ou lemme du papillon)

Le groupe $H \cap K'$ est distingué dans $H \cap K$ (quand on conjugue par un élément de H on reste dans H, et par un élément de K on reste dans K'. On a donc H', $H \cap K$ et $H \cap K'$ des sous-groupes de H, avec $H' \triangleleft H$. Ainsi, les ensembles $H'(H \cap K)$ et $H'(H \cap K')$ sont des sous-groupes de H.

Lemme. *Soit G un groupe et $L \triangleleft G$. Soient $K \triangleleft H$ sous-groupes de G.*

- *Si $\pi : G \to G/L$ est la surjection canonique alors $\pi^{-1}\big(\pi(H)\big) = LH$.*
- *On a $LK \triangleleft LH$.*

Démonstration.
- Pour $x \in G$ on a $x \in \pi^{-1}\big(\pi(H)\big) \iff \pi(x) \in \pi(H) \iff \pi(x) = \pi(h)$ pour un $h \in H \iff x \in Lh$ pour un $h \in H \iff x \in LH$.
- Tout d'abord, puisque $L \triangleleft G$ on a bien que LK et LH sont des groupes (sous-groupes de G). Si maintenant $\hat{k} \in LK$ et $\hat{h} \in LH$ on veut montrer que $\hat{h}\hat{k}\hat{h}^{-1} \in LK$ *i.e.* $\hat{h}\hat{k}\hat{h}^{-1} \in \pi^{-1}\big(\pi(K)\big)$ *i.e.* $\pi(\hat{h}\hat{k}\hat{h}^{-1}) \in \pi(K)$. Maintenant en écrivant $\hat{h} = \ell h$ et $\hat{k} = \ell' k$ pour $\ell, \ell' \in L$ et $h \in H$ et $k \in K$ on a $\pi(\hat{h}) = h$ et $\pi(\hat{k}) = k$ donc on trouve $\pi(\hat{h}\hat{k}\hat{h}^{-1}) = \pi(hkh^{-1})$, qui est bien dans $\pi(K)$ puisque $hkh^{-1} \in K \triangleleft G$.

□

On a vu que $H \cap K' \triangleleft H \cap K \leqslant H$, et puisque $H' \triangleleft H$ par le lemme on obtient $H'(H \cap K') \triangleleft H'(H \cap K)$. On considère maintenant l'application naturelle $f : H \cap K \to H'(H \cap K)/H'(H \cap K')$. C'est un morphisme, et il est surjectif car si $h \in H'$ et $k \in H \cap K$ alors $hk = f(k)$ puisque $h = h \cdot 1 \in H'(H \cap K')$.

On va maintenant montrer que $\ker f = (H \cap K')(H' \cap K)$. Tout d'abord, si $h \in H \cap K'$ et $k \in H' \cap K$ alors $f(hk) = 1$ puisque $h \in H \cap K'$ et $k \in H' \cap K \subseteq H'$. Si maintenant $x \in H \cap K$ vérifie $f(x) = 1$ alors $x \in H'(H \cap K')$ donc il existe $k \in H'$ et $h \in H \cap K'$ tel que $x = kh$. On a $k = xh^{-1} \in K$ donc on a $k \in H' \cap K$ et donc on a bien $x \in (H' \cap K)(H \cap K')$. Remarquons que puisque $H' \cap K \triangleleft H \cap K$ et $H \cap K' \subseteq H \cap K$ on a $(H' \cap K)(H \cap K') = (H \cap K')(H' \cap K)$ (cf. Exercice 2). On conclut par le premier théorème d'isomorphisme (l'autre partie de l'énoncé se déduit par symétrie).

Exercice 4 (Groupes simples abéliens)

Soit G abélien. Si G est (cyclique) d'ordre premier p alors le cardinal d'un sous-groupe divise p donc c'est 1 ou p donc G ne possède pas de sous-groupe propre non trivial donc G est simple. Réciproquement, supposons G simple et soit $x \in G$ non trivial. Le sous-groupe $\langle x \rangle$ est distingué dans G puisque G est abélien, et puisque G est simple on en déduit que x engendre G. Maintenant nécessairement G est fini de cardinal n, sinon G serait isomorphe à $\mathbb{Z}$ qui n'est pas simple (par exemple $2\mathbb{Z}$ est distingué). Si n n'est pas premier alors si m est un diviseur strict non trivial de n on a un sous-groupe (distingué) $m\mathbb{Z}/n\mathbb{Z}$ strict non trivial de G, ce qui est absurde puisque G est simple. Donc n est premier.

Résolubilité

Exercice 5 (Étude de $\mathfrak{S}_3$)

1. Une permutation $\sigma \in \mathfrak{S}_3$ détermine une *partition* de 3, c'est-à-dire une suite $\lambda = (\lambda_1, \lambda_2, \dots)$ décroissante d'entiers strictement positifs de somme 3, via sa décomposition en cycles à supports disjoints.. On liste les différentes partitions possibles (de façon algorithmique) : $(3), (2,1), (1,1,1)$. Il y a deux trois cycles, $\binom{3}{2} = 3$ transpositions et l'élément neutre (donc bien $3! = 6$ éléments). Les signatures sont respectivement $1, -1, 1$.
2. Le cardinal d'un sous-groupe divise 6 donc est soit 1 (groupe trivial), 2, 3 ou 6 (tout). Les sous-groupes de cardinal 2 (donc les 2-Sylow) sont engendré par un élément d'ordre 2 (une transposition), et ceux de cardinal 3 (donc les 3-Sylow) sont engendrés par un trois cycle (il y a donc un unique tel sous-groupe). Seul le sous-groupe d'ordre 3 est distingué parmi les sous-groupes strictes non triviaux (les éléments d'ordre 2 étant tous conjugués).
3. $\{1\} \triangleleft \mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ est une suite de composition à facteurs abéliens puisque $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ et $\mathfrak{S}_3/\mathfrak{A}_3 \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 6 (Suite dérivée de $\mathfrak{S}_4$)

1. Découle du fait que $\mathfrak{S}_4/\mathfrak{A}_4 \simeq \mathbb{Z}/2\mathbb{Z}$ est abélien.
2. On a $(12)(13)(12)(13) = (123)$ (on calcule les images successives) et $(123)(124)(132)(142) = (12)(34)$.
3. On a déjà une inclusion. Pour l'autre, rappelons que $\mathfrak{A}_4$ est constitué des permutations paires, donc ici les 3-cycles et les double transpositions. On vient de montrer que $D(\mathfrak{S}_4)$ contient un 3-cycle (resp. une double transposition) donc les contient tous, car les 3-cycles (resp. double transpositions) sont conjugués et $D(\mathfrak{S}_4)$ est distingué dans $\mathfrak{S}_4$. Donc $D(\mathfrak{S}_4) \supseteq \mathfrak{A}_4$ et c'est gagné. (Puisque $\mathfrak{A}_4$ est engendré par les 3-cycles il suffisait de les considérer.)
4. Même argument.
5. $V \triangleleft \mathfrak{S}_4$ (cf. type des permutations) donc puisque $\mathfrak{A}_4 \subseteq \mathfrak{S}_4$ on en déduit que $V \triangleleft \mathfrak{A}_4$. De plus $\mathfrak{A}_4/V$ est de cardinal $12/4 = 3$ donc est abélien. On en déduit le résultat.
6. On a montré $D(\mathfrak{A}_4) = V$ donc $D^2(\mathfrak{S}_4) = V$.
7. V est abélien donc $D(V) = \{1\} = D^i(\mathfrak{S}_4)$ pour $i \geqslant 3$.

Exercice 7 (Groupe triangulaire supérieur)

1. Si $f : \begin{pmatrix} 1 & x & . \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mapsto (x, y)$ alors on a par un produit matriciel que $f : H \to k^2$ est un morphisme surjectif de groupes. Son noyau est $\begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \simeq k$ par le calcul précédent. On a donc trouvé un sous-groupe de H isomorphe à k avec $H/k \simeq k^2$. Puisque k et k^2 sont abéliens, ils sont résolubles donc H aussi.
2. Même raisonnement avec cette fois-ci le morphisme surjectif $\begin{pmatrix} x & . & . \\ 0 & y & . \\ 0 & 0 & z \end{pmatrix} \mapsto (x, y, z) \in k^{\times 3}$ de noyau H.

Exercice 8 (Théorème de Feit-Thompson)

On suppose 1. Soit G un groupe fini simple et on suppose que G est d'ordre impair. Par hypothèse G est résoluble, donc $D(G) < G$. Puisque G est simple on a $D(G) = \{1\}$ donc G est abélien. Ainsi, tout groupe fini simple non abélien est nécessairement d'ordre pair.

On suppose maintenant 2. Soit G un groupe d'ordre impair. On va montrer par récurrence sur $|G|$ que G est résoluble. Si $|G| = 1$ c'est bon. Si G est abélien alors G est résoluble, sinon G est non abélien. Par hypothèse G n'est pas simple (sinon

il serait d'ordre pair) donc G possède un sous-groupe distingué propre non trivial H. Ainsi H et G/H sont d'ordre impair $< |G|$ donc résolubles par hypothèse de récurrence, donc G aussi.

p-groupes

Si p est un nombre premier, on appelle *p-groupe* un groupe fini non trivial d'ordre une puissance p.

Exercice 9 (Centre d'un p-groupe)

On fait agit G par conjugaison sur lui-même. Si Ω est l'ensemble des orbites, on a $|G| = \sum_{\omega\in\Omega} |\omega|$. On a $x \in Z(G) \iff x$ est dans une orbite de taille 1, donc on obtient

$$|G| = |Z(G)| + \sum_{\substack{\omega\in\Omega \\ |\omega|>1}} |\omega|.$$

Maintenant pour $\omega \in \Omega$ on a $|\omega|$ divise $|G|$, donc si ω n'est pas un singleton son cardinal est une puissance de p. En réduisant modulo p l'égalité ci-avant on obtient que $|Z(G)| = 0 \pmod p$, donc $p \mid |Z(G)|$ puisque $|Z(G)| \neq 0$ puisque $1 \in Z(G)$.

Exercice 10 (p-groupes élémentaires abéliens)

(D'après le théorème de classification des groupes abéliens finis, un p-groupe abélien élémentaire est un $(\mathbb{Z}/p\mathbb{Z})^n$.)

1. On regarde l'application $Z \times G \to G$ donnée par $(n, x) \mapsto nx$. On a $px = 0$ par hypothèse donc cette application se factorise en $\mathbb{F}_p \times G \to G$. On a donc bien la propriété de multiplication externe, et les autres se vérifient immédiatement.
2. Soit $f : G \to H$. On a $f(x + y) = f(x) + f(y)$ par définition, et pour $n \in \mathbb{Z}$ on a $f(nx) = nf(x)$ donc pour $\lambda \in \mathbb{F}_p$ on a $f(\lambda x) = \lambda f(x)$.
3. Si $f \in \mathrm{Aut}(G)$ alors par la question précédente f est un automorphisme d'un $\mathbb{F}_p$-espace vectoriel. Si $|G| = p^n$ alors $\dim_{\mathbb{F}_p} G = n$ et donc $\mathrm{Aut}(G) \simeq \mathrm{GL}_n(p)$.
4. Par la question précédente on a $\mathrm{Aut}(V) \simeq \mathrm{GL}_2(2) \simeq \mathfrak{S}_3$ (unique groupe non abélien d'ordre 6). Ainsi à toute permutation de $V \setminus \{1\}$ (qui est de cardinal 3) correspond un élément de $\mathrm{GL}_2(2) \setminus \{I_2\}$ et donc un automorphisme de V.

Exercice 11 (Groupes d'ordre p^2 et p^3)

1. On suppose que $G/Z(G)$ est cyclique. Soit $x \in G$ tel que $\overline{x}$ est un générateur. Alors $G = \sqcup_i x^i Z(G)$, ainsi si $y, z \in G$ on peut écrire $y = x^i\alpha$ et $z = x^j\beta$ avec $\alpha, \beta \in Z(G)$ donc y et z commutent.
2. Par un exercice précédent on sait que $Z(G)$ n'est pas trivial, donc si G n'est pas abélien alors $|Z(G)| = p$. Le centre est distingué donc on peut faire le quotient, qui est ici de cardinal $p^2/p = p$ donc cyclique. Par la question précédente, on en déduit que G est abélien. La liste est donc $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^2$.
3. On sait déjà que Z est non trivial. S'il est d'ordre p^2 alors on aurait G/Z d'ordre p donc cyclique donc G abélien ce qui est absurde. Si Z était d'ordre p^3 alors on aurait de même G abélien, finalement Z est d'ordre p. Ainsi G/Z est d'ordre p^2, par la question précédente c'est donc soit Z/p^2Z, impossible par la première question, c'est donc $(\mathbb{Z}/p\mathbb{Z})^2$. Finalement, le groupe G/Z est abélien donc $D(G) \subseteq Z$. Puisque Z est d'ordre p on a $D(G) = Z$ ou $D(G) = \{1\}$, mais ce dernier cas est exclus puisque G non abélien.

Exercice 12 (Sous-groupes de $U_3(\mathbb{F}_3)$)

On note $U = U_3(\mathbb{F}_3)$ le groupe des matrices carrées triangulaires supérieures de taille 3 avec des 1 sur la diagonale.

1. Montrer que U est un groupe non abélien dans lequel $x^3 = 1$ pour tout x, et calculer son cardinal.
2. Calculez le centre Z de U.
3. Décrivez les sous-groupes d'ordre 3 et donnez leur nombre.
4. Montrez que les sous-groupes d'ordre 9 contiennent tous le centre. En vous ramenant à U/Z, déduisez-en qu'ils sont tous distingués et donnez leur nombre.
5. Décrivez les sous-groupes d'ordre 9 de la manière suivante : notez $f : U \to (\mathbb{Z}/3\mathbb{Z})^2$ le morphisme qui à une matrice A associe les deux coefficients de sa première surdiagonale, et montrez que la considération des noyaux $H = \ker(\varphi \circ f)$ fournit suffisamment de sous-groupes d'ordre 9 à partir de formes $\mathbb{F}_3$-linéaires φ sur l'espace $E = (\mathbb{F}_3)^2$.

Actions de groupes

Exercice 13 (Théorème de Cauchy)

Démontrez que tout groupe fini d'ordre divisible par un nombre premier p possède un élément d'ordre p. *On pourra faire agir par permutation circulaire le groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des p-uplets $(x_1, \dots, x_p)$ de G tels que $x_1 \cdots x_p = 1$.*

Soit $H \coloneqq \{(x_1, \dots, x_p) \in G^p : x_1 \cdots x_p = 1\}$. Un élément $x \in G$ est d'ordre p ssi $x \neq 1$ et $(x, \dots, x) \in H$. Remarquons que H est non vide puisque $(1, \dots, 1) \in H$. Le groupe $\mathbb{Z}/p\mathbb{Z}$ agit sur H par permutations circulaires, notamment $1 \in \mathbb{Z}/p\mathbb{Z}$ envoie $(x_1, \dots, x_p) \in H$ sur $(x_p, x_1, \dots, x_{p-1})$. Cet élément est bien dans H car si $x_1 \cdots x_p = 1$ alors $x_1 \cdots x_{p-1} = x_p^{-1}$ et donc $x_p x_1 \cdots x_{p-1} = 1$. Par la relation orbite-stabilisateur, le cardinal d'une orbite divise celui de $\mathbb{Z}/p\mathbb{Z}$ donc est soit 1 soit p. Soit $X \subseteq H$ l'ensemble des points fixes de H sous l'action de $\mathbb{Z}/p\mathbb{Z}$. Remarquons que si $(x_1, \dots, x_p) \in X$ alors $x_1 = \cdots = x_p$ et $x_1^p = 1$. Par la formule des classes on a $X = |H| \pmod p$. On remarque que $(x_1, \dots, x_p) \in H$ ssi $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$, ainsi H est en bijection avec G^{p-1} et donc $|H| = 0 \pmod p$. Ainsi $p \mid |X|$, et puisque $(1, \dots, 1) \in X$ on en déduit par ce qui précède que G possède un élément d'ordre p.

Exercice 14 (Application des formules de comptage)

On fixe une action d'un groupe G sur un ensemble fini E.

1. On suppose que l'ordre de G est 15, que le cardinal de E est 17 et que E n'a pas de point fixé par tous les éléments du groupe G. Déterminer le nombre d'orbites et le cardinal de chacune d'elles.

2. Montrer que toute action d'un groupe d'ordre 143 sur un ensemble de cardinal 25 possède un point fixe.

1. Par la relation orbite-stabilisteur, le cardinal d'une orbite divise le cardinal $|G| = 15$ du groupe donc une orbite est de cardinal $15, 5, 3$ ou 1. Par hypothèse 1 est exclus, et par la formule des classes on a $17 = 15n_{15} + 5n_5 + 3n_3$ où $n_i \in \mathbb{N}$ est le nombre d'orbites de taille i. Nécessairement $n_{15} = 0$ puisque si $n_{15} \geqslant 1$ on aurait $2 \geqslant 5n_5 + 3n_3$ donc $n_5 = n_3 = 0$ ce qui est impossible puisqu'alors $17 \neq 15n_{15}$. Ainsi on a $17 = 5n_5 + 3n_3$. On a $n_5 \leqslant 3$, les cas $n_5 = 3, 2, 0$ sont impossibles puisque $3 \nmid 2, 7, 17$ respectivement. Il ne reste donc plus que $n_5 = 1$ et $n_3 = 4$.

2. On a $143 = 13 \times 11$ donc une orbite est de cardinal $143, 13, 11$ ou 1. Le cas 143 est impossible puisque $143 > 25$, et si on suppose qu'aucune orbite est triviale on doit trouver $n_{13}, n_{11} \in \mathbb{N}$ tels que $25 = 13n_{13} + 11n_{11}$. On a $n_{13} = 0$ ou 1 puisque $25 < 13 \times 2 = 26$, le cas 0 est impossible puisque $11 \nmid 25$ et le cas 1 aussi puisque $11 \nmid 12$. Ainsi au moins une orbite est triviale.

Exercice 15 (Sur la transitivité multiple)

Soit $k \geq 2$ entier. On dit que l'action d'un groupe G sur un ensemble X de cardinal au moins k est *k-transitive* si pour tout $x_1 \dots, x_k \in X$ distincts et tout $y_1, \dots, y_k \in X$ distincts, il existe $g \in G$ tel que $gx_i = y_i$ pour $i = 1, \dots, k$.

1. Montrer qu'une action est k-transitive si et seulement si elle est transitive et que l'action du stabilisateur de tout point $x \in X$ sur $X \smallsetminus \{x\}$ est $(k-1)$-transitive.

2. Montrer qu'une action est k-transitive si et seulement si elle est transitive et que l'action d'un stabilisateur d'un point $x \in X$ sur $X \smallsetminus \{x\}$ est $(k-1)$-transitive.

Faire des dessins !

1. On montre d'abord le sens direct.

- Montrons que l'action de G sur X est transitive. Soit $x, y \in X$. Par hypothèse, puisque X est de cardinal au moins k on peut trouver $x_2, \dots, x_k \in X$ (resp. $y_2, \dots, y_k \in X$) deux à deux distincts et différents de x (resp. de y). Par hypothèse encore, on peut trouver $g \in G$ tel que $gx = y$ (et $gx_i = y_i$ pour tout $x \geqslant 2$). On a bien montré que l'action de G sur X est transitive.
- Soit $x \in X$ et montrons que l'action de G_x sur $X_x \coloneqq X \setminus \{x\}$ est $(k-1)$-transitive. Pour cela, soient $x_2, \dots, x_k, y_2, \dots, y_k \in X_x$ avec $x_2, \dots, x_k$ (resp. $y_2, \dots, y_k$) deux à deux ditincts. C'est possible puisque X est de cardinal au moins k donc X_x est de cardinal au moins $k-1$. Par construction, les éléments $x, x_2, \dots, x_k$ (resp. $x, y_2, \dots, y_k$) sont deux à deux distincts donc il existe $g \in G$ tel que $gx = x$ et $gx_i = y_i$ pour tout $i \geqslant 2$. La première égalité montre que $g \in G_x$ et donc on a bien envoyé $(x_2, \dots, x_k)$ sur $(y_2, \dots, y_k)$ par un élément du stabilisateur de x. Autrement dit, l'action de G_x sur X_x est $(k-1)$-transitive.

Montrons maintenant le sens indirect. Soit $x_1, \dots, x_k \in X$ (resp. $y_1, \dots, y_k \in X$) distincts. C'est possible puisque $|X| \geqslant k$. Par hypothèse, l'action de G sur X est transitive donc il existe $g \in G$ tel que $gx_1 = y_1$. En particulier, on a $g \cdot (x_1, \dots, x_k) = (y_1, gx_2, \dots, gx_k)$ et $y_1, gx_2, \dots, gx_k$ sont deux à deux distincts (un élément de G agissant par permutation sur X). Toujours par hypothèse, l'action de G_{y_1} sur $X \setminus \{y_1\}$ est $(k-1)$-transitive donc il existe $h \in G_{y_1}$ tel que $h(gx_i) = y_i$ pour tout $i \geqslant 2$. Puisque $hy_1 = y_1$, on a donc $hgx_1 = hy_1 = y_1$ et pour tout $i \geqslant 2$

$$(hg)x_i = h(gx_i) = y_i.$$

On a donc bien trouvé un élément de G qui envoie $(x_1, \dots, x_k)$ sur $(y_1, \dots, y_k)$ ce qui montre que l'action de G sur X est k-transitive.

2. Le sens direct découle de la question précédente. Pour le sens indirect, on raisonne globalement comme avant, mais avec une étape en plus. Soit $z \in X$ tel que G_z agit $(k-1)$-transitivement sur X. Puisque l'action de G sur X est transitive, on peut trouver g_x (resp. g_y) dans G tel que $g_x x_1 = z$ (resp. $g_y y_1 = z$). Par propriété d'une action on a $g_x x_2, \dots, g_x x_k$ (resp. $g_y y_2, \dots, g_y y_k$) deux à deux distincts, donc on peut trouver $g \in G_z$ tel que $g(g_x x_i) = g_y y_i$ pour tout $i \geqslant 2$. Il ne reste plus qu'à se rendre compte que l'élément $g_y^{-1} g g_x$ envoie $(x_1, \dots, x_k)$ sur $(y_1, \dots, y_k)$.

Exercice 16 (Groupes finis résolubles)

1. Montrer par récurrence qu'un p-groupe est toujours résoluble.

2. Soient p, q deux nombres premiers distincts. Montrer qu'un groupe de cardinal pq est toujours résoluble.
Supposer $p > q$ et considérer un p-Sylow.

3. Soit G un groupe d'ordre 12. Montrer que G est résoluble.
En supposant les 3-Sylow non distingués, compter le nombre d'éléments d'ordre 3.

4. Soient p, q deux nombres premiers distincts. Montrer qu'un groupe de cardinal $p^2 q$ est toujours résoluble.

1. Le centre d'un p-groupe est non trivial, ainsi si G est un p-groupe, si G est commutatif (ce qui se produit nécessairement si $|G| = p$) alors $D(G) = \{1\}$ donc G est résoluble, et sinon $Z(G)$ et $G/Z(G)$ sont deux p-groupe de cardinaux strictement plus petits que celui de G donc par hypothèse de récurrence $Z(G)$ et $G/Z(G)$ sont résolubles donc G est résoluble.

2. Soit P un p-Sylow. On a $n_p = 1 \pmod p$ et $n_p \mid q$ donc $n_p \in \{1, q\}$ donc puisque $p > q$ on en déduit que $n_p = 1$ (car $q \neq 1 \pmod p$). Ainsi P est l'unique p-Sylow et est donc distingué. Les groupes P et G/P sont des p-groupes et sont donc résolubles par la question précédente, donc G aussi.

3. On a $n_3 = 1 \pmod 3$ et $n_3 \mid 4$. Si $n_3 = 1$ alors comme avant on en déduit que G est résoluble. Sinon, nécessairement on a $n_3 = 4$. Deux 3-Sylows distincts de G ne s'intersectant qu'en l'élément trivial (par le théorème de Lagrange), on en déduit que G possède exactement $2n_3 = 8$ éléments d'ordre 3 (un élément d'ordre 3 étant contenu dans le 3-Sylow qu'il engendre). Il reste exactement 4 éléments, qui sont nécessairement les éléments d'un unique 2-Sylow (les éléments non triviaux d'un 2-Sylow n'étant dans aucun 3-Sylow par Lagrange). Ainsi le 2-Sylow est distingué et on conclut comme au début de la question.

4. On a $n_p = 1 \pmod p$ et $n_p \mid q$ donc $n_p = 1$ (auquel cas il y a un unique p-Sylow, qui est donc distingué et donc on conclut comme avant) ou $n_p = q$, ce que l'on suppose maintenant. On a donc $q = 1 \pmod p$ donc $p \mid (q-1)$ donc $p \leqslant q - 1$.
On a $n_q = 1 \pmod q$ et $n_q \mid p^2$ donc $n_q \in \{1, p, p^2\}$. Si $n_q = 1$ c'est fini, si $n_q = p^2$ alors il y a $(q-1)p^2 = p^2 q - p^2$ éléments d'ordre q. Il reste p^2 éléments dans G, qui forment nécessairement l'unique p-Sylow qui est donc distingué et on conclut. On suppose donc $n_q = p$. On a donc $p = 1 \pmod q$ donc $q \mid (p-1)$ donc $q \leqslant p - 1$. Or $p \leqslant q - 1$ donc on trouve $q \leqslant q - 2$ donc ce cas est impossible.
Finalement, on a montré que nécessairement G est résoluble.

Exercice 17 (Lemme du ping-pong)

Soit G un groupe agissant sur un ensemble E. Soit E_1, E_2 deux parties non vides et disjointes de E et $g, h \in G$ deux éléments tels que $g^k(E_1) \subset E_2$ et $h^k(E_2) \subset E_1$ pour tout $k \in \mathbb{Z} \setminus \{0\}$.

1. Montrer qu'aucun « mot » de la forme $g^{k_1} h^{l_1} g^{k_2} h^{l_2} \cdots g^{k_d} h^{l_d} g^{k_{d+1}}$, avec $k_i, l_j \neq 0$, n'est égal à l'élément neutre.

2. En déduire en utilisant une conjugaison, qu'aucun mot du groupe engendré par g et h autre que le mot vide n'est égal à l'élément neutre. On dit alors que le groupe engendré par g et h est un *groupe libre*.

3. Montrer le sous groupe de $SL(2, \mathbb{Z})$ engendré par

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ et } B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

est libre, en considérant l'action naturelle sur $\mathbb{R}^2$ et les domaines $\{(x, y) \in \mathbb{R}^2, |x| < |y|\}$ et $\{(x, y) \in \mathbb{R}^2, |x| > |y|\}$ délimités par les diagonales.

1. Par construction, cet élément envoie E_1 dans E_2, donc est non trivial puisque ces ensembles sont disjoints.

2. Les exposants sont à chaque fois supposés non nuls.

- On considère $x = g^{k_1} h_{l_1} \cdots g^{k_d} h^{l_d}$. En conjuguant x par $g^{-k_1'}$ avec $k_1' \neq k_1$ on obtient $g^{-k_1'} x g^{k_1'} = g^{k_1 - k_1'} h_{l_1} g^{k_2} \cdots g^{k_d} h^{l_d} g^{k_1'}$. Par la question précédente on a donc $g^{-k_1'} x g^{k_1'} \neq 1$ donc $x \neq 1$.
- On considère $y = h^{l_1} g^{k_2} \cdots h^{l_d} g^{l_{d+1}}$. Par le point on a $y^{-1} \neq 1$ donc $y \neq 1$.
- On considère $z = h^{l_1} g^{k_2} h^{l_2} \cdots g^{k_d} h^{l_d}$. L'élément gzg^{-1} est non trivial par la question précédente, donc z également.

3. Soit E_1 (resp. E_2) le premier (resp. deuxième) domaine. On montre d'abord que $A^{\pm 1} E_1 \subseteq E_2$.

- Soit $(x,y) \in E_1$, donc $|x| < |y|$. On a $A^{-1} = \left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right)$ donc $A^{\pm 1}(x,y) = (x \pm 2y, y)$. Par la deuxième inégalité triangulaire on a
$$|x \pm 2y| \geqslant \big||x| - |\pm 2y|\big| = 2|y| - |x| = |y| + \big(|y| - |x|\big) > |y|,$$
donc $A^{\pm 1}(x,y) \in E_2$ et $A^{\mathbb{Z}} E_1 \subseteq E_2$.
- Avec $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = P^{-1}$ on a $B = PAP$ et $E_2 = PE_1$ donc
$$B^{\pm 1} E_2 = (PA^{\pm 1}P)(PE_1) = P(A^{\pm 1}E_1) \subseteq PE_2 = E_1.$$

Ordre des éléments

Exercice 18 (Ordre d'un produit)

Soit G un groupe et x, y deux éléments d'ordres finis égaux respectivement à m et n.

1. On suppose que x et y commutent et que m et n sont premiers entre eux. Démontrez que xy est d'ordre mn.

2. Peut-on étendre ce résultat au cas où x et y ne commutent pas ?

3. Peut-on étendre ce résultat au cas où m et n ne sont pas premiers entre eux ?

Exercice 19 (Sous-groupes finis du groupe multiplicatif d'un corps)

On note $\varphi(n)$ l'indicateur d'Euler de n, égal à $|(\mathbb{Z}/n\mathbb{Z})^\times|$ ou encore au nombre d'entiers $1 \leq k \leq n$ premiers avec n.

1. Rappeler pourquoi $\sum_{d|n} \varphi(d) = n$.
Partitionner $\mathbb{Z}/n\mathbb{Z}$ en fonction de l'ordre de ses éléments.

2. Démontrer que tout sous-groupe fini H du groupe multiplicatif d'un corps (commutatif) k est cyclique :

(i) montrez que pour chaque $d|n$ l'ensemble $H_d = \{x \in H, x^d = 1\}$ est d'ordre au plus d,

(ii) montrez que l'ensemble H_d^* des éléments d'ordre d dans H est d'ordre 0 ou $\varphi(d)$,

(iii) concluez en regardant la partition $H = \amalg_{d|n} H_d^*$.

Théorème de Sylow et produit semi-direct

Exercice 20 (Groupes d'ordre pq)

Soient $p < q$ deux nombres premiers. Soit G un groupe d'ordre pq.

1. Montrer que $s_q = 1$ où le nombre s_q est le nombre de q-Sylow de G.

2. En déduire que G est un produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$.

3. Montrer que si $p \nmid q - 1$ alors G est cyclique.

4. Montrer que si $p|q-1$ alors il existe à isomorphisme près deux groupes d'ordre pq : le groupe cyclique d'ordre pq et le groupe non-abélien d'ordre pq. (Remarque : le groupe diédral est l'exemple le plus simple du second cas.)

Exercice 21 (Groupes d'ordre p^2q)

Soient $p < q$ deux nombres premiers distincts. Nous allons montrer qu'aucun groupe G d'ordre p^2q n'est simple. On note s_q le nombre de q-Sylow de G.

1. Montrer que si $s_q \neq 1$ alors $p^2 \equiv 1[q]$.

2. En déduire qu'alors $p = 2$ et $q = 3$.

3. Montrer que si $p \neq 2$ ou $q \neq 3$, alors G n'est pas simple et est le produit semi-direct d'un p-Sylow et d'un q-Sylow.

Groupes symétriques et alternés

Exercice 22 ($\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6)

1. Soit H un sous-groupe d'ordre 6 de $\mathfrak{A}_4$. Montrer que pour tout $g \in \mathfrak{A}_4$, on a $g^2 \in H$.

2. En déduire que H contient tous les 3-cycles.

3. Conclure (éventuellement de deux manières...).

La réciproque au théorème de Lagrange est donc fausse. Il s'agit du plus petit contre-exemple.

Exercice 23 (Sous-groupes d'indice 2 de $\mathfrak{S}_n$)

1. Soit $f : \mathfrak{S}_n \to \{\pm 1\}$ un homomorphisme de groupes. Démontrer que les transpositions ont toutes la même image. En déduire que f est soit constante soit la signature.

2. Soit G d'indice 2 dans $\mathfrak{S}_n$. Démontrer que G est distingué puis que $G = \mathfrak{A}_n$.

Exercice 24 (Sous-groupes distingués de $\mathfrak{S}_n$)

Le but de l'exercice est de déterminer les sous-groupes distingués de $\mathfrak{S}_n$ (pour $n \geqslant 5$).

1. Soit H un sous-groupe distingué de $\mathfrak{S}_n$. Montrer que $H \cap \mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{A}_n$. En déduire que H contient $\mathfrak{A}_n$ ou que $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$.

2. On suppose que $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$. Montrer que la restriction à H du morphisme signature est injective. Montrer que dans ce cas que tous les éléments de H sont dans le centre de $\mathfrak{S}_n$ et en déduire que $H = \{\mathrm{Id}\}$.

3. On suppose que H contient $\mathfrak{A}_n$. Montrer alors que $H = \mathfrak{S}_n$ ou $H = \mathfrak{A}_n$ suivant l'indice de H dans $\mathfrak{S}_n$.

4. Conclure : si $n \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$..