UNIVERSITÉ DE RENNES 1

Théorie des Groupes et Géométrie

Feuille n°1

Sous-groupes distingués

Exercice 1 (Sous-groupes d'indice 2)

Démontrez que dans un groupe, tout sous-groupe d'indice 2 est distingué.
Correction : 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)

Soit G un groupe. Si S, T sont deux sous-groupes de G, on note $ST = \{st \in G; s \in S, t \in T\}$ l'ensemble des produits.

1. Démontrez que si S ou T est distingué dans G, alors ST est un sous-groupe mais que ce n'est pas le cas en général. *Utilisez par exemple la règle d'or du contre-exemple : commencer par la situation la plus simple possible et la compliquer progressivement jusqu'à trouver un contre-exemple.*
   Correction : 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. Démontrez que : si S et T sont distingués, alors ST aussi ; si de plus $S \cap T = 1$, on a un isomorphisme $ST \simeq S \times T$.
   Correction : On sait déjà que ST est bien un sous-groupe de G par la question précédente. On a $gstg^{-1} = (gsg^{-1}(gtg^{-1}) \in ST$ puisque S et T sont distingués donc ST est distingué dans G.
   On suppose maintenant $S \cap T = 1$. On va montrer que $f : S \times T \to ST$ donnée par $f(s,t) := st$ 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 $t^{-1}s'^{-1}ts' = 1$. Le morphisme f est surjectif par définition de ST, il reste donc à montrer qu'il est injectif. Mais si $st = 1$ alors $s = t^{-1} \in S \cap T = 1$ donc $s = t = 1$ donc $(s,t) = 1_{S\times T}$.
3. Démontrez que si S et T sont finis, alors ST est fini et on a l'égalité de cardinaux : $|ST| = |S||T|/|S \cap T|$.
   Introduisez et étudiez une application $f : S \times T \to ST$.
   Correction : L'application f précédente est toujours surjective. Notons que f n'est plus nécessairement un morphisme, ne serait-ce car ST n'est pas nécessairement un groupe. On va mesurer le défaut d'injectivité de f. On a $f(s,t) = f(s',t') \iff st = s't' \iff s'^{-1}s = t't^{-1} \in S \cap T$. Ainsi, les couples (s',t') qui ont la même image que (s,t) sont les (su^{-1}, ut) 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.

Exercice 3 (Sous-groupe de Frattini des p-groupes)

Soit G un groupe et p un nombre premier.

1. Démontrez que le sous-groupe G' engendré par les commutateurs $[x,y] := xyx^{-1}y^{-1}$ est distingué, et que le groupe quotient G/G' est abélien. *Correction : On va montrer un résultat plus fort : si H est un sous-groupe distingué de G alors G/H abélien ssi $H \supseteq G'$. (Cela conclura puisque G' est distingué dans G car caractéristique, i.e. stable par tout automorphisme de G.) Tout d'abord, si G/H est abélien alors l'image de $[x,y] \in G'$ est $[\bar{x}, \bar{y}] = 1$ par abélianité donc $\overline{[x,y]} = 1$ donc $[x,y] \in H$, ainsi $G' \subseteq H$. Réciproquement, on suppose $H \supseteq G'$ et soient $\gamma, \gamma' \in G/H$. Si $g, g' \in G$ sont des antécédents respectifs de γ, γ' alors $[g,g'] \in G' \subseteq H$ donc la classe de $[g,g']$ est nulle modulo H donc $[gamma, \gamma'] = 0$ dans G/H.*
2. Démontrez que le sous-groupe G^p engendré par les puissances p-ièmes x^p est distingué, et que le groupe quotient G/G^p est « tué par p » au sens où chacun de ses éléments a une puissance p-ième nulle.
   Correction : Tout d'abord, on note que G^p est bien un sous-groupe. Il est distingué puisque $x \mapsto gxg^{-1}$ est un automorphisme (intérieur), en particulier $gx^pg^{-1} = (gxg^{-1})^p$. Pour $g \in G$, on a $g^p \in G^p$ donc l'image de g^p (donc γ^p où $\gamma \in G/G^p$ est l'image de g) est nulle.

3. Démontrez que $G/G'G^p$ est un $\mathbb{F}_p$-espace vectoriel. *Correction : Tout d'abord, on remarque que G' et G^p sont distingués donc $G'G^p$ aussi par l'Exercice 2 donc $G/G'G^p$ a bien un sens. Par le résultat général de la question 1, on a $G'G^p \supseteq G'$ (puisque $g \cdot 1 \in G'G^p$) donc on sait que $G/G'G^p$ est un groupe abélien. Étant donné $\gamma \in G/G'G^p$, on a donc un morphisme de groupes $\mathbb{Z} \to G/G'G^p$ donnée par $n \mapsto n \odot \gamma \coloneqq \gamma^n$. Si $g \in G$ est un antécédent de γ, on a $g^p \in G^p \subseteq G'G^p$ donc $\gamma^p = 0$ donc le morphisme se factorise en $\mathbb{Z}/p\mathbb{Z} \to G/G'G^p$.*

Si G est un p-groupe fini, l'entier $r := \dim_{\mathbb{F}_p}(G/G'G^p)$ est fini et un théorème classique affirme que ses parties génératrices minimales sont toutes de même cardinal égal à r.

Exercice 4 (Lemme de Zassenhaus ou lemme du papillon)

Soient G un groupe et H', H, K', K des sous-groupes tels que $H' \lhd H$ et $K' \lhd K$. Montrez qu'on a un isomorphisme :

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{K'(H \cap K)}{K'(H' \cap K)}.$$

On pourra démontrer que les deux membres sont isomorphes à $(H \cap K)/((H \cap K')(H' \cap K))$.

Correction : 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 $H' \lhd H$. Ainsi, les ensembles $H'(H \cap K)$ et $H'(H \cap K')$ sont des sous-groupes de H.

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

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

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 $L \lhd G$ 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 $hkh^{-1} \in K \lhd G$.

□

On a vu que $H \cap K' \lhd H \cap K \leqslant H$, et puisque $H' \lhd H$ par le lemme on obtient $H'(H \cap K') \lhd H'(H \cap K)$. 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 $H' \cap K \lhd H \cap K$ 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 5 (Groupes simples abéliens)

Démontrez qu'un groupe abélien est simple si et seulement s'il est cyclique d'ordre premier. *Correction : 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.*

Exercice 6 (p-groupes élémentaires abéliens)

Un p-groupe G est dit *élémentaire abélien* s'il est abélien et vérifie $px = 0$ pour tout $x \in G$ (on dit que G est *d'exposant p*).

1. Montrez qu'un p-groupe élémentaire abélien peut être muni d'une unique structure de $\mathbb{F}_p$-espace vectoriel compatible avec sa structure de groupe. *Correction : (D'après le théorème de classification des groupes abéliens finis, un p-groupe abélien élémentaire est un $(\mathbb{Z}/p\mathbb{Z})^n$.) 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. Montrez qu'un morphisme entre deux p-groupes élémentaires abéliens est $\mathbb{F}_p$-linéaire. *Correction : 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. Calculez le groupe des automorphismes d'un p-groupe élémentaire abélien. *Correction : 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. Soit $V = (\mathbb{Z}/2\mathbb{Z})^2$ le groupe de Klein. Calculez $\mathrm{Aut}(V)$ et démontrez que n'importe quelle permutation de l'ensemble $V \setminus \{1\}$ définit un automorphisme de V. *Correction : 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.*

Résolubilité

Exercice 7 (Étude de $\mathfrak{S}_3$)

1. Donner les structures de cycles possibles dans $\mathfrak{S}_3$, le nombre d'éléments de $\mathfrak{S}_3$ ayant cette structure, et leur signature. *Correction : 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. Décrire les sous-groupes de $\mathfrak{S}_3$, et ceux qui sont distingués dans $\mathfrak{S}_3$. Déterminer les sous-groupes de Sylow de $\mathfrak{S}_3$. *Correction : 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. Trouver une suite de composition à facteurs abéliens de $\mathfrak{S}_3$. *Correction : $\{1\} \triangleleft \mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ 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 8 (Suite dérivée de $\mathfrak{S}_4$)

On note V le sous-groupe de $\mathfrak{S}_4$ composé des double-transpositions (produits de transpositions à supports disjoints) et 1.

1. Montrer que $D(\mathfrak{S}_4) \subset \mathfrak{A}_4$. *Correction : Découle du fait que $\mathfrak{S}_4/\mathfrak{A}_4 \simeq \mathbb{Z}/2\mathbb{Z}$ est abélien.*

2. Calculer les commutateurs $(1,2)(1,3)(1,2)^{-1}(1,3)^{-1}$ et $(1,2,3)(1,2,4)(1,2,3)^{-1}(1,2,4)^{-1}$.
Correction : On a $(12)(13)(12)(13) = (123)$ (on calcule les images successives) et $(123)(124)(132)(142) = (12)(34)$.

3. Montrer que $D(\mathfrak{S}_4) = \mathfrak{A}_4$. *Correction : 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. Montrer que $V \subset D(\mathfrak{A}_4)$. *Correction : Même argument.*

5. Vérifier que V est distingué dans $\mathfrak{A}_4$ et que le quotient $\mathfrak{A}_4/V$ est un groupe abélien. En déduire que $D(\mathfrak{A}_4) \subset V$. *Correction : $V \triangleleft \mathfrak{S}_4$ (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. En déduire $D^2(\mathfrak{S}_4)$. *Correction : On a montré $D(\mathfrak{A}_4) = V$ donc $D^2(\mathfrak{S}_4) = V$.*

7. Calculer les autres sous-groupes dérivés de $\mathfrak{S}_4$. *Correction : V est abélien donc $D(V) = \{1\} = D^i(\mathfrak{S}_4)$ pour $i \geqslant 3$.*

Exercice 9 (Transformations affines de la droite)

Soient k un corps et G l'ensemble des applications $f : k \to k$ de la forme $f(x) = ax + b$ avec $a, b \in k$, $a \neq 0$. Démontrez que G est un groupe résoluble. *Correction : Tout d'abord, l'ensemble G est bien un groupe : en particulier, si $f_{a,b}$ est l'application de l'énoncé alors $f_{a,b} \circ f_{a',b'} = f_{aa',b+ab'}$ (on voit donc que G est isomorphe à un produit semi-direct $k^\times \ltimes k$), ainsi $f_{a,b}$ est inversible et $f_{a,b}^{-1} = f_{a^{-1},-ba^{-1}}$. La formule de multiplication montre que $D(G)$ est inclus dans le sous-groupe K des translations (les $f_{1,b}$), or ce dernier est commutatif donc $D^2(G) = 1$ donc G est résoluble. (Voir aussi l'Exercice 18 sur le groupe triangulaire supérieur.)*

Exercice 10 (Théorème de Feit-Thompson)

Montrer que les assertions suivantes sont équivalentes :

1. Tout groupe d'ordre impair est résoluble.

2. Tout groupe fini simple non-abélien est d'ordre pair.

Le théorème de Feit-Thompson (1962) montre qu'elles sont vraies.

Correction : 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.

Actions de groupes

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

Exercice 11 (Centre d'un p-groupe)

Montrer que le centre d'un p-groupe n'est pas réduit à l'élément neutre.

Regardez la partition en orbites pour l'action de G par conjugaison sur lui-même.

Correction : 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 12 (Groupes d'ordre p^2 et p^3)

1. Montrer que si le quotient d'un groupe par son centre est cyclique alors le groupe est abélien, donc égal à son centre. *Correction : 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. Montrer qu'un groupe d'ordre p^2 est abélien. En déduire la liste des groupes d'ordre p^2. *Correction : 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. Soit G un groupe non abélien d'ordre p^3 et Z son centre. Montrez que :

   $$\text{(i) } Z \text{ est d'ordre } p, \qquad \text{(ii) } G/Z \simeq (\mathbb{Z}/p\mathbb{Z})^2, \qquad \text{(iii) } D(G) = Z.$$

   Correction : 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 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 $x_1 \cdots x_p = 1$.*

Correction : 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. *Correction : 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. Montrer que toute action d'un groupe d'ordre 143 sur un ensemble de cardinal 25 possède un point fixe. *Correction : 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 $x_1 \ldots, x_k \in X$ distincts et tout $y_1, \ldots, y_k \in X$ distincts, il existe $g \in G$ tel que $gx_i = y_i$ pour $i = 1, \ldots, k$.

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. *Correction : Faire des dessins !*

   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 $x_2, \ldots, x_k \in X$ (resp. $y_2, \ldots, y_k \in X$) 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 $x_2, \ldots, x_k, y_2, \ldots, y_k \in X_x$ avec $x_2, \ldots, x_k$ (resp. $y_2, \ldots, y_k$) 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 $x, x_2, \ldots, x_k$ (resp. $x, y_2, \ldots, y_k$) 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 $(x_2, \ldots, x_k)$ sur $(y_2, \ldots, y_k)$ 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 $x_1, \ldots, x_k \in X$ (resp. $y_1, \ldots, y_k \in X$) 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 $g \cdot (x_1, \ldots, x_k) = (y_1, gx_2, \ldots, gx_k)$ et $y_1, gx_2, \ldots, gx_k$ 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 $(x_1, \ldots, x_k)$ sur $(y_1, \ldots, y_k)$ ce qui montre que l'action de G sur X est k-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. *Correction : 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 $g_x x_2, \ldots, g_x x_k$ (resp. $g_y y_2, \ldots, g_y y_k$) 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 $(x_1, \ldots, x_k)$ sur $(y_1, \ldots, y_k)$.*

Produit semi-direct

Dans les deux exercices suivants, on utilisera librement les théorèmes de Sylow sur l'existence des sous-groupes de Sylow et les congruences classiques sur leur nombre.

Exercice 16 (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. *Correction : On rappelle que si $\#G = p^\alpha m$ avec $p \mid m$ alors $s_p \equiv 1 \pmod p$ et $s_p \mid m$. On trouve ici $s_q \mid p$ donc $s_q = 1$ ou p, mais puisque $s_q \equiv 1 \pmod q$ on en déduit que $s_q = 1, q+1, \ldots$, donc $s_q = 1$ puisque $1 < p < q$.*

2. En déduire que G est un produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$. *Correction : Soit Q l'unique q-Sylow de G. Par le théorème de Sylow il est distingué dans G (G agissant par conjugaison sur les Sylows de façon transitive), et si P est un p-Sylow alors nécessairement $P \cap Q = 1$ par Lagrange et $\#P\#Q = \#G$ donc $G \simeq Q \rtimes P$. On conclut puisqu'un groupe d'ordre premier r est isomorphe à $\mathbb{Z}/r\mathbb{Z}$ par Lagrange.*

3. Montrer que si $p \nmid q-1$ alors G est cyclique. *Correction : Dans ce cas $s_p \mid q$ donc $s_p = 1$ ou q, mais $s_p \equiv 1 \pmod p$ donc $p \mid s_p - 1$ donc $s_p \neq q$ donc $s_p = 1$. On conclut que P est distingué donc le produit semi-direct précédent est direct et on conclut par le théorème chinois.*

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.) *Correction : La réponse repose sur le lemme suivant.*

Lemme. *Soit $\phi : H \to \mathrm{Aut}(N)$ et $\alpha \in \mathrm{Aut}(H)$ deux morphismes. On a l'isomorphisme de groupes suivant :*

$$N \rtimes_{\phi\circ\alpha} H \simeq N \rtimes_{\phi} H,$$

un isomorphisme étant donné par $(n,h) \mapsto \big(n, \alpha(h)\big)$.

Puisque $p \mid q-1$, on peut écrire $q-1 = kp$ et donc si $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ (regarder l'image de 1 pour cet isomorphisme), on a nécessairement $q-1 \mid p\phi(1)$ et donc $k \mid \phi(1)$. Ainsi, on a $\phi(1) \in k\mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi, on peut noter $\phi = \phi_i$ où $i := \phi(1) \in \mathbb{Z}/p\mathbb{Z}$. On remarque que $\phi_i(n) = ikn = ink = \phi_1(in)$, donc $\phi_i = \phi_1 \circ \alpha_i$ où $\alpha_i : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est la multiplication par $i \in \mathbb{Z}/p\mathbb{Z}$. Si $i = 0$ alors $\phi_0 = \mathrm{id}_{\mathbb{Z}/q\mathbb{Z}}$ et le produit $\mathbb{Z}/p\mathbb{Z} \ltimes_{\phi_0} \mathbb{Z}/q\mathbb{Z}$ est direct (et cyclique), et sinon par le Lemme on trouve que $\mathbb{Z}/p\mathbb{Z} \ltimes_{\phi_i} \mathbb{Z}/q\mathbb{Z}$ est isomorphe au groupe obtenu pour $i = 1$ (puisque $\alpha_i \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ si $i \neq 0$). Pour conclure, il suffit de montrer que $\mathbb{Z}/p\mathbb{Z} \ltimes_{\phi_1} \mathbb{Z}/q\mathbb{Z}$ n'est pas abélien, en remarquant par exemple que $(b,1)\cdot(b',1) \neq (b',1)\cdot(b,1)$ pour $b \neq b' \in \mathbb{Z}/p\mathbb{Z}$.

Exercice 17 (Groupes finis résolubles)

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

Correction : 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. 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.*

Correction : 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. Soient p, q deux nombres premiers distincts. Montrer qu'un groupe de cardinal p^2q est toujours résoluble. *Correction : 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 $(q-1)p^2 = p^2q - p^2$ 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 18 (Groupe triangulaire supérieur)

1. Soit k un corps. Montrez que le groupe de Heisenberg $G = U_3(k)$ des matrices carrées triangulaires supérieures de taille 3 avec des 1 sur la diagonale est résoluble. *Correction : On a :*

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & z+z'+xy' \\ 0 & 1 & y+y' \\ 0 & 0 & 1 \end{pmatrix}.$$

Si $f : \begin{pmatrix} 1 & x & . \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mapsto (x, y)$ *alors on en déduit que* $f : G \to k^2$ *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* G *isomorphe à* k *avec* $G/k \simeq k^2$*. Puisque* k *et* k^2 *sont abéliens, ils sont résolubles donc* G *aussi. (On peut montrer de même que le groupe* T *de toutes les matrices triangulaires supérieures inversibles est résoluble, en considérant le morphisme* $\begin{pmatrix} x & . & . \\ 0 & y & . \\ 0 & 0 & z \end{pmatrix} \mapsto (x, y, z) \in k^{\times 3}$ *de noyau* G*. On trouve alors* $T/G \simeq k^{\times 3}$ *qui est résoluble donc* T *l'est (car* G *aussi).)*

2. On suppose désormais que $k = \mathbb{F}_3$. Montrez que tout élément $x \in G$ vérifie $x^3 = 1$ mais G n'est pas abélien. (On rappelle que si tout élément vérifie $x^2 = 1$, alors G est abélien. On ne peut donc pas remplacer 2 par 3 dans cet énoncé.) *Correction : Soit* $M \in G$*. Par définition la matrice* $M - I_3$ *est triangulaire supérieure de diagonale nulle donc* $(M - I_3)^3 = 0$*. On est sur* $\mathbb{F}_3$ *donc via le morphisme de Frobenius on trouve* $M^3 + (-I_3)^3 = 0$ *donc* $M^3 = I_3$*. Pour montrer que* G *n'est pas abélien, on écrit la formule complète d'un produit de deux éléments de* G*, où le coefficient de coin est* $xy' + z + z'$*. Le produit dans l'autre sens est* $x'y + z + z'$*, il suffit donc de prendre deux matrices avec* $xy' \neq x'y$*, par exemple :*

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

mais :

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

(et la preuve fonctionne sur n'importe quel corps).

3. Le groupe $G = U_3(\mathbb{F}_3)$ est-il un produit semi-direct ? *Correction : On aurait envie de considérer le sous-groupe* $N \coloneqq \begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *de* G *est distingué (par la question 1) et isomorphe à* k*, avec le sous-groupe* H *des matrices de la forme* $\begin{pmatrix} 1 & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$*. Ces sous-groupes vérifient* $\#H\#N = \#G$ *et il est immédiat que* $H \cap N = 1$ *donc* $G \simeq H \ltimes N \simeq k^2 \ltimes k$*. (Remarque : on a* $\#(HN) = \#H\#N$ *par l'exo 1.3 donc on a bien* $\#(HN) = \#G$ *donc* $HN = G$*.) Le seul problème est que le sous-groupe* H *n'est pas un sous-groupe !*

On doit alors changer de sous-groupe N*. On peut prendre* $N = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$*, qui est bien un sous-groupe distingué par la formule de la question 1, et pour* H *on n'a pas le choix de prendre* $H = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ *(qui est bien un sous-groupe par la formule de la question 1) ! On a bien* $H \cap N = \{1\}$ *et* $\#H\#N = \#G$ *donc* $G = N \rtimes H$*.*

Exercice 19 (Holomorphe d'un groupe)

On appelle *holomorphe* d'un groupe de G le produit semi-direct $\mathrm{Hol}(G) = G \rtimes_\varphi \mathrm{Aut}(G)$ défini par l'action tautologique $\varphi = \mathrm{Id} : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$ de $\mathrm{Aut}(G)$ sur G. Écrivez les formules décrivant le produit et l'inverse dans $\mathrm{Hol}(G)$. *Correction : On rappelle la formule générale pour* $N \rtimes_\phi H$ *(avec* $\phi : H \to \mathrm{Aut}(N)$*) :*

$$(n, h) \odot (n', h') \coloneqq (n\phi_h(n'), hh').$$

Pour $g, h \in G$ *et* $\alpha, \beta \in \mathrm{Aut}(G)$ *on a* $(g, \alpha)(h, \beta) = \big(g\alpha(h), \alpha\beta\big)$ *dans* $\mathrm{Hol}(G)$ *et* $(g, \alpha)^{-1} = \big(\alpha^{-1}(g^{-1}), \alpha^{-1}\big)$*.*

Exercice 20 (Sur-groupes et conjugaisons)

1. Soient G un groupe et $f : G \to G$ un automorphisme. Montrez qu'il existe un sur-groupe $G' \supset G$ tel que f est la restriction à G d'un automorphisme intérieur (ou conjugaison) de G'.

On pourra prendre pour G' *l'holomorphe* $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$*.*

Correction : On prend $G' = \mathrm{Hol}(G)$ *comme suggéré. Soit* $f \in \mathrm{Aut}(G)$ *et* $g \in G$*. L'élément* $g \in G$ *s'identifie à l'élément* $(g, 1) \in G'$ *(avec le* 1 *de droite étant* id_G*). On a* $\big(f(g), 1\big) = (1, f)(g, 1)(1, f)^{-1}$*, en effet d'après l'exercice précédent on a*

$(1,f)^{-1} = (1, f^{-1})$ *puis* $(1,f)(g,1) = \big(f(g), f)\big)$ *et*

$$(1,f)(g,1)(1,f)^{-1} = \big(f(g),f)\big)(1,f^{-1}) = \big(f(g)f(1),1\big) = \big(f(g),1\big),$$

qui s'identifie bien à $f(g) \in G$. *On a donc montré que la restriction à* G *de l'automorphisme intérieur donné par la conjugaison par* $(1,f)$ *dans* G *coïncide avec* f.

2. Soient G un groupe fini et $x, y \in G$ deux éléments de même ordre. Montrez qu'il existe un sur-groupe $G' \supset G$ tel que x et y sont conjugués dans G'.

On pourra prendre pour G' *le groupe symétrique* $\mathfrak{S}_G$.

Correction : Soit x' *l'image de* x *dans* G', *c'est-à-dire la multiplication à gauche par* x. *Par hypothèse, pour tout élément* $g \in G$ *on a* $x'^n g = g$, *et en fait la décomposition en cycles à supports disjoints de* x' *ne contient que des* n*-cycles. C'est la même chose pour* y' *donc* x' *et* y' *sont conjugués dans* G'.

Exercice 21 (Automorphismes du groupe diédral)

Soit $n \geq 3$ et $\mathbb{D}_n$ le groupe diédral engendré par deux élements r, s satisfaisant les relations $r^n = s^2 = (rs)^2 = 1$.

1. On rappelle que tout élément $x \in \mathbb{D}_n$ peut s'écrire d'une unique manière sous la forme $x = s^\epsilon r^i$ avec $\epsilon \in \{0,1\}$ et $i \in \mathbb{Z}/n\mathbb{Z}$. Montrez que le produit de $x = s^\epsilon r^i$ avec $y = s^\eta r^j$ est donné par la formule $xy = s^{\epsilon+\eta} r^{(1-2\eta)i+j}$. *Correction : Puisque* $(rs)^2 = 1$ *on a* $rs = (rs)^{-1} = sr^{-1}$. *On en déduit donc que, si* $\eta = 1$,

$$\begin{aligned} xy &= s^\epsilon r^i s r^j \\ &= s^\epsilon r \dots r s r^j \\ &= s^\epsilon s r^{-1} \dots r^{-1} r^j \\ &= s^{\epsilon+1} r^{-i+j} \\ &= s^{\epsilon+\eta} r^{(1-2\eta)i+j}. \end{aligned}$$

Si $\eta = 0$ *on a* $xy = s^\epsilon r^{i+j} = s^{\epsilon+\eta} r^{(1-2\eta)i+j}$ *également.*

2. Montrez que pour tout morphisme de groupes $f : \mathbb{D}_n \to H$, les éléments $R = f(r)$ et $S = f(s)$ vérifient les relations $R^n = S^2 = (RS)^2 = 1$. Réciproquement montrez que pour tout couple $(R,S) \in H^2$ tel que $R^n = S^2 = (RS)^2 = 1$ il existe un unique morphisme de groupes $f : \mathbb{D}_n \to H$ tel que $f(r) = R$ et $f(s) = S$. *Correction : La première assertion vient directement du fait que* f *est un morphisme. Pour la réciproque, on considère l'application* $f : \mathbb{D}_n \to H$ *donnée par* $s^\epsilon r^i \mapsto S^\epsilon R^i$ *(l'application* f *est bien définie par unicité de l'écriture, cf. rappel dans la question 1). Comme en question* 1, *on a* $(S^\epsilon R^i)(S^\eta R^j) = S^{\epsilon+\eta} R^{(1-2\eta)i+j}$, *ce qui montre que* f *est un morphisme puisque :*

$$\begin{aligned} f(s^\epsilon r^i \cdot s^\eta r^j) &= f(s^{\epsilon+\eta} r^{(1-2\eta)i+j}) \\ &= S^{\epsilon+\eta} R^{(1-2\eta)i+j} \\ &= (S^\epsilon R^i)(S^\eta R^j) \\ &= f(s^\epsilon r^i) f(s^\eta r^j). \end{aligned}$$

3. Déduisez de la question précédente que les automorphismes $f : \mathbb{D}_n \to \mathbb{D}_n$ sont les morphismes $f = f_{i,j}$ déterminés par $f(r) = r^i$ et $f(s) = sr^j$, pour $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $j \in \mathbb{Z}/n\mathbb{Z}$. *Correction : Vérifions d'abord que les applications proposées sont bien des automorphismes. Tout d'abord, ce sont bien des morphismes par la question précédente puisque* $(r^i)^n = 1$, *que* $(sr^j)^2 = sr^j sr^j = ssr^{-j} r^j = 1$ *et* $(r^i sr^j)^2 = (sr^{j-i})^2 = sr^{j-i} sr^{j-i} = ssr^{i-j} r^{j-i} = 1$. *On peut maintenant prouver que* $f_{i,j}$ *est surjectif, ce qui conclura : l'élément* $s^\epsilon r^k$ *est l'image de* $s^\epsilon r^{(k-j\epsilon)i^{-1}}$ *(on rappelle que* i *est inversible dans* $\mathbb{Z}/n\mathbb{Z}$*) puisque :*

$$\begin{aligned} f_{i,j}(s^\epsilon r^{(k-j\epsilon)i^{-1}}) &= f_{i,j}(s^\epsilon) f(r^{(k-j\epsilon)i^{-1}}) \\ &= (s^\epsilon r^{j\epsilon}) r^{k-j\epsilon} \\ &= s^\epsilon r^k. \end{aligned}$$

Montrons maintenant que tout automorphisme est de la forme $f_{i,j}$. *Soit* $f \in \mathrm{Aut}(\mathbb{D}_n)$. *Rappelons que dans* $\mathbb{D}_n$, *les éléments de la forme* sr^j *sont tous d'ordre* 2 *(les autres éléments étant de la forme* r^i*). Ainsi, puisque* $f(s)$ *est d'ordre* 2 *on sait que* $f(s) = sr^j$ *pour un certain* $j \in \mathbb{Z}/n\mathbb{Z}$. *De plus on sait que* $f(r)$ *est d'ordre* $n \geqslant 3$ *donc est nécessairement de la forme* r^i *pour* $i \in \mathbb{Z}/n\mathbb{Z}$. *Puisque* r *est d'ordre* n, *on a donc* $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. *On a donc montré que* $f = f_{i,j}$.

4. Montrez que $\mathrm{Aut}(\mathbb{D}_n)$ est l'holomorphe de $\mathbb{Z}/n\mathbb{Z}$.

On pourra montrer que $\mathrm{Aut}(\mathbb{D}_n) = N \rtimes H$ *avec* $N = \{f_{1,j};\, j \in \mathbb{Z}/n\mathbb{Z}\}$ *et* $H := \{f_{i,0};\, i \in (\mathbb{Z}/n\mathbb{Z})^\times\}$.

Correction : Écrivons tout d'abord la règle de multiplication dans $\mathrm{Aut}(\mathbb{D}_n)$. *On a :*

$$f_{i,j} f_{i',j'}(r) = f_{i,j}(r^{i'}) = r^{ii'},$$

et :

$$\begin{aligned} f_{i,j}f_{i',j'}(s) &= f_{i,j}(sr^{j'}) \\ &= f_{i,j}(s)f_{i,j}(r^{j'}) \\ &= sr^{j}r^{ij'} \\ &= sr^{j+ij'}, \end{aligned}$$

donc :

$$f_{i,j}f_{i',j'} = f_{ii',j+ij'}.$$

On « voit » donc la structure de produit semi-direct $(\mathbb{Z}/n\mathbb{Z})^\times \ltimes_\phi \mathbb{Z}/n\mathbb{Z}$, où $(\mathbb{Z}/n\mathbb{Z})^\times$ agit sur $\mathbb{Z}/n\mathbb{Z}$ par multiplication. On peut aussi constater que la formule du produit ci-dessus montre que les conditions nécessaires du cours sont bien satisfaites, à savoir :

- *N et H sont bien des sous-groupes de $\mathrm{Aut}(\mathbb{D}_n)$ avec N distingué dans $\mathrm{Aut}(\mathbb{D}_n)$;*
- *$NH = \mathrm{Aut}(\mathbb{D}_n)$ puisque $f_{i,j} = f_{1,j}f_{i,0}$;*

et on conclut que $N \rtimes H \simeq \mathrm{Aut}(\mathbb{D}_n)$ puisque $N \cap H = \{f_{1,0}\} = \mathrm{id}_{\mathbb{D}_n}$.

Exercice 22 (Ordre du produit de deux éléments)

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 le sous-groupe engendré par x et y est isomorphe au produit direct $\langle x\rangle \times \langle y\rangle$ et que xy est d'ordre mn. *Correction : On considère l'application $f : \langle x\rangle\times\rangle \times \langle y\rangle \to \langle x, y\rangle$ donnée par $(x^i, y^j) \mapsto x^iy^j$. Cette application est un morphisme surjectif par commutativité de x et y, et si $(x^i, y^j) \in \ker f$ alors $x^iy^j = 1$ donc $x^i = y^{-j} \in \langle x\rangle \cap \langle y\rangle = \langle 1\rangle$ par Lagrange, puisque m et n sont premiers entre eux, donc $x^i = y^j = 1$. On en déduit donc l'isomorphisme. Finalement, l'image inverse de xy est (x, y) donc ces éléments ont le même ordre. Si $(x, y)^i = 1$ alors $x^i = 1$ et $y^i = 1$ donc $m \mid i$ et $n \mid i$ donc $mn \mid i$ par Lagrange. Puisque $(x, y)^{mn} = (1, 1)$ on conclut.*
2. Peut-on étendre le résultat sur l'ordre au cas où m et n ne sont pas premiers entre eux ? *Correction : Non, puisque avec $y \coloneqq x^{-1}$ les éléments x et y commutent mais xy est d'ordre 1.*
3. Peut-on étendre le résultat sur l'ordre au cas où x et y ne commutent pas ? *Correction : Dans $G \coloneqq \mathfrak{S}_3$, les éléments $x \coloneqq (1, 2)$ et $y \coloneqq (1, 2, 3)$ ont des ordres (2 et 3 respectivement) premiers entre eux mais $xy = (1, 2)(1, 2, 3) = (2, 3)$ est d'ordre 2 (qui n'est ni le produit ni le ppcm). Cela montre en outre que x et y ne commutent pas, en fait on a même $yx = (1, 2, 3)(1, 2) = (1, 3)$. (Remarquons que dans un groupe, gh et hg ont toujours le même ordre car ces élément sont conjugués puisque $hg = h(gh)h^{-1}$.)*

Groupes symétriques et alternés

Exercice 23 ($\mathfrak{A}_4$ 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 $g^2 \in H$. *Correction : L'ordre de $\mathfrak{A}_4$ est $\frac{4!}{2} = 4 \cdot 3 = 12$. Ainsi, le sous-groupe H est d'indice 2 dans $\mathfrak{A}_4$ donc est distingué et $\mathfrak{A}_4/H \simeq \mathbb{Z}/2\mathbb{Z}$. Ainsi, pour $g \in \mathfrak{A}_4$ l'image de g^2 par la surjection canonique est nécessairement 0 donc $g^2 \in H$.*
2. En déduire que H contient tous les 3-cycles. *Correction : On a $(a, b, c) = (a, c, b)^2 (= (a, c, b)^{-1})$.*
3. Conclure (éventuellement de deux manières...). *Correction : On peut dire qu'alors $H = \mathfrak{A}_4$ puisque $\mathfrak{A}_n$ est engendré par les 3-cycles. On peut aussi dire que $\mathfrak{A}_4$ contient $2 \times \binom{4}{1} = 8$ éléments qui sont des 3-cycles donc $\#H \geqslant 8$ ce qui est absurde.*

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

Exercice 24 (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. *Correction : Les transpositions sont toutes conjuguées dans $\mathfrak{S}_n$ et ainsi ont toutes la même image puisque $\{\pm 1\}$ est abélien. Puisque $\mathfrak{S}_n$ est engendré par les transpositions, on en déduit que si leur image commune est 1 alors f est constante, et est la signature sinon (puisque f et la signature coïncident alors sur les transpositions).*
2. Soit G d'indice 2 dans $\mathfrak{S}_n$. Démontrer que G est distingué puis que $G = \mathfrak{A}_n$. *Correction : Le sous-groupe G est distingué puisque d'indice 2, ainsi $\mathfrak{S}_n/G \simeq \mathbb{Z}/2\mathbb{Z} \simeq \{\pm 1\}$. La surjection canonique est un morphisme non constant donc c'est la signature par la question précédente, donc le noyau est $G = \mathfrak{A}_n$.*

Exercice 25 (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 $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$. *Correction : $H \cap \mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$ donc dans $\mathfrak{A}_n$. Puisque $n \neq 4$ on en déduit que $H \cap \mathfrak{A}_n = 1$ ou $H \cap \mathfrak{A}_n = \mathfrak{A}_n$ i.e. $H \supseteq \mathfrak{A}_n$.*

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 $H = \{\mathrm{Id}\}$. *Correction : Le noyau de la restriction est justement $H \cap \mathfrak{A}_n$ donc cette restriction est bien injective. On en déduit donc que $\#H \leqslant 2$. Si $\#H = 2$, soit h l'unique élément non trivial de H. Puisque H est distingué dans $\mathfrak{S}_n$ on en déduit que h est dans le centre de $\mathfrak{S}_n$ (car la conjugaison conserve l'ordre) donc $h = 1$.*

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 $\mathfrak{S}_n$. *Correction : Par Lagrange on a $n! = k\#H$ pour $k \geqslant 1$. Puisque $\mathfrak{A}_n \subseteq H$ on a $\frac{n!}{2} \leqslant \frac{n!}{k}$ donc $k \leqslant 2$. On a donc $k \in \{1, 2\}$ et on conclut par égalité des cardinaux.*

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