104 : Groupes finis. Exemples et applications.

Dans toute la leçon, G désigne un groupe fini de neutre 1_G ou simplement 1 s'il n'y a pas d'ambiguïté.

I - Généralités sur les groupes finis

(1) Ordre d'un élément, ordre d'un sous-groupe

Déf 1 : L'ordre d'un sous-groupe $H \subset G$ est son cardinal, et l'ordre d'un élément $x \in G$ est l'ordre du sous-groupe $\langle x \rangle \subset G$ qu'il engendre, on les note $o(H)$ et $o(x)$.

Prop 2 : Soit $x \in G$. Alors $o(x) = \min\{n \geq 1 \mid x^n = 1\}$

Prop 3 : Soit $x, y \in G$ tels que $xy = yx$. Alors :
- (1) $\forall k \geq 1$, $o(x^k) = o(x)/o(x) \wedge k$.
- (2) $\langle x \rangle \cap \langle y \rangle = \{1\} \Rightarrow o(xy) = \text{ppcm}(o(x), o(y))$
- (3) $o(x) \wedge o(y) = 1 \Rightarrow o(xy) = o(x)o(y)$

Déf 4 : Soit $H \subset G$ un sous-groupe. On définit sur G une relation d'équivalence par : $\forall x, y \in G$, $x \mathcal{R} y \Leftrightarrow x^{-1}y \in H$. Les classes d'équivalences sont appelées les classes à gauche modulo H, et on note $G/H = G/\mathcal{R}$, et $[G:H] = |G/H|$ l'indice de H.

Th 5 (Lagrange) : Soit $H \subset G$ un sous-groupe. Alors $o(G) = o(H) \times [G:H]$. En particulier $o(H) \mid o(G)$.

Cor 6 : Soit $K \subset H \subset G$ des groupes finis. Alors
$$[G:K] = [G:H][H:K]$$

Cor 7 : Soit $x \in G$. Alors $o(x) \mid o(G)$, et donc
$$\forall x \in G,\ x^{|G|} = 1_G.$$

Rq 8 : L'ensemble G/H n'est en général pas un groupe.

Déf 9 : On dit qu'un sous-groupe $H \subset G$ est distingué dans G, et on note $H \lhd G$, si $\forall x \in G$, $xH = Hx$.

Prop 10 : Si $H \lhd G$, alors G/H est un groupe pour $(xH)\cdot(yH) = (xy)H$

Prop 11 : Si $H \subset G$ est un sous-groupe d'indice 2, alors $H \lhd G$.

Ex 12 : Le centre $Z(G) = \{x \in G \mid \forall y \in G,\ xy = yx\}$ est distingué dans G.
Le groupe dérivé $D(G) = \langle ghg^{-1}h^{-1},\ g,h \in G \rangle$ est distingué dans G et $G/D(G)$ est toujours commutatif.

Rq 13 : L'intérêt des groupes quotients est par exemple de rendre des morphismes bijectifs : si $\varphi : G \to H$ est un morphisme, alors on a l'isomorphisme $G/\ker\varphi \simeq \text{Im}\,\varphi$.

(2) Actions de groupes

Déf 14 : On dit que G agit sur un ensemble X si on dispose d'un morphisme φ de G dans S_X (les bijections de X dans X). On note alors pour tout $g \in G$ et tout $x \in X$, $g \cdot x = \varphi(g)(x)$.

Ex 15 : G agit sur lui-même par translation à gauche :
$$\forall g,h \in G,\ g \cdot h = gh,$$
ou par conjugaison :
$$\forall g,h \in G,\ g \cdot h = ghg^{-1}.$$
Le groupe S_n agit sur $[\![1,n]\!]$ "naturellement" par
$$\forall \sigma \in S_n,\ \forall i \in [\![1,n]\!],\ \sigma \cdot i = \sigma(i).$$

Th 16 (Cayley) : Il existe $n \geq 1$ tel que G soit isomorphe à un sous-groupe de S_n.

Déf 17 : Soit G agissant sur un ensemble X et $x \in X$. On définit l'orbite de x comme $\text{Orb}\,x = \{g \cdot x \mid g \in G\} \subset X$, et son stabilisateur $\text{Stab}\,x = \{g \in G \mid g \cdot x = x\} \subset G$.

Prop 18 : $\text{Stab}\,x$ est un sous-groupe de G et on dispose d'une bijection entre les ensembles $G/\text{Stab}(x)$ et $\text{Orb}(x)$.

Prop 19 : La relation définie sur X par $\forall x, y \in X$,
$$x \mathcal{R} y \Leftrightarrow y \in \text{Orb}\,x$$
est une relation d'équivalence dont les classes d'équivalences sont les orbites sous l'action de G.

Th 20 : (Équations aux classes)
Soit G agissant sur X fini, et Ω l'ensemble des orbites de cette action. Alors $|X| = \sum_{\omega \in \Omega} |\omega|$.

Rq21: On peut déjà appliquer ces notions pour démontrer des résultats intéressants, qui prolongent les points 11 et 7.

Th22: (Frobenius) Soit $H \subset G$ un sous-groupe d'indice le plus petit nombre premier divisant $|G|$. Alors $H \lhd G$.

Th23: (Cauchy) Si p est un nombre premier divisant $|G|$, alors il existe $x \in G$ d'ordre p.

3) p-Groupes

Déf24: G est appelé un p-groupe si $|G|$ est une puissance de p, p étant un nombre premier.

Prop25: Si G est un p-groupe, alors $Z(G) \neq \{1_G\}$.

Prop26: (1) Si G est d'ordre p, alors G est cyclique.
(2) Si G est d'ordre p^2, alors G est commutatif.

Rq27: L'exemple du sous-groupe de $GL_3(\mathbb{F}_p)$ constitué des matrices unipotentes montre qu'il existe des groupes d'ordre p^3 non commutatifs.

Déf28: Un p-Sylow de G est un sous-groupe $S \subset G$ qui est un p-groupe maximal, i.e. tel que $p \nmid [G:S]$.

Ex29: Évidemment, cette notion n'a d'intérêt que quand $p \mid |G|$. L'exemple 27 nous fournit un p-Sylow de $GL_3(\mathbb{F}_p)$ (cela marche pour $n \geq 3$ quelconque)

Déf29: On note $Syl_p(G)$ l'ensemble des p-Sylows de G et $n_p(G) = |Syl_p(G)|$.

Th30: (Sylow) On suppose $p \mid |G|$. DEV1
Alors: (1) $n_p(G) \equiv 1 [p]$; en particulier $n_p(G) \neq 0$.
(2) Si $S, S' \in Syl_p(G)$, alors il existe $g \in G$ tel que $S' = gSg^{-1}$
(3) $n_p(G) \mid [G:S]$ où $S \in Syl_p(G)$

Ex31: Tout groupe d'ordre 33 est cyclique.
Tout groupe d'ordre 63 est simple.

II - Groupes abéliens finis.

1) Groupes cycliques

Th32: Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Th33: Supposons G cyclique d'ordre n.
Alors: Pour tout diviseur d de n, il existe un unique sous-groupe $H \subset G$ d'ordre d.

Cor34: Sous les mêmes hypothèses, il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

Rq35: Le point 33 fournit une réciproque partielle du théorème de Lagrange.

2) Exposant d'un groupe

Déf36: On définit l'exposant de G comme $\exp G := \min\{n \geq 1 \mid \forall x \in G, x^n = 1\}$.

Prop37: $\exp G = \operatorname{ppcm}_{x \in G} o(x)$.

Prop38: Si G est commutatif, il existe $x \in G$ d'ordre $\exp G$.

Cor39: Si G est commutatif, alors $\exp G = G$ ssi G est cyclique.

Th40: Soit K un corps et $G \subset K^*$ un sous-groupe fini. Alors G est cyclique.

Ex41: $\mathbb{F}_q^*$ est cyclique, et donc $\mathbb{F}_q = \mathbb{F}_p[\alpha]$ pour un $\alpha \in \mathbb{F}_q^*$.

3) Structure des groupes abéliens

Déf 43 : Un caractère linéaire de G est un morphisme $\chi : G \to \mathbb{C}^*$. On note $\hat{G}$ l'ensemble de ces morphismes.

Rq 43 : C'est l'analogue du dual dans les espaces vectoriels.

Prop 44 : Si $H \subset G$ est un sous-groupe et $\chi \in \hat{H}$, alors il existe $\tilde{\chi} \in \hat{G}$ tel que $\tilde{\chi}_{|H} = \chi$. (G commutatif) DEV 2

Th 45 : Soit G un groupe abélien fini. Alors il existe une suite $d_r \mid d_{r-1} \mid \dots \mid d_1 = \exp G$ telle que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$

Rq 46 : La théorie des modules permet de montrer l'unicité, mais le théorème des restes chinois permet de se satisfaire de cet énoncé.

III - Le groupe symétrique

1) Décomposition en cycles

Déf 47 : Un cycle de S_n est une permutation qui n'a qu'une seule orbite non triviale quand on la fait agir naturellement sur $[\![1,n]\!]$.

Déf 48 : Le support de $\sigma \in S_n$ est l'ensemble $\mathrm{Supp}\,\sigma = \{i \in [\![1,n]\!] \mid \sigma(i) \neq i\}$.

Prop 49 : Si $\sigma, \tau \in S_n$ sont telles que $\mathrm{Supp}\,\sigma \cap \mathrm{Supp}\,\tau = \emptyset$, alors $\sigma\tau = \tau\sigma$.

Th 50 : Toute permutation s'écrit de manière unique comme un produit de cycles à support disjoints.

Cor 51 : S_n est engendrés par les cycles, mais également par les transpositions.

Cor 52 : Si $\sigma \in S_n$ s'écrit en produit de cycles $\sigma = c_1 \dots c_k$, alors $o(\sigma) = \mathrm{ppcm}(o(c_1), \dots, o(c_k))$.

2) Signature, groupe alterné

Prop 53 : Il existe un unique morphisme $S_n \to \mathbb{C}^*$ non trivial, noté ε et appelé signature.

Déf 54 : Le groupe alterné A_n est défini comme le noyau de la signature sur S_n.

Prop 55 : $A_n \lhd S_n$ et $[S_n : A_n] = 2$.

Prop 56 : Si $\sigma = (i_1, \dots, i_k)$ est un k-cycle, alors $\varepsilon(\sigma) = (-1)^{k-1}$

Prop 57 : A_n est engendré par les 3-cycles, et pour $n \geq 5$ ils sont tous conjugués dans A_n.

Rq 58 : C'est faux pour $n=4$, $(1,2,3)$ et $(1,3,2)$ n'y sont pas conjugués.

Th 59 : Pour $n \geq 5$, A_n est simple.

Prop 60 : A_5 est l'unique groupe simple à 60 éléments.

Prop 61 : Les sous-groupes distingués de S_n sont S_n, A_n et $\{1\}$.

IV - Le groupe diédral

Déf 62 : Un groupe G est dit diédral de type n s'il est engendré par deux éléments ρ et σ vérifiant : ρ d'ordre $n \geq 1$, σ d'ordre 2, $\sigma\rho$ d'ordre 2.

Th 63 : Si G est diédral de type n avec $G = \langle \rho, \sigma \rangle$, alors $G = \{1_G, \rho, \dots, \rho^{n-1}, \sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$ et donc il y a unicité à isomorphisme près des groupes diédraux de type n, on les note D_n.

Th 64 : Si $\Gamma_n = \{e^{2ik\pi/n}, k \in [\![0, n-1]\!]\}$, alors le groupe $G = \{u \in O_2(\mathbb{R}) \mid u(\Gamma_n) = \Gamma_n\}$ est diédral de type n.

ANNEXE: Classification des groupes finis jusqu'à l'ordre 8.

1	2	3	4	5	6	7	8
$\{1\}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$; $\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$; S_3	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, H_8

Tirage :
— 104 : Groupes finis. Exemples et applications. **(Choisie)**
— 155 : Exponentielle de matrices. Applications.

Développements proposés :
— Théorèmes de Sylow **(Choisi par le jury)**
— Structure des groupes abéliens finis

Petite trace écrite du développement[1] :
Soit G un groupe fini d'ordre mp^s où p premier ne divise pas m. On note $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylow de G et $n_p(G) = |\mathrm{Syl}_p(G)|$. Le but de ce développement est de montrer que :

1. $n_p \equiv 1\ [p]$ donc en particulier $\mathrm{Syl}_p(G) \neq \emptyset$
2. $\forall S, S' \in \mathrm{Syl}_p(G),\ \exists g \in G,\ S' = gSg^{-1}$
3. $n_p \mid m$

Preuve du premier point. On fait agir G sur l'ensemble X de ses parties à p^s éléments par translation à gauche, i.e. $g \cdot A := gA = \{ga \mid a \in A\}$.
Soit $A \in X$. Étudions son stabilisateur $\mathrm{Stab}(A) = \{g \in G \mid gA = A\}$. Soit $a \in A$ fixé. On considère l'application

$$\begin{aligned} i_a : \mathrm{Stab}(A) &\to A \\ g &\mapsto ga \end{aligned}$$

qui est injective, ce qui implique que $|\mathrm{Stab}(A)| \leq |A| = p^s$. Intéressons nous au cas d'égalité, ce qui est naturel puisque si $|\mathrm{Stab}(A)| = p^s$, alors $\mathrm{Stab}(A)$ est un p-Sylow de G.
Plus précisément, on montre que $|\mathrm{Stab}(A)| = p^s$ si et seulement si $A = Sx$ pour S un p-Sylow de G et $x \in G$. Le sens direct est facile puisque dans ce cas on a i_a surjective et donc $A = \mathrm{Stab}(A)\, a$. Pour l'autre sens, **je ne me souviens plus** comment le prouver et je décide de le passer.
En étudiant l'équation aux classes, on obtient[2] que $n_p \equiv 1\ [p]$.

1. Je suis un peu obligé sinon il n'est pas trop possible de comprendre une partie des questions.
2. Je passe les détails parce que je n'ai pas eu de question sur cette partie du développement.

Preuve du deuxième point. Soit $S, H \in \mathrm{Syl}_p(G)$. On note $Y = \mathrm{Orb}_G(S)$ et on s'intéresse à l'action de H par translation à gauche sur Y. L'équation aux classes s'écrit

$$m = |Y| = \sum_{\omega \in \Omega_H} |\omega|$$

si on note Ω_H l'ensemble des orbites sous l'action de H. On passe modulo p et on obtient qu'il existe une orbite $\omega \in \Omega_H$ telle que $|\omega| \not\equiv 0\ [p]$, puis $\omega = xS$ pour un $x \in G$ et en remarquant que $H = \mathrm{Stab}_H(xS)$ on obtient $H \subset xSx^{-1}$ puis l'égalité.

Preuve de troisième point. Se déduit rapidement de l'équation aux classes de l'action de G par conjugaison sur $\mathrm{Syl}_p(G)$.

Questions sur le développement :

1. Preuve du point que j'ai laissé en suspens dans mon développement (dans le premier point, en gras).

   Je continue à bloquer puis finis par me rappeler qu'il suffit de montrer que $S \subset \mathrm{Stab}(A)$ pour avoir l'égalité pour raison de cardinaux. Pour montrer cela il faut écrire que pour tout $s \in S$, $sA = sSx = Sx = A$.

2. Dans le deuxième point, pourquoi $|Y| = m$?

   C'est parce que $|\mathrm{Stab}_G(S)| = p^s$ car on a toujours $|\mathrm{Stab}_G(S)| \leq |S|$ et S est un groupe donc $S \subset \mathrm{Stab}_G(S)$. On obtient alors que $|Y| = |\mathrm{Orb}_G(S)| = \frac{|G|}{|\mathrm{Stab}_G(S)|} = m$.

Questions autour de la théorie de Sylow :

1. Montrer que le centre d'un p-groupe est non trivial.

   On fait agir le groupe sur lui-même par conjugaison et l'équation aux classes s'écrit $p^s = |G| = \sum_{i \in I} |\mathrm{Orb}(x_i)| = |Z(G)| + \sum_{x_i \notin Z(G)} |\mathrm{Orb}(x_i)|$. L'idée est de passer modulo p.[3]

2. Donner un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$

   L'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale convient.

3. Le jury m'a interrompu à ce moment en me disant qu'ils étaient convaincus.

3. Pourquoi c'est bien un p-Sylow ? Quel est le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$?

   Compter le nombre d'éléments de $\mathrm{GL}_n(\mathbb{F}_p)$ *revient à compter le nombre de bases de* $\mathbb{F}_p^n$*, i.e. de famille libre à* n *éléments. Pour le premier vecteur on a tous les vecteurs possibles sauf* 0*, soit* $p^n - 1$ *vecteurs. Pour le deuxième il faut et il suffit qu'il ne soit pas colinéaire au premier, on a donc* $p^n - p$ *choix. Pour le troisième on a par le même raisonnement* $p^n - p^2$ *choix, etc, jusqu'à obtenir que*

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \times ...(p^n - p^{n-1}) = p^{n(n-1)/2} \times m$$

   avec p *ne divisant pas* m*. Le groupe mentionné plus haut est donc de bon cardinal pour être un* p*-Sylow de* $\mathrm{GL}_n(\mathbb{F}_p)$*.*

4. Combien y a-t-il de 5-Sylow dans $\mathfrak{S}_7$?

   On commence par écrire $|\mathfrak{S}_7| = 7! = 7 \times 5 \times 3^2 \times 2^4$*. Je commence par regarder ce que donne les relations du théorème de Sylow, sans résultat. On me fait ensuite remarquer que les* 5*-Sylows sont d'ordre* 5*. Ils sont donc cycliques, engendrés par des éléments d'ordre* 5*, or dans* $\mathfrak{S}_7$ *seuls les* 5*-cycles sont d'ordre* 5*. On me fait remarquer que dans* $\mathfrak{S}_{10}$ *par exemple il y aurait aussi les produits de* 5*-cycles. La question est donc une question de dénombrement, en l'occurence des* 5*-cycles dans* $\mathfrak{S}_7$*. J'essaie de les compter "à la main" sans grand succès. Le jury me dit d'admettre le résultat et me demande comment en déduire la réponse à la question initiale. La réponse est qu'il faut diviser le nombre de* 5*-cycles par* 4 *car il y a* 4 5*-cycles différents dans chaque* 5*-Sylow.*

   Interlude : Comment compter les k-cycles dans $\mathfrak{S}_n$? On commence par se donner un support, il y a $\binom{n}{k}$ choix. Notons $(i_1, ..., i_k)$ un support possible. Compter les k-cycles à support $(i_1, ..., i_k)$ dans $\mathfrak{S}_n$ revient à compter les k-cycles dans $\mathfrak{S}_k$, par le biais de la bijection entre $\{1, ..., k\}$ et $\{i_1, .., i_k\}$ qui envoie j sur i_j. Ensuite, il y a $(k-1)!$ k-cycles dans $\mathfrak{S}_k$ car quand on a fixé l'image de 1 on permute les autres éléments de $[|1, k|]$ comme on veut. Il y a donc $(k-1)!$ éléments de $\mathfrak{S}_k$ qui sont des k-cycles, et donc $(k-1)!\binom{n}{k}$ k-cycles dans $\mathfrak{S}_n$.

Questions sur les groupes abéliens finis :

Commençons par un peu de contexte (présent dans mon plan). Si G est un groupe fini, on appelle *caractère linéaire* de G un morphisme de groupes

de G dans $\mathbb{C}^*$, et on apelle groupe dual de G, noté $\widehat{G}$, l'ensemble de ses caractères linéaires. C'est bien un groupe pour la multiplication des applications : $\chi_1.\chi_2(g) := \chi_1(g) \times \chi_2(g)$. C'est l'analogue du dual pour les espaces vectoriels.

1. D'où tirent leur nom les caractères linéaires ?

   Cette terminologie vient du fait que si on fait agir un groupe fini G de manière linéaire sur un espace vectoriel E, on obtient un morphisme $\rho : G \to \mathrm{GL}(E)$. On appelle caractère de ρ l'application $\chi_\rho : g \mapsto \mathrm{Tr}(\rho(g))$ Dans le cas où E est de dimension 1, on a que $\mathrm{GL}(E)\mathbb{C}^*$, et $\chi_\rho = \rho$, donc dans ce cas χ_ρ est un morphisme de G dans $\mathbb{C}^*$.

2. Quel est le dual d'un groupe cyclique ?

   Si $G = \langle a \rangle$ est cyclique d'ordre n, et $\chi \in \widehat{G}$, alors $1 = \chi(1) = \chi(a^n) = \chi(a)^n$, donc $\chi(a) = \exp(2ik\pi/n)$ pour un $k \in [|0, n-1|]$, puis a engendre G donc χ est entièrement déterminé par son image de a. Réciproquement, tous les $\chi_k : a \mapsto \exp(2ik\pi/n)$ sont bien définis, sont des morphismes, et sont deux à deux distincts donc $\widehat{G} = \{\chi_k \mid k \in [|0, n-1|]\}$, et $\chi_k = \chi_1^k$ donc $\widehat{G}$ est lui-même cyclique d'ordre n, donc G et $\widehat{G}$ sont isomorphes.

3. Que dire si G est un groupe abélien fini quelconque ?

   G est encore isomorphe à son dual, mais la preuve que j'avais lue n'est pas simple et utilise la théorie des caractères. Le jury me dit qu'en fait cela se déduit de la structure des groupes abéliens finis en produit direct de groupes cycliques. En effet, en utilisant la question précédente pour les groupes cycliques et le fait que $\widehat{H_1 \times H_2}$ est toujours isomorphe à $\widehat{H_1} \times \widehat{H_2}$.

4. Donner tous les groupes abéliens d'ordre 150 à isomorphisme près.

   On commence par écrire $150 = 2 \times 3 \times 5^2$, et par la classification des groupes abéliens finis ainsi que le théorème des restes chinois que les seuls groupes possibles sont[4] *$C_2 \times C_3 \times {C_5}^2$ et $C_2 \times C_3 \times C_{25}$.*

5. Retrouver les facteurs invariants dans chacun des cas.

   Je dis essentiellement des choses fausses jusqu'à me faire reprendre par le jury, qui me fait signaler que le deuxième groupe que j'ai écrit

4. Je me permets de noter C_n pour désigner $\mathbb{Z}/n\mathbb{Z}$, ce qui est sans ambiguité puisque tous les groupes cycliques d'ordre n sont isomorphes.

est cyclique, et donc qu'il n'y a qu'un seul facteur invariant : 150. *Pour le premier, je finis par penser au fait que le premier facteur invariant est donné par le ppcm des ordres, qui dans ce cas est* $2 \times 3 \times 5 = 30$, *le groupe cyclique correspondant est* $C_{30} = C_2 \times C_3 \times C_5$, *il ne reste donc que* C_5 *et donc le deuxième et dernier facteur invariant est* 5.

Exercices

1. Montrer que tout sous-groupe d'indice 2 est distingué.

   J'écris des choses au tableau sur les classes à droite qui ne servent pas à grand chose, jusqu'à ce que le jury m'indique sue je peux aussi considérer les classes à gauche. La solution est la suivante, si $x \in G \setminus H$, *alors il y a deux classes à gauches :* H *et* Hx, *et deux classes à droite :* H *et* xH. *On en déduit que* $xH = Hx$, *et donc* $H \triangleleft G$.

2. Soit p premier impair. On note D_p le groupe diédral à $2p$ éléments[5]. Soit $\phi : D_p \to \mathbb{Z}/p\mathbb{Z}$ un morphisme de groupes. Que dire de ϕ ?

   On a $|\mathrm{Ker}\phi| \in \{2, p, 2p\}$ *d'après le théorème de Lagrange, le cas* $|\mathrm{Ker}\phi| = 2p$ *n'étant pas intéréssant car alors* ϕ *est trivial. Le cas* $|\mathrm{Ker}\phi| = 2$ *est impossible car le noyau d'une symétrie n'est jamais distingué dans* D_p. *Pour montrer que le cas* $|\mathrm{Ker}\phi| = p$ *également impossible, commençons par remarquer que si on note* $D_p = \langle r, s\rangle$ *avec* r *d'ordre* p *et* s *d'ordre* 2, *alors l'ordre de* $\phi(r)$ *divise* p, *i.e. vaut* 1 *ou* p. *Dans le premier cas,* $r \in \mathrm{Ker}\phi$, *donc* $\langle r\rangle < \mathrm{Ker}\phi$, *puis* $\langle r\rangle = \mathrm{Ker}\phi$, *ce qui est impossible car alors l'ordre de* $\phi(s)$ *divise* 2 *mais également* p *donc* $\phi(s) = 0$, *et alors* ϕ *annule* r *et* s *donc est trivial. Dans l'autre cas, à savoir* $\phi(r)$ *d'ordre* p, *alors* $|\mathrm{Ker}\phi| = p$ *est impossible car les* r^k *ne sont pas dedans.*

5. Comme font tous les humains normalement constitués...