Les exercices étoilés (*) s'adressent aux seuls étudiants inscrits à l'unité MO12

Corrigé de la feuille d'exercices 2

1 Polyèdres réguliers

1.1 Trois polyèdres réguliers et leurs groupes.

Exercice 1. *Le tétraèdre régulier: on note $\mathcal{I}_T$ le groupe des isométries qui laissent le tétraèdre globalement invariant et $\mathcal{D}_T$ le sous-groupe de $\mathcal{I}_T$ constitué par les déplacements de $\mathcal{I}_T$.*

(i) Montrez que l'on peut considérer $\mathcal{I}_T$ (resp. $\mathcal{D}_T$) comme un sous-groupe de $O(3)$ (resp. $SO(3)$).

(ii) Montrez que $\mathcal{I}_T$ est fini de cardinal $\leqslant 24$.

(iii) Montrez que $\mathcal{I}_T \simeq \mathcal{S}_4$ et $\mathcal{D}_T \simeq \mathcal{A}_4$.

Preuve : (i) L'isobarycentre O du tétraèdre est invariant par tout élément de $\mathcal{I}_T$ de sorte que l'application $vect : g \in \mathcal{I}_T \mapsto \vec{g} \in O(3)$ définie par $\vec{g}(\vec{v}) = Og(\vec{M})$ où M est tel que $O\vec{M} = \vec{v}$ est un morphisme de groupe injectif.

(ii) Une application affine est déterminée par les images de 4 points non coplanaires. Tout élément de $\mathcal{I}_T$ permute les 4 sommets, de sorte que l'on a une injection $i : \mathcal{I}_T \longrightarrow \mathcal{S}_4$.

(iii) Il suffit de vérifier que la transposition (12) est dans l'image de i; en effet toute transposition est alors dans l'image et comme les transpositions engendrent $\mathcal{S}_4$, i sera alors un isomorphisme. La transposition (12) est l'image par i de la réflexion par rapport au plan médiateur du segment $[1, 2]$. Le sous-groupe $\mathcal{D}_T$ étant d'indice 2, il en est de même de son image soit $\mathcal{D}_T \simeq \mathcal{A}_4$. □

Exercice 2. *Le cube: avec des notations analogues on introduit $\mathcal{I}_C$ et $\mathcal{D}_C$.*

(i) Montrez que $\mathcal{I}_C$ est fini. Quel est l'indice $[\mathcal{I}_C : \mathcal{D}_C]$.

(ii) En faisant opérer $\mathcal{I}_C$ sur l'ensemble Δ des 4 diagonales, montrez que $\mathcal{D}_C$ est isomorphe à $\mathcal{S}_4$.

(iii) Décrivez $\mathcal{I}_C$.

Preuve : (i) Comme précédemment on a une injection $i : \mathcal{I}_C \hookrightarrow \mathcal{S}_8$. L'indice $[\mathcal{I}_C : \mathcal{D}_T]$ est comme toujours 2.

(ii) On remarque que les grandes diagonales sont les plus grandes distances entre deux éléments du cubes et sont donc conservées par toute isométrie. On obtient ainsi un morphisme $f : \mathcal{I}_C \longrightarrow \mathcal{S}_4$. Soit alors $g \in \operatorname{Ker} f$, on vérifie aisément que $g = \pm Id$. Pour montrer la surjectivité, il suffit comme précédemmment de montrer que la transposition (12) est obtenue. Notons $abcd$ les sommets de la face du dessus du cube et $a'b'c'd'$ les points de la face du dessous de sorte que les grandes diagonales soient aa', bb', cc' et dd'. La réflexion par rapport au plan contenant

aa' et la direction orthogonale à la face du dessus, a pour image la transposition qui échange bb' et dd' et laisse fixe aa' et cc'. On obtient ainsi que f induit un isomorphisme de $\mathcal{D}_C$ sur $\mathcal{S}_4$.

(iii) La suite exacte

$$1 \longrightarrow \mathcal{D}_C \longrightarrow \mathcal{I}_C \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

est scindée, un relèvement étant donné par $\{\pm Id\}$ de sorte que $\mathcal{I}_C$ est isomorphe au produit direct de $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

□

Exercice 3. *L'octaèdre: soit S la sphère circonscrite à l'octaèdre. On introduit le cube dont les faces sont les plans polaires aux 6 sommets de l'octaèdre par rapport à S. On l'appelle le cube dual à l'octaèdre, pourquoi?*

Montrez qu'une isomètrie laisse l'octaèdre globalement invariant si et seulement si il laisse son cube dual globalement invariant. Conclure.

Quel est le dual du tétraèdre?

Preuve : On rappelle que le plan polaire d'un point $P \neq O$ est $\{M \ / \ (\vec{OM}, \vec{OP}) = 1\}$. De même le point dual d'un plan H est le point P tel que $(\vec{OP}, \vec{OM}) = 1$ pour tout point M de H. En particulier la bidualité est l'identité et une isométrie préservant le produit scalaire, on en déduit que le groupe de l'octaèdre est celui du cube.
Remarque: Le tétraèdre est autodual.

□

1.2 Les sous-groupes finis de $SO(3)$

Soit Γ un sous-groupe fini de $SO(3)$ et N son cardinal.

Exercice 4. *Equation aux classes: on appelle pôle de Γ, un élément de la sphère unité tel qu'il existe un élément $\gamma \in \Gamma$ tel que $\gamma(x) = x$.*

(i) Soit x un pôle de Γ, décrivez le stabilisateur Γ_x. On note n_x le cardinal de Γ_x.

(ii) On note $\mathcal{O}_x$ l'orbite de x sous Γ. Montrez que tout élément de $\mathcal{O}_x$ est un pôle de Γ et que pour tout $x' \in \mathcal{O}_x$ on a $n_{x'} = n_x$. On note $\mathcal{C}$ l'ensemble des orbites et pour $C \in \mathcal{C}$, on note n_C le nombre n_x pour $x \in C$.

(iii) On considère les couples (γ, x) où $\gamma \in \Gamma \backslash \{e\}$ et où x est un pôle relatif à γ. En comptant ces couples de deux manières différentes, montrer que l'on a l'équation aux classes:

$$2 - \frac{2}{N} = \sum_{C \in \mathcal{C}} (1 - \frac{1}{n_C}).$$

Preuve : (i) Les éléments de $SO(3, \mathbb{R})$ sont des rotations, définies donc par un axe et un angle. Le stabilisateur G_x d'un élément x de la sphère est donc constitué de rotations d'axe (Ox).

(ii) Soit $x' = gx \in \mathcal{O}_x$ et $g \in \Gamma$, avec $g_0 x = x$ pour $g_0 \in \Gamma$; on a alors $(gg_0g^{-1}x' = x'$ et donc x' est un pole de Γ. En particulier on obtient $\Gamma_{x'} = g\Gamma_x g^{-1}$ et donc $n_x = n_{x'}$.

(iii) Tout élément $g \in \Gamma$ autre que l'identité a exactement deux pôles opposés; ainsi le cardinal des couples (γ, x) pour $\gamma \neq 1 \in \Gamma$ et x pôle de γ est égal à $2(N-1)$. Ce nombre est aussi égal à la somme

$$\sum_{C \in \mathcal{C}} \sum_{x \in C} (|\Gamma_x| - 1) = \sum_{C \in \mathcal{C}} \frac{|\Gamma|}{|\Gamma_x|} (|\Gamma_x| - 1)$$

ce qui donne l'égalité demandée.

□

Exercice 5. *(*) Discussion de l'équation aux classes: montrez qu'il y a* 2 *ou* 3 *orbites.*

(i) Cas de 2 *orbites: résoudre l'équation aux classes et donner les sous-groupes correspondants.*

(ii) Cas de 3 *orbites: on classe les* n_C*:* $2 \leqslant n_1 \leqslant n_2 \leqslant n_3$*. Montrer que* $n_1 = 2$ *puis que* $n_2 = 2$ *ou* 3.
Montrez que dans le cas où $n_1 = n_2 = 2$*, on trouve le groupe diédral* $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.
Montrez que dans le cas où $n_1 = 2$*,* $n_2 = 3$ *il y a* 3 *possibilités* $n_3 = 3$ *et* $N = 12$ *ou* $n_3 = 4$ *et* $N = 24$ *ou* $n_3 = 5$ *et* $N = 60$.
On pourra se référer à Arnaudiès **Les cinq polyèdres réguliers de** $\mathbb{R}^3$ **et leurs groupes.** *pour l'étude de ces* 3 *cas. Le résultat final est que l'on retrouve les groupes* $\mathcal{A}_4, \mathcal{S}_4$ *et* $\mathcal{A}_5$*. On décrit aussi les pôles dans chacun des cas.*

Preuve : La quantité $2 - 2/N$ est strictement inférieure à 2. Or pour tout $C \in \mathcal{C}$ on a $n_C \geqslant 2$ et donc $1 - 1/n_C \geqslant 1/2$, de sorte qu'il ne peut y avoir plus de trois termes non nuls dans la somme $\sum_{C\in\mathcal{C}}(1 - 1/n_C)$. En outre s'il n'y avait qu'une seule telle orbite, on aurait

$$0 < \frac{1}{n_C} = \frac{2}{N} - 1 \leqslant 0$$

ce qui est impossible. Finalement il ya 2 ou 3 orbites

(i) Soient alors C_1, C_2 les deux orbites et n_1, n_2 leurs cardinaux respectifs qui sont donc des diviseurs de N soit $N = n_i d_i$ pour $i = 1, 2$. La relation précédente s'écrit alors

$$2 - \frac{2}{N} = 2 - \frac{d_1}{N} - \frac{d_2}{N}$$

et donc $2 = d_1 + d_2$ soit $d_1 = d_2 = 1$. Ainsi on obtient deux pôles qui sont invariants par tous les éléments de Γ ce qui signifie qu'ils sont sur les axes des rotations des éléments de Γ; ces deux pôles sont donc opposés et les éléments de Γ sont tous des rotations de même axe (celui déterminé par ces pôles). Le groupe Γ est donc abélien; leur restriction au plan orthogonal à leur axe commun, forme un sous-groupe fini de $SO(2, \mathbb{R})$ qui est donc cyclique, engendré par une rotation d'angle $2\pi/n$. Ainsi Γ est constitué des rotations d'axe fixe et d'angle $2k\pi/n$ pour $0 \leqslant k < n$.

(ii) Soient C_1, C_2, C_3 les trois orbites, $n_1 \leqslant n_2 \leqslant n_3$ leurs cardinaux respectifs. On a alors

$$1 + \frac{2}{N} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$$

Si $n_1 \geqslant 3$, alors le membre de droite de l'égalité ci-dessus est inférieur ou égal à 1 tandis que celui de gauche est strictement plus grand que 1. Ainsi on a $n_1 = 2$. De même si $n_2 \geqslant 4$, le membre de gauche est plus petit que $1/2 + 1/4 + 1/4 \leqslant 1$ ce qui ne convient pas, soit $n_2 = 2$ ou 3.

Cas $n_1 = n_2 = 2$: on a alors $n_3 = N/2$. On a donc au moins trois pôles, or sachant que le nombre de pôles est pair, on en déduit qu'au moins un pôle et son inverse sont dans la même orbite. Si $N = 4$, on peut supposer qu'il est dans C_3 et si $N \geqslant 6$ (N est pair) comme pour tout $\Gamma_x = \Gamma_{-x}$ on en déduit que $C_3 = \{\pm x_0\}$ pour un point $x_0 \in S$. Le sous-groupe Γ_{x_0} étant d'indice

2, est donc distingué dans Γ. Tous les éléments de Γ_{x_0} sont des rotations d'axe x_0 de sorte que Γ_{x_0} est le groupe abélien des rotations d'axe x_0 et d'angle $2k\pi/n$, $0 \leqslant k < n = N/2$. Les points $\pm x_0$ étant dans la même orbite, les éléments de $\Gamma \backslash \Gamma_{x_0}$ sont alors des rotations d'angle π et d'axe appartenant au plan orthogonal de x_0. Un tel élément constitue alors un relèvement de la suite exacte

$$0 \longrightarrow \Gamma_{x_0} \longrightarrow \Gamma \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

de sorte que Γ est isomorphe à un produit semi-direct de $\mathbb{Z}/(N/2)\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ non abélien, i.e. il est isomorphe au groupe diédral. On vérifie alors aisément que Γ est le sous-groupe de $SO(3,\mathbb{R})$ qui laisse stable un $N/2$-polygone régulier dessiné sur le plan orthogonal à x_0. En particulier les autres pôles correspondent aux sommets et aux milieux des segments du polygone régulier et selon la parité de $N/2$, x et $-x$ sont (cas où $N/2$ est pair) ou ne sont pas dans la même orbite.
Cas $n_1 = 2$ et $n_2 = 3$: il vient alors $1/6 + 2/N = 1/n_3$ et donc $3 \leqslant n_3 < 6$ selon N, i.e. pour $N = 12$ (resp. 24, resp. 60) on a $n_3 = 3$ (resp. 4, resp. 5).
Remarque: On vérifie aisément que les groupes $\mathcal{D}_T$, $\mathcal{D}_C$ et $\mathcal{D}_I$ réalisent bien ces trois cas, le problème est de montrer que ce sont les seuls.

□

2 Produits semi-direct

2.1 Définition et généralités: rappels du cours

Soient N et H deux groupes, $\Psi : H \longrightarrow \mathrm{Aut}(N)$ un morphisme de groupe. Soit $G = N \times H$ en tant qu'ensemble.

- Montrez que G peut être muni d'une structure de groupe via la formule suivante:

  $$(n,h).(n',h') := (n\Psi(h)(n'), hh')$$

  On notera $h.n$ pour $\Psi(h)(n)$. L'ensemble G muni de cette structure de groupe sera appelé le produit semi-direct de N par H et noté $N \rtimes_\Psi H$.

  Remarque: Si $\Psi(h) = \mathrm{Id}_N$ pour tout $h \in H$, quelle structure de groupe retrouve-t-on?

- Montrez que dans G, on retrouve deux sous-groupes $\overline{N}$ et $\overline{H}$ isomorphes respectivement à N et H. Montrez que $\overline{N}$ est distingué dans G et que $\overline{h.n} = \overline{h}\,\overline{n}\,\overline{h^{-1}}$. Montrez que l'on a une suite exacte courte

  $$1 \longrightarrow N \longrightarrow N \rtimes_\Psi H \longrightarrow H \longrightarrow 1$$

Preuve: (a) La loi de composition ainsi définie est clairement interne, vérifions son associativité:

$$\begin{aligned}[(n_1,h_1).(n_2,h_2)].(n_3,h_3) &= (n_1\Psi(h_1)(n_2), h_1h_2).(n_3,h_3) = (n_1\Psi(h_1)(n_2)\Psi(h_1h_2)(n_3), h_1h_2h_3)\\ &= (n_1\Psi(h_1)(n_2)\Psi(h_1)\circ\Psi(h_2)(n_3), h_1h_2h_3) = (n_1\Psi(h_1)(n_2\Psi(h_2)(n_3)), h_1h_2h_3)\\ &= (n_1,h_1).(n_2\Psi(h_2)(n_3), h_2h_3) = (n_1,h_1).[(n_2,h_2).(n_3,h_3)]\end{aligned}$$

où on utilise que $\Psi : H \longrightarrow \mathrm{Aut}(N)$ est un morphisme de groupe, i.e. $\Psi(h_1h_2) = \Psi(h_1)\circ\Psi(h_2)$ et que $\Psi(h_1)$ *in* $\mathrm{Aut}(N)$ est un morphisme de groupe, i.e. $\Psi(h_1)(n_1n_2) = \Psi(h_1)(n_1)\Psi(h_1)(n_2)$. On vérifie aisément que $(1_N, 1_H)$ est un élément neutre pour cette loi et que l'inverse de (n,h) est

$(\Psi(h^{-1})(n^{-1},h^{-1}))$. On remarque aussi que si Ψ est triviale, i.e. $\Psi(h)=\mathrm{Id}_N$ pour tout $h\in H$, on retrouve la définition du produit direct de deux groupes.

(b) Soient $\overline{N}=\{(n,1_H)\in G\ /\ n\in N\}$ et $\overline{H}=\{(1_N,h)\in G\ /\ h\in H\}$. L'application naturelle $f_N: N\longrightarrow \overline{N}$ définie par $f_N(n)=(n,1_H)$ (resp. $F_H: H\longrightarrow \overline{H}$ définie par $f_H(h)=(1_N,h)$), est clairement bijective et est un morphisme de groupe: $f_N(n_1n_2)=(n_1n_2,1_H)=(n_1,1_H).(n_2,1_H)$ car $\Psi(1_H)=\mathrm{Id}_N$. On notera $\overline{n}$ (reps. $\overline{h}$) pour $(n,1_H)$ (resp. $(1_N,h)$). Montrons que le sous-groupe $\overline{N}$ de G est distingué: comme $(n,h)=\overline{n}\overline{h}$, il suffit de montrer que $\overline{N}$ est laissé stable par les automorphismes intérieurs définis par les $\overline{h}$, la stabilité sous les automorphismes intérieurs associés aux éléments du type $\overline{n}$ étant évidente:

$$\overline{h}\overline{n}\overline{h}^{-1}=\overline{h}(n,h^{-1})=(\Psi(h)(n),1_H)=\overline{\Psi(h)(n)}$$

En outre la suite

$$\begin{array}{ccccccc} 1 & \longrightarrow & N & \longrightarrow & N\rtimes_\Psi H & \longrightarrow & H\longrightarrow 1\\ & & n & \longmapsto & (n,1) & & \\ & & & & (n,h) & \longmapsto & h \end{array}$$

est clairement exacte.

□

2.2 Suite exacte scindée

Soient G un groupe et N un sous-groupe distingué de G. On dit d'un sous-groupe H de G qu'il est un relèvement de G/N, si la surjection canopnique $G\longrightarrow G/N$ induit un isomorphisme de H vers G/N. On dit aussi que la suite exacte

$$1\longrightarrow N\longrightarrow N\rtimes_\Psi H\longrightarrow H\longrightarrow 1$$

est scindée. Montrez que si G/N admet un relèvement H alors G est isomorphe à un produit semi-direct $N\rtimes_\Psi H$ et précisez Ψ.

Preuve: Le groupe N étant distingué dans G, H y agit par automorphismes intérieurs $\Psi: H\longrightarrow \mathrm{Aut}(N)$ avec $\Psi(h)(n)=hnh^{-1}$. Soit alors $f: N\rtimes_\Psi H\longrightarrow G$ défini par $f(n,h)=nh$; f est un morphisme de groupe car $f(1_N,1_H)=1_G$ et $f((n,h).(n',h'))=f(nhn'h^{-1},hh')=nhn'h^{-1}hh'=nhn'h'=f(n,h)f(n',h')$. Soit $(n,h)\in\mathrm{Ker}\, f$, soit $nh=1_G$ et donc $n=h^{-1}\in N\cap H$; or $\pi: G\longrightarrow G/N$ induit un isomorphisme $\pi_{|H}: H\simeq G/N$ d'où $\pi(n)=1_{G/N}$ et comme $n\in H$, on en déduit $n=1_H=1_G$ et $(n,h)=(1_N,1_H)$, d'où l'inectivité. Pour montrer la surjectivité, soit $g\in G$ et soit $h\in H$ tel que $\pi(h)=\pi(g)$; on a alors $n=gh^{-1}\in\mathrm{Ker}\,\pi=N$, soit $g=nh$.

Réciproquement $\overline{H}$ est un relèvement de la suite exacte $1\longrightarrow N\longrightarrow N\rtimes H\longrightarrow H\longrightarrow 1$.
Remarque: En particulier $N\rtimes_\Psi H$ est abélien si et seulement si N et H le sont et si le produit est direct.

□

2.3 Isomorphismes entre produits semi-directs

Soient ψ,ϕ des morphismes de H vers $\mathrm{Aut}(N)$. Montrez que dans les deux situations suivantes, on a $N\rtimes_\psi H\simeq N\rtimes_\phi H$:

- on suppose qu'il existe $\alpha\in\mathrm{Aut}(H)$ tel que $\psi=\phi\circ\alpha$;

- on suppose qu'il existe $u \in \mathrm{Aut}(N)$ tel que $\forall h \in H$, $\phi(h) = u\psi(h)u^{-1}$.

Preuve: (i) Soit $f : N \rtimes_\Psi H \longrightarrow N \rtimes_\Phi H$ défini par $f(n,h) = (n, \alpha(h))$; f est un morphisme car $f((n,h)(n',h')) = f(n\Psi(h)(n'), hh') = (n\Psi(h)(n'), \alpha(hh'))$ qui est égal à $f(n,h)f(n',h') = (n, \alpha(h))(n', \alpha(h')) = (n\Phi(\alpha(h))(n'), \alpha(h)\alpha(h'))$ car $\Psi = \Phi \circ \alpha$ et que $\alpha(hh') = \alpha(h)\alpha(h')$. De même on a un morphisme $g : N \rtimes_\Phi H \longrightarrow N \rtimes_\Psi H$ défini par $g(n,h) = (n, \alpha^{-1}(h))$ qui est clairement inverse de f, d'où le résultat.

(ii) Soit $f : N \rtimes_\Psi H \longrightarrow N \rtimes_\Phi H$ défini par $f(n,h) = (u(n), h)$; f est un morphisme car $f((n,h)(n',h')) = f(n\Psi(h)(n'), hh') = (u(n\Psi(h)(n')), hh') = (u(n)\Phi(h)(n'), hh')$ qui est donc bien égal à $f(n,h)f(n',h')$. Comme précédemment $g : N \rtimes_\Phi H \longrightarrow N \rtimes_\Psi H$ défini par $g(n,h) = (u^{-1}(n), h)$ est clairement le morphisme inverse de f, d'où le résultat.

□

2.4 Le groupe diédral

Dans le plan affine, on considère le polygone régulier à n cotés, formé par les points d'affixe les racines n-ièmes de l'unité. On considère le sous-groupe G du groupe des isométries du plan, constitués des isométries qui laissent stable ce polygone. Montrez que G est un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$ pour $\psi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ que l'on précisera. Le groupe G ainsi défini est le groupe diédral noté D_n.

Preuve: Claasiquement toute application affine du plan qui laisse globalement stable le polygone régulier en question, laisse le barycentre invariant et correspond à une isométrie vectorielle. L'ensemble G de ces isométries vectorielle est donc constitués des rotations d'angle $2k\pi/n$ et des reflexions par rapport aux médiatrices des segments constituants le polygone régulier. La loi sur G est bien évidemment donnée par la composition des applications linéaires; $|G| = 2n$. Dans G, le sous-groupe N des isométries positives est cyclique engendré par exemple par la rotation r d'angle $2\pi/n$; il est distingué car c'est le noyau du déterminant; $N \simeq \mathbb{Z}/n\mathbb{Z}$. On considère la suite exacte $1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$ qui est scindée, un relèvement de $G/N \simeq \mathbb{Z}/2\mathbb{Z}$ étant donné par le choix d'une quelconque réflexion s de G. Ainsi on a $G \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\Psi \mathbb{Z}/2\mathbb{Z}$, où $\Psi(1)(1)$ est l'entier k modulo n tel que $srs = r^k$; classiquement on obtient $k = -1$.

□

2.5 $\mathcal{S}_n$

- Montrez que $\mathcal{S}_n$ peut s'écrire comme produit semi-direct $\mathcal{A}_n \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$.
- Peut-on faire en sorte que le produit soit direct ?
- Montrez que $\mathcal{S}_3 \simeq D_3$.

Preuve: La suite exacte courte $1 \longrightarrow \mathcal{A}_n \longrightarrow \mathcal{A}_n \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$ est clairement scindée, un relèvement étant donné par un élément τ quelconque d'ordre 2 de $\mathcal{S}_n \backslash \mathcal{A}_n$, de sorte que $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes_\Psi \mathbb{Z}/2\mathbb{Z}$, $\Psi(1)$ étant donné par $\Psi(1)(\sigma) = \tau\sigma\tau$. Tous ses produits semi-directs sont isomorphes (car isomorphes à $\mathcal{S}_n$), et on se trouve dans la situation (ii) de l'exercice précédent.

Le produit ne peut pas être direct car sinon, l'élément τ du relèvement serait dans le centre de $\mathcal{A}_n$ qui, on l'a déjà vu, est réduit à l'identité: $\Psi(1) = \mathrm{Id} \Leftrightarrow \tau\sigma\tau = \sigma$ pour tout $\sigma \in \mathcal{A}_n$.

Il n'y a que deux produits semi-directs $\mathbb{Z}/3\mathbb{Z} \rtimes_\Psi \mathbb{Z}/2\mathbb{Z}$; en effet $\Psi(1)$ doit être un élément d'ordre divisant 2 dans $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$; si cet ordre est 1, alors le produit est direct et on trouve $\mathbb{Z}/6\mathbb{Z}$ qui est commutatif; sinon soit Ψ tel que $\Psi(1) \neq \mathrm{Id}$. Ainsi D_3 et $\mathcal{S}_3$ qui sont deux tels produits semi-directs non commutatifs, sont isomorphes à $\mathbb{Z}/3\mathbb{Z} \rtimes_\Psi \mathbb{Z}/2\mathbb{Z}$.

□

2.6 $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$

Exercice 1. *Etude de quelques $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$:*

(a) Quels sont les produit semi-directs $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$?

(b) Même question pour $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$.

(c) Même question pour $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ avec p et q premiers impairs.

(d) Même question pour $\mathbb{Z}/15\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

(e) Soit p premier impair. Etudier les produits semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ et construire un groupe non abélien d'ordre p^3. Que peut-on dire de l'ordre d'un élément non trivial de ce groupe ?

(f) On considère la suite exacte suivante

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Peut-on en trouver une section telle qu'éventuellement le produit soit direct ?

(g) On note $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ le groupe de Klein. Montrez qu'il existe des produits semi-directs non triviaux $V \rtimes \mathbb{Z}/3\mathbb{Z}$ et qu'ils sont tous isomorphes. Même question avec $\mathbb{Z}/3\mathbb{Z} \rtimes V$.

Preuve: (a) Il existe deux morphismes $\Psi : \mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$, le morphisme nul et l'identité; au premier correspond le produit direct $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et au deuxième le groupe diédral D_4.

(b) Un morphisme $\Psi : \mathbb{Z}/3\mathbb{Z} \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ est caractérisé par la donnée de $\Psi(1)$ qui doit être un élément de $\mathbb{Z}/2\mathbb{Z}$ d'ordre divisant 3; dans $\mathbb{Z}/2\mathbb{Z}$ il n'y a pas d'élément d'ordre 3 soit $\Psi(1) = 0$ et le produit est direct: on obtient $\mathbb{Z}/12\mathbb{Z}$.

(c) Un morphisme $\Psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ (car q est premier) est déterminé par $\Psi(1)$ qui doit être un élément d'ordre divisant p, i.e. d'ordre 1 ou p. Si $\Psi(1)$ est d'ordre 1, alors Ψ est triviale et le produit en question est direct: $\mathbb{Z}/pq\mathbb{Z}$ par le lemme chinois. Si p ne divise pas $q-1$, $\Psi(1)$ ne peut pas être d'ordre p et dans ce cas il n'existe donc qu'un seul produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ à savoir $\mathbb{Z}/pq\mathbb{Z}$.

Supposons donc que p divise $q-1$; dans $\mathbb{Z}/(q-1)\mathbb{Z}$, il y a exactement $p-1$ éléments d'ordre p, à savoir les $k(q-1)/p$ pour $0 < k < p$. On obtient ainsi outre le morphisme trivial, $p-1$ application $\mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/q\mathbb{Z})^\times$, que l'on note Ψ_k définie par $\Psi_k(1) = k(q-1)/p$. Ainsi à priori, outre le produit direct, on obtient $p-1$ produits semi-directs $G_k := \mathbb{Z}/q\mathbb{Z} \rtimes_{\Psi_k} \mathbb{Z}/p\mathbb{Z}$. Nous allons montrer qu'en fait tous les G_k sont isomorphes pour $0 < k < p$, en appliquant le critère (i) de l'exercice (**??**). Soit en effet $\alpha_k \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ défini par $\alpha_k(1) = k$; on a alors $\Psi_k = \Psi_1 \circ \alpha_k$: pour le vérifier il suffit en effet de tester cette égalité sur 1:

$$\Psi_1 \circ \alpha_k(1) = \Psi_1(k) = k\Psi_(1) = \Psi_k(1).$$

On remarque aussi que le produit semi-direct G_1 n'est pas isomorphe au groupe abélien $\mathbb{Z}/pq\mathbb{Z}$, car G_1 n'est pas commutatif.

(d) Comme précédemment on cherche les éléments d'ordre 2 de $(\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$. En remarquant que 2 (resp -1) est un générateur de $(\mathbb{Z}/5\mathbb{Z})^\times$ (resp. de $(\mathbb{Z}/3\mathbb{Z})^\times$), on obtient un isomorphisme $f_5 : (\mathbb{Z}/5\mathbb{Z})^\times \longrightarrow \mathbb{Z}/4\mathbb{Z}$ (resp. $f_3 : (\mathbb{Z}/3\mathbb{Z})^\times \longrightarrow \mathbb{Z}/2\mathbb{Z}$) défini par $f_5(2^k))k$ (resp. $f_3((-1)^k) = k$). Or les éléments d'ordre 2 de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont $(0,1)$, $(2,0)$, $(2,1)$ et correspondent dans $\mathbb{Z}/15\mathbb{Z})^\times$ à respectivement -4, 4 et -1. Ainsi outre le produit direct $\mathbb{Z}/30\mathbb{Z}$, on obtient à priori 3 autres produits semi-directs G_λ correspondant aux morphismes Ψ_λ pour $\lambda = -4, 4, -1$, définis par $\Psi_\lambda(1) = \lambda \in (\mathbb{Z}/15\mathbb{Z})^\times$. Pour $\lambda = -1$, on reconnait le groupe diédral D_{15}. Nous allons montrer que les 4 groupes obtenus ne sont pas isomorphes. Clairement le produit direct n'est isomorphe à aucun des G_λ pour $\lambda = 4, -4, -1$ car ces derniers ne sont pas commutatifs. Nous allons prouver que G_4 n'est pas isomorphe à G_{-4}, les autres cas se traitant de manière similaire.

Le groupe G_4 est de cardinal 30, ses éléments sont $\mathrm{Id}, \sigma_+, \sigma_+^2, \cdots, \sigma_+^{14}, \tau_+, \sigma_+\tau_+, \cdots, \sigma_+^{14}\tau_+$, où σ_+ est d'ordre 15, $\sigma_+^1 5 = 1$, et τ_+ d'ordre 2, $\tau_+^2 = 1$; en outre on a la relation de conjugaison donnée par Ψ_4: $\tau_+\sigma_+\tau_+ = \sigma_+^4$. En language savant, on vient de donner une présentation par générateurs et relations de G_4. De la même façon, G_{-4} a deux générateurs σ_- et τ_- avec les relations $\sigma_-^{15} = \tau_-^2 = 1$ et $\tau_-\sigma_-\tau_- = \sigma_-^{-4}$. Considérons alors un isomorphisme $f : G_4 \longrightarrow G_{-4}$: $f(\sigma_+)$ doit être un élément d'ordre 15, soit $f(\sigma_+) = \sigma_-^i$ pour $i \in (\mathbb{Z}/15\mathbb{Z})^\times$ et de même $f(\tau_+)$ doit être d'ordre 2, soit $f(\tau_+) = \sigma_-^j\tau_-\sigma_-^{-j}$ pour un entier j. On doit aussi avoir $f(\sigma_+^4) = f(\tau_+\sigma_+\tau_+)$ soit $\sigma_-^j\tau_-\sigma_-^i\tau_-\sigma_-^{-j} = \sigma_-^{-4i} = \sigma_-^{4i}$; contradiction car $i \in (\mathbb{Z}/15\mathbb{Z})^\times$. Les autres cas se traitent de manière similaire, et on obtient finalement 4 produits semi-direct $\mathbb{Z}/15\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

(e) Le cas $p = 2$ ayant été traité en (a), on suppose donc p impair. Comme précédemment, on cherche les morphismes $\Psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p^2\mathbb{Z})^\times \simeq \mathbb{Z}/p(p-1)\mathbb{Z} \simeq GL_2(\mathbb{Z}/p\mathbb{Z})$, qui sont déterminés par $\Psi(1)$ qui doit être d'ordre divisant p, soit $\Psi(1) = k(p-1) \in \mathbb{Z}/p(p-1)\mathbb{Z}$ et $0 \leqslant k < p$, ou encore dans $GL_2(\mathbb{Z}/p\mathbb{Z})$, $\Psi(1)$ est conjugué à $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Pour $k = 0$, on retrouve le produit direct qui est commutatif et soit Ψ_k défini par $\Psi_k(1) = k(p-1)$ ou dans $GL_2(\mathbb{Z}/p\mathbb{Z})$, $\Psi_k(1) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.[1] Comme dans (c), soit $\alpha_k \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ définie par $\alpha_k(1) = k$, on a alors $\Psi_k = \Psi_1 \circ \alpha_k$, de sorte que tous les produits semi-directs $\mathbb{Z}/p^2\mathbb{Z} \rtimes_{\Psi_k} \mathbb{Z}/p\mathbb{Z}$ sont isomorphes pour $0 < k < p$ et non abéliens.
Tout élément de ce groupe s'écrit sous la forme (X, k) avec $X \in (\mathbb{Z}/p\mathbb{Z})^2$ et en notant $N = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on a

$$(X, k)^i = ((Id + N^k + \cdots + N^{k(i-1)})X, ik)$$

en particulier on note qu'un tel élément non trivial est toujours d'ordre p.

(f) Soit α une section de $\mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, d'où $\alpha(1) = 1$ ou 3, or ni 1 ni 3 ne sont d'ordre 2 et donc $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à un produit semi-direct $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. On aurait aussi pu remarquer que le seul morphisme $\mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^\times$ est le morphisme trivial de sorte qu'il n'y a qu'un seul produit semi-direct, à savoir le produit direct. Or dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ les éléments autres que $(0,0)$ sont tous d'ordre 2, alors que dans $\mathbb{Z}/4\mathbb{Z}$ il y a un élément d'ordre 4, d'où la contradiction.

(g) Le groupe des automorphismes de V est isomorphe à $GL_2(\mathbb{Z}/2\mathbb{Z})$, de cardinal 6 et, on l'a vu, isomorphe à $\mathcal{S}_3$ quand on le voit permuter les droites du plan $(\mathbb{Z}/2\mathbb{Z})^2$. Ces droites sont $\binom{1}{0}$, $\binom{0}{1}$ et $\binom{1}{1}$. Ses éléments d'ordre 3 sont les deux 3-cycles ce qui donne les matrices

[1] La conjugaison ne fournit de nouveaux groupes en vertu **??** (ii).

$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. On obtient ainsi outre le produit direct, deux autres produits semi-direct donnés par $\Phi_1(1) = M$ et $\Phi_2(1) = M^2$ où α est une quelconque des matrices d'ordre 3. Comme précédemment on a $\Phi_2 = \Phi_1 \circ \alpha$, où $\alpha \in \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ est défini par $\alpha(1) = 2$, de sorte que les deux produits semi-directs en question sont isomorphes.

Un morphisme $\Phi : V \longrightarrow (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ est une $\mathbb{Z}/2\mathbb{Z}$-forme linéaire sur $(\mathbb{Z}/2\mathbb{Z})^2$; il en existe des non triviales. Soit Ψ_1 et Ψ_2 deux telles formes linéaires non triviales et soient $e_1, e_2, f_1, f_2 \in (\mathbb{Z}/2\mathbb{Z})^2$ non nuls, tels que $\Psi_i(e_i) = 1$, $\Psi_i(f_i) = 0$ pour $i = 1, 2$; (e_1, f_1) et (e_2, f_2) sont des bases de V. Soit donc $M \in GL_2(\mathbb{Z}/2\mathbb{Z})$ la matrice de passage $M(e_1) = e_2$ et $M(f_1) = f_2$, on a alors $\Psi_2 = \Psi_1 \circ M$ de sorte que les produits semi-directs $\mathbb{Z}/2\mathbb{Z} \rtimes_{\Psi_i} V$ pour $i = 1, 2$ sont isomorphes, de sorte qu'outre le produit direct, on obtient un unique produit semi-direct.

□

2.7 Groupes classiques

Soient n un entier strictement positif et $\mathbb{K}$ un corps.

- On note $T(n, \mathbb{K})$ (resp. $D(n, \mathbb{K})$, resp. $U(n, \mathbb{K})$) le sous-groupe de $GL_n(\mathbb{K})$ formé des matrices triangulaires supérieures (resp. diagonales, resp. triangulaires supérieures avec des 1 sur la diagonale). "Montrez" que $T_(n, \mathbb{K}) = U(n, \mathbb{K}) \rtimes D(n, \mathbb{K})$.

- On s'intéresse à la suite exacte

$$1 \longrightarrow SL_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K}) \xrightarrow{\det} \mathbb{K}^\times \longrightarrow 1$$

  - Montrez que $GL_n(\mathbb{K})$ est produit semi-direct de $SL_n(\mathbb{K})$ par $\mathbb{K}^\times$.
  - Montrez que cette suite exacte possède une section qui identifie $GL_n(\mathbb{K})$ au produit direct $SL_n(\mathbb{K}) \times \mathbb{K}^\times$ si et seulement si il existe un homomorphisme de groupes $\phi : \mathbb{K}^\times \longrightarrow \mathbb{K}^\times$ tel que pour tout $x \in \mathbb{K}^\times$, on ait $\phi(x)^n = x$.
  - En supposant $\mathbb{K} = \mathbb{R}$, quelles sont les valeurs de n pour lesquelles il existe une section qui identifie $GL_n(\mathbb{R})$ au produit direct $SL_n(\mathbb{R}) \times \mathbb{R}^\times$?
  - Même question avec $\mathbb{K} = \mathbb{C}$ et $\mathbb{K}$ fini.

- (*) Soit G le sous-groupe de $GL_2(\mathbb{K})$ formé des matrices de la forme $\begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix}$ avec $a \in \mathbb{K}^\times$ et $b \in \mathbb{K}$. On considère la suite exacte suivante

$$0 \longrightarrow \mathbb{K} \longrightarrow G \longrightarrow \mathbb{K}^\times \longrightarrow 0$$

  Peut-on en trouver une section telle qu'éventuellement le produit soit direct ?

Preuve: (a) Il suffit simplement de remarquer que toute matrice T de $T(n, \mathbb{K})$ s'écrit de manière unique sous la forme DU avec $D \in D(n, \mathbb{K})$ et $U \in U(n, \mathbb{K})$, de sorte que $D(n, \mathbb{K})$ est un relèvement de $T(n, \mathbb{K}) \longrightarrow T(n, \mathbb{K})/U(n, \mathbb{K})$.

(b) (i) L'ensemble des matrices diagonales de la forme $(x, 1, \cdots, 1)$ avec $x \in \mathbb{K}^\times$, est clairement un sous-groupe de $GL_n(\mathbb{K})$ qui relève le déterminant, d'où le résultat.

(ii) Supposons que l'on puisse prendre des racines n-ièmes de manière compatible, i.e. qu'il existe $\phi : \mathbb{K}^\times \longrightarrow \mathbb{K}^\times$ un morphisme de groupe tel que $\phi(x)^n = x$, considérons alors l'ensemble

$D_\phi(n,\mathbb{K}) = \{\phi(x)\mathrm{Id} \ / \ x \in \mathbb{K}^\times\}$. Il est alors clair que $D_\phi(n,\mathbb{K})$ est un sous-groupe qui est un relèvement du déterminant. Par ailleurs $D_\phi(n,\mathbb{K})$ est dans le centre de $GL_n(\mathbb{K})$ de sorte que le morphisme $\Psi : D_\phi(n,\mathbb{K}) \longrightarrow \mathrm{Aut}(SL_n(\mathbb{K}))$ défini par $\Psi(D)(M) = DMD^{-1}$ est trivial, i.e. le produit est direct.

Réciproquement, supposons qu'il existe une section au déterminant de sorte que le produit soit direct, cela signifie qu'il existe un sous-groupe $\mathcal{D}$ de $GL_n(\mathbb{K})$ qui relève le déterminant et dont tous les éléments commutent à tous les éléments de $SL_n(\mathbb{K})$. Or c'est un exercice classique d'algèbre linéaire, les matrices qui commutent à tous les éléments de $SL_n(\mathbb{K})$, sont les matrices scalaires: $\mathcal{D} \subset \{\lambda\mathrm{Id} \ / \ \lambda \in \mathbb{K}^\times\}$. Ainsi à tout $x \in \mathbb{K}^\times$ correspond une unique matrice de $\mathcal{D}$ de la forme $\phi(x)\mathrm{Id}$; on construit ainsi l'application $\phi : \mathbb{K}^\times \longrightarrow \mathbb{K}^\times$ telle que $\phi(x)^n = x$. Il ne reste plus qu'à vérifier que ϕ est un morpisme de groupe: $\phi(x_1x_2)\mathrm{Id}$ est l'unique matrice de $\mathcal{D}$ de déterminant x_1x_2, or $\phi(x_1)\mathrm{Id}$ et $\phi(x_2)\mathrm{Id}$ sont des éléments de $\mathcal{D}$ et donc $\phi(x_1)\phi(x_2)\mathrm{Id}$ est un élément de $\mathcal{D}$ (car $\mathcal{D}$ est un groupe) de déterminant x_1x_2, soit $\phi(x_1x_2)\mathrm{Id} = \phi(x_1)\phi(x_2)\mathrm{Id}$, d'où le résultat.

(iii) Pour n pair, il n'y a pas de racine n-ième d'un nombre négatif de sorte que le produit semi-direct $GL_n(\mathbb{R}) \simeq SL_n(\mathbb{R}) \rtimes \mathbb{R}^\times$ ne peut pas être direct pour n pair. Pour n impair, le morphisme de groupe $f : \mathbb{R}^\times \longrightarrow \mathbb{R}^\times$ défini par $f(x) = x^n$ est un isomorphisme, de sorte que $\phi = f^{-1}$ convient, i.e. on a un isomorphisme $GL_n(\mathbb{R}) \simeq SL_n(\mathbb{R}) \times \mathbb{R}^\times$, pour n impair.

(iv) Pour $\mathbb{K} = \mathbb{C}$, $\mathbb{C}^\times$ n'étant pas simplement connexe, il n'est pas possible de définir une fonction racine n-ième, continue sur $\mathbb{C}^\times$.

Soit $\mathbb{K} =$ un corps fini de cardinal q [2]. Si le morphisme de groupe $f : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$ défini par $f(x) = x^n$, est une bijection, i.e. $\mathrm{Ker}\, f = \{1\}$, alors $\phi = f^{-1}$ convient, sinon f n'étant pas surjectif, l'existence de ϕ ne se peut pas. La condition d'injectivité de f revient à dire qu'il n'y a pas dans $\mathbb{F}_q^\times$ d'élément d'ordre divisant n autre que 1. Or on a vu que $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, de sorte que la condition d'injectivité est équivalente au fait que n et $q-1$ sont premiers entre eux.

(c) On commence par remarquer que cette suite exacte est scindée, un relèvement étant par exemple donné par l'ensemble des matrices de dilatation $\mathrm{diag}(1,a)$, $a \in \mathbb{K}^\times$. L'existence d'une section telle que le produit soit direct, revient à trouver un sous-groupe de G qui relève $G \longrightarrow \mathbb{K}^\times \to 0$ et dont tous les éléments commutent aux matrices de transvection $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Or il est aisé de montrer que les matrices de G qui commutent à toutes les matrices de transvection sont les matrices de transvection qui sont dans le noyau de $G \longrightarrow \mathbb{K}^\times$, de sorte qu'il n'est pas possible d'obtenir un produit direct.

□

3 (*) Groupes de Sylow et simplicité

Exercice 1. *(*) Soit G un groupe d'ordre $11^2 13^2$. Montrez, en étudiant ses sous-groupes de Sylow, qu'un tel groupe est nécessairement abélien. En déduire la classification à isomorphisme près des groupes ayant cet ordre.*

Preuve: On note k_{11} (resp. k_{13}) le nombre de 11-Sylow (resp. de 13-Sylow) de G; les théorèmes de Sylow donnent $k_{11} \equiv 1 \bmod 11$ et k_{11} divise 13^2, soit $k_{11} = 1$. De même on a $k_{13} = 1$. Soit

[2] On admet ici qu'un tel corps est forcément commutatif. En outre il s'avère que q est une puissance d'un nombre premier p.

alors P_{11} (resp. P_{13}) l'unique 11-Sylow (resp. 13-Sylow) de G. D'après un exercice précédent, P_{11} et P_{13} sont abéliens soit $P_{11} \simeq \mathbb{Z}/11^2\mathbb{Z}$ ou $(\mathbb{Z}/11\mathbb{Z})^2$, et $P_{13} \simeq \mathbb{Z}/13^2\mathbb{Z}$ ou $(\mathbb{Z}/13\mathbb{Z})^2$. On a la suite exacte $1 \longrightarrow P_{13} \longrightarrow G \longrightarrow G/P_{13} \longrightarrow 1$ et P_{11} est une section de cette suite exacte; en effet $P_{11} \cap P_{13} = \{1\}$ et par cardinalité la projection $G \longrightarrow G/P_{13}$ induit un isomorphisme $P_{11} \simeq G/P_{13}$. Etudions alors les morphismes $\Psi : P_{11} \longrightarrow \mathrm{Aut}(P_{13})$; or le cardinal de $\mathrm{Aut}(P_{13})$ est $13(13-1)$ dans le cas où P_{13} est cyclique, et $(13^2-1)(13^2-13) = |GL_2(\mathbb{Z}/13\mathbb{Z})|$ dans le cas où $P_{13} \simeq (\mathbb{Z}/13\mathbb{Z})^2$. Dans les deux cas 11 ne divise pas $|\mathrm{Aut}(P_{13})|$ de sorte que Ψ est trivial et le produit est direct. Ainsi G en tant que produit direct de deux groupes abélien est abélien, de sorte que G est isomorphe à l'un des 4-groupes suivant que l'on écrit sous la forme des facteurs invariants: $\mathbb{Z}/13^2 11^2\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11.13^2\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13.11^2\mathbb{Z}$ et $(\mathbb{Z}/11.13\mathbb{Z})^2$.

□

Exercice 2. *(*) Groupes d'ordre pq, pq^2: soient p et q deux entiers premiers distincts.*

(a) Déterminez à isomorphisme près tous les groupes d'ordre pq.
Indication: On écrit $p < q$; montrez qu'il existe un unique q-Sylow, puis que G est un produit semi-direct.

(b) Prouvez qu'un groupe d'ordre pq^2 n'est pas simple.
Indication: Dans le cas où $p < q$, montrez qu'il existe un unique q-Sylow dans G. Dans le cas où $q < p$, montrez qu'il existe un unique p-Sylow dans G.

Preuve: (a) Soit k_q le nombre de q-Sylow de G; on a $k_q \equiv 1 \bmod q$ et k_q divise p et comme $p < q$, on en déduit $k_q = 1$, de sorte que l'unique q-Sylow Q de G est distingué dans G. La suite exacte $1 \longrightarrow Q \longrightarrow G \longrightarrow G/Q \longrightarrow 1$ est scindée, un relèvement étant donné par un p-Sylow P; en effet $P \cap Q = \{1\}$ car un tel élément est d'ordre un diviseur de p et de q, et par cardinalité la restriction de la projection $G \longrightarrow G/Q$ se restreint en un isomorphisme $P \simeq G/Q$. Ainsi G est un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_\Psi \mathbb{Z}/p\mathbb{Z}$. On a déja vu qu'outre le produit direct, il existe un unique produit semi-direct.

(b) On a $k_q \equiv 1 \bmod q$ et k_q divise p, de sorte que si $p < q$ alors $k_q = 1$ et G n'est pas simple. Dans le cas $q < p$, on a $k_p \equiv 1 \bmod p$ et k_p divise q^2, soit $k_p = 1, q^2$. Supposons donc $k_p = q^2$. On remarque que l'intersection de deux p-Sylow distincts est réduite à l'élément neutre; en effet tout élément non trivial d'un p-Sylow, l'engendre. On obtient ainsi $q^2(p-1)$ éléments d'ordre p, ce qui laisse exactement q^2 éléments qui constituent l'unique q-Sylow.

□

Exercice 3. *(*) Etude de la simplicité des groupes de cardinal $\leqslant 100$:*

(a) Soit G un groupe ayant k p-Sylow ($k \geqslant 2$). Montrez que l'on a un morphisme $\phi : G \longrightarrow S_k$ non trivial.

(b) Soit S un 2-Sylow de G supposé cyclique. Montrez que G n'est pas simple.
Indication: considérer l'opération de G sur lui-même par translation à gauche et en déduire un morphisme non trivial de G dans $\{-1, 1\}$. En déduire que si G est simple et $|G|$ est pair ($|G| \geqslant 2$) alors 4 divise $|G|$.

(c) Soit G un groupe de cardinal n, non premier et $n \leqslant 100$ avec $n \neq 60$. Montrez que G n'est pas simple. Quand est-il pour $n = 60$?

Preuve: (a) On considère l'action de G sur l'ensemble S_p des p-Sylow définie comme suit: $\phi : g \in G \mapsto \sigma_g \in \mathcal{S}(S_p)$ avec $\sigma_g(P) = gPg^{-1}$; il est immédiat de vérifier que σ_g est une permutation de $\mathcal{S}(S_p)$. En outre pour $P_1 \neq P_2$ deux p-Sylow de G, les théorèmes de Sylow nous disent qu'il existe $g \in G$ tel que $\sigma_g(P_1) = P_2$ de sorte que ϕ est non trivial.

(b) On considère l'action de G sur lui-même par translation à gauche et on étudie la permutation σ_s associé à un générateur s de S. On partitionne G par les classes de $S\backslash G$; chaque classe est stable et correspond à une orbite. Soit $\overline{h}$ une telle classe à gauche: $\overline{h} = \{h, sh, s^2h, \cdots, s^{2^r-1}h\}$ où 2^r est le cardinal de S. On remarque alors que σ_s sur cette orbite, est le cycle de longueur 2^r; $s.s^ih = s^{i+1}h$. Ainsi σ_s est le produit de m cycles de longueur 2^r, avec $m = |S\backslash G|$ impair. On en déduit alors que la signature de σ_s est $((-1)^{2^r-1})^m = -1$, de sorte que le noyau de $G \longrightarrow \mathcal{S}(G) \xrightarrow{\epsilon} \{\pm 1\}$ est un sous-groupe distingué non trivial de G dès que $|G| > 2$, soit G n'est pas simple. On en déduit que si le cardinal de G est pair et G simple alors 4 divise $|G|$.

(c) On a vu que les groupes de cardinaux p^r, pq, pq^2 et $n \equiv 2 \bmod 4$ alors G n'est pas simple, p, q premier. Ainsi il reste à étudier les groupes G de cardinal $n = 24, 36, 40, 48, 56, 60, 72, 80, 84, 88, 96$.
$n = 24$: on a $k_2 \equiv 1 \bmod 2$ et k_2 divise 3, soit $k_2 = 1, 3$; or si $k_2 = 3$, d'après (a), on obtient un morphisme non trivial $G \longrightarrow \mathcal{S}_3$ qui par cardinalité ne peut pas être injectif, de sorte que le noyau donne un sous-groupe distingué non trivial.
$n = 36$: on a $k_3 \equiv 1 \bmod 3$ et k_3 divise 4, soit $k_3 = 1, 4$; si $k_3 = 4$, on obtient d'après (a), un morphisme non trivial $G \longrightarrow \mathcal{S}_4$ qui ne peut pas être injectif car $36 > 24$ et donc G n'est pas simple.
$n = 40$: on a $k_5 \equiv 1 \bmod 5$ et k_5 divise 8 soit $k_5 = 1$ et donc G n'est pas simple car son 5-Sylow est distingué.
$n = 48$: on a $k_2 = 1, 3$ et $k_2 = 3$ fournit un morphisme $G \longrightarrow \mathcal{S}_3$ qui a un noyau non trivial.
$n = 56$: on a $k_7 \equiv 1 \bmod 7$ et k_7 divise 8, soit $k_7 = 1, 8$; or si $k_7 = 8$, on a alors $8 \times 6 = 48$ éléments d'ordre 7, car les 7-Sylow étant cycliques d'ordre premier, deux 7-Sylow ont une intersection réduite à l'élément neutre. Ce qui ne laisse que 8 éléments qui constituent alors l'unique 2-Sylow qui est donc distingué.
$n = 60$: $\mathbb{Z}/60\mathbb{Z}$ n'est pas simple alors que $\mathcal{A}_5$ l'est.
$n = 72$: on a $k_3 \equiv 1 \bmod 3$ et k_3 divise 8, soit $k_3 = 1, 4$; si $k_3 = 4$, on a alors un morphisme non trivial $G \longrightarrow \mathcal{S}_4$ qui a un noyau non trivial et G n'est aps simple.
$n = 80$: on a $k_5 \equiv 1 \bmod 5$ et k_5 divise 16 soit $k_5 = 1, 16$; or si $k_5 = 16$, on a 4×16 éléments d'ordre 5 ce qui laisse 16 éléments qui constituent alors l'unique 2-Sylow distingué de G et G n'est pas simple.
$n = 84$: on a $k_7 \equiv 1 \bmod 7$ et k_7 divise 12 soit $k_7 = 1$ et G n'est aps simple.
$n = 88$: on a $k_1 1 \equiv 1 \bmod 11$ et $k_1 1$ divise 8 soit $k_1 1 = 1$ et G n'est pas simple.
$n = 96$: on a $k_2 \equiv 1 \bmod 2$ et k_2 divise 3 soit $k_2 = 1, 3$; si $k_2 = 3$ alors on a un morphisme non trivial $G \longrightarrow \mathcal{S}_3$ qui a un noyau non trivial.

□

Exercice 4. *(*) Soient G un groupe d'ordre 30 et P_3 (resp. P_5) un 3-Sylow (resp. un 5-Sylow) de G.*

(a) Montrez que soit P_3 soit P_5 est distingué dans G puis que si P_5 est distingué dans G alors P_3 aussi. En déduire que P_3 et P_5 sont tous deux distingués dans G.
Indication: considérer G/P_5 et ses 3-Sylow puis conclure par un argument de comptage sur les éléments d'ordre 3 de G.

(b) On pose $N = P_3.P_5$. Montrez que N est cyclique. On note alors a un générateur de N.

(c) Montrez qu'il existe un élément de G d'ordre 2, que l'on note b.

(d) Montrez qu'il existe un entier i congru à 1 modulo 15 tel que $bab^{-1} = a^i$.

(e) Montrez qu'à isomorphisme près les groupes d'ordre 30 sont

$$\mathbb{Z}/30\mathbb{Z} \quad D_{15} \quad \mathbb{Z}/3\mathbb{Z} \times D_5 \quad \mathbb{Z}/5\mathbb{Z} \times D_3$$

(on montrera en particulier que ces groupes ne sont pas isomorphes).

Preuve: (a) Les théorèmes de Sylow donnent $k_3 \equiv 1 \bmod 3$, $k_5 \equiv 1 \bmod 5$, k_3 divise 10 et k_5 divise 6. Supposons donc k_3 et k_5 distincts de 1, soit $k_3 = 10$ et $k_5 = 6$. Les 3 et 5-Sylow étant cycliques, on obtient alors 20 éléments d'ordre 2 et 24 éléments d'ordre 5 soit plus de 30 éléments , d'où la contradiction.
On suppose $k_5 = 1$, soit P_5 distingué dans G de sorte que G/P_5 est un groupe d'ordre 6 qui possède donc un unique 3-Sylow, ou autrement dit G/P_5 possède 2 éléments d'ordre 3. On en déduit alors que G possède au plus 2×5 éléments d'ordre 3; en effet un élément d'ordre 3 de G s'envoie par la projection $G \longrightarrow G/P_5$ sur un élément d'ordre 3, et la classe de tout élément de G/P_5 est constitué de 5 éléments . Ainsi on ne peut avoir $k_3 = 10$ car alors on aurait 20 éléments d'ordre 3.
De même supposons $k_3 = 1$, soit P_3 distingué et G/P_3 est un groupe de cardinal 10 qui possède un unique 5-Sylow et donc 4 éléments d'ordre 5. Ainsi comme précédemment on en déduit que G possède au plus 12 éléments d'ordre 5 et donc $k_5 \neq 6$ soit $k_5 = 1$.

(b) Les groupes P_3 et P_5 étant distingués dans G, on en déduit que $N = P_3P_5$ est un sous-groupe distingué de G de cardinal 15; or tout groupe de cardinal 15 est cyclique (cf. exo précédent) soit $N \simeq \mathbb{Z}/15\mathbb{Z}$.

(c) Soit b un élément non trivial d'un 2-Sylow; il est alors d'ordre 2.

(d) La suite exacte $1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$ est scindée, un relèvement étant donné par $\{1, b\}$; en effet b n'appartient pas à N car 2 ne divise pas $15 = |N|$ et G/N est de cardinal 2, de sorte que la projection naturelle $\pi : G \longrightarrow G/N$ induit un isomorphisme $(b) \longrightarrow G/N \simeq \mathbb{Z}/2\mathbb{Z}$. On en déduit alors que G est isomorphe au produit semi-direct $N \rtimes (b)$ avec $b \longrightarrow (a \mapsto bab = a^i) \in \mathrm{Aut}(N)$. En outre comme b est d'ordre 2, on doit avoir $i^2 \equiv 1 \bmod 15$ soit $i = \pm 1, \pm 4$.

(e) Dans le cas $i = 1$, on obtient le produit direct $\mathbb{Z}/30\mathbb{Z}$; le cas $i = -1$ donne le groupe diédral D_{15}. Lorsque $i = 4$ (resp. $i = -4$), on note G_+ (resp. G_-) le groupe obtenu et on remarque que a^5 (resp. a^3) commute avec b; en effet on a $ba^5b = a^{20} = a^5$ (resp. $ba^3b = a^{-12} = a^3$) de sorte que (a^5) (resp. (a^3)) est inclu dans le centre de G. On a alors la suite exacte $1 \longrightarrow (a^5) \longrightarrow G \longrightarrow G/(a^5) \longrightarrow 1$ (resp. $1 \longrightarrow (a^3) \longrightarrow G \longrightarrow G/(a^3) \longrightarrow 1$) qui est scindée, un relèvement étant donné par $< b, a^3 >$ (resp. $< b, a^5 >$). En effet $< b, a^3 >$ (resp. $< b, a^5 >$) est bien un sous-groupe de G car $ba^3b = a^{12} = a^{-3}$ (resp. $ba^5b = a^{-20}a^{-5}$) isomorphe à D_5 (resp. D_3) et la projection naturelle $\pi_+ : G_+ \longrightarrow G_+/(a^5)$ (resp. $\pi_- : G_- \longrightarrow G_-/(a^3)$) est clairement injective et donc bijective par cardinalité. Ainsi G_+ (resp. G_-) est isomorphe au produit direct $D_5 \times \mathbb{Z}/3\mathbb{Z}$ (resp. $D_3 \times \mathbb{Z}/5\mathbb{Z}$), le produit étant direct car (a^5) (resp. (a^3)) est dans le centre. On remarque en particulier que les 4 groupes obtenus ne sont pas isomorphes car ils ont des centres distincts.

□

4 (*) Groupes résolubles et nilpotents: rappels et compléments

Exercice 1. *Soient G un groupe et H, K des sous-groupes.*

(a) On suppose H distingué dans G et $K \subset G$. Montrez que $H \cap K$ est distingué dans K et que $K/(K \cap H) \simeq HK/H$.

(b) On suppose H et K distingué dans G et $H \subset K$. Montrez que H est distingué dans K, que K/H est distingué dans G/H et que

$$\frac{G/H}{K/H} \simeq G/K$$

(c) On note $[H, K]$ le sous-groupe engendré par les commutateurs $hkh^{-1}k^{-1}$ avec $(h, k) \in H \times K$; on remarquera que si K est distingué alors $[H, K] \subset K$ et si de plus H est aussi distingué alors $[H, K]$ l'est aussi.

(i) Montrez que le groupe dérivé $[G, G]$ est le plus petit sous-groupe distingué N de G tel que G/N est abélien.

(ii) On pose $D_0(G) = G$ et pour $i > 0$, $D_i(G) = [D_{i-1}(G), D_{i-1}(G)]$; $(D_i(G))_i$ est appelé la suite dérivée de G. Le groupe G sera dit résoluble s'il existe $n \geqslant 0$ tel que $D_n(G) = (e)$.

- Montrez que G est résoluble si et seulement s'il existe une suite décroissante $(0) = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$, avec G_i distingué dans G_{i-1} et G_{i-1}/G_i abélien.

- Montrez que si G est résoluble alors tout sous groupe H de G l'est aussi.

- Soit H un sous-groupe distingué de G. Montrez que si G est résoluble alors G/H aussi. Réciproquement si H et G/H sont résolubles montrez que G aussi.

Preuve : (a) Soit $(h, k) \in (H \cap K) \times K$, alors $khk^{-1} \in K$ car K est un sous-groupe et $khk^{-1} \in H$ car H est distingué dans G, soit $H \cap K$ est distingué dans K.
On rappelle que HK est **l'ensemble** des éléments hk avec $h \in H$ et $k \in K$; c'est un sous-groupe lorsque H est distingué dans G; en effet on a $hkh'k' = h(kh'h^{-1})kk' = h_1k_1$ avec $h_1 = h(kh'k^{-1}) \in H$ et $k_1 = kk' \in K$. Soit alors $f : hk \in HK \mapsto \overline{k} \in K/(K \cap H)$; f est bien défini car si $hk = h'k'$ alors $k = h^{-1}h'k'$ avec $h^{-1}h' = k(k')^{-1} \in H \cap K$ et donc $\overline{k} = \overline{k}'$. En outre f est un morphisme de groupes car

$$f(hkh'k')f(h(kh'k^{-1})kk') = \overline{kk'} = \overline{kk}' = f(hk)f(h'k')$$

Le morphisme f étant clairement surjectif, soit $hk \in \operatorname{Ker} f$; on a alors $k \in H$ et $hk \in H$ de sorte que f défini l'isomorphisme demandé.

(b) Le groupe H est clairement distingué dans K et de même K/H est distingué dans G/H. On vérifie aisément que l'application $f : \overline{g}^H \in G/H \mapsto \overline{g}^K \in G/K$ est un morphisme de groupe surjectif dont le noyau est K/H, cqfd.

(c) (i) Si K est distingué dans G, alors le commutateur $[h, k] := (hkh^{-1})k^{-1}$, pour $k \in K$, appartient à K, de sorte que $[H, K]$ qui est le plus petit sous-groupe de G contenant tous les $[h, k]$ pour $(h, k) \in H \times K$, est contenu dans K. Si on suppose en outre que H est aussi distingué dans G, on a alors $g[h, k]g^{-1} = [ghg^{-1}, gkg^{-1}] \in [H, K]$ de sorte que $[H, K]$ est distingué dans G.

D'après ce qui précède $[G,G]$ est un sous-groupe distingué de G. Il est tout d'abord évident que le groupe quotient $G/[G,G]$ est abélien, car $[\overline{g}_1,\overline{g}_2]=\overline{e}_G$, où e_G est l'élément neutre de G, soit $\overline{g}_1\overline{g}_2=\overline{g}_2\overline{g}_1$. Soit alors G' un groupe abélien et $f:G\longrightarrow G'$ un morphisme de groupe; on a alors $f([g_1,g_2])=0$ soit $[G,G]\subset \operatorname{Ker} f$ de sorte que f se factorise en un morphisme $\overline{f}:G/[G,G]\longrightarrow G'$; on dit que alors que $[G,G]$ est universel, au sens où pour tout $f:G\longrightarrow G'$ avec G' abélien alors $[G,G]$ est contenu dans $\operatorname{Ker} f$. En appliquant ce résultat à un quotient G/N abélien pour un sous-groupe distingué N de G, on en déduit que $[G,G]$ est contenu dans N.

(ii) - Supposons G résoluble, la suite $G_i=D_i(G)$ convient d'après (i). Réciproquement, d'après (i), on montre par récurrence que $D_i(G)$ est inclu dans G_i et donc $D_n(G)=\{e_G\}$ soit G résoluble.

- Supposons G résoluble et soit $(G_n,\cdots,G_0)$ une suite de résolubilité de G; soit $H_i:=G_i\cap H=G_i\cap H_{i-1}$ qui est distingué dans H_{i-1} d'après (a). En outre on a

$$H_{i-1}/H_i=\frac{G_{i-1}\cap H}{G_i\cap(G_{i-1}\cap H)}\simeq\frac{G_i(G_{i-1}\cap H)}{G_i}$$

d'après (a), qui est donc abélien comme sous-groupe de G_{i-1}/G_i, et donc H est résoluble.

- Supposons G résoluble et soit $(G_n,\cdots,G_0)$ une suite de résolubilité de G. Pour tout i, H est distingué dans G_iH, lui-même distingué dans $G_{i-1}H$ et donc G_iH/H est distingué dans $G_{i-1}H/H$. Ainsi $(G_nH/H,\cdots,G_0H/H)$ constitue une suite de résolubilité de G/H car d'après (b)

$$\frac{G_{i-1}H/H}{G_iH/H}\simeq\frac{G_{i-1}H}{G_iH}$$

qui est abélien car $\frac{G_{i-1}H}{G_iH}=\frac{G_{i-1}(G_iH)}{G_iH}\simeq\frac{G_{i-1}}{G_{i-1}\cap G_iH}\simeq\frac{G_{i-1}/G_i}{(G_{i-1}\cap G_iH)/G_i}$ abélien comme quotient de G_{i-1}/G_i, et donc G/H résoluble.

- Soit $(H_n,\cdots,H_0)$ une suite de résolubilité de H et $(K_s,\cdots,K_0)$ une suite de résolubilité de G/H. On note G_i $(0\leqslant i\leqslant s)$ le sous-groupe de G image réciproque de K_i par la projection canonique $G\longrightarrow G/H$. On a alors

$$\{1\}=H_n\subset H_{n-1}\subset\cdots\subset H_0=G_s\subset G_{s-1}\subset\cdots\subset G_0=G$$

Il suffit alors de vérifier que le quotient G_{i-1}/G_i est abélien, ce qui est le cas car d'après (b), il est isomorphe à

$$\frac{G_{i-1}/H}{G_i/H}$$

□

Exercice 2. *(a) Montrez que , $\mathcal{S}_4$ et D_n sont résolubles.*

(b) Montrez que dans un groupe résoluble G, un sous-groupe non trivial H de G distingué et minimal pour cette propriété est nécessairement abélien. Dans le cas où H est fini, soit p premier divisant $|H|$; montrez que $H\simeq(\mathbb{Z}/p\mathbb{Z})^n$.

(c) On pose $C_0(G)=G$ et pour $i>0$, $C_i(G)=[G,C_{i-1}(G)]$. La suite $(C_i(G)_i$ est appelée la suite centrale descendante de G. Le groupe G sera dit nilpotent s'il existe $n\geqslant 0$ tel que $C_n(G)=(e)$.

- Montrez que $C_i(G)$ est un sous-groupe caractéristique de G; on rappelle qu'un sous-groupe H de G est dit caractéristique si pour tout $\phi \in \mathrm{Aut}\, H$, on a $\phi(H) = H$.

- Montrez ensuite que $C_{i+1}(G)$ est le plus petit sous-groupe distingué N de G contenu dans $C_i(G)$ tel que $C_i(G)/N$ soit contenu dans le centre $Z(G/N)$ de G/N.

- On construit par récurrence un suite ascendante $Z_i(G)$ de sous-groupe de G, définie par $Z_0(G) = \{e_G\}$ et $Z_i(G)$ est tel que $Z_i(G)/Z_{i-1}(G)$ est le centre de $G/Z_{i-1}(G)$. Montrez que G est nilpotent si et seulement si il existe n tel que $Z_n(G) = G$. En déduire que tout p-groupe est nilpotent. A quelle condition D_n est-il nilpotent ?

(d) (i) Soit G un groupe nilpotent et H un sous-groupe propre de G; montrez que H est inclu strictement dans $N_G(H)$.

(ii) Soit G fini et P un p-Sylow de G; montrez que pour tout sous-groupe H de G contenant $N_G(P)$, on a $H = N_G(H)$.

(iii) Soit G fini; montrez que les 3 conditions suivantes sont équivalentes

(1) G est nilpotent;

(2) pour tout sous-groupe propre H de G, on a H inclu strictement dans $N_G(H)$;

(3) G est produit direct de ses sous-groupes de Sylow.

Preuve: (a) Pour $\mathcal{S}_4$, on a $(0) \subset \{\mathrm{Id}, (1\ 2)(3\ 4)\} \subset V_4 \subset \mathcal{A}_4 \subset \mathcal{S}_4$, où

$$V_4 = \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

avec $\mathcal{S}_4/\mathcal{A}_4 \simeq \mathbb{Z}/2\mathbb{Z} \simeq V_4/\{\mathrm{Id}, (1\ 2)(3\ 4)\}$ et $\mathcal{A}_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$, de sorte que $\mathcal{S}_4$ est résoluble.
Pour le groupe diédral on a $(0) \subset \mathbb{Z}/2\mathbb{Z} \subset D_n$ avec $D_n/(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.

(b) Soit H un sous-groupe distingué minimal de G; d'après ce qui précède $[H, H]$ est un sous-groupe distingué de G de sorte que $[H, H]$ est soit trivial soit égal à H; or si $[H, H] = H$ alors H n'est pas résoluble ce qui ne se peut pas car G l'est. Ainsi on a $[H, H] = \{e_G\}$ soit H abélien.
Supposons de plus H fini et soit p premier divisant $|H|$; on considère K l'ensemble des éléments d'ordre p de H auquel on rajoute l'élément neutre; H étant commutatif, K est clairement un sous-groupe de H: en effet pour $x, y \in H$ d'ordre p, xy est un élément de H qui est d'ordre un diviseur de p, i.e. qui est soit d'ordre p soit l'élément neutre. En outre H étant distingué dans G, K l'est aussi. Or K n'est pas réduit à l'élément neutre, car H possède un élément d'ordre p, il suffit pour cela de considérer un élément h d'un p-Sylow de H; l'ordre de h est p^r pour $r \geqslant 1$ de sorte que $h^{p^{r-1}}$ est d'ordre p. Par minimalité de H, on en déduit $K = H$ soit H est un groupe abélien dont tous ses éléments autre que l'élément neutre sont d'ordre p, de sorte que H est un p-groupe isomorphe à $(\mathbb{Z}/p\mathbb{Z})^m$ pour un certain entier $m \geqslant 1$.

(c) On raisonne par récurrence; $C_0(G) = G$ étant clairement un sous-groupe caractéristique. Supposons donc $C_i(G)$ caractéristique, et soit $[g, c] \in C_{i+1}(G)$ avec donc $c \in C_i(G)$; pour $\phi \in \mathrm{Aut}\, G$, on a alors $\phi([g, c]) = [\phi(g), \phi(c)] \in C_{i+1}(G)$ car d'après l'hypothèse de récurrence, $c \in C_i(G)$. On en déduit alors que $\phi(C_{i+1}(G)) \subset C_{i+1}(G)$ soit $C_{i+1}(G)$ caractéristique.

Dans le quotient $G/C_{i+1}(G)$, on a $\overline{cg} = \overline{gc}$, pour tout $g \in G$ et $c \in C_i(G)$, de sorte que $C_i(G)/C_{i+1}(G)$ est contenu dans le centre de $G/C_{i+1}(G)$. Soit alors N un sous-groupe de $C_i(G)$ tel que $C_i(G)/N$ est contenu dans le centre de G/N; on a alors pour tout $g \in G$ et $c \in C_i(G)$, $\overline{gc} = \overline{cg}$ soit $[g, c] \in N$ et donc N contient $C_{i+1}(G)$, d'où le résultat.

Supposons que G est nilpotent et montrons par récurrence que $Z_i(G)$ contient $C_{n-i}(G)$; c'est clairement vrai pour $i = 0$ et supposons le résultat vérifié au rang i. On considère alors la projection canonique $G/C_{n-i}(G) \longrightarrow G/Z_i(G)$; d'après ce qui précède $C_{n-i-1}(G)/C_{n-i}(G)$ est contenu dans le centre $Z_{i+1}(G)/Z_i(G)$ de $G/Z_i(G)$, soit $C_{n-i-1}(G) \subset Z_{i+1}(G)$, de sorte que par récurrence $G = C_0(G) \subset Z_n(G)$. Réciproquement supposons qu'il existe n tel que $Z_n(G) = G$ et montrons par récurrence que $C_i(G) \subset Z_{n-i}(G)$, ce qui est clairement vrai pour $i = 0$; $C_{i+1} = (G) = [G, C_i(G)] \subset [G, Z_{n-i}(G)] \subset Z_{n-i-1}(G)$ car $Z_{n-i}(G)/Z_{n-i-1}(G)$ est contenu dans le centre de $G/Z_{n-i-1}(G)$; ainsi par récurrence on a $C_n(G) \subset Z_0(G) = \{e_G\}$, d'où le résultat.
Soit alors G un p-groupe; on a vu dans un exercice précédent que le centre de G n'est pas réduit à l'élément neutre de sorte que $Z_1(G)$ est strictement plus grand que $Z_0(G)$; le quotient $G/Z_i(G)$ étant un p-groupe, on montre de même que $Z_{i+1}(G)$ contient strictement $Z_i(G)$ de sorte qu'il existe n tel que $Z_n(G) = G$, soit G nilpotent.
On remarque qu'un élément de D_n est dans son centre si et seulement si il commute à s un élément d'ordre 2; on note ainsi que le centre Z_n de D_n est non trivial si et seulement si n est pair; il est alors égal à $\{1, r^{n/2}\}$ où r est un élément d'ordre n; le quotient D_n/Z_n est alors isomorphe à $D_{n/2}$. Ainsi D_n est nilpotent si et seulement si n est une puissance de 2.

(d) (i) Soit i tel que $Z_i(G) \subset H$ et $Z_{i+1}(G) \not\subset H$; soit alors $g \in Z_{i+1}(G)$ et $g \notin H$; pour tout $h \in H$, on a $[g, h] \in Z_i(G) \subset H$ soit $ghg^{-1} \in H$ et donc $g \in N_G(H)$, d'où le résultat.

(ii) Soit H contentant $N_G(P)$ et $g \in N_G(H)$; gPg^{-1} est alors un p-Sylow de H de sorte que d'après les théorèmes de Sylow, il existe $h \in H$ tel que $gPg^{-1} = hPh^{-1}$ et donc $h^{-1}g \in N_G(P) \subset H$ et donc $g \in H$, d'où le résultat, l'inclusion inverse étant évidente.

(iii) On a déjà vu les implications (1) $\Rightarrow$ (2) et (3) $\Rightarrow$ (1); montrons donc (2) $\Rightarrow$ (3). D'après (ii), on en déduit que pour tout Sylow P, on a $N_G(P) = G$, soit P distingué et donc pour tout premier p, l'unicité d'un p-Sylow. En outre pour $p_1 \neq p_2$ des premiers distincts et P_1, P_2 les Sylow correspondant, on a $[P_1, P_2] \subset P_1 \cap P_2 = \{e_G\}$, ou autrement dit les éléments de deux p-Sylow distincts commutent. On considère alors l'application $f : P_1 \times \cdots \times P_r \longrightarrow G$ définie par $f(g_1, \cdots, g_r) = g_1.\cdots.g_r$, où les P_i sont les Sylow de G; comme les g_i commutent entre eux, on en déduit que f est un morphisme de groupe. En outre f est injectif car si $g_1 \cdots g_r = 1$, on a alors $g_2^{q_1} \cdots g_r^{q_1} = 1$ où q_1 est une puissance de p_1 telle que $g_1^{q_1} = 1$; par récurrence on en déduit que $g_i^{q_1} = 1$ soit $g_i = 1$ car l'ordre de g_i est premier avec q_1; ainsi par cardinalité f est un isomorphisme d'où (iii).

□

5 Groupes orhtogonaux euclidiens

Soit donc q une forme quadratique définie positive sur un $\mathbb{R}$-espace vectoriel E de dimension $n \geqslant 1$ et soit $O(q)$ le groupe orthogonal associé.

Exercice 1. *Donnez le centre Z de $O(q)$ (resp. Z^+ de $O^+(q)$) et montrez que $O(q)$ est un produit semi-direct de $O^+(q)$ par $\mathbb{Z}/2\mathbb{Z}$; a quelle condition ce produit semi-direct peut-il être pris direct ?*

Preuve : Il est clair que $\{Id, -Id\} \subset Z$; réciproquement soit $z \in Z$ et τ_D une réflexion de droite D. On a $z\tau_D z^{-1} = \tau_D = \tau_{z(D)}$ de sorte que z laisse stable toutes les droites de l'espace; c'est donc une homothétie (résultat classique) et donc $z = \pm Id$.

En ce qui concerne Z^+ remarquons que $-Id$ appartient à $O^+(q)$ si et seulement si n est pair. Pour $n \geqslant 3$ soit τ_P un renversement de plan P; on a $z\tau_P z^{-1} = \tau_P = \tau_{z(P)}$ de sorte que z laisse stable tous les plans de l'espace. Toute droite étant l'intersection de deux plans, on en déduit de même que z laisse stable toutes les droites de l'espace, soit $Z^+ = \{Id\}$ pour n impair et sinon $Z^+ = Z$ pour n pair. Pour $n = 2$, il est bien connu que O^+ est commutatif.

Il est clair que la suite exacte $1 \to O^+(q) \longrightarrow O(q) \longrightarrow \mathbb{Z}/2\mathbb{Z} \to 0$ est scindée, un relèvement étant donné par exemple par une réflexion quelconque. Pour obtenir un produit direct, il faut trouver un élément d'ordre 2 qui n'est pas dans O^+ et qui commute à tous les éléments de O^+; la seule possibilité est alors $-Id$ en dimension impaire.

□

Exercice 2. *Soit $u \in O(q)$ et $F_u = \{x \in E \ / \ u(x) = x\}$ et on note $p_u = n - \dim F_u$. Montrez par récurrence sur p_u, que u est le produit d'au plus p_u réflexions. Montrez ensuite que u est le produit d'au moins p_u réflexions.*

Preuve : On raisonne par récurrence sur p_u, le cas $p_u = 0$ correspondant à $u = Id$. Supposons donc $p_u > 0$ et soit $x \in F_u^\perp$ non nul et soit $y = u(x) \neq x$ car $x \notin F_u$; on a $y \in F_u^\perp$ car F_u étant stable par u, $F_u^\perp$ l'est aussi. De plus comme x et y on même norme, on en déduit que $(x - y, x + y) = 0$ (triangle isocèle). On considère alors la réflexion τ définie par $x - y$ de sorte que $\tau(x-y) = y-x$ et $\tau(x+y) = x+y$ soit donc $\tau(y) = x$ avec $\tau_{|F_u} = Id$. Ainsi on a $F_u \subset F_{\tau \circ u}$ ce dernier contenant x de sorte que $p_{\tau\circ u} < p_u$ et on conclut par récurrence.

En outre si u est le produit de r réflexions alors F_u est clairement de dimension supérieure ou égale à $n - r$ (l'intersection de r hyperplans) soit donc $p_u \leqslant r$.

□

Exercice 3. *Montrez que pour $n \geqslant 3$, tout élément de $O^+(q)$ est produit d'au plus n renversements.*

Preuve : Le cas $n = 3$ est évident en remarquant que si τ est une réflexion, alors $-\tau$ est un renversement de sorte que le produit de deux réflexions (et donc tout produit d'un nombre pair) est un produit de deux renversements $\tau_1 \circ \tau_2 = (-\tau_1) \circ (-\tau_2)$.

Pour $n \geqslant 3$, soient τ_1 et τ_2 des réflexions par rapport aux hyperplans H_1 et H_2 et $u = \tau_1 \circ \tau_2$. Soit alors $V \subset H_1 \cap H_2$ un sous-espace de dimension $n - 3$: $u_{|V} = Id$ et $V^\perp$ est stable sous u. D'après le cas $n = 3$, on a $u_{V^\perp} = \sigma_1 \circ \sigma_2$ où σ_1, σ_2 sont des renversements de $V^\perp$. On obtient le résultat en prolongeant les σ_i par l'identité sur V.

□

Exercice 4. *Soient u_1 et u_2 deux symétries orthogonales de même nature (i.e. tels que $\dim \mathrm{Ker}(u_1 - Id) = \dim \mathrm{Ker}(u_2 - Id)$). Montrez que u_1 et u_2 sont conjuguées par $O^+(q)$. En déduire alors que $D(O(q)) = D(O^+(q)) = O^+(q)$.*

Preuve : On décompose l'espace $E = E_1 \oplus E_1^\perp = E_2 \oplus E_2^\perp$ où $E_i = \mathrm{Ker}(u_i - Id)$. On choisit alors des bases orthonormées (e_i^1) et (e_i^2) de E adaptées à ces décompositions. Soit alors u tel que $u(e_i^1) = e_i^2$; u est une isométrie et quitte à changer ϵ_1 en $-\epsilon_1$, on peut supposer que u est positive. On vérifie alors immédiatement que $u \circ u_1 \circ u^{-1} = u_2$.

L'inclusion $D(O(q)) \subset O^+(q)$ est évidente; réciproquement soient τ_1 et τ_2 deux réflexions et soit u tel que $u \circ \tau_1 \circ u^{-1} = \tau_2$ de sorte que $\tau_1 \circ \tau_2 = [\tau_1, u]$. Comme tout élément de $O^+(q)$ est le produit d'un nombre pair de réflexions, on obtient bien l'inclusion réciproque.

De même pour montrer que $O^+(q) \subset D(O^+(q))$ pour $n \geqslant 3$, il suffit de montrer que tout renversement est un commutateur. Soit V un sous-espace de dimension 3 et (e_1, e_2, e_3) une base orthonormée. Soient $\sigma_1, \sigma_2, \sigma_3$ les renversements définis par $(\sigma_i)_{|V^\perp} = Id$ et $\sigma_i(e_i) = e_i$) et donc $\sigma_i(e_j) = -e_j$ pour $i \neq j$. On a alors $\sigma_3 = \sigma_1 \circ \sigma_2$. En outre il existe $u \in O^+(q)$ tel que $\sigma_2 = u \circ \sigma_1 \circ u^{-1}$ et donc $\sigma_3 = [\sigma_1, u]$.

□

Exercice 5. *Montrez que pour tout $u \in O(q)$, il existe une décomposition orthogonale*

$$E = \mathrm{Ker}(u - Id) \oplus \mathrm{Ker}(u + Id) \oplus P_1 \oplus \cdots \oplus P_r$$

où les P_i sont des plans stables par u, tels que la restriction de u y soit une rotation.

Preuve : On procède par récurrence sur la dimension, les cas $n = 1$ et $n = 2$ étant bien connus. Si u admet une valeur propre réelle (forcément ± 1), c'est terminé (en particulier si n est impair). Sinon soit $\lambda \in \mathbb{C}$ une valeur propre du complexifié de $u_{\mathbb{C}}$, de sorte que $\overline{\lambda}$ est aussi valeur propre. Soit alors $x \in E \otimes_{\mathbb{R}} \mathbb{C}$ un vecteur propre du complexifié relativement à λ et soit $\overline{x}$ son conjugué qui est alors propre pour $\overline{\lambda}$ relativement à $u_{\mathbb{C}}$. Le plan complexe $P = \mathbb{C}x + \mathbb{C}\overline{x}$ est alors invariant par $u_{\mathbb{C}}$. On remarque alors que les vecteurs $\frac{x+\overline{x}}{2}$ et $\frac{x-\overline{x}}{2i}$ sont réels et forment une base de P de sorte que le plan réel qu'ils engendrent et stable sous u.

□

Exercice 6. - *On veut prouver la simplicité de $O^+(3, \mathbb{R})$. Soit donc N un sous-groupe distingué non réduit à l'identité; expliquez pourquoi il suffit de montrer que N contient un renversement.*

- Soit alors $u \in N$, une rotation d'axe D et soit P le plan orthogonal à D à l'origine de sorte que la restriction de u à P est une rotation d'angle θ que l'on suppose $0 < \theta < \pi$. Soient alors x et $y = u(x)$ des points de la sphère unité de E; on note d la distance entre x et y. Montrez que pour tout $0 \leqslant d' \leqslant d$, il existe x_1, x_2 des points de la sphère unité à distance d' l'un de l'autre et tels que $x_2 = u(x_1)$.

- Déduire de ce qui précède qu'étant donnés y_1, y_2 des points de la sphère unité distant de d' avec $0 \leqslant d' \leqslant d$, il existe $u' \in N$ tels que $u'(y_1) = y_2$. En considérant la rotation d'axe z et d'angle π/m pour m assez grand, construire un retournement de N et conclure.

Preuve : - Comme les renversements engendrent $O^+(3, \mathbb{R})$ et sont conjugués sous $O^+(3, \mathbb{R})$, il suffit de montrer que N en contient un.

- Un calcul classique donne $d^2 = 2(1 - \cos\theta)$. Soit a un des points de $D \cap S^2$; le résultat découle de l'observation que u envoie le méridien contenant a et x, sur celui contenant a et y et que lorsque x_1 varie de x à a, la distance $||x_1 - u(x_1)||$ varie continument de d à 0. De façon précise, on considère $x + \lambda a$ de norme au carré égale à $1 + \lambda^2$ de sorte que $x_1 = \frac{x+\lambda a}{\sqrt{1+\lambda^2}} \in S^2$. On a alors $||u(x_1) - x_1|| = \frac{d}{\sqrt{1+\lambda^2}}$ de sorte qu'il suffit de prendre $\lambda = \frac{\sqrt{d^2-m^2}}{m}$.

- Soit x_3 (resp. y_3) un vecteur de norme 1 orthogonal au plan engendré par x_1 et x_2 (resp. y_1 et y_2) et soit u tel que $s(x_i) = y_i$ pour $i = 1, 2, 3$. Il est clair que s conserve le produit scalaire et donc $u \in O(3, \mathbb{R})$; quitte à changer y_3 en $-y_3$, on peut supposer que s est positive. On pose $u' := s \circ u \circ s^{-1} \in N$ et $u'(y_1) = y_2$. Soit alors r_n la rotation d'angle π/n et d'axe a. Comme $\mathbb{R}$ est archimédien, le rapport π/n tend vers 0 quand n tend vers $+\infty$ et donc pour n assez grand $||x - r_n(x)|| \leqslant d$. On pose alors $x_0 = x$ et $x_{i+1} = r_n(x_i)$ avec donc $x_n = -x$. Comme on a $||x_{i+1} - x_i|| \leqslant d$ il existe alors $u_i \in N$ tel que $u(x_i) = x_{i+1}$ de sorte que $v = u_n \circ \cdots \circ u_1 \in N$ et $v(x) = -x$ et v est donc un renversement, d'où le résultat.

□

6 Le corps des quaternions

Exercice 1. *On note H le corps des quaternions et soit G ceux de norme 1: $G = \{a + bi + cj + dk \ / \ a^2 + b^2 + c^2 + d^2 = 1\}$. On considère alors l'action de G sur H par automorphismes intérieurs. En restreignant cette action à l'ensemble P des quaternions purs, montrez que l'on obtient alors un isomorphisme $G/\{\pm 1\} \simeq O(3,\mathbb{R})^+$. La suite exacte associée est-elle scindée ?*

Preuve : On a $P \simeq \mathbb{R}^3$ et on vérifié aisément que l'action de conjugaison de G est $\mathbb{R}$-linéaire et conserve la norme de sorte qu'elle définit un morphisme de groupes $G \longrightarrow O(3,\mathbb{R})$. On note en outre que $G \simeq S^3$ est connexe et que le morphisme précédent est continue de sorte que l'image de $G \to O(3,\mathbb{R}) \to \{\pm 1\}$ est connexe et donc égale à $\{1\}$. On obtient donc bien un morphisme de groupe $\phi : G \longrightarrow O^+(3,\mathbb{R})$. Montrons la surjectivité: soit $p \in P \cap G$, on a $\phi_p(p) = p$ ce qui prouve que ϕ_p fixe p (et est non triviale), c'est donc une rotation d'axe p. En outre on a $p^2 = -1$ soit ϕ_p d'ordre 2; c'est donc un renversement. On obtient donc tous les renversements, or ceux-ci engendrent $O^+(3,\mathbb{R})$, d'où la surjectivité. Pour le noyau, on a $\phi_g(p) = p$ pour tout $p \in P$ si et seulement si g commute à tous les éléments de P et donc à tous les éléments de H, soit donc $g \in \mathbb{R} \cap G = \{\pm 1\}$.

Si la suite exacte

$$1 \to \{\pm 1\} \longrightarrow G \xrightarrow{\phi} O^+(3,\mathbb{R}) \to 1$$

était scindée, on aurait un sous-groupe H de G tel que $\phi_{|H}$ soit un isomorphisme de H sur $O^+(3,\mathbb{R})$. Mais alors pour $g \in G$, on aurait g ou $-g$ qui appartiendrait à H. En prenant $o \in P \cap G$, on a $p^2 = (-p)^2 = -1$ soit donc $-1 \in H$, contradiction.

□

Exercice 2. *On considère l'action de $G \times G$ sur H définie par $(q_1, q_2).q := q_1 q \overline{q}_2$. Montrez que l'on définit ainsi un isomorphisme $G \times G/\{(1,1),(-1,-1)\} \simeq O(4,\mathbb{R})^+$ et en déduire que $PO(4,\mathbb{R})^+ \simeq O(3,\mathbb{R})^+ \times O(3,\mathbb{R})^+$.*

Preuve : L'application ϕ_{q_1,q_2} est clairement $\mathbb{R}$-linéaire et conserve la norme. Par continuité, on conclut comme précédemment que son image est contenue dans les isométries positives soit donc

$$\phi : G \times G \longrightarrow O^+(4,\mathbb{R})$$

Soit $(q_1, q_2) \in \operatorname{Ker}\phi$, i.e. $q_1 q \overline{q}_2 = q$ pour tout $q \in H$. Pour $q = 1$, on trouve $q_1 = q_2$ de sorte qu'ensuite q_1 est central et donc $\operatorname{Ker}\phi = \{(1,1),(-1,-1)\}$.

Pour la surjectivité, soit $u \in O^+(4,\mathbb{R})$, si on a $u(1) = 1$, comme $P = 1^\perp$, on a $u(P) = P$ avec $u_{|P} \in O^+(3,\mathbb{R})$ et d'après ce qui il existe $q \in G$ tel que $\phi_{q,q} = u$. Si on a $u(1) = g$, on a alors $\phi_{\overline{g},1} \circ u(1) = 1$ et on conclut grâce au cas précédent. Finalement on obtient donc

$$G \times G/\{(1,1),(-1,-1)\} \simeq O(4,\mathbb{R})^+$$

En passant au groupe projectif, on cherche les couples (q_1, q_2) tels que $\phi_{q_1,q_2} = -Id$, i.e. $q_1 q \overline{q}_2 = -q$ pour tout $q \in H$. En faisant $q = 1$, on obtient $q_1 = -q_2$, puis on voit que q_1 est central soit alors

$$G \times G/V \simeq PO(4,\mathbb{R})^+$$

où $V = \{(1,1),(1,-1),(-1,1),(-1,-1)\}$. En outre la projection canonique $G \to G/\{\pm 1\}$ induit un isomorphisme

$$(G \times G)/V \simeq G/\{\pm 1\} \times G/\{\pm 1\}$$

et donc d'après ce qui précède

$$PO(4,\mathbb{R})^+ \simeq O(3,\mathbb{R})^+ \times O(3,\mathbb{R})^+.$$

□