

# TD1 : OUTILS DE LA THÉORIE DES GROUPES

Diego Izquierdo

*Il se peut qu'il y ait des coquilles (voire des erreurs...) : n'hésitez pas à me les signaler !  
Et si vous avez des questions, n'hésitez pas à m'écrire (diego.izquierdo@ens.fr) ou venir me voir (bureau T12) ! Les exercices 1 et 2 ont été traités pendant la séance.*

### Exercice 3 : Sous-groupes de $D_8$

On appelle  $D_8$  le groupe des isométries du carré. Quels sont les sous-groupes de  $D_8$  ? Lesquels sont distingués ?

**Indications :** Soit  $r$  la rotation d'angle  $\pi/2$  et  $s$  la symétrie par rapport à l'une des diagonales du carré. Alors  $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ , et on a les relations  $r^4 = 1$ ,  $s^2 = 1$ ,  $srs = r^{-1}$ .

- Sous-groupes d'ordre 1 :  $\{1\}$ .
  - Sous-groupes d'ordre 2 :  $\{1, r^2\}$ ,  $\{1, s\}$ ,  $\{1, sr\}$ ,  $\{1, sr^2\}$ ,  $\{1, sr^3\}$ .
  - Sous-groupes d'ordre 4 : le seul sous-groupe cyclique d'ordre 4 de  $D_8$  est  $\{1, r, r^2, r^3\}$ . Pour trouver les sous-groupes isomorphes à  $(\mathbb{Z}/2\mathbb{Z})^2$ , on remarque qu'ils sont tous des réunions de trois sous-groupes parmi  $\{1, r^2\}$ ,  $\{1, s\}$ ,  $\{1, sr\}$ ,  $\{1, sr^2\}$ ,  $\{1, sr^3\}$ . On vérifie alors aisément que ce sont les sous-groupes  $\{1, r^2, s, sr^2\}$  et  $\{1, r^2, sr, sr^3\}$ .
  - Sous-groupes d'ordre 8 :  $D_8$ .
- Parmi ces sous-groupes, les sous-groupes distingués sont  $\{1\}$ ,  $\{1, r^2\}$ ,  $\{1, r, r^2, r^3\}$ ,  $\{1, r^2, s, sr^2\}$ ,  $\{1, r^2, sr, sr^3\}$ ,  $D_8$ .

### Exercice 4 : Sous-groupes transitifs du groupe symétrique

Soit  $n \geq 1$ . Un sous-groupe de  $S_n$  est dit transitif s'il agit transitivement sur  $\{1, 2, \dots, n\}$ .

1. Montrer que  $n$  divise l'ordre de tout sous-groupe transitif de  $S_n$ .

**Indications :** Cela découle immédiatement de la formule des classes.

2. En déduire quels sont les sous-groupes transitifs de  $S_p$  pour  $p$  premier.

**Indications :** Si  $H$  est un sous-groupe transitif de  $S_p$ , alors  $p \mid |H|$ , et donc  $H$  contient un  $p$ -cycle. Réciproquement, un sous-groupe de  $S_p$  contenant un  $p$ -cycle est bien transitif.

3. Montrer que tout conjugué d'un sous-groupe transitif est transitif.

**Indications :** Soit  $H$  un sous-groupe transitif de  $S_p$ . Soient  $g \in S_p$  et  $x \in \{1, 2, \dots, p\}$ . Comme  $H$  est transitif, il existe  $h \in H$  tel que  $hg^{-1}(1) = g^{-1}(x)$ . Donc  $ghg^{-1}(1) = x$ , ce qui montre que  $gHg^{-1}$  est transitif.

4. Nous allons déterminer tous les sous-groupes transitifs de  $S_4$ .

(a) Quels sont les sous-groupes transitifs de  $S_4$  d'ordre 12 ?

**Indications :** Soit  $H$  un sous-groupe d'ordre 12 de  $S_4$ . D'après le lemme d'Ore,  $H$  est un sous-groupe distingué de  $S_4$ . Par conséquent, s'il contient une transposition, il contient toutes les transpositions, et comme les transpositions engendrent  $S_4$ , on obtient  $H = S_4$  : absurde ! Donc  $H$  ne contient aucune transposition. Comme toute permutation impaire est produit d'un nombre impair de transpositions, cela entraîne que  $H$  est contenu dans  $A_4$ . Comme  $H$  est d'ordre 12, on en déduit que  $H = A_4$ . C'est le seul sous-groupe (transitif) d'ordre 12 de  $S_4$ .

- (b) Exhiber un 2-Sylow  $H$  de  $S_4$  et montrer que  $H \cong D_8$ .

**Indications :** Le groupe  $S_4$  est d'ordre 24. Il suffit donc d'exhiber un sous-groupe de  $S_4$  isomorphe à  $D_8$ . Pour ce faire, on remarque que le groupe  $D_8$  agit sur l'ensemble des sommets d'un carré. Cette action étant fidèle, elle induit un morphisme de groupes injectif  $D_8 \hookrightarrow S_4$ . L'image de ce morphisme est donc un sous-groupe de  $S_4$  isomorphe à  $D_8$ . Plus explicitement, il s'agit du sous-groupe de  $S_4$  engendré par  $s = (1\ 3)$  et  $r = (1\ 2\ 3\ 4)$ .

- (c) Déterminer tous les sous-groupes transitifs de  $H$ . On pourra utiliser l'exercice 3.

**Indications :** Soit  $K$  un sous-groupe transitif contenu dans  $H$ . D'après la question 1, son ordre est multiple de 4. En regardant la liste faite dans l'exercice 3, on voit que les sous-groupes transitifs de  $H$  sont  $H$ ,  $\{1, r^2, sr, sr^3\}$  et  $\{1, r, r^2, r^3\}$ .

- (d) Quels sont les sous-groupes transitifs de  $S_4$  à conjugaison près ?

**Indications :** Soit  $K$  un sous-groupe transitif de  $S_4$ . D'après la question 1, l'ordre de  $K$  est multiple de 4. Si  $K$  est d'ordre au moins 12, alors  $K$  est  $A_4$  ou  $S_4$  d'après 3.(a). Reste donc à étudier les cas où  $K$  est d'ordre 4 ou 8. Mais dans ce cas, d'après les théorèmes de Sylow,  $K$  est conjugué à un sous-groupe de  $H$ . En utilisant la question précédente, on déduit que les sous-groupes transitifs de  $S_4$  sont  $S_4$ ,  $A_4$ , et tous ceux qui sont conjugués à  $H = \langle (1\ 3), (1\ 2\ 3\ 4) \rangle$ , à  $\langle (1\ 3)(2\ 4), (1\ 2)(3\ 4) \rangle$  ou à  $\langle (1\ 2\ 3\ 4) \rangle$ .

### Exercice 5 : Générateurs du groupe symétrique

1. Soit  $n \geq 1$ . Montrer que la transposition  $(1\ 2)$  et le  $n$ -cycle  $(1\ 2\ \dots\ n)$  engendrent  $S_n$ .

**Indications :** Soit  $H = \langle (1\ 2), (1\ 2\ \dots\ n) \rangle$ . On remarque que :

$$(1\ 2\ \dots\ n)^k (1\ 2) (1\ 2\ \dots\ n)^{-k} = ((k+1)\ (k+2))$$

pour  $1 \leq k \leq n-2$ . Donc  $(1\ 2), (2\ 3), \dots, ((n-1)\ n)$  sont dans  $H$ . Soient  $a$  et  $b$  deux éléments de  $\{1, 2, \dots, n\}$  tels que  $a < b$ . On remarque alors que :

$$(a\ b) = (a\ (a+1))((a+1)\ (a+2))\dots$$

$$\dots((b-2)\ (b-1))((b-1)\ b)((b-2)\ (b-1))\dots$$

$$\dots((a+1)\ (a+2))(a\ (a+1)).$$

On en déduit que  $(a\ b) \in H$ , et donc que  $H$  contient toutes les transpositions. Par conséquent,  $H = S_n$ .

2. Dans le cas où  $n$  est premier, montrer que l'on peut remplacer la transposition  $(1\ 2)$  par n'importe quelle transposition et le  $n$ -cycle  $(1\ 2\ \dots\ n)$  par n'importe quel  $n$ -cycle.

**Indications :** On note  $n = p$ . Soient  $\tau$  une transposition et  $\sigma$  un  $p$ -cycle. Il existe  $g \in S_p$  et  $k \in \{2, 3, \dots, p\}$  tels que  $\tau = (g(1) \ g(k))$  et  $\sigma = (g(1) \ g(2) \ \dots \ g(p))$ . Comme  $p$  est premier,  $\sigma^{k-1}$  est un  $p$ -cycle qui envoie  $g(1)$  sur  $g(k)$ , et  $\langle \tau, \sigma \rangle = \langle \tau, \sigma^{k-1} \rangle$ . Mais, en notant  $\sigma_0 = (1 \ 2 \ \dots \ p)$ , on a  $\langle \tau, \sigma^{k-1} \rangle = (g\sigma_0^{k-1})\langle (1 \ 2), (1 \ 2 \ \dots \ p) \rangle(g\sigma_0^{k-1})^{-1} = (g\sigma_0^{k-1})S_p(g\sigma_0^{k-1})^{-1} = S_p$ , ce qui achève la preuve.

3. Soit  $p$  un nombre premier. Soit  $G$  un groupe fini qui agit fidèlement et transitivement sur un ensemble  $X = \{x_1, \dots, x_p\}$  à  $p$ -éléments. Supposons qu'il existe  $g \in G$  tel que  $g \cdot x_1 = x_2$ ,  $g \cdot x_2 = x_1$  et  $g \cdot x_i = x_i$  pour  $i \geq 2$ . Montrer que  $G \cong S_p$ .

**Indications :** L'action étant fidèle, elle induit un morphisme injectif  $i : G \hookrightarrow S_p$ . Montrons que  $i$  est un isomorphisme. L'action étant transitive, l'ordre de  $G$  est divisible par  $p$ . Comme de plus  $|G| \nmid p!$ , on déduit que  $v_p(|G|) = 1$ . Par conséquent, un  $p$ -Sylow de  $G$  est d'ordre  $p$ , ce qui montre que  $G$  possède un élément d'ordre  $p$  : l'image de cet élément par  $i$  est un  $p$ -cycle. De plus, l'image de l'élément  $g$  décrit dans l'énoncé par  $i$  est la transposition  $(1 \ 2)$ . La question précédente permet alors de conclure que l'image de  $i$  est tout  $S_p$ . Autrement dit,  $i$  est un isomorphisme.

**Exercice 6 : Autour du groupe affine**

Soient  $m \geq 1$  un entier naturel et  $R$  un anneau. Posons :

$$GA_m(R) = \left\{ \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \mid A \in GL_m(R), a \in R^m \right\} \subseteq GL_{m+1}(R).$$

1. Pour  $g \in GA_m(R)$  et  $x \in R^m$ , on pose  $g \cdot x = Ax + a$ . Montrer que cela définit une action fidèle et transitive sur  $R^m$ .

**Indications :** Vérification immédiate.

À partir de maintenant, on suppose que  $m = 1$  et que  $R = \mathbb{Z}/n\mathbb{Z}$ .

2. Montrer que  $GA_1(\mathbb{Z}/n\mathbb{Z})$  s'identifie à un sous-groupe transitif de  $S_n$ , autrement dit, montrer qu'il existe un morphisme de groupes injectif  $f : GA_1(\mathbb{Z}/n\mathbb{Z}) \rightarrow S_n$ .

**Indications :** D'après 1.,  $GA_1(\mathbb{Z}/n\mathbb{Z})$  agit fidèlement et transitivement sur  $\mathbb{Z}/n\mathbb{Z}$ .

3. Montrer que  $GA_1(\mathbb{Z}/n\mathbb{Z})$  possède un sous-groupe distingué isomorphe à  $D_{2n}$ . Pour quelles valeurs de  $n$  l'image de ce sous-groupe par  $f$  est-elle contenue dans  $A_n$  ?

**Indications :** Considérons :

$$H = \left\{ \begin{pmatrix} \epsilon & a \\ 0 & 1 \end{pmatrix} \mid \epsilon \in \{-1, 1\}, a \in R^m \right\}.$$

On montre immédiatement que  $H$  est un sous-groupe de  $GA_1(\mathbb{Z}/n\mathbb{Z})$  d'ordre  $2n$ . Il est engendré par  $r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  et par  $s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ . Ces éléments vérifient les relations  $r^n = 1$ ,  $s^2 = 1$  et  $srs = r^{-1}$ . Par conséquent, le groupe  $H$  s'identifie à un quotient de  $D_{2n}$ . Or  $H$  et  $D_{2n}$  ont même ordre. Donc ils sont isomorphes. L'image de  $H$  par  $f$  est engendrée par  $(1 \ 2 \ \dots \ n)$  et  $(1 \ (n-1))(2 \ (n-2)) \dots \left(\left[\frac{n-1}{2}\right] \ (n - \left[\frac{n-1}{2}\right])\right)$ . Ces deux éléments sont dans  $A_n$  si, et seulement si,  $n$  et  $\frac{n-1}{2}$  sont des entiers impair. Donc  $f(H) \subseteq A_n$  si, et seulement si,  $n \equiv 3 \pmod{4}$ .

4. Montrer que pour  $n \in \{3, 4, 6\}$  on a  $GA_1(\mathbb{Z}/n\mathbb{Z}) \cong D_{2n}$ .

**Indications :** On vérifie immédiatement que, pour de tels  $n$ , on a  $|GA_1(\mathbb{Z}/n\mathbb{Z})| = |D_{2n}|$ . La question précédente permet alors de conclure.

5. Dresser la liste des sous-groupes de  $GA_1(\mathbb{Z}/5\mathbb{Z})$ . Lesquels sont distingués ?

**Indications :** On a  $|GA_1(\mathbb{Z}/5\mathbb{Z})| = 20$ . Il est engendré par  $r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  et par  $t = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ . Plus précisément, on a  $r^5 = t^4 = 1$ ,  $trt^{-1} = r^2$ , et  $GA_1(\mathbb{Z}/5\mathbb{Z}) = \{r^j t^k \mid 0 \leq j < 5, 0 \leq k < 4\}$ .

- Sous-groupes d'ordre 1 :  $\{1\}$ .
- Sous-groupes d'ordre 2 :  $\{1, t^2\}$  car  $t^2$  est le seul élément d'ordre 2 de  $GA_1(\mathbb{Z}/5\mathbb{Z})$ .
- Sous-groupes d'ordre 4 :  $\langle t \rangle, \langle rt \rangle, \langle r^2 t \rangle, \langle r^3 t \rangle, \langle r^4 t \rangle$ , puisque tous les 2-Sylow sont conjugués à  $\langle t \rangle$ .
- Sous-groupes d'ordre 5 :  $\langle r \rangle$  puisque c'est un groupe distingué et tous les 5-Sylow sont conjugués.
- Sous-groupes d'ordre 10 : un tel sous-groupe contient un élément d'ordre 2 et un élément d'ordre 5 : il contient donc  $t^2$  et  $r$ . Comme  $\langle t^2, r \rangle$  est d'ordre 10, c'est le seul sous-groupe d'ordre 10 de  $GA_1(\mathbb{Z}/5\mathbb{Z})$ .
- Sous-groupes d'ordre 20 :  $GA_1(\mathbb{Z}/5\mathbb{Z})$ .

Les sous-groupes distingués sont  $GA_1(\mathbb{Z}/5\mathbb{Z}), \langle t^2, r \rangle, \langle r \rangle$  et  $\{1\}$ .

**Exercice 7 : Groupes résolubles**

On rappelle qu'un groupe  $G$  est dit résoluble s'il existe une suite de sous-groupes emboîtés  $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = 1$ , telle que  $G_{i+1}/G_i$  est abélien pour  $i \in \{0, 1, \dots, r-1\}$ . Pour chaque groupe  $G$  on note  $D(G)$  son sous-groupe dérivé et  $D^n(G) = D(D^{n-1}(G))$ .

1. Montrer qu'un groupe  $G$  est résoluble si, et seulement si, il existe un entier naturel  $n$  tel que  $D^n(G) = 1$ .

**Indications :** Voir le théorème 5.12 du polycopié d'Algèbre 1.

2. (a) Montrer que tout sous-groupe d'un groupe résoluble est résoluble.

- (b) Montrer que tout quotient d'un groupe résoluble est résoluble.
- (c) Montrer que si  $G$  est un groupe possédant un sous-groupe distingué résoluble  $H$  tel que  $G/H$  est résoluble, alors  $G$  est résoluble.

**Indications :** Voir la proposition 5.14 du polycopié d'Algèbre 1.

3. (a) Pour quelles valeurs de  $n$  le groupe  $S_n$  est-il résoluble ?

**Indications :** Pour  $n = 1$  ou  $n = 2$ , le groupe  $S_n$  est abélien donc résoluble. Pour  $n = 3$ , la suite  $S_3 \triangleright \langle (1\ 2\ 3) \rangle \triangleright 1$  montre que  $S_3$  est résoluble. Pour  $n = 4$ , la suite  $S_4 \triangleright A_4 \triangleright \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \triangleright 1$  montre que  $S_4$  est résoluble. Pour  $n \geq 5$ , le groupe  $A_n$  est simple et non abélien, donc non résoluble : on déduit alors de 2.(a) que  $S_n$  n'est pas résoluble.

- (b) Pour quelles valeurs de  $n$  le groupe  $D_{2n}$  est-il résoluble ?

**Indications :** Soit  $r$  une rotation d'ordre  $n$  dans  $D_{2n}$ . La suite  $D_{2n} \triangleright \langle r \rangle \triangleright 1$  montre que  $D_{2n}$  est toujours résoluble.

- (c) Pour quelles valeurs de  $n$  le groupe  $GA_1(\mathbb{Z}/n\mathbb{Z})$  est-il résoluble ?

**Indications :** Notons  $r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . La suite  $GA_1(\mathbb{Z}/n\mathbb{Z}) \triangleright \langle r \rangle \triangleright 1$  montre que  $GA_1(\mathbb{Z}/n\mathbb{Z})$  est toujours résoluble.

**Exercice 8 (difficile) : Sous-groupes résolubles transitifs de  $S_p$**

Soit  $p$  un nombre premier. Dans cet exercice, nous allons étudier les sous-groupes résolubles transitifs de  $S_p$ . Pour ce faire, on rappelle qu'il est possible de voir  $GA_1(\mathbb{Z}/p\mathbb{Z})$  comme sous-groupe de  $S_p$ , et on note  $\tau \in GA_1(\mathbb{Z}/p\mathbb{Z})$  la translation  $x \mapsto x + 1$ .

0. (*Question préliminaire*) Montrer que si  $g \in S_p$  vérifie  $g\tau g^{-1} \in GA_1(\mathbb{Z}/p\mathbb{Z})$ , alors  $g \in GA_1(\mathbb{Z}/p\mathbb{Z})$ .

**Indications :** Dans tout cet exercice, on verra  $S_p$  comme le groupe des permutations de  $\mathbb{Z}/p\mathbb{Z}$  (au lieu de  $\{1, 2, \dots, p\}$ ). Les seuls éléments d'ordre  $p$  dans  $GA_1(\mathbb{Z}/p\mathbb{Z})$  sont les  $\tau^k$  avec  $k \in \{1, \dots, p-1\}$ . Il existe donc  $k \in \{1, \dots, p-1\}$  tel que  $g\tau g^{-1} = \tau^k$ . Autrement dit :  $(g(0)\ g(1)\ \dots\ g(p-1)) = (0\ k\ 2k\ \dots\ (p-1)k)$ . Donc  $g(x) = g(0) + kx$ , et  $g \in GA_1(\mathbb{Z}/p\mathbb{Z})$ .

1. Montrer que tout sous-groupe de  $S_p$  conjugué à un sous-groupe de  $GA_1(\mathbb{Z}/p\mathbb{Z})$  contenant  $\tau$  est un sous-groupe résoluble transitif de  $S_p$ .

**Indications :** D'après la question 3.(c) de l'exercice 7, le groupe  $GA_1(\mathbb{Z}/p\mathbb{Z})$  est résoluble. Donc, d'après la question 2.(a) de l'exercice 7, tout sous-groupe de  $GA_1(\mathbb{Z}/p\mathbb{Z})$  est résoluble. Il est alors immédiat de voir que tout conjugué de  $GA_1(\mathbb{Z}/p\mathbb{Z})$  dans  $S_p$  est résoluble. Pour conclure, il suffit donc d'invoquer les questions 2. et 3. de l'exercice 4.

2. Soit  $H$  un sous-groupe résoluble transitif de  $S_p$ . On considère une suite de sous-groupes emboîtés  $H = H_0 \triangleright H_1 \triangleright \dots \triangleright H_r = 1$  telle que, pour  $i \in \{0, \dots, r-1\}$ , le groupe  $H_i/H_{i+1}$  est cyclique d'ordre premier.

- (a) Expliquer pourquoi une telle suite existe.

**Indications :** D'après la question 2 de l'exercice 7, les facteurs simples de  $H$  sont résolubles. Mais les groupes simples résolubles sont les groupes cycliques d'ordre premier.

- (b) En tant que sous-groupes de  $S_p$ , les  $H_i$  (pour  $i \in \{0, \dots, r\}$ ) agissent sur  $\mathbb{Z}/p\mathbb{Z}$ . Montrer que  $H_{r-1}$  agit transitivement sur  $\mathbb{Z}/p\mathbb{Z}$ , puis que  $H_{r-1} \cong \mathbb{Z}/p\mathbb{Z}$ .

**Indications :** On sait que  $H = H_0$  agit transitivement sur  $\mathbb{Z}/p\mathbb{Z}$ . Soit  $j \in \{0, \dots, r-2\}$  tel sur  $H_j$  agit transitivement sur  $\mathbb{Z}/p\mathbb{Z}$ . On sait que  $\text{Stab}_0(H_j)$  est d'indice  $p$  dans  $H_j$ . Donc le groupe  $\langle H_{j+1}, \text{Stab}_0(H_j) \rangle$  est soit  $\text{Stab}_0(H_j)$  soit  $H_j$ .

- Dans le premier cas,  $H_{j+1} \subseteq \text{Stab}_0(H_j)$ . Pour chaque  $x \in \mathbb{Z}/p\mathbb{Z}$ , il existe  $h_x \in H_j$  tel que  $h_x \cdot 0 = x$ . On a alors, pour  $h \in H_{j+1}$ , la relation  $h \cdot x = (hh_x) \cdot 0 = h_x \cdot ((h_x^{-1}h h_x) \cdot 0) = h_x \cdot 0 = x$ . C'est absurde car  $H_{j+1} \neq \{1\}$ .
- Dans le deuxième cas, comme  $H_{j+1}$  est distingué dans  $H_j$ , on a  $H_j = \{hs \mid h \in H_{j+1}, s \in \text{Stab}_0(H_j)\}$ . Comme  $H_j$  agit transitivement, on déduit que  $H_{j+1}$  agit transitivement.

On a donc montré par récurrence que  $H_{r-1}$  agit transitivement sur  $\mathbb{Z}/p\mathbb{Z}$ . On en déduit que  $p$  divise l'ordre de  $H_{r-1}$ . Donc  $H_{r-1} \cong \mathbb{Z}/p\mathbb{Z}$ .

- (c) En déduire que  $H$  est conjugué à un sous-groupe de  $GA_1(\mathbb{Z}/p\mathbb{Z})$  contenant  $\tau$ .

**Indications :** Soit  $\sigma$  un générateur de  $H_{r-1}$ . C'est un  $p$ -cycle. Il existe donc  $g \in S_p$  tel que  $g\sigma g^{-1} = \tau$ . On en déduit que  $gH_{r-1}g^{-1} \subseteq GA_1(\mathbb{Z}/p\mathbb{Z})$ . Soit maintenant  $j \in \{1, 2, \dots, r-1\}$  tel que  $gH_jg^{-1} \subseteq GA_1(\mathbb{Z}/p\mathbb{Z})$ . Comme  $gH_jg^{-1}$  est distingué dans  $gH_{j-1}g^{-1}$ , la question préliminaire permet de conclure que  $gH_{j-1}g^{-1} \subseteq GA_1(\mathbb{Z}/p\mathbb{Z})$ . On obtient donc par récurrence que  $gHg^{-1} \subseteq GA_1(\mathbb{Z}/p\mathbb{Z})$ .

- (d) Combien de sous-groupes résolubles transitifs possède  $S_p$  à conjugaison près ?

**Indications :** On a montré que les sous-groupes résolubles transitifs sont, à conjugaison près, ceux qui sont contenus dans  $GA_1(\mathbb{Z}/p\mathbb{Z})$  et qui contiennent  $\tau$ . Ils sont donc en bijection avec les sous-groupes de  $GA_1(\mathbb{Z}/p\mathbb{Z})/\langle \tau \rangle \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ . Il y en a donc  $\phi(p-1)$ .

3. Montrer qu'un élément non trivial d'un sous-groupe résoluble transitif de  $S_p$  possède au plus un point fixe.

**Indications :** Cette propriété est aisément vérifiée pour les éléments de  $GA_1(\mathbb{Z}/p\mathbb{Z})$ .

4. Soit  $H$  un sous-groupe transitif de  $S_p$  tel que tout élément de  $H$  a au plus un point fixe. Soit  $S$  l'ensemble des éléments de  $H$  n'ayant pas de point fixe.

- (a) Montrer que  $S$  est stable par conjugaison par tout élément de  $H$ .

**Indications :** Vérification facile.

- (b) Montrer que  $|S| = p-1$ , puis qu'il existe un  $p$ -cycle  $\sigma$  tel que  $S = \{\sigma, \sigma^2, \dots, \sigma^{p-1}\}$ .

**Indications :** Comme tout élément de  $H$  a au plus un point fixe, les  $(\text{Stab}_x(H) \setminus \{1\})_{x \in \mathbb{Z}/p\mathbb{Z}}$  et  $S$  forment une partition de  $H \setminus \{1\}$ . Par conséquent,  $\sum_x (|\text{Stab}_x(H)| - 1) + |S| = |H| - 1$ . Or  $H$  est un sous-groupe transitif de  $S_p$ . Donc, pour tout  $x$ , on a  $|H| = p|\text{Stab}_x(H)|$ . On en déduit que  $|S| = p - 1$ . Comme  $H$  est un sous-groupe transitif de  $S_p$ , il contient un  $p$ -cycle  $\sigma$ . On remarque alors que  $\sigma, \sigma^2, \dots, \sigma^{p-1}$  sont dans  $S$ . Comme  $|S| = p - 1$ , on a bien  $S = \{\sigma, \sigma^2, \dots, \sigma^{p-1}\}$ .

(c) Dédurre de ce qui précède que  $H$  est un groupe résoluble.

**Indications :** Soit  $g \in S_p$  tel que  $g\sigma g^{-1} = \tau$ . D'après la question (a), l'ensemble  $gSg^{-1}$  est stable par conjugaison par tout élément de  $gHg^{-1}$ . En utilisant la question préliminaire, on déduit que  $gHg^{-1} \subseteq GA_1(\mathbb{Z}/p\mathbb{Z})$ , et donc que  $H$  est résoluble.

### Exercice 9 : Produits semi-directs

1. Montrer que  $S_n \cong A_n \rtimes \mathbb{Z}/2\mathbb{Z}$ . Le produit est-il direct ?

**Indications :** La suite exacte  $1 \rightarrow A_n \rightarrow S_n \rightarrow \{-1, 1\} \rightarrow 1$  induite par la signature est scindée, puisque  $S_n$  contient des éléments d'ordre 2. Donc  $S_n \cong A_n \rtimes \mathbb{Z}/2\mathbb{Z}$ . Pour  $n > 2$ , si  $\tau$  est une transposition, le sous-groupe  $\{1, \tau\}$  n'est pas distingué, et donc le produit n'est pas direct. Pour  $n \leq 2$ , le produit est évidemment direct.

2. Montrer que  $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ . Le produit est-il direct ?

**Indications :** Soit  $r$  une rotation d'ordre  $n$  dans  $D_{2n}$ . On a alors une suite exacte  $1 \rightarrow \langle r \rangle \rightarrow D_{2n} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1$ . Elle est scindée puisque  $D_{2n}$  contient des éléments d'ordre 2, et donc  $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ . Le produit n'est pas direct pour  $n > 2$  puisque  $D_{2n}$  n'est pas abélien. Pour  $n \leq 2$ , le produit est bien direct.

3. Montrer que  $GA_m(R) \cong R^m \rtimes GL_m(R)$ . Le produit est-il direct ?

**Indications :** Notons :

$$H = \left\{ \begin{pmatrix} Id & a \\ 0 & 1 \end{pmatrix} \mid a \in R^m \right\}.$$

On a une suite exacte  $1 \rightarrow H \rightarrow GA_m(R) \rightarrow GL_m(R) \rightarrow 1$ . Elle est scindée par :

$$GL_m(R) \rightarrow GA_m(R), A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix},$$

et  $H$  est isomorphe à  $R^m$  en tant que groupe. Donc  $GA_m(R) \cong R^m \rtimes GL_m(R)$ . Le produit est direct si, et seulement si, pour tout  $A \in GL_m(R)$  et tout  $a \in R^m$ , on a  $Aa = a$ . Cela n'est possible que si  $m = 1$  et  $R^\times = 1$ . En particulier, pour que le produit soit direct, il faut que  $R$  soit de caractéristique 2.