Feuille d'exercices n° 4 : Théorèmes de Sylow

Exercice 1

1. Quels sont les sous-groupes de Sylow de $\mathcal{A}_4$?
2. Déterminer l'ordre de tous les éléments de $\mathcal{A}_4$.
   Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.
   Montrer que H contient au moins trois éléments d'ordre 3.
   Peut-il être isomorphe à $\mathcal{S}_3$?
   En déduire qu'il n'y a pas de sous-groupe d'ordre 6 dans $\mathcal{A}_4$.
4. Donner la liste des sous-groupes de $\mathcal{A}_4$.

Solution 1

1. Déterminons les les sous-groupes de Sylow de $\mathcal{A}_4$.
   L'ordre de $\mathcal{A}_4$ est $12 = 2^2 \times 3$. Soient n_2 le nombre de sous-groupes de Sylow d'ordre $2^2 = 4$ et n_3 le nombre de sous-groupes de Sylow d'ordre 3. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \qquad n_2 | 3$$

   $$n_3 \equiv 1 \bmod 3 \qquad n_3 | 2^2 = 4$$

   autrement dit que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$.
   Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois donc $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4 isomorphe au groupe de Klein, *i.e.* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (en effet d'après le théorème de Lagrange un sous-groupe K de $\mathcal{A}_4$ d'ordre 4 contient des éléments d'ordre 1, 2 ou 4 ; mais $\mathcal{A}_4$ ne contient pas d'élément d'ordre 2 donc K contient des éléments d'ordre 1 ou 4. Comme $\mathcal{A}_4$ contient un seul élément d'ordre 1 et trois éléments d'ordre 4 il contient un seul sous-groupe d'ordre 4).
   Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.
2. Déterminons l'ordre de tous les éléments de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?
   Le groupe $\mathcal{A}_4$ contient trois éléments d'ordre 2, huit éléments d'ordre 3 et un élément d'ordre 1. Le groupe $\mathcal{A}_4$ ne contient donc aucun élément d'ordre 6 et ne contient donc pas de sous-groupe cyclique d'ordre 6.
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.
   Notons que
   $$(a\ b)(c\ d)(a\ b\ c) = (b\ d\ c)$$
   Le groupe H contient les 3-cycles : $(a\ b\ c)$, $(a\ c\ b)$ et $(b\ d\ c)$ donc les trois sous-groupes d'ordre 3

   $$\langle (a\ b\ c) \rangle, \qquad \langle (a\ c\ b) \rangle, \qquad \langle (b\ d\ c) \rangle.$$

   Un groupe d'ordre 6 ne contient qu'un sous-groupe d'ordre 3 (en effet soit K un sous-groupe d'ordre $6 = 2 \times 3$. Désignons par n_3' le nombre de 3-Sylow de K ; d'une part $n_3' \equiv 1 \bmod 3$ d'autre part $n_3' | 2$ donc $n_3' = 1$). Par conséquent le groupe H n'est pas d'ordre 6. En particulier H ne peut pas être isomorphe à $\mathcal{S}_3$ qui est d'ordre 6.

4. Le groupe $\mathcal{A}_4$ contient :
   — un sous-groupe d'ordre 1 : $\{\mathrm{id}\}$;
   — trois sous-groupes d'ordre 2 :

$$\langle(1\ 2)(3\ 4)\rangle \qquad \langle(1\ 3)(2\ 4)\rangle \qquad \langle(1\ 4)(2\ 3)\rangle;$$

   — quatre sous-groupes d'ordre 3 :

$$\langle(1\ 2\ 3)\rangle \qquad \langle(1\ 2\ 4)\rangle \qquad \langle(1\ 3\ 4)\rangle \qquad \langle(2\ 3\ 4)\rangle;$$

   — un sous-groupe d'ordre 4 :

$$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Exercice 2 [Simplicité de $\mathcal{A}_n$, $n \geqslant 5$]

I) Commençons par démontrer que le groupe $\mathcal{A}_5$ est simple.
Soit G un groupe. Un sous-groupe H de G est caractéristique si pour tout automorphisme φ de G on $\varphi(\mathrm{H}) \subset \mathrm{H}$.

I) a) Montrer que tout p-Sylow distingué d'un groupe d'ordre fini est caractéristique.

I) b) Montrer que tout groupe d'ordre 15 est cyclique.

I) c) Montrer que tout groupe d'ordre 30 contient un sous-groupe distingué d'ordre 15.

I) d) Montrer que tout groupe d'ordre 30 ne contient qu'un seul 5-Sylow (d'ordre 5).

I) e) Montrer que tout groupe d'ordre 20 contient un seul sous-groupe d'ordre 5.

I) f) Montrer que tout groupe d'ordre 12 contient un sous-groupe caractéristique.

I) g) Montrer que tout groupe d'ordre 6 contient un sous-groupe caractéristique.

I) h) Montrer que tout groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow est simple.

I) i) Montrer que le groupe $\mathcal{A}_5$ est simple.

II) Soit $n \geqslant 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué de $\mathcal{A}_n$ non trivial.

II) a) Montrer qu'il existe $\tau \in \mathrm{H}$ distinct de l'identité qui a au moins un point fixe.

II) b) Montrer que pour tout $1 \leqslant j \leqslant n$ le sous-groupe $\mathrm{G}_j = \mathrm{Stab}_{\mathcal{A}_n}(\{j\})$ est inclus dans H.

II) c) Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$. Montrer que $\mathcal{A}_n = \mathrm{H}$.

II) d) En déduire que $\mathcal{A}_n$ est simple pour $n \geqslant 5$.

Solution 2

I) a) Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué. Soit φ un automorphisme de G. L'image de H par φ est un sous-groupe de même ordre que H, *i.e.* $\varphi(\mathrm{H})$ est un p-Sylow de G. Mais H est l'unique p-Sylow de G car H est distingué. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$.

I) b) Soit H un groupe d'ordre 15. Il a exactement un sous-groupe d'ordre 5 et un sous-groupe d'ordre 3. Ces deux sous-groupes sont distingués dans H. Par suite $\mathrm{H} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ et est donc cyclique.

I) c) Soit G un groupe d'ordre 30. Remarquons tout d'abord que tout sous-groupe d'ordre 15 de G est distingué dans G car il est d'indice 2 dans G.
Il suffit donc de démontrer l'existence d'un sous-groupe d'ordre 15 dans le groupe G.
   — Supposons que G contienne plus d'un seul 5-Sylow, *i.e.* $n_5 > 1$. Puisque

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \mid 6$$

   on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant id fait 25 éléments de G. Il y a donc exactement un seul 3-Sylow que nous noterons K (sinon il y en aurait 10 donc 20 éléments d'ordre 3 soit 45 éléments au moins dans G). En particulier K est distingué dans G. Si H est l'un des sous-groupes d'ordre 5, $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 de G.
   — Supposons que G contienne un seul 5-Sylow H ; il est alors distingué dans G. Si K est l'un des sous-groupes d'ordre 3 de G (il y en a au moins un) $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

I) d) Au I) c) on a vu d'une part que tout groupe G d'ordre 30 contient un sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 5 et d'autre part que K ou H est distingué dans G.

Les groupes K et H sont distingués dans KH et sont donc caractéristiques (voir I)a)) dans le groupe KH qui est cyclique et distingué dans G (car d'indice 2 dans G). Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow.

I) e) Soit G un groupe d'ordre $20 = 2^2 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 4$$

d'où $n_5 = 1$.

I) f) Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

— Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué dans G ; ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (cf I) a)).

— Si $n_3 = 4$, on dénombre $4 \times 2 = 8$ éléments d'ordre 3 ; en ajoutant le neutre on compte donc 9 éléments. Considérons maintenant les 2-Sylow de G. D'après les théorèmes de Sylow on a

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \,|\, 3$$

Ainsi n_2 appartient à $\{1, 3\}$. Si $n_2 = 3$, on a trois sous-groupes d'ordre 4, soit trop d'éléments. Ainsi $n_2 = 1$, l'unique 2-Sylow est distingué dans G et donc caractéristique dans G (cf I) a)).

I) g) Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ses 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et I) b) permet de conclure.

I) h) Soit G un groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow. D'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 12$$

d'où $n_5 \in \big\{1, 6\big\}$. Par hypothèse $n_5 \neq 1$ donc $n_5 = 6$.

Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G. Notons que

$$|\mathrm{H}| \in \big\{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\big\}.$$

- ◇ Si |H| est divisible par 5 alors H contient au moins un 5-Sylow de G. Mais H est distingué et les 5-Sylow se déduisent les uns des autres par conjugaison ; ainsi H contient tous les 5-Sylow de G. On en déduit que H contient déjà 6×4 éléments d'ordre 5. Par ailleurs |H| divise 60 donc $|\mathrm{H}| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|\mathrm{H}| < 60$). Mais dans ce cas H ne contient qu'un seul sous-groupe d'ordre 5 (voir I)d)) : contradiction avec le fait qu'il en contient 6. Par suite |H| n'est pas divisible par 5.
- ◇ Si |H| appartient à $\{6, 12\}$, alors il existe un sous-groupe caractéristique de H d'ordre 2, 3 ou 4 (d'après I)f) et I)g)). Ce sous-groupe caractéristique de H, qui est lui-même distingué dans G, est distingué dans G.
- ◇ Nous pouvons donc maintenant supposer que H est d'ordre 2, 3 ou 4. Dans ce cas G/H est d'ordre 30, 20 ou 15 (on renvoie à I)d) si G/H est d'ordre 30, à I)e) si G/H est d'ordre 20 ; enfin si G/H est d'ordre $15 = 3 \times 5$ et si n_5 est le nombre de 5-Sylow de G/H, les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et n_5 divise 3 donc $n_5 = 1$). Donc G/H contient un sous-groupe K distingué d'ordre 5. Considérons la surjection canonique $\pi : \mathrm{G} \to \mathrm{G}/\mathrm{H}$. Le sous-groupe $\pi^{-1}(\mathrm{K})$ contient H et est distingué dans G. Or $\pi^{-1}(\mathrm{K})/\mathrm{H}$ est isomorphe à $\mathrm{K} = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction (voir le premier ◇ du I)h)).

I) i) Le groupe $\mathcal{A}_5$ est d'ordre 60 et contient au moins deux 5-Sylow distincts engendrés par les 5-cycles (1 2 3 4 5) et (1 3 2 4 5). D'après I) h) le groupe $\mathcal{A}_5$ est simple.

II) a) **Remarque**. Supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Alors si τ_1 et τ_2 sont deux éléments de H qui coïncident en un point i, ils sont égaux. En effet si $\tau_1(i) = \tau_2(i)$ alors $\tau_2^{-1}\tau_1(i) = i$. De plus $\tau_2^{-1}\tau_1$ appartient à H donc par hypothèse $\tau_2^{-1}\tau_1 = \mathrm{id}$, *i.e.* $\tau_1 = \tau_2$.

Raisonnons par l'absurde : supposons qu'aucun élément non trivial de H n'a de point fixe, *i.e.* supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$.

- ◇ Montrons dans un premier temps qu'aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre $\geqslant 3$. Raisonnons par l'absurde : supposons qu'il existe τ dans H tel que la décomposition de τ en produit de cycles disjoints contient un cycle d'ordre $\geqslant 3$ alors on peut écrire

$$\tau = (a_1\ a_2\ a_3\ \ldots)(b_1\ b_2\ \ldots)\ldots$$

Puisque $n \geqslant 6$ il existe σ dans $\mathcal{A}_n$ tel que $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ et $\sigma(a_3) \neq a_3$. Alors

$$\sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ \ldots)(\sigma(b_1)\ \sigma(b_2)\ \ldots)\ldots$$

Ainsi $\sigma\tau\sigma^{-1}(a_1) = \tau(a_1) = a_2$. À noter que $\sigma\tau\sigma^{-1}$ appartient à H car H est distingué. La remarque qui précède assure donc que $\sigma\tau\sigma^{-1} = \tau$. Mais $\sigma\tau\sigma^{-1}(a_2) = \sigma(a_3) \neq a_3$ et $a_3 = \tau(a_2)$ donc $\sigma\tau\sigma^{-1}(a_2) \neq \tau(a_2)$: contradiction. Ainsi aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre $\geqslant 3$. Les éléments de H sont donc des produits de transpositions disjointes.

- ◇ Considérons un élément τ de H. D'après ce qui précède τ est un produit de transpositions disjointes. À noter que si τ est une double transposition alors elle laisse fixe un élément ce qui est contraire à l'hypothèse. Ainsi τ s'écrit

$$\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\ldots$$

Soit $\sigma = (a_1\ a_2)(a_3\ a_5)$. Alors on a

$$\sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\ldots$$

D'une part $\sigma\tau\sigma^{-1}(a_2) = \tau(a_2)$ donc $\sigma\tau\sigma^{-1} = \tau$ (cf Remarque). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction.

Le groupe H contient donc au moins un élément non trivial qui possède un point fixe.

II) b) Soit τ un élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ pour lequel il existe $1 \leqslant i \leqslant n$ tel que $\tau(i) = i$ (l'existence d'un tel τ est assurée par II) a)). Ainsi τ appartient à $\mathrm{G}_i \cap \mathrm{H}$ qui est un sous-groupe distingué de G_i. Or G_i est isomorphe à $\mathcal{A}_{n-1}$ donc l'hypothèse de récurrence implique que G_i est simple donc ou bien $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$ ou bien $\mathrm{G}_i \cap \mathrm{H} = \{\mathrm{id}\}$. Or τ est un élément non trivial de $\mathrm{G}_i \cap \mathrm{H}$ donc $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$, c'est-à-dire G_i est inclus dans H.

Par ailleurs pour tout σ dans $\mathcal{S}_n$ on a $\sigma\mathrm{G}_i\sigma^{-1} = \mathrm{G}_{\sigma(i)}$ d'où $\mathrm{G}_i \subset \mathrm{H}$ donc $\mathrm{G}_{\sigma(i)} = \sigma\mathrm{G}_i\sigma^{-1} \subset \sigma\mathrm{H}\sigma^{-1} = \mathrm{H}$. Autrement dit pour tout $1 \leqslant j \leqslant n$ on a l'inclusion $\mathrm{G}_j \subset \mathrm{H}$.

II) c) Bien sûr $\mathrm{H} \subset \mathcal{A}_n$ donc pour montrer que $\mathcal{A}_n = \mathrm{H}$ il suffit de montrer que $\mathcal{A}_n \subset \mathrm{H}$. Considérons un élément g de $\mathcal{A}_n$. C'est un produit d'un nombre pair de transpositions, il s'écrit donc

$$g = t_1 t_2 \ldots t_k$$

où chaque t_j est un produit de deux transpositions. Le support de chaque t_j contient au plus quatre éléments donc t_j appartient à G_i pour un i extérieur à ce support. Par suite $\mathcal{A}_n \subset \mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n$. Mais $\mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n \subset \mathrm{H}$ (cf II) b)). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$.

II) d) Le groupe $\mathcal{A}_5$ est simple (I)i)). Pour $n \geqslant 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (cf II) c)).

Exercice 3 Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_2)$ le groupe des matrices à coefficients dans le corps à deux éléments et de déterminant 1.

1. Quel est l'ordre de G ? Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
2. Soit X l'ensemble des 2-Sylow de G. Donner la liste de ses éléments.
   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

$$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}$$

Montrer par un calcul direct que cette action est transitive.
Quel est le stabilisateur de

$$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\} ?$$

3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.
   Montrer que

$$\phi\colon \mathrm{G} \to \mathcal{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.

Solution 3

1. Déterminons l'ordre de G. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de G. Nous avons $ad + bc = \overline{1}$ donc
   — ou bien $ad = \overline{1}$ et $bc = \overline{0}$;
   — ou bien $ad = \overline{0}$ et $bc = \overline{1}$.
   On a $ad = \overline{1}$ et $bc = \overline{0}$ si et seulement si $(a, b, c, d) = (1, 0, 1, 1)$ ou $(a, b, c, d) = (1, 1, 0, 1)$ ou $(a, b, c, d) = (1, 0, 0, 1)$ ce qui donne 3 possibilités.
   De même $ad = \overline{0}$ et $bc = \overline{1}$ donne 3 possibilités.
   Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
   Soient n_2 le nombre de 2-Sylow de G et n_3 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_2 \equiv 1 \bmod 2 \qquad n_2 | 3$$

   et

$$n_3 \equiv 1 \bmod 3 \qquad n_3 | 2$$

   Par conséquent $n_3 = 1$, *i.e.* G contient un unique 3-Sylow qui est donc distingué dans G. Le seul sous-groupe d'ordre 3 est constitué de l'identité, de $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $D^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.
   Les éléments d'ordre 2 sont

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

2. Soit X l'ensemble des 2-Sylow de G. La liste des éléments de X est : $\big\{\langle A\rangle, \langle B\rangle, \langle C\rangle\big\}$.
   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

$$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}$$

   Montrons par un calcul direct que cette action est transitive :

$$B \cdot \langle A\rangle = \langle C\rangle \qquad A \cdot \langle C\rangle = \langle B\rangle \qquad C \cdot \langle B\rangle = \langle A\rangle$$

   Quel est le stabilisateur de

$$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\} ?$$

   Déterminons le stabilisateur de $\langle A\rangle$. C'est un sous-groupe de G dont l'ordre divise $|\mathrm{G}|$. Il contient Id et A mais ni B, ni C. Par ailleurs $B \cdot \langle A\rangle = \langle C\rangle$. Ce stabilisateur est donc $\langle A\rangle$.

3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.
   Montrer que

$$\phi\colon \mathrm{G} \to \mathcal{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.
   Puisque G agit sur X le morphisme ϕ est un morphisme de groupes. Il est injectif car $\ker \phi = \{e_{\mathrm{G}}\}$. Comme $\mathcal{S}_X$ et G ont même ordre (6) nous obtenons que ϕ est un isomorphisme.

Exercice 4 Montrer que $\mathcal{S}_4$ possède trois 2-sous-groupes de Sylow isomorphes à D_8.

Solution 4 Le groupe $\mathcal{S}_4$ est d'ordre $24 = 2^3 \times 3$. Par ailleurs D_8 est le groupe des isométries du plan qui conservent un carré donc $D_8 \subset \mathcal{S}_4$.

Soit n_2 le nombre de 2-Sylow de $\mathcal{S}_4$. Le groupe D_8 est l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathcal{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation (1 2 3 4). Notons que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathcal{S}_4$. Il y a donc 3 sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathcal{S}_4$.

Exercice 5 Soit G un groupe. Soit p un nombre premier divisant $|G|$.

Montrer que si H est un p-sous-groupe de G distingué dans G, alors H est contenu dans tout p-sous-groupe de Sylow de G.

Solution 5 Si H est un p-sous-groupe de G, il existe un p-Sylow de G qui contient H. Puisque $H \triangleleft G$ et que les p-Sylow sont conjugués entre eux, H se trouve dans tous les p-Sylow de G.

Exercice 6 Montrer qu'un groupe d'ordre 56 n'est pas simple.

Solution 6 Soit G un groupe d'ordre $56 = 2^3 \times 7$. Soit n_2 le nombre de 2-Sylow et n_7 le nombre de 7-Sylow.

D'après les théorèmes de Sylow

$$n_2 \equiv 1 \pmod 2 \qquad n_2 | 7$$

$$n_7 \equiv 1 \pmod 7 \qquad n_7 | 8$$

Par conséquent $n_2 \in \{1, 7\}$ et $n_7 \in \{1, 8\}$.

Si $n_7 = 1$, alors d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Supposons que $n_7 \neq 1$, alors $n_7 = 8$ et G compte huit sous-groupes d'ordre 7, c'est-à-dire déjà $8(7-1) = 48$ éléments d'ordre 7 (remarque : $7-1$ = nombre d'éléments non triviaux d'un sous-groupe d'ordre 7). En ajoutant l'élément neutre nous avons donc "listé" 49 éléments du groupe G. Si $n_2 \neq 1$, alors $n_2 = 7$, on a donc au moins deux sous-groupes de G distincts d'ordre $2^3 = 8$ qui sont isomorphes ce qui ajoute plus de sept éléments. Le groupe G compte donc plus de 56 éléments : contradiction. Par suite $n_2 = 1$; d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Exercice 7 Montrer qu'un groupe d'ordre pq, où p et q sont premiers et distincts, ne peut être simple.

Solution 7 Soit G un groupe d'ordre pq. Quitte à renommer p et q nous pouvons supposer que $p > q$. Soit n_p le nombre de p-Sylow de G.

Les théorèmes de Sylow assurent que $n_p \equiv 1 \pmod p$ et n_p divise q, autrement dit que $n_p \equiv 1 \pmod p$ et $n_p \in \{1, q\}$. Mais comme $p > q$, $q \not\equiv 1 \pmod p$. Par suite $n_p = 1$, *i.e.* il y a un seul p-Sylow dans G qui est un sous-groupe d'ordre p distingué dans G et propre. Il s'en suit que G n'est pas simple.

Exercice 8 Soient p et q deux nombres premiers.

Montrer qu'il existe au plus deux structures de groupes d'ordre pq.

Solution 8

Exercice 9 Soit $G = SL(2, \mathbb{F}_3)$ le groupe des matrices 2×2 de déterminant égal à 1 et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

1. Montrer que G est d'ordre 24.
2. Quel est l'ordre des éléments $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de G ?
3. Combien G a-t-il de 3-sous-groupes de Sylow ?

4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.
5. Montrer que G est produit semi-direct de H par un sous-groupe K d'ordre 3.
6. Montrer que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.
7. Montrer que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} \simeq \mathcal{A}_4$ (rappelons que les éléments (1 2 3), (1 2)(3 4) et (1 3)(2 4) engendrent le groupe $\mathcal{A}_4$).

Solution 9

1. Montrons que G est d'ordre 24.
   Une matrice de G s'écrit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = \overline{1}$ et a, b, c et d dans ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$. Cela donne 24 cas possibles pour M.
2. Les ordres cherchés sont des diviseurs de 24 bien sûr. La matrice $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 6. Les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sont d'ordre 3.
3. Soit n_3 le nombre de 3-Sylow de G qui est d'ordre $24 = 2^3 \times 3$. Notons que les 3-Sylow sont donc d'ordre 3. Les théorèmes de Sylow assurent que $n_3 \equiv 1 \pmod 3$ et que n_3 divise $2^3 = 8$. Il s'en suit que $n_3 \in \{1, 4\}$. D'après 2. il y a au moins deux sous-groupes de G d'ordre 3. Par conséquent $n_3 = 4$.
4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.
   Vérifions dans un premier temps que H est d'ordre 8. En effet $A^2 = B^2 = -\mathrm{id}$ donc A et B sont d'ordre 4. Posons $C = AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. On vérifie que
   $$\mathrm{H} = \{\mathrm{id}, -\mathrm{id}, A, -A, B, -B, C, -C\}$$
   (le groupe H est le groupe des quaternions).
   Soit $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors $N^{-1} = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}$.
   Posons $M = NAN^{-1}$ et $L = NBN^{-1}$. Remarquons que si x appartient à ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$ et $x \neq \overline{O}$, alors $x^2 = \overline{1}$.
   Un calcul montre que
   $$M = \begin{pmatrix} bd + ac & -(a^2 + b^2) \\ (c^2 + d^2) & -(bd + ac) \end{pmatrix}$$
   Comme N appartient à G, nous avons $ad - bc = \overline{1}$.
   Si $a = \overline{0}$, alors $-bc = \overline{1}$ et $b = -c$. Si $d = \overline{0}$, alors $M = A$ appartient à H. Si $d \neq \overline{0}$, alors $M = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -C$ ou $M = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = -M$; dans les deux cas M appartient à H.
   Si maintenant $abcd \neq \overline{0}$, alors $a = -d$ et $b = c$ donc $M = -A$ appartient à H.
   On démontre de manière analogue que L appartient à H. Ainsi H est distingué dans G. Of H est un 2-Sylow de G. Par suite il n'y a qu'un seul 2-Sylow dans G puisque par conjugaison à partir d'un 2-Sylow on obtient tous les 2-Sylow. Or les 2-Sylow sont les sous-groupes d'ordre 8 de G. Il y a donc un unique sous-groupe d'ordre 8 dans G qui est H.
5. Montrons que G est produit semi-direct de H par un sous-groupe K d'ordre 3.
   Soit K l'un des sous-groupes d'ordre 3 de G. Nous avons les propriétés suivantes : $\mathrm{H} \cap \mathrm{K} = \{e\}$, H est distingué dans G et $3 \times 8 = 24$. Il s'en suit que G est un produit semi-direct de H par K.
   Nous avons $\mathrm{G} = \mathrm{H} \rtimes_\rho \mathrm{K}$ où $\rho \colon \mathrm{K} \to \mathrm{Aut(H)}$ est tel que $\rho(k)$ est l'automorphisme intérieur associé à l'élément $k \in \mathrm{K}$.
6. Montrons que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.
   Un élément M de G appartient à $Z(\mathrm{G})$ si en particulier $MA = AM$ et $MB = BM$.

Or $AM = MA$ si et seulement si

$$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

et $BM = MB$ si et seulement si

$$\begin{pmatrix} a+b & b+d \\ a+c & b-d \end{pmatrix} = \begin{pmatrix} a+b & a-b \\ c+d & c-d \end{pmatrix}.$$

Ces deux égalités conduisent à $a = d$, $b = -c$, $b + d = a - b$, $a = d$ et $b = c$, soit à $a = d$ et $b = c = 0$, *i.e.* à $M = \pm\mathrm{id}$. Par suite $Z(\mathrm{G}) = \{\mathrm{id}, \mathrm{id}\}$.

7. Montrons que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} \simeq \mathcal{A}_4$.

Considérons ici G comme produit semi-direct de H par K. Définir un morphisme φ de G dans $\mathcal{A}_4$ c'est définir φ sur H et K en respectant l'action de K sur H. Définir φ sur H c'est le définir sur les générateurs A et B en s'assurant que leurs images vérifient les mêmes relations, c'est-à-dire $A^2 = B^2 = (AB)^2$. On vérifie que φ défini par

$$\varphi(A) = (1\ 2)(3\ 4) \qquad \varphi(B) = (1\ 3)(2\ 4) \qquad \varphi(C) = (1\ 2\ 3)$$

convient et que $\ker\varphi = \{\mathrm{id}, -\mathrm{id}\}$. Par suite ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} = {}^{\mathrm{G}}\!/_{\ker\varphi} \simeq \mathcal{A}_4$.

Exercice 10 Soit G′ un sous-groupe d'ordre $p(p-1)$ de $\mathcal{S}_p$.
Montrer que G′ est le normalisateur d'un p-Sylow de $\mathcal{S}_p$.
En déduire que K est conjugué de tous les sous-groupes d'ordre $p(p-1)$ de $\mathcal{S}_p$.

Solution 10

Exercice 11 Si G est un groupe, on peut faire agir G par conjugaison sur lui-même.
(1) Montrer que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.
(2) (i) Si G est un p-groupe, p premier, montrer que le centre de G n'est pas réduit à $\{1\}$.
(ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ soit cyclique. Montrer qu'alors G est abélien.
(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Solution 11
(1) Montrons que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.
C'est la définition du centre :

$$Z(\mathrm{G}) = \{x \in \mathrm{G} \,|\, gxg^{-1} = x \text{ pour tout } g \in \mathrm{G}\}.$$

(2) (i) Si G est un p-groupe, p premier, montrons que le centre de G n'est pas réduit à $\{1\}$.
Notons Ω_i, $i \in I$, les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|\mathrm{G}|$ chaque $|\Omega_i|$ est une puissance de p distincte de 1. En écrivant G comme une union disjointe d'orbites on obtient

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_i |\Omega_i|$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Ceci montre que $|Z(\mathrm{G})| \neq 1$.
(ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ soit cyclique. Montrons qu'alors G est abélien.
Par hypothèse il existe un élément a de G dont la classe $\overline{a} \in {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ engendre ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(\mathrm{G})$. Puisque

$$a^k h \cdot a^{k'} h' = a^{k+k'} hh' = a^{k+k'} h'h = a^{k'} h' a^k h$$

le groupe G est aélien.

(3) Montrons que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.
Chacun des coefficients $*$ est un élément arbitraire de $\mathbb{F}_p$ d'où p^3 choix possibles ; de plus

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas d'où le résultat.

Exercice 12 Soit G un groupe fini d'ordre $|\mathrm{G}| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $S \subset \mathrm{G}$ un p-Sylow et H un sous-groupe de G. Montrer qu'il existe $g \in \mathrm{G}$ tel que $gSg^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Solution 12 On a $|\mathrm{G}| = p^a m$ et $|\mathrm{H}| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Notons que $g' \in \mathrm{Stab}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble X est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal p^c pour un certain $c \leqslant b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |\mathrm{H}| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu.

Exercice 13

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}(n, \Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]
(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Solution 13

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathcal{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |\mathrm{G}|$ convient. De plus le groupe symétrique $\mathcal{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathcal{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.
(2) Le cardinal de $\mathrm{GL}(n, \mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\dots+(n-1)} m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.

Exercice 14 Supposons qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente six 5-Sylow.
b) Montrer que G contient dix 3-Sylow. Montrer que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$ (Indication : considérer les ordres possibles pour le centralisateur de g, observer qu'un groupe d'ordre 18 admet un unique 3-Sylow).
c) Conclure.

Solution 14

a) Montrons que G contient trente six 5-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_5 divise 36 et $n_5 \equiv 1 \pmod 5$. Ceci implique que n_5 appartient à $\{1, 6, 36\}$. Puisque par hypothèse G est simple on ne peut avoir $n_5 = 1$ (sinon l'unique 5-Sylow serait distingué dans G). Il en résulte que n_5 appartient à $\{6, 36\}$. Supposons que $n_5 = 6$. Alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $\mathrm{G} \to \mathcal{S}_6$. Le groupe G étant par hypothèse simple, le noyau de ce morphisme est trivial, *i.e.* ce morphisme est injectif. Le morphisme $\mathrm{G} \to \mathbb{Z}/2\mathbb{Z}$ donné par la signature a nécessairement un noyau trivial donc G est un sous-groupe de $\mathcal{A}_6$. D'une part $|\mathcal{A}_6| = \frac{|\mathcal{S}_6|}{2} = \frac{6!}{2} = 360$, d'autre part $|\mathrm{G}| = 180$, autrement dit G est d'indice 2 dans $\mathcal{A}_6$. Le groupe G est donc un sous-groupe distingué non trivial et propre de $\mathcal{A}_6$: contradiction avec le fait que $\mathcal{A}_6$ est simple. Par conséquent $n_5 = 36$.

b) Montrons que G contient dix 3-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise 20 et $n_3 \equiv 1 \pmod 3$. Ceci implique que n_3 appartient à $\{1, 4, 10\}$. Puisque par hypothèse G est simple on ne peut avoir $n_3 = 1$ (sinon l'unique 3-Sylow serait distingué dans G). Si n_3 était égal à 4, on en déduirait comme au a) un morphisme injectif de G dans $\mathcal{S}_4$ ce qui est impossible car $180 = |\mathrm{G}| > |\mathcal{S}_4| = 4! = 24$. Ainsi $n_3 = 10$.

Montrons que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_\mathrm{G}$.
Soient S et T deux 3-Sylow de G distincts. Soit $g \in S \cap T$. Notons $Z = \{x \in \mathrm{G} \,|\, xg = gx\}$ le centralisateur de g dans G. Supposons que $g \neq e_\mathrm{G}$. Un groupe d'ordre 9 étant abélien, Z contient S et T. Par conséquent $|Z| \in \{18, 36, 45, 90\}$. L'action transitive de G sur G/Z induit un morphisme injectif de G vers $\mathcal{S}_{\mathrm{G}/Z}$. Or $|\mathrm{G}| = 180$ et $|\mathcal{S}_{\mathrm{G}/Z}| \in \{2, 4! = 24, 5! = 120, 10!\}$ donc $\left|\mathcal{S}_{\mathrm{G}/Z}\right| = 10!$ et $|Z| = 18$. Ainsi S et T sont des 3-Sylow de Z et un groupe d'ordre 18 admet un unique 3-Sylow d'où $S = T$: contradiction. Finalement $S \cap T = \{e_\mathrm{G}\}$.

c) D'après a) le groupe G contient exactement $36 \times 4 = 144$ éléments d'ordre 5.
D'après b) le groupe G contient dix 3-Sylow dont les intersections deux à deux sont triviales. Par suite il y a dans G exactement $10 \times 8 = 80$ éléments distincts de e_G d'ordre divisant 9.
Ainsi G possède au moins $144 + 80 = 224 > 180$ éléments distincts : contradiction.
Il n'existe donc pas de groupe simple d'ordre 180.

Exercice 15 Expliciter les sous-groupes de Sylow des groupes alternés $\mathcal{A}_4$ et $\mathcal{A}_5$.

Solution 15 Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.
Les théorèmes de Sylow assurent que
— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;
— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.
Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Si c'est 4 l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathcal{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathcal{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_5$ ne contient par d'élément d'ordre 4. En effet les éléments d'ordre 4 du groupe symétrique $\mathcal{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de {1, 2, 3, 4, 5}. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à {e}. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.

les sous-groupes d'ordre 4 de $\mathcal{A}_5$ sont engendrés par les paires de transpositions disjointes : on a 5 paires de transpositions distinctes (elles sont déterminées par le seul élément de $\{1, 2, 3, 4, 5\}$ qui reste fixe par la double transposition) qui engendrent des sous-groupes distincts. Cela fait donc déjà cinq 2-Sylow isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Par ailleurs $n_2 \equiv 1 \pmod 2$ et n_2 divise 15 donc n_2 appartient à $\{1, 3, 5, 15\}$. En utilisant ce qui précède on se ramène à $n_2 \in \{5, 15\}$. De plus il y a au plus $60 - 45 - 1 = 14$ éléments d'ordre 2. Finalement $n_2 = 5$.

Exercice 16 Expliciter les sous-groupes de Sylow des groupes diédraux D_8 et D_{10}.

Solution 16

i) Déterminons les sous-groupes de Sylow du groupe D_8. Le groupe D_8 est d'ordre $2^3 = 8$. Les 2-Sylow sont d'ordre 2^3, il n'y en a donc qu'un, c'est D_8.

ii) Déterminons les sous-groupes de Sylow du groupe D_{10}. Le groupe D_{10} est le groupe des isométries du plan qui conservent un pentagone régulier, il est d'ordre $2 \times 5 = 10$.

Soit n_2 le nombre de ses 2-Sylow, *i.e.* le nombre de ses sous-groupes d'ordre 2. D'après les théorèmes de Sylow $n_2 \equiv 1 \pmod 2$ et n_2 divise 5. Ainsi $n_2 \in \{1, 5\}$. Par ailleurs les sous-groupes de D_{10} engendrés par les cinq symétries par rapport aux médiatrices de chacun des côtés du pentagone sont cinq groupes d'ordre 2. Il s'en suit que $n_2 = 5$.

Soit n_5 le nombre de 5-Sylow de D_{10}, *i.e.* le nombre de sous-groupes d'ordre 5 de D_{10}. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \pmod 2$ et n_5 divise 2. Il n'y a donc qu'un unique 5-Sylow, le sous-groupe engendré par la rotation d'angle $\frac{2\pi}{5}$ dont le centre est le centre du pentagone.

Exercice 17

a) Quel est l'ordre d'un p-Sylow de $\mathcal{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathcal{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire

$$(p-1)! \equiv -1 \bmod p.$$

Solution 17

a) L'ordre de $\mathcal{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathcal{S}_p$ est d'ordre p.

b) Pour déterminer le nombre de p-Sylow de $\mathcal{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathcal{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathcal{S}_p$ car $\mathcal{S}_p/C$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathcal{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathcal{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p - 1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 18 On cherche à montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathcal{A}_5$.

b) Montrer que $\mathcal{A}_5$ est simple.

c) Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geqslant 1$ et m non divisible par p. Notons n_p le nombre de p-Sylow de G. Montrer que $|\mathrm{G}|$ divise $n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

e) En déduire que G contient un sous-groupe d'ordre 12.

f) Conclure.

Solution 18

a) Faisons la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif.
Les 60 éléments de $\mathcal{A}_5$ sont les suivants :
- l'identité d'ordre 1 qui forme une classe de conjugaison ;
- les double transpositions $(a\ b)(c\ d)$ où $\{a, b, c, d\}$ est de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2 et elles forment une classe de conjugaison ;
- les 3-cycles $(a\ b\ c)$ où $\{a, b, c\}$ est de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3 et forment une classe de conjugaison ;
- les 5-cycles $(a\ b\ c\ d\ e)$ où $\{a, b, c, d, e\}$ est de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5 et forment deux classes de conjugaison : celle de (1 2 3 4 5) et (2 1 3 4 5).

Nous avons bien énuméré tous les éléments de $\mathcal{A}_5$: $1 + 15 + 20 + 24 = 60$.

b) Montrons que $\mathcal{A}_5$ est simple. Soit $\mathrm{H} \neq \{e\}$ un sous-groupe distingué de $\mathcal{A}_5$. Puisque H est distingué, H est réunion de classes de conjugaison dans $\mathcal{A}_5$. Comme aucun des entiers $1+15 = 16$, $1+12 = 13$, $1+24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 20 + 15 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$ ne divise $60 = |\mathcal{A}_5|$, le théorème de Lagrange assure que H contient nécessairement toutes les classes de conjugaison de $\mathcal{A}_5$, donc $\mathrm{H} = \mathcal{A}_5$.

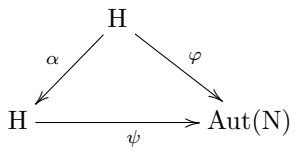
c) Regardons l'action transitive de G par conjugaison sur l'ensemble Syl_p de ses p-Sylow. Comme G est simple $n_p > 1$. On obtient donc un morphisme non trivial $\mathrm{G} \to \mathcal{S}_{\mathrm{Syl}_p} \simeq \mathcal{S}_{n_p}$. Puisque G est simple ce morphisme est injectif. Il en résulte que $|\mathrm{G}|$ divise $|\mathcal{S}_{n_p}| = n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrons que le nombre de 2-Sylow de G est égal à 5 ou à 15.
Soit n_2 le nombre de 2-Sylow. Les théorèmes de Sylow assurent que n_2 est impair et divise 15 ; par suite n_2 appartient à $\{1, 3, 5, 15\}$. Le groupe G étant simple, $n_2 \neq 1$, *i.e.* n_2 appartient à $\{3, 5, 15\}$. Le groupe G est d'ordre $2^2 \cdot 15$; d'après le c) $|\mathrm{G}|$ divise $n_2!$ donc $n_2 \neq 3$. Ainsi n_2 vaut 5 ou 15.

e) Montrons que G contient un sous-groupe d'ordre 12.
Supposons dans un premier temps que $n_2 = 5$; alors le normalisateur d'un 2-Sylow de G est de cardinal $60/5 = 12$ d'où le résultat.
Supposons désormais que $n_2 = 15$. Montrons qu'il existe deux 2-Sylow distincts S et T tels que $|\mathrm{S} \cap \mathrm{T}| = 2$. Sinon on aurait exactement $15 \cdot 3 + 1 = 46$ éléments d'ordre divisant 4. De plus les théorèmes de Sylow assurent que $n_5 = 6$ donc que G contient $6 \cdot 4 = 24$ éléments d'ordre 5. Ainsi d'une part G contient au moins $46 + 24 = 70$ éléments et d'autre par $|\mathrm{G}| = 60$: contradiction. On dispose donc de deux 2-Sylow distincts S et T tels que $\mathrm{S} \cap \mathrm{T} = \{e, g\}$ avec g d'ordre 2. Désignons par H le centralisateur de g dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6. Ainsi $|\mathrm{H}|$ appartient à $\{12, 20, 60\}$. Si $|\mathrm{H}| = 20$, alors l'action transitive de G sur G/H induit un morphisme injectif $\mathrm{G} \to \mathcal{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathcal{S}_3$: contradiction. Si $|\mathrm{H}| = 60$, alors g est dans le centre de G ce qui assure que le centre $Z(\mathrm{G})$ de G est non trivial : contradiction avec le fait que G est simple. Il s'en suit que $|\mathrm{H}| = 12$.

f) Soit H le sous-groupe de G d'ordre 12 construit au e). L'action transitive de G sur G/H induit un morphisme injectif $\varphi\colon \mathrm{G} \to \mathcal{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathcal{S}_5$. Ainsi G est isomorphe à un sous-groupe d'ordre 60 de $\mathcal{S}_5$ qui est nécessairement $\mathcal{A}_5$.

Exercice 19 Rappelons l'énoncé suivant dont nous aurons besoin : Soient H et N deux groupes. Soient φ et ψ deux opérations de H sur N et α un automorphisme de H tels que le diagramme suivant commute



i.e. $\varphi = \psi \circ \alpha$.

L'application $(n, h) \mapsto (n, \alpha(h))$ est un isomorphisme de $\mathrm{N} \rtimes_\psi \mathrm{H}$ sur $\mathrm{N} \rtimes_\varphi \mathrm{H}$.

Soient p et q des nombres premiers avec $p < q$. Montrer que

1. Si p ne divise pas $q-1$, alors tout groupe d'ordre pq est cyclique.
2. Si p divise $q-1$, alors il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi-direct non abélien.

Indication : $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ ([Perrin, Cours d'algèbre, p. 24])

Solution 19

Soit G un groupe d'ordre pq où p et q désignent des nombres premiers tels que $p < q$. Soit Q un q-Sylow de G.

D'après les théorèmes de Sylow

$$\begin{cases} n_q \text{ divise } p \\ n_q \equiv 1 \bmod q \end{cases}$$

où n_q est le nombre de q-Sylow de G. Par suite $n_q = 1$ et Q est distingué dans G.

Puique p est premier, $\mathbb{Q} \simeq \mathbb{Z}/q\mathbb{Z}$. De même $\mathrm{G}/\mathrm{Q} \simeq \mathbb{Z}/p\mathbb{Z}$. Si P est un p-Sylow quelconque il fournit un relèvement de G/Q et donc

$$\mathrm{G} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Calculons ces produits. On a $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. L'opération de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ correspond donc à un morphisme

$$\varphi \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}.$$

On a l'alternative suivante :

- p ne divise pas $q-1$, alors φ est trivial, le produit est direct et $\mathrm{G} \simeq \mathbb{Z}/pq\mathbb{Z}$ est cyclique.
- p divise $q-1$, $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p, il y a donc une opération non triviale. De plus deux telles opérations diffèrent d'un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. L'énoncé rappelé assure que les produits correspondants sont isomorphes.

Exercice 20

Soit $n \geqslant 1$. On note $\mathrm{Int}(\mathcal{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathcal{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathcal{S}_n)$ tel que ϕ transforme toute transposition en une transposition.
Montrer que ϕ est intérieur.

b) Soit $\sigma \in \mathcal{S}_n$. Déterminer le cardinal du commutant

$$Z(\sigma) = \left\{\tau \in \mathcal{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\right\}$$

de σ.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$.

d) Soit $n \geqslant 5$ tel que $\mathrm{Int}(\mathcal{S}^n) = \mathrm{Aut}(\mathcal{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathcal{S}_n$ sont conjugués.

e) En utilisant les 5-Sylow de $\mathcal{S}_5$ montrer qu'il existe un sous-groupe H d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Soit q une puissance d'un nombre premier et $n \geqslant 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}_n(\mathbb{F}_q) \to \mathcal{S}_N$ avec $N = \frac{q^n-1}{q-1}$.

g) Construire géométriquement un sous-groupe H' d'indice 6 dans $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

h) En déduire que $\mathrm{Aut}(\mathcal{S}_6) \neq \mathrm{Int}(\mathcal{S}_6)$.

Solution 20

a) Soit $\phi \in \mathrm{Aut}(\mathcal{S}_n)$ tel que ϕ transforme toute transposition en une transposition.
Montrons que ϕ est intérieur.
Puisque tout automorphisme de $\mathcal{S}_i$ est intérieur dès que $i \leqslant 3$ (à vérifier) on peut supposer que $n \geqslant 4$.
Le groupe symétrique est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geqslant 2$. Comme τ_i et τ_j ne commutent pas si $i \neq j$ les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun noté α_1. Puisque $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ils ont nécessairement tous α_1 en commun. Écrivons $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. L'application φ étant injective $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{1, 2 \ldots, n\}$. Définissons la permutation $\alpha \in \mathcal{S}_n$ par $\alpha(i) = \alpha_i$ pour tout $1 \leqslant i \leqslant n$. Ainsi φ est la conjugaison par α et φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.

b) Soit $\sigma \in \mathcal{S}_n$. Déterminons le cardinal du commutant

$$Z(\sigma) = \left\{\tau \in \mathcal{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\right\}$$

de σ. Décomposons σ en produit de cycles à supports disjoints, k_1 cycles de longueur 1, …, k_n cycles de longueur n, avec $n = \sum_i ik_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ et donc envoyer le support d'un k-cycle sur celui d'un autre k-cycle, en respectant l'ordre cyclique du support de ces cycles pour tout k. Ainsi le commutant d'un n-cycle de $\mathcal{S}_n$ est composé des puissances de ce dernier. Finalement on obtient

$$|Z(\sigma)| = \prod_i k_i! i^{k_i}.$$

c) Montrons que si $n \neq 6$, on a $\mathrm{Int}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$. Soit φ un automorphisme de $\mathcal{S}_n$. Si τ est une transposition de $\mathcal{S}_n$, alors $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de k transpositions à supports disjoints. On a $|Z(\tau)| = |Z(\varphi(\tau))|$ ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Puisque $n \neq 6$ on a $k = 1$. D'après a) φ est donc intérieur.

d) Soit $n \geqslant 5$ tel que $\mathrm{Int}(\mathcal{S}^n) = \mathrm{Aut}(\mathcal{S}_n)$. Montrons que tous les sous-groupes d'indice n de $\mathcal{S}_n$ sont conjugués. Soit H un sous-groupe d'indice n de $\mathcal{S}_n$. L'action transitive de $\mathcal{S}_n$ sur $\mathcal{S}_n/\mathrm{H}$ induit un morphisme de groupes

$$\phi\colon \mathcal{S}_n \to \mathcal{S}_{\mathcal{S}_n/\mathrm{H}} \simeq \mathcal{S}_n.$$

Puisque $\ker\phi$ est un sous-groupe distingué de $\mathcal{S}_n$, $\ker\phi \in \{\{\mathrm{id}\}, \mathcal{A}_n, \mathcal{S}_n\}$. Le groupe $\ker\phi$ agit trivialement sur la classe de H dans $\mathcal{S}_n/\mathrm{H}$, d'où $\ker\phi \subset \mathrm{H}$. Il en résulte que $\ker\phi = \{\mathrm{id}\}$, *i.e.* que ϕ est injective. Ainsi φ appartient à $\mathrm{Aut}(\mathcal{S}_n)$. Par hypothèse il existe une permutation σ telle que ϕ soit la conjugaison par σ. Or par construction ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathcal{S}_{\mathcal{S}_n/\mathrm{H}} \simeq \mathcal{S}_n$. Enfin dans $\mathcal{S}_n$ les stabilisateurs d'un point de $\{1, 2, \ldots, n\}$ sont tous conjugués.

e) En utilisant les 5-Sylow de $\mathcal{S}_5$ montrons qu'il existe un sous-groupe H d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$. Les théorèmes de Sylow assurent que $\mathcal{S}_5$ admet un ou six 5-Sylow. Comme $\mathcal{A}_5$ est simple $\mathcal{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5 et $\mathcal{S}_5$ admet exactement six 5-Sylow. Notons X l'ensemble des 5-Sylow de $\mathcal{S}_5$. L'action de $\mathcal{S}_5$ sur X par conjugaison est transitive et induit un morphisme de groupes

$$\mu\colon \mathcal{S}_5 \to \mathcal{S}_X \simeq \mathcal{S}_6$$

dont le noyau est trivial (les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$). Le groupe $\mathrm{H} = \mu(\mathcal{S}_5) \subset \mathcal{S}_6$ est un sous-groupe d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Preuve géométrique, par récurrence sur n : l'espace projectif $\mathbb{P}^{n-1}(\Bbbk)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur $\Bbbk$ (disons $\Bbbk^n$) et d'un hyperplan projectif de dimension $n-2$, *i.e.* isomorphe à un $\mathbb{P}^{n-2}(\Bbbk)$, appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(\Bbbk) = \Bbbk^{-1} \sqcup \mathbb{P}^{n-2}(\Bbbk)$. On en déduit par récurrence la formule suivante

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + \ldots + q + 1.$$

Autre preuve : le groupe $\mathrm{PGL}(\mathbb{F}_q^n)$ agit fidèlement sur $\mathbb{P}(\mathbb{F}_q^n)$ d'où le morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathcal{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = \mathbb{F}_q^n \smallsetminus \{0\}/\mathbb{F}_q^*$ donc $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1}$. Par conséquent il existe un morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathcal{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

g) Construisons géométriquement un sous-groupe H′ d'indice 6 dans $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$. Le groupe $\mathrm{H}' = \mathrm{PGL}(2, \mathbb{F}_5)$ vu comme sous-groupe de $\mathcal{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ n'est pas conjugué à $\mathcal{S}_5 = \mathrm{Stab}(6) \subset \mathcal{S}_6$ puisqu'il ne fixe aucun point.

h) Montrons que $\mathrm{Aut}(\mathcal{S}_6) \neq \mathrm{Int}(\mathcal{S}_6)$.
Les d), e) et g) assurent que le groupe $\mathcal{S}_6$ possède au moins un automorphisme extérieur.

Exercice 21 [Simplicité de $\mathcal{A}_n$, $g \geqslant 5$, version 2]

a) Montrer que le groupe $\mathcal{A}_5$ est simple.

b) Soit $n \geqslant 3$. Montrer que les 3-cycles engendrent $\mathcal{A}_n$.

c) Montrer que $\mathcal{A}_n$ est simple dès que $n \geqslant 5$.

d) Montrer que $\mathcal{A}_4$ n'est pas simple.

e) Soit $n \geqslant 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Montrer que

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

f) Soit $n \geqslant 3$. Montrer que le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.

g) Soit $n \geqslant 5$. Montrer que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

Solution 21

a) Le groupe $\mathcal{A}_5$ a 60 éléments :
— le neutre ;
— 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;
— 20 éléments d'ordre 3 (3-cycles) ;
— 24 éléments d'ordre 5 (5-cycles).
Les 3-cycles sont conjugués dans $\mathcal{A}_5$ [1]. Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.
Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (resp. 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément donc tous les 5-sous-groupes de Sylow puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.
Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|\mathrm{H}| \geqslant 15 + 20 + 1 + 36.$$

Comme $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$ on obtient $|\mathrm{H}| = 60$ et $\mathrm{H} = \mathcal{A}_5$.

b) Puisque le groupe $\mathcal{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

c) Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \setminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.
Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geqslant 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E \setminus F} = \mathrm{id}_{|E \setminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.
Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes

1. Le groupe $\mathcal{A}_5$ est 3 fois transitif sur $\{1, 2, \ldots, 5\}$, *i.e.* si a_1, a_2, a_3 sont distincts et b_1, b_2, b_3 sont distincts il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, 5\} = \{a_1, a_2, \ldots, a_5\} = \{b_1, b_2, \ldots, b_5\}$$

et considérons $\sigma \in \mathcal{S}_5$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, 5$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_4\ a_5)$.
Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_5$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

— $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;
— $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \,|\, \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. Alors
— $\mathrm{H}_0 \lhd \mathcal{A}(F)$;
— $\rho_{|F} \in \mathrm{H}_0$;
— $\rho_{|F} \neq \mathrm{id}_F$.
Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $\mathrm{H}_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ [2] ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (cf b)) on a $\mathrm{H} = \mathcal{A}_n$.

d) Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

e) Calcul direct.

f) Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite d'après e)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

g) Soit $\mathrm{H} \lhd \mathcal{S}_n$. Alors $\mathrm{H} \cap \mathcal{A}_n \lhd \mathcal{A}_n$ donc $\mathrm{H} \cap \mathcal{A}_n \in \big\{\mathrm{id},\ \mathcal{A}_n\big\}$.
Si $\mathrm{H} \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathrm{H} = \mathcal{A}_n$ ou $\mathrm{H} = \mathcal{S}_n$.
Si $\mathrm{H} \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(\mathrm{H}) \subset \{1, -1\}$. Par suite $|\mathrm{H}| \leqslant 2$.
Si $|\mathrm{H}| = 2$, alors $\mathrm{H} = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathcal{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$.
Autrement dit σ appartient au centre de $\mathcal{S}_n$ d'où $\sigma = \mathrm{id}$ (f)) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$.

2. Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$, *i.e.* si $a_1, a_2, \ldots, a_{n-2}$ sont distincts et b_1, b_2, b_{n-2} sont distincts il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, b_2, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et considérons $\sigma \in \mathcal{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, n$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_{n-1}\ a_n)$.
Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ \ldots\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_n$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$