105. Groupes des permutations d'un ensemble fini : éléments de solutions

1. a) Si l'on conjugue la double transposition $(a,b)(c,d)$ par une permutation σ, on obtient $(\sigma(a),\sigma(b))(\sigma(c),\sigma(d))$, ce qui montre que V_4 est distingué dans $\mathcal{S}_4$, et donc a fortiori dans $\mathcal{A}_4$. Ensuite, comme G/V_4 est de cardinal $12/4 = 3$, il est cyclique de cardinal 3 (car 3 est premier) et en particulier abélien, ce qui montre que $D(G) \subset V_4$.

b) On voit facilement que G n'est pas abélien, donc $D(G) \neq \{1\}$. D'autre part un sous-groupe H de G de cardinal 2 est composé de l'identité et d'une double transposition $\tau = (a,b)(c,d)$. Si l'on conjugue τ par $\sigma \in G$, on obtient $(\sigma(a),\sigma(b))(\sigma(c),\sigma(d))$, qui ne reste pas dans H si on choisit par exemple $\sigma \in G$ telle que $\sigma(a) = a$ et $\sigma(b) = c$, ce qui est toujours possible.

c) On a vu que $D(G) \subset V_4$, donc le cardinal de $D(G)$ divise 4, mais on a aussi vu que ce ne peut être ni 1 ni 2, donc c'est 4 et $D(G) = V_4$.

d) Soit $a \notin H$. Comme le cardinal de l'ensemble G/H des classes à gauche est 2, cet ensemble est composé de H et de la classe aH, qui est le complémentaire de H dans A. De même l'ensemble $H \setminus G$ des classes à droite est composé de H et de Ha, qui est aussi le complémentaire de H dans A.Ainsi $aH = Ha$, et ceci reste vrai quand $a \in H$. Finalement $aHa^{-1} = H$ pour tout $a \in A$, autrement dit $H \lhd A$.

e) D'après d), on a $H \lhd G$. Alors, le groupe G/H est abélien puisque de cardinal 2, ce qui montre que $H \supset D(G)$. Mais d'après c), le groupe $D(G)$ est de cardinal 4 alors que H est de cardinal 6, ce qui contredit le théorème de Lagrange.

f) C'est clair pour $d = 1$ et $d = 24$. Pour $d = 2$, on prend le groupe engendré par une transposition, pour $d = 3$ celui engendré par un 3-cycle et pour $d = 4$ celui engendré par un 4-cycle. Pour $d = 6$, le sous-groupe des permutations laissant fixe 1 est isomorphe à $\mathcal{S}_3$, il est donc de cardinal 6. Pour $d = 12$, on prend le sous-groupe $\mathcal{A}_4$. Reste le cas $d = 8$, auquel cas on a un sous-groupe isomorphe au groupe diédral D_4 (cf. exercice 4), par exemple celui engendré par un 4-cycle et une transposition.

2. On note déjà que comme la signature d'un commutateur est 1, on a toujours $D(\mathcal{S}_n) \subset \mathcal{A}_n$.

a) Pour $n = 2$, on a $\mathcal{S}_2$ abélien et $\mathcal{A}_2$ trivial, donc $\mathcal{A}_2$ est bien le sous-groupe dérivé de $\mathcal{A}_2$. Pour $n = 3$, le sous-groupe dérivé de $\mathcal{S}_3$ est non trivial car $\mathcal{S}_3$ est non commutatif, et inclus dans $\mathcal{A}_3$ qui est de cardinal premier, donc c'est forcément $\mathcal{A}_3$.

b) Soit $c = (a, b, c)$. Si τ est la transposition (b, c), alors $\tau c = (a, c)$, qui s'écrit $\sigma\tau\sigma^{-1}$, où σ est une permutation envoyant b sur a et c sur c.

c) D'après b), le 3-cycle $c = \tau^{-1}\sigma\tau\sigma^{-1}$ est bien un commutateur. Ainsi $D(\mathcal{S}_n)$ contient n'importe quel 3-cycle, donc contient $\mathcal{A}_n$ (qui est engendré par les 3-cycles). Finalement $D(\mathcal{S}_n) = \mathcal{A}_n$.

3. L'observation importante est que commme $\mathbf{Z}/12\mathbf{Z}$ est abélien, le noyau d'un tel morphisme contient le sous-groupe dérivé de $\mathcal{S}_n$ (en effet l'image de tout commutateur est triviale). Comme ce sous-groupe est $\mathcal{A}_n$ (cf. exercice 2.), un tel morphisme est trivial, ou bien se factorise en un morphisme injectif $\mathcal{S}_n/\mathcal{A}_n \simeq \{\pm 1\} \to \mathbf{Z}/12\mathbf{Z}$, l'isomorphisme étant induit par la signature. Ainsi, le seul morphisme non trivial est celui obtenu en composant la signature avec le morphisme envoyant 1 sur $\bar{0}$ et -1 sur $\bar{6}$. Ceci s'applique encore à $n = 4$. Si on remplace $\mathbf{Z}/12\mathbf{Z}$ par un groupe abélien A, les morphismes non triviaux sont obtenus en composant la signature avec le morphisme envoyant 1 sur le neutre de A et -1 sur un élément arbitraire d'ordre 2 de A.

4. Soient a_1, a_2, a_3, a_4 les quatre sommets du carré et O son centre. Toute isométrie du plan qui laisse stable l'ensemble $\{a_1, ..., a_4\}$ permute les sommets, d'où un morphisme $\Phi : D_4 \to \mathcal{S}_4$ qui est clairement injectif car une application affine induisant l'identité sur un ensemble de trois points non alignés est l'identité. On observe que D_4 contient déjà au moins 8 éléments : l'identité, les rotations de centre O et d'angles $\pi/2$,$-\pi/2$, π, et les quatre symétries orthogonales d'axes respectifs les deux diagonales et les deux médiatrices des cotés. Ainsi le cardinal de D_4 est au moins 8 et divise 24, mais ce n'est pas 24 car Φ n'est pas surjectif (par exemple, il ne contient pas la permutation envoyant a_1 sur lui-même et a_2 sur a_3 si a_1a_2 est un côté et a_1a_3 une diagonale). Finalement le cardinal de D_4 est exactement 8. Or $\mathcal{S}_4$ n'a pas de sous groupe distingué d'ordre 8, car un tel sous-groupe H vérifierait $\mathcal{S}_4/H$ abélien (puisque de cardinal 3), et H devrait contenir le sous-groupe dérivé de $\mathcal{S}_4$, lequel est de cardinal 12 via l'exercice 2.

5. Comme le cardinal de $\mathcal{S}_p$ est $p!$, un tel p-Sylow est de cardinal p, donc est cyclique. Ainsi les p-Sylow sont tout simplement les p-cycles.

6. a) Soient $\sigma_1, ..., \sigma_n$ les polynômes symétriques élémentaires. Le théorème de structure des polynômes symétriques dit exactement que le morphisme de K-algèbres de A dans B qui envoie tout polynôme P sur $P(\sigma_1, ..., \sigma_n)$ est un isomorphisme !

b) On a clairement $P^{\sigma\tau} = (P^\sigma)^\tau$ (autrement dit l'application de $\mathcal{S}_n \times A$ dans A qui envoie (σ, P) sur P^σ est une opération à droite); de plus $P \mapsto P^\sigma$ est un automorphisme de K-algèbres pour toute permutation σ. On en déduit immédiatement que S vérifie $S^\tau = \tau$ pour toute permutation τ, autrement dit S est symétrique.

c) Soit $F = G/H$ une fraction rationnelle symétrique, avec G et H dans A. On a aussi

$$F = \frac{\prod_{\sigma \in \mathcal{S}_n} G^\sigma}{H. \prod_{\sigma \neq id} G^\sigma}.$$

D'après b), le numérateur est dans B. C'est aussi le cas du dénominateur D, car pour toute permutation τ, on a

$$D^\tau = H^\tau . \prod_{\sigma \neq \tau} G^\sigma = H. \prod_{\sigma \neq id} G^\sigma,$$

vu que $H^\tau . G = H . G^\tau$ via l'hypothèse que F est symétrique.

d) Le quotient de deux polynômes symétriques est clairement dans M, et le c) nous dit que la réciproque est vraie. Ainsi on a bien $M = \operatorname{Frac} B$. Le a) implique alors que L et M sont des corps isomorphes (et même qu'il y a un isomorphisme de corps de L sur M qui est aussi un isomorphisme de K-algèbres, autrement dit qui induit l'identité sur K).