

## 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  $\sigma$ , 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  $\tau$  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  $H \backslash G$  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  $H \triangleleft A$ .

e) D'après d), on a  $H \triangleleft G$ . 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 3), par exemple celui engendré par un 4-cycle et une transposition. On peut aussi invoquer

le théorème de Sylow pour obtenir l'existence d'un sous-groupe de cardinal 8.

**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  $\tau$  est la transposition  $(b, c)$ , alors  $\tau c = (a, c)$ , qui s'écrit  $\sigma\tau\sigma^{-1}$ , où  $\sigma$  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.** 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  $\{a_1, \dots, a_4\}$  permute les sommets, d'où un morphisme  $\Phi : D_4 \rightarrow \mathcal{S}_4$  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  $\pi/2, -\pi/2, \pi$ , 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  $\Phi$  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.

**4.** 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.

**5.** a) Soient  $\sigma_1, \dots, \sigma_n$  les  $n$  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  $P(\sigma_1, \dots, \sigma_n)$  est un isomorphisme !

b) L'application de  $\mathcal{S}_n \times A$  dans  $A$  qui envoie  $(\sigma, P)$  sur  $\sigma.P$  est une opération à gauche; de plus  $P \mapsto \sigma.P$  est un automorphisme de  $K$ -algèbres

pour toute permutation  $\sigma$ . On en déduit immédiatement que  $S$  vérifie  $\tau.S = S$  pour toute permutation  $\tau$ , autrement dit  $S$  est symétrique.

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

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

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

$$\tau.D = (\tau.H) \prod_{\sigma \neq \tau} \sigma.G = H \cdot \prod_{\sigma \neq id} \sigma.G,$$

vu que  $(\tau.H)G = H(\tau.G)$  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  $M = \text{Frac } B$ . 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  $K$ ).

**6.** a) L'indice  $[\mathcal{S}_n : \mathcal{A}_n]$  est 2, donc si  $H \supset \mathcal{A}_n$ , l'indice de  $H$  dans  $\mathcal{S}_n$  est au plus 2 et n'est pas 1 car  $H \neq \mathcal{S}_n$ . Ainsi cet indice est 2, donc  $H$  a même cardinal que  $\mathcal{A}_n$ , donc  $H = \mathcal{A}_n$ .

b) Comme  $H$  est distingué dans  $\mathcal{S}_n$ , le groupe  $H \cap \mathcal{A}_n$  est a fortiori distingué dans  $\mathcal{A}_n$  (qui est simple) et ce n'est pas  $\mathcal{A}_n$  vu que  $H$  ne contient pas  $\mathcal{A}_n$ . La seule possibilité est donc que  $H \cap \mathcal{A}_n$  est le groupe trivial. Soit alors  $\tau$  un élément non trivial de  $H$ , il est de signature  $-1$ ; alors tout élément de  $H$  autre que  $\text{Id}$  est de signature  $-1$ , donc si  $\sigma$  est un tel élément, on doit avoir  $\sigma\tau = \text{Id}$  puisqu'alors  $\sigma\tau$  est de signature 1. La seule possibilité est donc que les seuls éléments non triviaux de  $H$  soient  $\tau$  et  $\tau^{-1}$ , donc  $H$  est de cardinal au plus 3.

c) Il suffit d'après a) et b) de traiter le cas où  $H \cap \mathcal{A}_n$  est trivial. Si le cardinal de  $H$  est 3, alors les éléments non triviaux de  $H$  sont d'ordre 3, mais ce n'est pas possible puisque leur signature est  $-1$ . Reste le cas où  $H = \{\text{Id}, \tau\}$  avec  $\tau$  d'ordre 2, mais un tel sous-groupe n'est jamais distingué dans  $\mathcal{S}_n$  (écrire  $\tau$  comme un produit de transpositions à supports disjoints, par exemple  $\tau = (1, 2)\dots$ , et conjuguer  $\tau$  par une permutation qui laisse fixe 1 et envoie 2 sur 3). Finalement on a  $H = \{\text{Id}\}$  dès que  $H \cap \mathcal{A}_n = \{\text{Id}\}$ .

d) Le résultat ne vaut plus pour  $n = 4$  : le sous-groupe  $V_4$  composé de l'identité et des doubles transpositions est en effet distingué dans  $\mathcal{S}_4$ .