Université Pierre & Marie Curie — Année 2008-2009
Master de Mathématiques — MM014 Théorie des groupes
Professeur: J.F. Dat — A. Guilloux

Feuille 3

Corrigé

Groupes de transformations de polyèdre

Solution 1 *Les rotations en question permutent les quatre sommets du tétraèdre, et il s'agit d'une action fidèle : si une transformation laisse fixe les 4 sommets, c'est l'identité. On en déduit que* G_T *est un sous-groupe de* $\mathcal{S}_4$*, mais il est facile de voir que la seule transformation linéaire qui induit une transposition* τ_{AB} *sur les sommets est la symétrie orthogonale par rapport au plan qui contient les deux autres sommets et le milieu de* AB*. Ce n'est donc pas une rotation. On a donc* $G_T \subset \mathcal{A}_4$*. Mais* G_T *contient les demi-tours d'axe joignant les milieux de deux côtés opposés, réalisant la permutation* $(AB)(CD)$ *et les tiers de tour d'axe joignant un sommet et le milieu de la face opposée, réalisant* (ABC)*. En résumé, toutes les permutations paires sont réalisées, et* $G_T \simeq \mathcal{A}_4$*.*

Solution 2 *Le cube a 4 diagonales et* G_C *les permute. Cette action est fidèle : si un endomorphisme de* $\mathbb{R}^3$ *laisse stable (admet comme droites propres) les quatre diagonales, c'est un scalaire, et la seule rotation de* $\mathbb{R}^3$ *qui est scalaire est* Id*. On a donc une injection de* G_C *dans* $\mathcal{S}_4$*. On obtient la transposition de deux diagonales en prenant le demi-tour d'axe perpendiculaire au plan engendré par les deux autres diagonales. L'image de* G_C *dans* $\mathcal{S}_4$ *contient les transpositions : c'est* S_4 *tout entier. Les milieux des faces d'un cube forment un octaèdre régulier et les milieux des faces d'un octaèdre régulier forment un cube. On dit que le cube et l'octaèdre régulier sont* duaux*. On en déduit facilement que* $G_O = G_C \simeq \mathcal{S}_4$*.*

Remarque Les 20 sommets d'un dodécaèdre régulier D peuvent (de deux façons possibles) être partitionnés en cinq groupes, chaque groupe formant les sommets d'un tétraèdre régulier. Le groupe G_D des rotations de $\mathbb{R}^3$ qui laissent D stable agit sur cet ensemble de 5 tétraèdres, et on peut montrer que cette action est fidèle et induit un isomorphisme de G_D sur $\mathcal{A}_5$. Comme l'icosaèdre régulier est dual du dodécaèdre régulier, on a encore $G_I = G_D \simeq \mathcal{A}_5$.

Théorèmes de Sylow

Solution 3

a) Le nombre n_q de q-Sylows de G est un diviseur de p congru à 1 modulo q. Il y en a donc un seul, S_q, qui est distingué et isomorphe à $\mathbb{Z}/q\mathbb{Z}$. Si S_p est un p-Sylow, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On a $S_p \cap S_q = \{e\}$ et $S_pS_q = G$, donc $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. On a vu à l'exercice 8 qu'il n'y a que deux possibilités : le groupe (produit direct) cyclique $\mathbb{Z}/pq\mathbb{Z}$ et, si q est congru à 1 modulo p, un autre.

b) Notons n_p (respectivement n_q) le nombre de p-Sylows (respectivement q-Sylows) de G. On a $n_p = 1$ ou q et $n_q = 1$, p ou p^2. Si G n'a pas de sous-groupe distingué, $n_p = q$ et $n_q = p$ ou p^2. On a donc $q \equiv 1 \pmod p$, ce qui interdit $n_q = p$. Il y a donc p^2 q-Sylows distincts. Comme l'intersection de deux d'entre eux est réduite à $\{e\}$, leur réunion a donc exactement $p^2(q-1)$ éléments l'ordre q et les p-Sylows sont inclus dans le complémentaire qui est de cardinal p^2. Il y a donc un seul p-Sylow, une contradiction.

Solution 4

a) En reprenant les mêmes notations qu'à l'exercie précédent, on a $n_3 = 1$ ou 10 et $n_5 = 1$ ou 6. Si ni P_3 ni P_5 ne sont distingués, il y a dans G $10(3-1) = 20$ éléments d'ordre 3 et $6(5-1) = 24$ éléments d'ordre 5. Comme G n'a que 30 éléments, c'est impossible.

b) Si P_5 ou P_3 est distingué, $N = P_3P_5$ est un sous-groupe de G d'indice 2, donc distingué. On a vu dans l'exercice précédent que le seul groupe d'ordre 15 est $\mathbb{Z}/15\mathbb{Z}$, qui n'a qu'un seul sous-groupe d'ordre 3 (respectivement 5). Les 3-Sylows de G sont conjugués à P_3 donc inclus dans N donc égaux à P_3, donc $n_3 = 1$. De même, $n_5 = 1$.

c) Soit P_2 un 2-Sylow de G. On voit que G est produit semi-direct de $\mathbb{Z}/15\mathbb{Z}$ par P_2, ce qui nous ramène à l'exercice 8.

Solution 5

a) Le nombre de 17-Sylows est un diviseur de 15 congru à 1 modulo 17. Il vaut donc 1 et S_{17} est distingué. En particulier, $H = S_5S_{17}$ est un sous-groupe de G.

b) L'indice de H est 3, le plus petit diviseur premier de G. On a vu dans l'exercice 13 de la feuille 1 que cela impliquait que H est normal. Comme $17 \not\equiv 1 \pmod 5$, H est cyclique et S_5 est normal dans H.

Si $g \in G$, comme H est normal dans G et que S_5 est un sous groupe de H, alors gS_5g^{-1} est un sous groupe de H. Comme H n'a qu'un seul 5-Sylow, on a forcément $gS_5g^{-1} = S_5$, c'est à dire S_5 est distingué dans G.

c) On a $H \cap S_3 = \{e\}$ et $HS_3 = G$, donc $G = N \rtimes \mathbb{Z}/3\mathbb{Z}$. Mais $Aut(H) \simeq (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/17\mathbb{Z})^*$ est un groupe à 2^6 éléments, il n'y a donc pas d'action *non triviale de $S_3 \simeq \mathbb{Z}/3\mathbb{Z}$ sur H et le produit est en fait direct : $G \simeq \mathbb{Z}/255\mathbb{Z}$.*

Solution 6

a) Les diviseurs de $540/5 = 108 = 2^2 3^3$ sont

$$\{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\},$$

parmi lesquels seuls 1, $a = 6$ et $b = 36$ sont congrus à 1 modulo 5. Comme tous les 5-Sylows sont conjugués entre eux, n_5 est le nombre de conjugués de S_5, c'est à dire l'indice de son normalisateur. Donc $[G : N_5] = n_5 = 1$, 6 ou 36.

b) Il y a six 5-Sylows distincts. L'action de G par conjugaison permute ces six éléments, d'où un morphisme de G dans $\mathcal{S}_6$. Comme cette action est transitive, le noyau H de cette action n'est pas G tout entier. L'indice $[G : H]$ est le cardinal de l'image de G dans $\mathcal{S}_6$. Comme ce dernier groupe est de cardinal $6!$ et que $|G| = 540$ ne divise pas $6!$, H n'est pas réduit à $\{e\}$. Finalement, H est un sous-groupe normal non trivial et G n'est pas simple.

c) L'ordre de N_5 est $540/36 = 15$. On a vu à l'exercice 7 de la feuille 2 que le seul groupe d'ordre 15 est cyclique. Si deux éléments distincts x et x' de S_5 étaient conjugués, ce seraient deux générateurs de S_5 et on aurait $x' = gxg^{-1}$ pour un certain élément de G. On en déduit que $S_5 =< x' >=< gxg^{-1} >= g < x > g^{-1} = gS_5g^{-1}$, c'est à dire que $g \in N_5$. Mais N_5 est commutatif, donc $x' = x$, une contradiction.

d) L'existence et l'unicité de $\tau(i)$ et de s_i sont évidentes. Montrons que τ est injective : Si i et j sont tels que $\tau(i) = \tau(j)$, on a

$$y_i^{-1} y_j = (gy_i)^{-1}(gy_j) = (y_{\tau(i)} s_i)^{-1} y_{\tau(j)} s_j = s_i^{-1} s_j,$$

donc $y_j \in y_i S_5$ et $i = j$. On a donc montré $\tau \in \mathcal{S}_k$. Notons $g' y_i = y_{\tau'(i)} s'_i$. On a

$$gg' y_i = g y_{\tau'(i)} s'_i = y_{\tau(\tau'(i))} s_{\tau'(i)} s'_i$$

et donc $\varphi(gg') = \prod_i s_{\tau'(i)} \prod_i s'_i = \varphi(g)\varphi(g')$ puisque $\tau'(i)$ parcourt $\{1..k\}$ quand i parcourt $\{1..k\}$, et que S_5 est abélien.

e) Si y'_i est un autre système de représentants, il existe un famille $(t_i)_{1 \leq i \leq k}$ d'éléments de S_5 telle que $y'_i = y_i t_i$. On a alors

$$g y'_i = y_{\tau(i)} s_i t_i = y'_{\tau(i)} t_{\tau(i)}^{-1} s_i t_i$$

et, comme S_5 est commutatif,

$$\varphi'(g) = \prod_i t_{\tau(i)}^{-1} \varphi(g) \prod_i t_i = \varphi(g).$$

f) Comme $u^5 = e$, l'existence de $r \leq 5$ est évidente. Montrons que l'on a $u^r y = yu^r$. En effet, $z = y^{-1}u^r y$ est un conjugué de u^r qui appartient à S_5. D'après la question c), cela implique $z = u^r$.

On voit que S_5 agit par translation à gauche sur G/S_5. En choisissant dans chaque orbite un représentant y de cet élément, ainsi que $u^j y$ pour $j < r$, on trouve un système de représentants de G/S_5. Pour chaque élément de ce système, $uy_i = y_{i+1}$ si $j < r-1$ et $uy_i = y_{i+1-r}u^r$ si $j = r-1$. Donc le produit des s_i correspondant à cette orbite est u^r, où r est le cardinal de l'orbite (en fait $r = 1$ ou $r = 5$ selon que y appartient ou non à N_5). Pour calculer $\varphi(u)$ il faut rassembler toutes les orbites : on trouve $\varphi(u) = u^{|G/S_5|} = u^{108}$. Comme 108 n'est pas un multiple de 5, $\varphi(u)$ est un générateur de S_5 et φ est surjectif.

g) Le noyau de φ est un sous-groupe distingué d'indice 5, donc non trivial, et G n'est pas simple, conclusion que l'on a obtenue quel que soit l'indice de N_5 dans G.

Solution 7 *Si un p-Sylow n'est pas normal, G agit transitivement (par conjugaison) sur l'ensemble des p-Sylow. Cela induit un homomorphisme non trivial de G sur $\mathcal{S}_{n_p}$. le noyau de ce morphisme est un sous-groupe normal de G différent de G et d'indice divisant $n_p!$. On en conclut que si $|G|$ ne divise pas $n_p!$, G n'est pas simple.*

a) Le cas $r = 0$ ne dépend pas de p et se résout directement. Soit G un groupe d'ordre $12 = 2^2 3$. On sait d'après l'exercice 9 question b) que $n_2 = 1$ ou $n_3 = 1$, ce qui implique que G n'est pas simple.

Cela implique aussi que $G = S_3 \rtimes S_2$ ou $G = S_2 \rtimes S_3$. On a $S_3 = \mathbb{Z}/3\mathbb{Z}$ et $S_2 = \mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$. Comme $Aut(\mathbb{Z}/3\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, $Aut(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ et $Aut\,(\mathbb{Z}/2\mathbb{Z})^2 = \mathcal{S}_3$, on trouve facilement tous les groupes G possibles :

$$\mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z},$$

$$\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2 = D_6, \quad \textit{et} \quad (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} = \mathcal{A}_4$$

(dans tous les cas, il existe un unique produit semi direct non trivial)

b) Ici $n_2 = 1$ ou 3, et le cardinal de G est plus grand que $6 = 3!$, donc G n'est pas simple.

c) Ici $n_3 = 1$ ou 4, et le cardinal de G est plus grand que $24 = 4!$, donc G n'est pas simple.

d) Ici, n_5 est un diviseur de 12 congru à 1 $\pmod 5$. Donc $n_5 = 1$ ou 6. Si $r > 1$, le cardinal de G ne peut diviser $120 = 6!$, donc G n'est pas simple. Pour $r = 1$, le groupe a 60 éléments.

Soit x un élément d'ordre 2, et H son normalisateur. Il existe un 2-Sylow S_2 contenant x, et comme $|S_2| = 4$, S_2 est abélien. En particulier, $S_2 < H$. Donc $4 \setminus |H| \setminus 60$, donc $|H| = 4, 12, 20$ ou 60. Si $|H| = 60$, alors

$< x > \lhd G$ et G n'est pas simple. G agit transitivement par multiplication à gauche sur G/H, ce qui nous donne un morphisme non trivial $G \to \mathcal{S}_{[G:H]}$. Si $|H| = 20$, on a donc un morphisme $G \to \mathcal{S}_3$ de noyau non trivial donc G n'est pas simple.

Si $|H| = 12$, on a un morphisme non trivial $G \to \mathcal{S}_5$. Si G est simple, ce morphisme est donc injectif, et G est isomorphe à un sous groupe d'indice 2 de $\mathcal{S}_5$. Comme $\mathcal{A}_5$ est le seul sous groupe de $\mathcal{S}_5$ d'indice 2, on a $G \simeq \mathcal{A}_5$.

Si $|H| = 4$, alors $H = S_2$. Donc l'intersection de deux 2-Sylow est réduite à 1. En effet, si $x \in S_2 \cap S_2'$, alors $S_2 \cup S_2' \subset H$ et donc $S_2 = S_2'$. Donc on a

$$|G| \geq 4n_5 + 2n_3 + 3n_2 + 1$$

Si G est simple, alors $n_5 = 6$, $n_3 = 4$ ou 10 et $n_2 = 3, 5$ ou 15. Si $n_3 = 4$, G n'est pas simple par le même raisonnement qu'à la question c), donc $n_3 = 10$. De même, $n_2 \neq 3$. Si $n_2 = 15$, alors $|G| \geq 90$ ce qui est impossible. Donc $n_2 = 5$ et on a encore une injection $G \to \mathcal{S}_5$.

e) Ici, n_{11} est un diviseur de 12 congru à 1 $\pmod{11}$. Donc $n_{11} = 1$ ou 12. Si $r > 1$, le cardinal de G ne peut diviser $120 = 6!$, donc G n'est pas simple. Si $r = 1$, le groupe a 132 éléments dont 120 sont d'ordre 11 puisque les 12 11-Sylow sont "disjoints" deux à deux. Il reste 12 éléments pour les autres ordres. Il y a $2n_3$ éléments d'ordre 3. Si $n_3 > 1$, cela impose $n_3 = 4$ et il reste 4 éléments qui forment l'unique 2-Sylow et G n'est pas simple.

f) Si G est simple, pour $p > 3$, n_p est un diviseur de 12 congru à 1 $\pmod{p}$. Donc $n_p \in \{1, 2, 3, 4, 6, 12\}$ et, si $n_p \neq 1$, $p \in \{2, 3, 5, 11\}$. On a donc étudié tous les cas possibles et le seul groupe simple trouvé est $\mathcal{A}_5$.