UFR Mathématiques, Université de Rennes 1
Licence de Mathématiques

# ALGEBRE ET APPLICATIONS GEOMETRIQUES

## Corrigé de contrôle du 17 mars 2001

**1.** a. Le sous-ensemble $G$ de $S_4$ est l'ensemble de tous les mots (à puissances $\pm 1$) dans $S_4$ sur $\{a, b\}$. Comme $a$ et $b$ sont d'ordre fini dans $S_4$, le sous-ensemble $G$ est aussi l'ensemble des mots sur $\{a, b\}$ à puissances égales à 1. Comme $ba = a^3b$, le sous-ensemble $G$ est encore égal à l'ensemble $\{a^i b^j \mid i, j \in \mathbb{N}\}$. Comme $a^4 = \mathrm{id}$ et $b^2 = \mathrm{id}$,

$$G = \{\mathrm{id}, a, a^2, a^3, b, ab, a^2b, a^3b\}, \quad (2 \text{ pt})$$

et ces éléments de $S_4$ sont deux-à-deux distincts. En particulier, $G$ est d'ordre 8 (1 pt). Voici la table de $G$ (2 pt):

| $x \cdot y$ | $x = \mathrm{id}$ | $x = a$ | $x = a^2$ | $x = a^3$ | $x = b$ | $x = ab$ | $x = a^2b$ | $x = a^3b$ |
|---|---|---|---|---|---|---|---|---|
| $y = \mathrm{id}$ | id | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
| $y = a$ | $a$ | $a^2$ | $a^3$ | id | $a^3b$ | $b$ | $ab$ | $a^2b$ |
| $y = a^2$ | $a^2$ | $a^3$ | id | $a$ | $a^2b$ | $a^3b$ | $b$ | $ab$ |
| $y = a^3$ | $a^3$ | id | $a$ | $a^2$ | $ab$ | $a^2b$ | $a^3b$ | $b$ |
| $y = b$ | $b$ | $ab$ | $a^2b$ | $a^3b$ | id | $a$ | $a^2$ | $a^3$ |
| $y = ab$ | $ab$ | $a^2b$ | $a^3b$ | $b$ | $a^3$ | id | $a$ | $a^2$ |
| $y = a^2b$ | $a^2b$ | $a^3b$ | $b$ | $ab$ | $a^2$ | $a^3$ | id | $a$ |
| $y = a^3b$ | $a^3b$ | $b$ | $ab$ | $a^2b$ | $a$ | $a^2$ | $a^3$ | id |

b. L'élément neutre id est d'ordre 1, les éléments $a^2, b, ab, a^2b, a^3b$ sont d'ordre 2, les éléments $a, a^3$ sont d'ordre 4 (1 pt).

c. Tout d'abord, $\{\mathrm{id}\}$ et $G$ sont des sous-groupes distingués de $G$ (1 pt). Les sous-groupes cycliques non triviaux sont (1 pt):

$$\langle a \rangle,\ \langle a^2 \rangle,\ \langle b \rangle,\ \langle ab \rangle,\ \langle a^2b \rangle \text{ et } \langle a^3b \rangle.$$

Le premier est d'ordre 4, les autres sont d'ordre 2. Ils sont deux-à-deux distincts. Comme $\langle a \rangle$ est le seul sous-groupe cyclique d'ordre 4 de $G$, il est distingué (0.5 pt). Comme $\langle a^2 \rangle$ est le seul sous-groupe non trivial du groupe distingué $\langle a \rangle$, il est également distingué (0.5 pt). Comme

$$a\langle b \rangle a^{-1} = \langle aba^{-1} \rangle = \langle a^2b \rangle \quad \text{et} \quad a\langle ab \rangle a^{-1} = \langle a^2ba^{-1} \rangle = \langle a^3b \rangle,$$

les autres sous-groupes cycliques de $G$ ne sont pas distingués (0.5 pt).

Pour finir on détermine les sous-groupes non triviaux et non cycliques de $G$. Soit $H$ un tel sous-groupe. D'après le cours, l'ordre de $H$ divise l'ordre de $G$. Comme $H$ est non trivial et non cyclique, l'ordre de $H$ est égal à 4. Comme $H$ n'est pas cyclique $a, a^3 \notin H$. Par conséquent, il existe $i, j \in \{0, 1, 2, 3\}$ avec $i < j$ tels que $a^i b \in H$ et $a^j b \in H$. Ceci implique que $a^{j-i} = (a^j b)(a^i b)^{-1} \in H$. Donc $j - i = 2$ et $a^2 \in H$. Il s'ensuit que $H = \langle a^2, b\rangle$ ou $H = \langle a^2, ab\rangle$. Les deux sous-groupes

$$\langle a^2, b\rangle \quad \text{et} \quad \langle a^2, ab\rangle$$

sont bien des sous-groupes non triviaux et non cycliques de $G$. De plus, ils sont deux-à-deux distincts. D'après ce qui précède, ce sont les seuls sous-groupes non triviaux et non cycliques de $G$ (1 pt). Comme ils sont d'indice 2 dans $G$ ils sont bien distingués (0.5 pt).

**2.** a. Comme l'action de $G$ sur $E$ est non triviale, il existe un élément $x \in E$ dont l'orbite $Gx$ est de cardinal au moins 2. Comme le cardinal de $E$ est égal à 6, le cardinal de $Gx$ est au plus 6. D'où les inégalités

$$2 \leq |G| \leq 6. \quad \text{(1 pt)}$$

D'après le cours,

$$|G| = |G_x| \cdot |Gx|. \quad \text{(1 pt)}$$

En particulier, $|Gx|$ divise $|G| = 35$. Or, 5 est le seul diviseur de 35 compris entre 2 et 6. Par conséquent, $|Gx| = 5$. Comme $E$ est la réunion disjointe de ses orbites, $Gx$ est la seule orbite de cardinal 5 (1 pt).

b. Il y a 6 sous-ensembles de $E$ de cardinal 5 (1 pt). Tout ordre cyclique sur un tel sous-ensemble donne lieu à une et une seule action de $G$ sur $E$. Comme il y a $\frac{5!}{5} = 4!$ de tels ordres sur un ensemble à 5 éléments (1 pt), il y a $6 \times 4!$ actions à gauche non triviales de $G$ sur $E$ d'après le a.

**3.** Il y a plusieurs façons de montrer l'assertion. On en donne deux:

**1ère methode:** Supposons que $S_{36}$ est isomorphe à $A_{36} \times \mathbb{Z}/2\mathbb{Z}$. Le groupe $S_{36}$ contient un élément d'ordre $4 \times 31$ (1 pt pour l'idée). Donc le groupe $A_{36} \times \mathbb{Z}/2\mathbb{Z}$ contient également un élément d'ordre $4 \times 31$. Soit $(\sigma, x)$ un tel élément. L'ordre de $(\sigma, x)$ est égal au ppcm de l'ordre de $\sigma$ et l'ordre de $x$. Comme $x$ est d'ordre 1 ou 2 et comme l'ordre de $(\sigma, x)$ est égal à $4 \times 31$, l'élément $\sigma \in A_{36}$ est d'ordre $4 \times 31$ (1 pt). Ecrire $\sigma$ comme produit de cycles disjoints :

$$\sigma = \sigma_1 \cdots \sigma_n,$$

où $\sigma_i \in S_{36}$. Soit $\ell_i$ la longueur de $\sigma_i$. Quitte à rajouter des cycles de longueur 1, on peut supposer que

$$\ell_1 + \cdots + \ell_n = 36.$$

Le ppcm des ordres des $\sigma_i$ est égal à l'ordre de $\sigma$. Autrement dit,

$$\mathrm{ppcm}(\ell_1, \ldots, \ell_n) = 4 \times 31.$$

Comme 31 est premier, l'un des $\ell_i$, disons $\ell_1$, est divisible par 31. Comme $\ell_1 \leq 36$, $\ell_1 = 31$ (0.5 pt). D'où

$$\ell_2 + \cdots + \ell_n = 5 \quad \text{et} \quad 4 \mid \mathrm{ppcm}(\ell_2, \ldots, \ell_n).$$

Comme 4 est une puissance d'un nombre premier, l'un des $\ell_2, \ldots, \ell_n$ doit être divisible par 4. On peut supposer que $\ell_2$ est divisible par 4. Il s'ensuit que $\ell_2 = 4$, que $\ell_3 = 1$ et que $n = 3$ (0.5 pt). Par conséquent, $\sigma$ est le produit d'un 31-cycle et un 4-cycle et est donc impair (1 pt). Contradiction.

**2ème methode:** Pour un groupe $G$, soit $C(G)$ le centre de $G$. Deux groupes qui sont isomorphes ont des centres isomorphes (1 pt). D'après les TD, $C(S_{36}) = \{\mathrm{id}\}$, i.e., le centre de $S_{36}$ est trivial (1 pt). Mais, évidemment,

$$C(A_{36} \times \mathbb{Z}/2\mathbb{Z}) = C(A_{36}) \times C(\mathbb{Z}/2\mathbb{Z}) \quad (1 \text{ pt})$$

qui contient au moins les éléments $(\mathrm{id}, \overline{0})$ et $(\mathrm{id}, \overline{1})$ (1 pt). Donc le centre de $A_{36} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas trivial. Par conséquent, $S_{36}$ n'est pas isomorphe à $A_{36} \times \mathbb{Z}/2\mathbb{Z}$.