UFR Mathématiques, Université de Rennes 1
Licence de Mathématiques

ALGEBRE ET APPLICATIONS GEOMETRIQUES

Corrigé, examen terminal, 28 mai 2002

1. Le cardinal d'une orbite de E divise l'ordre de G. Comme l'ordre de G est égal à $143 = 11 \times 13$, le cardinal d'une orbite de E est égal à 1, 11, 13 ou 143. Comme G agit sans point fixe, E ne contient pas d'orbite de cardinal 1. Comme le cardinal de E est égal à 142, E ne contient pas non plus d'orbite de cardinal 143. Par conséquent, chaque orbite de E est de cardinal 11 ou 13.

Soit a le nombre d'orbites de E de cardinal 11 et soit b le nombre d'orbites de E de cardinal 13. Comme E est la réunion disjointe de ses orbites, on a

$$11a + 13b = 142.$$

On va résoudre l'équation $11a+13b = 142$ dans $\mathbb{Z}$. Comme $11 \times (-1) + 13 \times 1 = 2$, on voit tout de suite une solution particulière :

$$11 \times (-71) + 13 \times 71 = 142.$$

Par conséquent, la solution générale est de la forme

$$a = -71 + 13k \quad \text{et} \quad b = 71 - 11k,$$

où $k \in \mathbb{Z}$.

Maintenant, $a \geq 0$ et $b \geq 0$. Donc $13k \geq 71$ et $11k \leq 71$. La première inégalité donne $k \geq 6$, la deuxième donne $k \leq 6$. Par conséquent, $k = 6$. Il s'ensuit que $a = 7$ et $b = 5$. Le nombre d'orbites de E est donc égal à $7 + 5 = 12$.

2. a. Soit f un morphisme de D_{13} dans $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Soit ρ un élément de D_{13} d'ordre 13. Comme 13 et 6×10 sont premiers entre eux, ρ appartient à $\ker(f)$. Le sous-groupe $H = \langle \rho \rangle$ de D_{13} est donc entièrement contenu dans $\ker(f)$.

Comme H est d'indice 2 dans D_{13}, il est distingué et le quotient D_{13}/H est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Soit $\pi\colon D_{13} \to \mathbb{Z}/2\mathbb{Z}$ un morphisme de noyau H. Comme $H \subseteq \ker(f)$, il existe un et un seul morphisme $\overline{f}$ de $\mathbb{Z}/2\mathbb{Z}$ dans G tel que $\overline{f} \circ \pi = f$. Par conséquent, il y a une correspondance bijective entre l'ensemble de morphismes de D_{13} dans G d'une part, et l'ensemble de morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans G d'autre part. Il suffit donc de compter le nombre de morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans G.

Soit f un morphisme de $\mathbb{Z}/2\mathbb{Z}$ dans G. L'élément $f(\overline{1})$ de G satisfait $2f(\overline{1}) = (\overline{0}, \overline{0})$. Réciproquement, pour tout élément x de G satisfaisant $2x = (\overline{0}, \overline{0})$, il existe un unique morphisme f de $\mathbb{Z}/2\mathbb{Z}$ dans G tel que $f(\overline{1}) = x$. Par conséquent, le nombre de morphismes cherché est égal au nombre d'éléments x de G satisfaisant $2x = (\overline{0}, \overline{0})$. Or, il y en a 4:

$$(\overline{0}, \overline{0}),\ (\overline{0}, \overline{5}),\ (\overline{3}, \overline{0}) \text{ et } (\overline{3}, \overline{5}).$$

b. Soit f un morphisme de $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ dans D_{13}. Soit H le sous-groupe $2\mathbb{Z}/6\mathbb{Z} \times 2\mathbb{Z}/10\mathbb{Z}$ de G. L'ordre de H est égal à 15. Comme 15 et 26 sont premiers entre eux, $H \subseteq \ker(f)$.

Le quotient G/H est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soit donc π un morphisme de G dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ de noyau H. Comme $H \subseteq \ker(f)$, il existe un et un seul morphisme $\overline{f}$ de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{13} tel que $\overline{f} \circ \pi = f$. Par conséquent, il y a une correspondance bijective entre l'ensemble de morphismes de G dans D_{13} d'une part, et l'ensemble de morphismes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{13} d'autre part. Il suffit donc de compter le nombre de morphismes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{13}.

Soit f un morphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{13}. Les éléments $x = f(\overline{1}, \overline{0})$ et $y = f(\overline{0}, \overline{1})$ de D_{13} satisfont $x^2 = y^2 = e$. Réciproquement, pour tous les éléments x, y de D_{13} satisfaisant $x^2 = y^2 = e$, il y a un et un seul morphisme f de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{13} tel que $x = f(\overline{1}, \overline{0})$ et $y = f(\overline{0}, \overline{1})$. Par conséquent, le nombre de morphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{13} est égal au nombre de couples $(x, y) \in D_{13} \times D_{13}$ satisfaisant $x^2 = y^2 = e$. Or, il y en a 14^2, car il y a 14 éléments $z \in D_{13}$ satisfaisant $z^2 = e$.

3. a. La décomposition de 2002 en facteurs premiers est $2 \times 7 \times 11 \times 13$. Déterminons le nombre s_7 de 7-sylows de G. D'après Sylow, $s_7 \equiv 1 \mod 7$ et s_7 divise $2 \times 11 \times 13$. Comme $2, 11, 13$ sont respectivement congrus à $2, -3, -1$ modulo 7, $s_7 = 1$ ou 22. Par hypothèse $s_7 \neq 22$. Il s'ensuit que $s_7 = 1$. Soit donc S_7 l'unique 7-sylow de G. Comme $s_7 = 1$, S_7 est distingué dans G.

Déterminons le nombre s_{11} de 11-sylows de G. D'après Sylow, $s_{11} \equiv 1 \mod 11$ et s_{11} divise $2 \times 7 \times 13$. Comme $2, 7, 13$ sont respectivement congrus à $2, -4, 2$ modulo 11, $s_{11} = 1$. Soit donc S_{11} l'unique 11-sylow de G. Comme $s_{11} = 1$, S_{11} est distingué dans G.

Comme S_7 et S_{11} sont distingués dans G, le sous-ensemble $K = S_7 S_{11}$ est un sous-groupe distingué de G. De plus, comme $|S_7|$ et $|S_{11}|$ sont premiers entre eux, $S_7 \cap S_{11} = \{e\}$. Il s'ensuit que $|K| = |S_7| \times |S_{11}| = 7 \times 11 = 77$.

b. Le groupe K est un groupe d'ordre 7×11. Comme $7 - 1 \not\equiv 0 \mod 11$, K est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. Comme 7 et 11 sont premiers entre eux, ce dernier groupe est isomorphe à $\mathbb{Z}/77\mathbb{Z}$.

c. D'après Sylow, il existe un 13-sylow S_{13} de G. Comme K est distingué dans G, le sous-ensemble $H = KS_{13}$ est un sous-groupe de G. Comme $|K|$ et $|S_{13}|$ sont premiers entre eux, $K \cap S_{13} = \{e\}$. Il s'ensuit que $|H| = |K| \times |S_{13}| = 77 \times 13 = 1001$. De plus, comme H est d'indice 2 dans G, H est distingué.

d. Le sous-groupe K de H est distingué. De plus $KS_{13} = H$ et $K \cap S_{13} = \{e\}$. Il s'ensuit que H est isomorphe à un produit semi-direct de K et S_{13}. D'après le b, K est isomorphe à $\mathbb{Z}/77\mathbb{Z}$. Comme 13 est premier, S_{13} est isomorphe à $\mathbb{Z}/13\mathbb{Z}$. Par conséquent, H est isomorphe au produit semi-direct de $\mathbb{Z}/77\mathbb{Z}$ et $\mathbb{Z}/13\mathbb{Z}$ relativement à une action de $\mathbb{Z}/13\mathbb{Z}$ sur $\mathbb{Z}/77\mathbb{Z}$. Comme $\mathrm{Aut}(\mathbb{Z}/77\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, tout morphisme de $\mathbb{Z}/13\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/77\mathbb{Z})$ est trivial. Par conséquent, H est isomorphe à $\mathbb{Z}/77\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Comme 77 et 13 sont premiers entre eux, ce dernier groupe est isomorphe à $\mathbb{Z}/1001\mathbb{Z}$.

e. D'après Sylow, il existe un 2-sylow S_2 dans G. Comme $|H|$ et $|S_2|$ sont premiers entre eux, $H \cap S_2 = \{e\}$. Il s'ensuit que le cardinal du sous-ensemble HS_2 de G est égal à $1001 \times 2 = 2002 = |G|$. Par conséquent, $HS_2 = G$. D'après le c, H est distingué dans G. Il s'ensuit que G est isomorphe à un produit semi-direct de H et S_2. D'après le d, H est isomorphe à $\mathbb{Z}/1001\mathbb{Z}$. Comme $|S_2| = 2$, S_2 est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Donc G est isomorphe à un produit semi-direct de $\mathbb{Z}/1001\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$. Il s'ensuit que G est isomorphe à $\mathbb{Z}/1001\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2002\mathbb{Z}$ ou à D_{1001}.

4. Soit $H' = i(H)$. On a $N \cap H' = \{e\}$. En effet, soit $g \in N \cap H'$. Comme $g \in H'$, il existe $h \in H$ tel que $i(h) = g$. Comme $g \in N$, on a $p(g) = e$ dans H. Il s'ensuit que

$$h = (p \circ i)(h) = p(i(h)) = p(g) = e$$

dans H. Donc aussi $g = i(h) = i(e) = e$ dans G. Cela montre que $N \cap H' = \{e\}$.

Montrons que $NH' = G$. Soit $g \in G$. Posons $h = p(g)$ et $h' = i(h)$. On a bien $h' \in H'$. Soit $n = g \cdot (h')^{-1}$. Comme,

$$p(n) = p(g \cdot (h')^{-1}) = p(g) \cdot p(h')^{-1} = h \cdot (p \circ i)(h)^{-1} = h \cdot h^{-1} = e$$

$n \in N$ et $g = nh'$. cela montre que $NH' = G$.

Comme N est distingué dans G, G est le produit semi-direct de N et H'. Comme i est un isomorphisme de H sur H', G est isomorphe à un produit semi-direct de N et H.