Université Claude Bernard Lyon 1

Correction du PARTIEL M1-Algèbre de Novembre 2014

Exercice 1.

1. La propriété universelle des groupes libres et le passage au quotient permet de voir que f est bien définie si r^a et $r^b s$ vérifient les relations de r et s. On vérifie donc les formules $(r^a)^n = 1$, $(r^b s)^2 = 1$ et enfin $(r^b s) r^a (r^b s)^{-1} = r^{-a}$. Ce qui se fait droit devant. Le morphisme est unique car r et s sont des générateurs du groupe de départ.
2. On trouve $f_{a,b} \circ f_{a',b'}(r) = r^{aa'}$ et $f_{a,b} \circ f_{a',b'}(s) = r^{ab'+b}s$. Ainsi, par unicité, on a $f_{a,b} \circ f_{a',b'} = f_{aa',ab'+b}$.
3. L'identité de D_n s'écrit $f_{1,0}$, donc, on voit que $f_{a,b}$ est un automorphisme si et seulement si a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.
4. Si on associe (a, b) de $(\mathbb{Z}/n\mathbb{Z})^* \times \mathbb{Z}/n\mathbb{Z}$ à $f_{a,b}$ dans $\mathrm{Aut}(D_n)$, on définit un isomorphisme entre $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$, où l'action de $(\mathbb{Z}/n\mathbb{Z})^*$ sur $\mathbb{Z}/n\mathbb{Z}$ se fait par multiplication à gauche : $b \mapsto ab$ (cela se voit par la formule trouvée en question 2).
5. Si $t = r^k$, on trouve $\gamma_t = f_{1,2k}$ et si $t = r^k s$, alors on trouve $\gamma_t = f_{-1,2k}$
6. Du coup, $\mathrm{Int}(D_n)$ est le produit semi-direct $2\mathbb{Z}/n\mathbb{Z} \rtimes \{1, -1\}$. Si n est pair, alors $2\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\frac{n}{2}\mathbb{Z}$, sinon 2 est inversible et donc $2\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$.

Exercice 2.

1. On trouve $\alpha = (1i)(2j)$ et $\alpha(12k)\alpha^{-1} = (ijk)$ par la formule de conjugaison. Du coup, tous les 3-cycles sont engendrés par ceux de la forme $(12i)$. Comme les 3-cycles engendrent le groupe alterné, on obtient un système de générateurs plus restreint donné par les $(12i)$.
2. C'est encore la propriété universelle et le passage au quotient qui montrent que l'on a un morphisme de G_n dans $\mathfrak{A}_{n+2}$ qui envoie les x_i sur les $(12i)$, la vérification des relations étant immédiate par ce qui précède. La surjectivité provient du fait que qu'un système de générateurs du groupe alterné est atteint.
3. On vérifie la stabilité par multiplication par x_n, en faisant un cas par cas et en utilisant les relations. Par exemple, $x_n(x_n H) = x_n^2 H$, $x_n(x_i x_n H) = x_n(x_n^2 x_i^2 H) = x_n^3 H = H$. On vérifie ensuite la stabilité par multiplication pour les autres x_i, par exemple $x_i(x j x_n H) = x_i x_n^2 x_j^2 H = x_i x_n^2 H = x_n x_i^2 H = x_n H$. Les autres vérifications sont du même acabit.
4. On vérifie que les b_i vérifient les relations de x_i dans G_6, on peut le faire sur sage pour en être sûr, mais en temps limité et sans machine, on se base sur quelques petits calculs piochés au hasard et une confiance méritée du cadre enseignant. Une fois ces vérifications faites, on a un morphisme surjectif de G_6 sur $\mathrm{GL}_4(\mathbb{F}_2)$ donc, un morphisme surjectif de $\mathfrak{A}_8$ dans $\mathrm{GL}_4(\mathbb{F}_2)$, forcément iso par cardinalité.

Exercice 3.

1. Le nombre de 7-Sylow divise 3 et est congru à 1 modulo 7. Il n'y a donc qu'un seul 7-Sylow, et du coup, il est distingué. Comme il est d'ordre 7^2, c'est le carré d'un nombre premier, il est forcément abélien et donc isomorphe, soit à $(\mathbb{Z}/p\mathbb{Z})^2$, soit à $\mathbb{Z}/p^2\mathbb{Z}$.
2. L'ordre de $(\mathbb{Z}/7^2\mathbb{Z})^*$ est $7^2 - 7 = 42$. Nombre qui, selon wikipedia, succède à 41 tout en précédant 43. Ce qui lui a valu une réputation qui dépasse largement le cadre de ce modeste cours.

3. Comme $\mathbb{Z}$ est un groupe libre, il suffit d'envoyer $1 \in \mathbb{Z}$ sur une puissance g^k, $0 \leq k \leq 41$ de g telle que $(g^k)^3 = e$. Comme g est d'ordre 42, on obtient que 42 divise $3k$ et donc, $k = 0, 14$, ou 28.
4. Comme le groupe additif $(\mathbb{F}_7, +)$ est engendré par 1, tout morphisme du groupe $(\mathbb{F}_7^2, +)$ est un morphisme du $\mathbb{F}_7$-espace vectoriel $\mathbb{F}_7^2$ dans lui-même. On a donc l'isomorphisme voulu.
5. Toute matrice d'ordre 3 est donc annulée par le polynôme $X^3 - 1$. Or, ce polynôme est scindé simple sur $\mathbb{F}_7$ puisque ses racines sont 1, 2, 4. Donc, toute matrice d'ordre 3 est diagonalisable. Deux matrices d'ordre 3 sont donc conjuguées si et seulement si elles ont même spectre, et les spectres possibles sont au nombre de 5 : $\{1, 2\}$, $\{1, 4\}$, $\{2, 2\}$, $\{2, 4\}$, $\{4, 4\}$, (bien sûr, $\{1, 1\}$ ne fait pas partie du lot, puisque la matrice serait alors d'ordre 1).
6. Conclure en trouvant au final (au plus) six classes de groupes d'ordre 147.

   Le cas abélien donne facilement deux groupes non isomorphes par le théorème de structure.

   Soit maintenant G un groupe d'ordre 147 non abélien. Tout d'abord, la question 1 prouve facilement que G est un produit semi-direct de la forme $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. Mais il y a beaucoup de morphismes possibles du groupe de droite vers celui des automorphismes de celui de gauche.

   On utilise donc la proposition du cours pour réduire au maximum les classes d'isomorphismes de produits semi-directs. On réduit « à gauche » par l'automorphisme $z \mapsto z^2$ de $\mathbb{Z}/3\mathbb{Z}$, et on réduit « à droite » par la conjugaison pour trouver au final 4 produits semi-directs : 1) $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où φ envoie 1 sur g^{14}, 2) $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où φ envoie 1 sur une matrice de spectre soit $\{1, 2\}$, (ou son carré $\{1, 4\}$, ce qui donne un groupe isomorphe), soit $\{2, 2\}$ (et donc $\{4, 4\}$), $\{2, 4\}$ (et donc $\{4, 2\}$).

   Question bonus : En fait il y a exactement 6 classes d'isomorphisme de groupes d'ordre 147. Les deux abéliens $(\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont non isomorphes et ne peuvent être isomorphes aux non abéliens. Le PSD $(\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ ne peut être isomorphe à un PSD $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, car sinon, leurs uniques 7-Sylow seraient isomorphes entre eux. Reste à différencier les trois PSD correspondant aux trois classes de conjugaison. Soit g dans G (que l'on suppose sous une de ces trois formes) d'ordre 3. Alors, g se décompose dans $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ sous la forme, disons, ab, où a est dans $(\mathbb{Z}/p\mathbb{Z})^2$ et où b agit sur $(\mathbb{Z}/p\mathbb{Z})^2$ avec comme spectre $\{x, y\}$. Mais dans ce cas, comme $(\mathbb{Z}/p\mathbb{Z})^2$ est abélien l'action de a par conjugaison sur $(\mathbb{Z}/p\mathbb{Z})^2$ est triviale et donc le spectre de g est égal au spectre de b. Donc, comme un isomorphisme envoie le 7-Sylow sur le 7-Sylow et un élément d'ordre 3 sur un élément d'ordre 3, les classes d'isomorphismes de ces trois groupes sont bien caractérisées par leur spectre.