Éléments de correction du DM

Exercice 1.

1. D'après le théorème de Lagrange, l'ordre de H divise l'ordre p^n de G, donc $\mathcal{E} = \{p^i : i = 0, 1 \ldots, n\}$.
2. D'après le théorème du cours sur la structure de sous-groupes d'un groupe cyclique, il existe, pour tout diviseur d de p^n un unique sous-groupe de G d'ordre d. De plus ce sous-groupe est nécessairement cyclique. Ainsi, pour tout $j = p^i \in \mathcal{E}$, il existe un unique sous-groupe H, nécessairement cyclique, d'ordre j dans G.
3. Si $p = 2, n = 3$ alors, $G = \mathbb{Z}/8\mathbb{Z}$ et un sous-groupe d'indice 4 est d'ordre 2 d'après le théorème de Lagrange. Or $\bar{4}$ est d'ordre 2 dans $\mathbb{Z}/8\mathbb{Z}$. Donc $\langle\bar{4}\rangle$ est un sous-groupe d'indice 4 de G. (C'est l'unique tel sous-groupe d'après la question 2.)
4. (a) Si $a \in \mathbb{Z}$ alors $\bar{a} \in (\mathbb{Z}/8\mathbb{Z})^\times$ si et seulement si $\mathrm{pgcd}(a, 8) = 1$. Ainsi $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. L'ordre de $\bar{1}$ vaut 1. Comme $\bar{3}^2 = \bar{9} = \bar{1}$, l'ordre de $\bar{3}$ est 2. De même $\bar{5}^2 = \bar{7}^2 = \bar{1}$. Donc tous les éléemnts de $(\mathbb{Z}/8\mathbb{Z})^\times$ sont d'ordre 2, hormis $\bar{1}$ qui est d'ordre 1.

   (b) $(\mathbb{Z}/8\mathbb{Z})^\times$ est d'ordre 4 mais ne contient pas d'élément d'ordre 4 ; il n'est donc pas cyclique.
5. (a) Bien sûr pour tout entier x, on a $\bar{1} \cdot \bar{x} = \bar{x}$. Aussi, si $y, z \in \mathbb{Z}$ sont premiers à 9, alors $\bar{y} \cdot \overline{zx} = \overline{yzx} = (\bar{y}\bar{z}) \cdot \bar{x}$, par définition de la multiplication dans $\mathbb{Z}/9\mathbb{Z}$. L'application de l'énoncé définit donc une action du groupe $(\mathbb{Z}/9\mathbb{Z})^\times$ sur $\mathbb{Z}/9\mathbb{Z}$.

   (b) Dans $(\mathbb{Z}/9\mathbb{Z})^\times$, on a $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \overline{-1}$, $\bar{2}^4 = \overline{-2}$, $\bar{2}^5 = \bar{5}$. $\bar{2}^6 = \bar{1}$. Or $(\mathbb{Z}/9\mathbb{Z})^\times$ est d'ordre 6, donc $(\mathbb{Z}/9\mathbb{Z})^\times = \langle\bar{2}\rangle$. Les orbites dans l'action de la question (a) sont donc obtenues par multiplication itérée des éléments de $\mathbb{Z}/9\mathbb{Z}$ par $\bar{2}$. Ces orbites sont :

$$\{\bar{0}\},\ \{\bar{1}, \bar{2}, \bar{4}, \bar{8}, \bar{7}, \bar{5}\}, \{\bar{3}, \bar{6}\}\,.$$

Exercice 2.

1. On a $|\mathcal{A}_4| = 4!/2 = 12$.
2. (a) D'après Lagrange, l'ordre de $\pi(a)$ divise $|G/N| = (G : N)$. Aussi, on a $a^m = 1$ dans G. En appliquant le morphisme π on obtient $\pi(a)^m = 1_{G/N}$. Donc l'ordre de $\pi(a)$ divise m.

   (b) Par hypothèse $\mathrm{pgcd}(m, (G : N)) = 1$. En combinant avec la question 1, on déduit donc que $\pi(a)$ est d'ordre 1 dans G/N. Ainsi $\pi(a)$ est la classe triviale de G modulo N, autrement dit $a \in N$.
3. Par l'absurde, soit N un sous-groupe d'indice 2 dans $\mathcal{A}_4$. C'est un sous-groupe distingué d'ordre 6. D'après la question 2, tout élément a d'ordre impair de $\mathcal{A}_4$ est élément de N. Ainsi N contient tous les 3-cycles de $\mathcal{A}_4$. Le nombre de 3 cycles dans $\mathcal{A}_4$ est $(4 \times 3 \times 2)/3 = 8$. C'est la contradiction cherchée. (Alternativement, on peut invoquer le fait que les 3-cycles engendrent $\mathcal{A}_4$.)
4. En plus des 8 3-cycles mentionnés à la question 3, il y a dans $\mathcal{A}_4$ des produits de 2 transpositions à supports disjoints : (12)(34), (13)(24), (14)(23). En rajoutant l'identité, on a énuméré tous les éléments de $\mathcal{A}_4$. Les éléments d'ordre 2 de $\mathcal{A}_4$ sont donc (12)(34), (13)(24), (14)(23) . Ces 3 éléments, auxquels on adjoint l'identité, forment le sous-groupe H recherché.
5. Le conjugué par tout $\tau \in \mathcal{A}_4$ d'un élément quelconque $\sigma \in \mathcal{A}_4$ a même ordre que σ. Donc le conjugué d'un produit de 2 transpositions à supports disjoints est encore un élément d'ordre 2 de $\mathcal{A}_4$ (i.e. c'est encore un produit de 2 transpositions à supports disjoints). Donc H est stable par conjugaison dans $\mathcal{A}_4$, c'est donc un sous-groupe distingué de $\mathcal{A}_4$. Un ensemble de représentants pour $\mathcal{A}_4/H$ est par exemple $\{\mathrm{Id}, (123), (132)\}$. En effet $(123)(132)^{-1} = (123)^2$ est d'ordre 3 et n'est donc pas dans H.

6. $d = 1$: il y a un seul sous-groupe d'indice 1, c'est $\mathcal{A}_4$ tout entier. $d = 2$: d'après la question 3, il n'y a pas de sous-groupe d'indice 2 dans $\mathcal{A}_4$. $d = 3$: le sous-groupe H est d'indice 3 dans $\mathcal{A}_4$ d'après la question 4. $d = 4$: un sous-groupe d'indice 4 est un sous-groupe d'ordre 3. Il y a de tels sous-groupes dans $\mathcal{A}_4$, par exemple $\langle(123)\rangle$. $d = 6$: un sous-groupe d'indice 6 est un sous-groupe d'ordre 2. Il y a de tels sous-groupes dans $\mathcal{A}_4$, par exemple $\langle(12)(34)\rangle$.

Exercice 3.

1. $\mathbb{Z}/4\mathbb{Z}$ est cyclique. Ses générateurs sont les classes d'entiers premiers à 4, c'est à dire les classes de 1 et 3.
2. $\star$ est bien une loi interne sur H. On voit que $(0, 0)$ (chaque coordonnée est le neutre de $\mathbb{Z}/4\mathbb{Z}$) est le neutre de $\star$. On vérifie l'associativité en prenant 3 éléments (a, b), (c, d), (e, f) de H et en voyant que $a + (-1)^b c + (-1)^{b+d} e = a + (-1)^b (c + (-1)^d e)$. (L'associativité "sur la seconde coordonnée" est triviale car "+" est associative sur $\mathbb{Z}/4\mathbb{Z}$.) L'inverse de (a, b) pour $\star$ est $((-1)^{b+1} a, -b)$. Donc $(H, \star)$ est un groupe. Enfin l'ordre de $(H, \star)$ est le cardinal de H, c'est-à-dire 16.
3. On a $(1, 1) \star (1, 2) = (0, 3)$ et $(1, 2) \star (1, 1) = (2, 3)$ donc $\star$ n'est pas une loi commutative.
4. $(a, b) \star (2, 2) = (a + (-1)^b 2, b + 2)$ et $(2, 2) \star (a, b) = (2 + (-1)^2 a, 2 + b)$. Comme $2 \equiv -2 (\text{mod } 4)$ et que "+" est commutative, on voit que ces deux quantités sont égales à $(a + 2, b + 2)$.
5. L'élément $(2, 2)$ de $(H, \star)$ est d'ordre 2 d'après le calcul fait à la question précédente. Donc $K = \langle(2, 2)\rangle$ est un sous-groupe d'ordre 2 du centre de $(H, \star)$ il est donc distingué et d'indice 8, i.e. H/K est un groupe d'ordre 8.
6. On calcule $(1, 0) \star (0, 1) = (1, 1)$ et $(0, 1) \star (1, 0) = (3, 1)$. Comme ces couples sont distincts et que $(1, 1) \star (2, 2) \neq (3, 1)$ on conclut que les classes à gauche de $(1, 0)$ et $(0, 1)$ modulo K ne commutent pas.
7. On a $(a, b) \star (a, b) = (a(1 + (-1)^b), 2b)$. On cherche les a, b possibles dans $\mathbb{Z}/4\mathbb{Z}$ pour que cet élément soit dans K. Déjà il faut que b soit distinct de 1 et 3 modulo 4, sinon cet élément vaut $(0, 2)$ qui n'est pas dans K. Si $b = 0$ dans $\mathbb{Z}/4\mathbb{Z}$, alors l'élément ci-dessus vaut $(2a, 0)$. Alors a est distinct de 1 et 3 car $(2, 0) \notin K$. Ainsi $(a, b) = (0, 0)$ dont la classe modulo K est d'ordre 1 ou bien $(a, b) = (2, 0)$. De même si $b = 2$ dans $\mathbb{Z}/4\mathbb{Z}$ alors l'élément considéré est $(2a, 2)$. Les cas $a = 1$ et $a = 3$ redonnent $(2, 2)$ dont la classe modulo K est triviale. On trouve finalement 2 possibilités pour (a, b) : $(0, 2)$ et $(2, 0)$. Comme $(0, 2) \star (2, 2) = (2, 0)$, on conclut que $(0, 2)$ et $(2, 0)$ représentent la même classe modulo K : l'unique classe d'ordre 2 de H/K.

   Comme $(a, b) \star (0, 2) = (a, b + 2)$ et que $(0, 2) \star (a, b) = (a, b + 2)$, on en déduit que la classe de $(0, 2)$ est dans le centre de H/K.
8. On a vu que H/K est d'ordre 8. Bien sûr H/K et $\{1_{H/K}\}$ sont distingués dans H/K. Par Lagrange, les autres indices possibles pour un sous-groupe de H/K sont 2 et 4. Tout sous-groupe d'indice 2 est distingué. Un sous-groupe d'indice 4 est d'ordre 2 et on a vu à la question précédente qu'il n'y a qu'un seul sous-groupe d'ordre 2 et que ce sous-groupe est distingué puisque contenu dans le centre. Donc tous els sous-groupes de H/K sont distingués dans H/K.