Algèbre et arithmétique 4
DEVOIR MAISON N° 1

Exercice 1 (*Le groupe* $(\mathbb{Z}/n\mathbb{Z})^*$)

1) La question la moins bien réussie du devoir... Il s'agissait ici, comme le disait l'énoncé, de définir précisémment le sens de la multiplication sur $\mathbb{Z}/n\mathbb{Z}$. En particulier, écrire $\times_n(a,b) = \overline{a}\overline{b}$ constituait déjà une erreur puisque l'opération de multiplier une classe par une autre n'est pas définie, c'est justement ce que l'on cherche à faire. Par contre $\overline{ab}$ a un sens, c'est juste la classe du produit de deux entiers.
La relation d'équivalence à considérer ici est la relation modulo $n\mathbb{Z} \times n\mathbb{Z}$, qui est bien un sous groupe distingué de $\mathbb{Z} \times \mathbb{Z}$. Soient donc $(a,b) \in \mathbb{Z}^2$ et $(c,d) \in \mathbb{Z}^2$ qui soient en relation modulo n. Le critère de passage au quotient nous dit que l'on doit montrer que $\times_n(a,b) = \times_n(c,d)$. C'est à dire $a - c \in n\mathbb{Z}$ et $b - d \in n\mathbb{Z}$, il existe donc $u, v \in \mathbb{Z}$ tels que $a = c + nu, b = d + nv$. Ainsi $ab = cd + n(ud + vc + nuv)$ et donc $\overline{ab} = \overline{cd}$, ce qui conclut.
2) Soient $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$. Donc les représentants entiers a et b sont premiers à n, et donc ab aussi (on peut aussi le redémontrer avec Bézout). Donc $\overline{ab}$ est bien dans $(\mathbb{Z}/n\mathbb{Z})^*$.
3) L'erreur la plus commune ici consistait à réecrire les axiomes d'un groupe en espérant qu'ils soient vrais, sans réellement les vérifier.
Vérifions l'associativité :

$$(\overline{a}\overline{b})\overline{c} = \overline{ab}\overline{c} = \overline{abc} = \overline{a}\overline{bc} = \overline{a}(\overline{b}\overline{c}).$$

(ici, chaque passage d'égalité correspond précisémment à l'application de la définition du produit sur $\mathbb{Z}/n\mathbb{Z}$ ci-dessus).
Il y a un élément neutre qui est $\overline{1}$: en effet, 1 est bien premier à n, est donc dans $(\mathbb{Z}/n\mathbb{Z})^*$ et on a bien pour tout $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, $\overline{1}\overline{x} = \overline{x}\overline{1} = \overline{x}$. Existence d'un inverse : soit $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, d'après Bézout, il existe des entiers u, v tels que $xu + nv = 1$. Et donc $\overline{xu} = \overline{1}$. Il reste à vérifier que $\overline{u}$ est bien dans $(\mathbb{Z}/n\mathbb{Z})^*$; ceci est donné par l'équation de Bézout $xu + nv = 1$.
4) 5 est premier à 6, donc 5 est un des générateurs de $(\mathbb{Z}/6\mathbb{Z}, +)$. Il est donc d'ordre 6. Dans $\overline{5}^2 = \overline{1}$ modulo 6 mais $\overline{5} \neq \overline{1}$, donc son ordre est 2 dans le groupe multiplicatif
5) De même 3 étant premier avec 7, $\overline{3}$ est automatiquement d'ordre 7 dans le groupe additif. Par contre, pour le groupe multiplicatif, il faut calculer ses puissances jusqu'à obtenir le neutre :

$$\langle\overline{3}\rangle = \langle\overline{3}, \overline{3}^2 = \overline{2}, \overline{3}^3 = \overline{6}, \overline{3}^4 = \overline{4}, \overline{3}^5 = \overline{5}, \overline{3}^6 = \overline{1}\rangle.$$

Et donc $\overline{3}$ est d'ordre 6 dans le groupe multiplicatif.
6) Ici une petite erreur dans l'énoncé : il y a plus d'un isomorphisme entre ces deux groupes, on doit donc pas lire 'L'isomorphisme' mais plutôt 'UN isomorphisme' . On peut répondre à la première partir de la question de manière théorique : le groupe $(\mathbb{Z}/7\mathbb{Z})^*$ est cyclique de générateur $\overline{3}$ d'après le 5). Donc il est isomorphe au groupe $(\mathbb{Z}/6\mathbb{Z}, +)$, d'après le cours. On sait que $\phi : \mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^*$, $\phi(n) = \overline{3}^n$, est un morphisme ; il est surjectif. Comme $\overline{3}$ est d'ordre 6, le noyau est $6\mathbb{Z}$, et donc ϕ passe au quotient en un isomorphisme de $\mathbb{Z}/6\mathbb{Z}$ dans $(\mathbb{Z}/7\mathbb{Z})^*$, et que l'on connait explicitement :

$$\tilde{\phi}(\tilde{0}) = \overline{1}, \tilde{\phi}(\tilde{1}) = \overline{3}, \tilde{\phi}(\tilde{2}) = \overline{2}, \tilde{\phi}(\tilde{3}) = \overline{6}, \tilde{\phi}(\tilde{4}) = \overline{4}, \tilde{\phi}(\tilde{5}) = \overline{5}.$$

Ici on a noté $\tilde{.}$ les classes modulo 6 et $\bar{.}$ les classes modulo 7. On demandait dans l'énoncé le morphisme dans l'autre sens mais il est maintenant facile d'inverser.

Exercice 2 (*Le groupe diédral D_n*)

Corrigé rapide, on trouvera plus d'infos dans le livre de Calais.

1. La stratégie la plus courte ici est de montrer que $O(2)$ est un sous-groupe d'un groupe déjà connu (cf cours) : $GL(2,\mathbb{R})$. Il suffit donc de vérifier que $O(2)$ est non vide (c'est clair car il contient I_2), et que si $A, B \in O(2)$, alors $AB \in O(2)$ et $A^{-1} \in O(2)$. Le premier point s'obtient en calculant ${}^t(AB)AB = {}^t B\,{}^t AAB = {}^t BB = I_2$. Le deuxième est un peu plus délicat puisque l'on doit montrer que ${}^t(A^{-1})A^{-1} = I_2$. Il y a plusieurs manières de faire celà. Déjà comme ${}^t AA = I_2$, on sait que $A^{-1} = {}^t A$. Ainsi ${}^t(A^{-1})A^{-1} = {}^t({}^t A)A^{-1} = AA^{-1} = I_2$, ce qui conclut.
Mais ce n'est pas la stratégie adoptée dans nombre de copies : on peut aussi montrer directement que c'est un groupe ; l'associativité est juste l'associativité du produit matriciel ; l'élément neutre est I_2, et beaucoup pensent à vérifier que la loi est bien interne, en posant le calcul ci-dessus. Par contre pour l'existence d'un inverse, tous se contentent de montrer que la matrice $A \in O(2)$ est bien un matrice inversible, sans se préoccuper de savoir si l'inverse est bien une matrice dans $O(2)$, ce qui est une erreur assez subtile mais une erreur quand même ! ; le montrer revient à faire comme ci-dessus également. D_n est défini comme les $f \in O(2)$ tels que $f(\mathcal{P}_n) = \mathcal{P}_n$. Soient $f, g \in D_n$, alors
$$fg^{-1}(\mathcal{P}_n) = fg^{-1}(g(\mathcal{P}_n)) = f(\mathcal{P}_n) = \mathcal{P}_n,$$
ce qui montre que D_n est un sous-groupe.
2. Tout ceci est très géométrique : ρ envoie A_i sur A_{i+A}, sauf A_n qui est envoyé sur A_1. Comme ρ^k est une rotation d'angle $2k\pi/n$, il est clair que ρ est d'ordre n. Sa matrice est $\begin{bmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{bmatrix}$, où $\theta = 2\pi/n$.
3. Il faut bien comprendre que lorsqu'on demande de montrer que quelquechose est bien défini, c'est probablement qu'il y a un soucis quelque part... Ici le soucis est que l'on associe à une classe $\overline{k}$ un itéré k fois, k étant un représentant de la classe en question. Pour ce faire il faut vérifier que ça ne dépend pas du représentant choisi, ce qui découle du fait que ρ est d'ordre n.
4. La symétrie s est d'ordre 2, de matrice $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
5. Géométriquement, ce qui se passe est qu'une isométrie linéaire M préservant le polygône soit conserve l'ordre trigonométrique des sommets (auquel cas c'est simplement une rotation d'angle multiple de $2\pi/n$, et donc un élément de Γ_n), soit elle renverse cet ordre et alors sM préserve l'ordre trigonométrique, et est donc dans Γ_n.
6. Tout élément de D_n est donc soit dans Γ_n, soit dans $s\Gamma_n$, ce qui montre que D_n/Γ_n est de cardinal 2. D_n est donc d'ordre $2n$. Une interprétation est que Γ_n est constitué des isométries directes, càd les rotations, tandis que les autres sont les isométries indirectes, càd les symétries axiales.
7. Le calcul matriciel explicite suffit ici à voir que $s\rho s \neq s^2\rho$.