Corrigé du DL n° 4.

Problème 1

Partie 1

1. Calculs laissés au lecteur.
2. 0 pour $\oplus$ et 1 pour $\otimes$.
3. Soit $a \in \mathbb{Z}/n\mathbb{Z}$. On a $(n-a)+a = n \equiv 0 \mod n$, donc $\boxed{(n-a) \oplus a = 0}$, donc, comme $\oplus$ est commutative et $n-a \in \mathbb{Z}/n\mathbb{Z}$, $\boxed{\text{l'opposé de } a \text{ est } n-a}$.
4. Les lois $\oplus$ et $\otimes$ sont des lci associatives, commutatives sur $\mathbb{Z}/n\mathbb{Z}$, et $\otimes$ est distributive sur $\oplus$. Elles admettent chacune un élément neutre, et tout élément admet un symétrique pour $\oplus$: c'est un anneau commutatif.
5. Soit $a \in \mathbb{Z}/n\mathbb{Z}$, $a \neq 0$.
   — L'élément neutre de $\otimes$ est 1, et $\otimes$ est commutative, donc par définition, a est inversible si et seulement s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \otimes b = 1$, ce qui par définition signifie $ab \equiv 1 \mod n$.
   — Supposons a inversible. Il existe donc $b\mathbb{Z}/n\mathbb{Z}$ tel que $ab \equiv 1 \mod n$, donc il existe $\ell \in \mathbb{Z}$ tel que $ab - \ell n = 1$. Par le théorème de Bézout, $a \wedge n = 1$.
   — Réciproquement, si $a \wedge n = 1$, la relation de Bézout nous donne l'existence de $u, v \in \mathbb{Z}$ tels que $au + nv = 1$, donc $au \equiv 1 \mod n$. Soit alors b le reste de la division de u par n. Alors $b \in \mathbb{Z}/n\mathbb{Z}$, et $b \equiv u \mod n$, donc par produit de congruences entières, $ab \equiv au \mod n$, donc $ab \equiv 1 \mod n$, et a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.
6. On sait que $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif. C'est donc un corps si et seulement si tout élément différent de 0 est inversible, donc par 1(b), si et seulement si tout $a \in [\![1, n-1]\!]$ est premier avec n, donc si et seulement si n est premier.
7. Supposons n non premier. Il existe donc $a, b \in [\![2, n-1]\!]$ tels que $ab = n$, donc $a, b \in \mathbb{Z}/n\mathbb{Z}$, $a, b \neq 0$, et $a \otimes b = 0$: a et b sont des diviseurs de 0, et $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Partie 3 : carrés dans $\mathbb{Z}/n\mathbb{Z}$

1. Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \mod p$. On en déduit, comme n est premier, qui si $a \in (\mathbb{Z}/n\mathbb{Z})^*$, alors $a^n = a$ dans $\mathbb{Z}/n\mathbb{Z}$ (petit théorème de Fermat). Mais a est inversible, donc on peut simplifier par a la relation précédente, et $a^{n-1} = 1$.
2. — Soient $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$. Alors

$$a^2 = b^2 \iff a^2 - b^2 = 0 \iff (a-b)(a+b) = 0 \iff a - b = 0 \text{ ou } a + b = 0,$$

   où la dernière équivalence provient du fait que n est premier, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc n'a pas de diviseur de 0.
   — On en déduit que b^2 admet comme antécédents b et $\ominus b (= n - b)$. Mais $b \neq n - b$ car n est impair, donc b^2 admet exactement deux antécédents.

— Comme n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps et $(\mathbb{Z}/n\mathbb{Z})^* = [\![1, n-1]\!]$, donc $(\mathbb{Z}/n\mathbb{Z})^*$ a $n-1$ éléments. D'après 2(b), pour tout $a \in [\![1, n-1]\!]$, a et $n-a$ ont le même carré, et si $b \notin \{a, n-a\}$, $a^2 \neq b^2$. Il y a donc $\frac{n-1}{2}$ carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$. Mais $0^2 = 0$, donc il y a $\frac{n-1}{2} + 1 = \frac{n+1}{2}$ carrés dans $\mathbb{Z}/n\mathbb{Z}$.

3. — Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Supposons que a soit un carré modulo n. Il existe donc $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a = b^2$ dans $\mathbb{Z}/n\mathbb{Z}$.On en déduit que $a^{\frac{n-1}{2}} = b^{n-1} = 1$ d'après la question 1.
   — On en déduit que les $\frac{n-1}{2}$ carrés de $(\mathbb{Z}/n\mathbb{Z})^*$ sont solutions de l'équation $t^{\frac{n-1}{2}} = 1$ (d'inconnue $t \in \mathbb{Z}/n\mathbb{Z}$), qui a au plus $\frac{n-1}{2}$ solutions, qui sont donc les carrés de $(\mathbb{Z}/n\mathbb{Z})^*$. Donc si $a^{\frac{n-1}{2}} = 1$, a est un carré modulo n.
4. -1 est un carré modulo n s'il existe $x \in \mathbb{Z}$ tel que $-1 \equiv x^2 \mod n$. On utilise la question 3 : $(-1)^{\frac{n-1}{2}} \equiv 1 \mod n \iff \frac{n-1}{2} \equiv 0 \mod 2 \iff n-1 \equiv 0 \mod 4$.

Problème 2

Partie 1

1. Montrons que $G \cap \mathbb{R}_+^* \neq \emptyset$. Comme G n'est pas réduit à 0, il existe $x \neq 0$ dans G. Si $x > 0$, alors $x \in G \cap \mathbb{R}_+^*$. Sinon, $-x \in G$ puisque G est un sous-groupe de $(\mathbb{R}, +)$. Or, $-x > 0$ donc $-x \in G \cap \mathbb{R}_+^*$ qui est un ensemble non vide. Comme il est minoré par 0, il admet une borne inférieure $a \geqslant 0$.
2. (a) — Comme $a > 0$, on a $2a > a$. On en déduit que $2a$ n'est pas un minorant de $G \cap \mathbb{R}_+^*$ (car a est le plus grand des minorants), donc qu'il existe $x \in G \cap \mathbb{R}_+^*$ tel que $x < 2a$.
   — Comme a est un minorant de $G \cap \mathbb{R}_+^*$, on a $a \leqslant x$. Mais on a supposé que $a \notin G$, donc $a \neq x$, et $a < x$.
   — Comme $a < x$, x n'est pas un minorant de $G \cap \mathbb{R}_+^*$: il existe donc $y \in G \cap \mathbb{R}_+^*$ tel que $y < x$, et de même, $a < y$.
   — Par définition de y, on a $y < x$, donc $x - y > 0$. Mais on a $a < y < x < 2a$, donc $x - y < 2a - a = a$.
   — Comme $y \in G$ et que G est un sous-groupe de $(\mathbb{R}, +)$, on a $-y \in G$. Mais $x \in G$, donc (sous-groupe de $(\mathbb{R}, +)$), $x - y = x + (-y) \in G$. Or, $x - y > 0$, donc $x - y \in G \cap \mathbb{R}_+^*$. Par définition de a, on a donc $a \leqslant x - y$. Or, $x - y < a$: contradiction. On en déduit que l'hypothèse $a \notin G$ est absurde, donc que $\boxed{a \in G}$.

   (b) — Comme $a \in G$, on montre facilement que $a\mathbb{Z} \subset G$.
   — Réciproquement soit $x \in G$, $x > 0$. Soit $p = \left\lfloor \frac{x}{a} \right\rfloor \in \mathbb{N}$. Par définition de p, on a $p \leqslant \dfrac{x}{a} < p + 1$. Or, $a > 0$, donc $ap \leqslant x < ap + a$ et donc $0 \leqslant x - ap < a$. Comme $a \in G$, et $p \in \mathbb{Z}$, on a $ap \in G$. Or, $x \in G$ par définition, donc $\boxed{x - ap \in G}$ car G est un sous-groupe de $(\mathbb{R}, +)$. Or, $x - ap < a$, donc par définition de a, $x - ap = 0$, *i.e.* $x = ap$, et par stabilité par passage à l'opposé, on a $G \subset a\mathbb{Z}$.
3. (a) Comme $z - y > 0$ et $0 = \inf(G \cap \mathbb{R}_+^*)$, $z - y$ n'est pas un minorant de $G \cap \mathbb{R}_+^*$, donc il existe $x \in G \cap \mathbb{R}_+^*$ tel que $0 < x < z - y$.

   (b) Soit $n = \left\lfloor \dfrac{y}{x} \right\rfloor + 1 \in \mathbb{Z}$. On a donc
   $$n - 1 \leqslant \frac{y}{x} < n.$$
   Or, $x > 0$, donc $nx - x \leqslant y < nx$ puisque $x > 0$. Mais $x < z - y$, donc
   $$nx = (n-1)x + x < (n-1)x + (z - y) \leqslant y + (z - y) = z,$$
   et donc $y < nx < z$. Or, $nx \in G$ puisque G est un sous-groupe de $(\mathbb{R}, +)$, donc pour tous $y, z \in \mathbb{R}$ avec $y < z$, il existe $x' \in G$ tel que $y < x' < z$: G est dense dans $\mathbb{R}$.

Partie 2

1. On a $0 = 0 + 0.\omega \in G_\omega$. De plus, si $a, a', b, b' \in \mathbb{Z}$, on a
$$(a + b\omega) + (a' + b'\omega) = (a + a') + (b + b')\omega \in G_\omega \quad \text{et} \quad -(a + b\omega) = -a - b\omega \in G_\omega$$
puisque $\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$, donc G_ω est un sous-groupe de $(\mathbb{R}, +)$.
2. — Soient $u, v \in \mathbb{Z}$ tels que $up + vq = 1$. On a alors
$$\frac{1}{q} = \frac{up + vq}{q} = v + u\frac{p}{q} = v + u\omega \in G_\omega.$$
Comme $\frac{1}{q}$ est un élément du sous-groupe G_ω de $\mathbb{R}$, pour tout $n \in \mathbb{Z}$, $\frac{n}{q} \in G_\omega$, (*cf* partie AI) *i.e.* $\frac{1}{q}\mathbb{Z} \subset G_\omega$.
— Réciproquement, Soient $a, b \in \mathbb{Z}$. Alors
$$a + b\omega = a + b\frac{p}{q} = \frac{aq + bp}{q} \in \frac{1}{q}\mathbb{Z},$$
car $aq + bp \in \mathbb{Z}$. Donc $G_\omega = \frac{1}{q}\mathbb{Z}$.
3. On raisonne par l'absurde. D'après la partie 1, comme $G \neq \{0\}$ et que G_ω n'est pas dense dans $\mathbb{R}$, il existe $\alpha \in \mathbb{R}_+^*$ tel que $G_\omega = \alpha\mathbb{Z}$. Comme $\omega = 0 + 1 \times \omega$, on a $\omega \in G_\omega$: il existe donc $n \in \mathbb{Z}$ tel que $\omega = n\alpha$. Or, $\omega \neq 0$ (car $\omega \notin \mathbb{Q}$), donc $\alpha = \frac{\omega}{n}$. Mais, $\omega \notin \mathbb{Q}$, et $n \in \mathbb{Z}$, donc $\frac{\omega}{n} \notin \mathbb{Q}$, *i.e.* $\boxed{\alpha \notin \mathbb{Q}}$.

Or, $\boxed{1 \in G_\omega}$ puisque $1 = 1 + 0 \times \omega$. Il existe donc $n \in \mathbb{Z}$ tel que $1 = n\alpha$. Comme $1 \neq 0$, on a $n \neq 0$, donc $\alpha = \frac{1}{n} \in \mathbb{Q}$: contradiction : $\boxed{G_\omega \text{ est dense dans } \mathbb{R}}$.

Partie 3

1. Lorsqu'on déplie une fois le billard horizontalement vers la droite, l'abscisse de l'image est $2\ell - x_0$. Un nouveau dépliage horizontal vers la droite donne comme abscisse $2\ell + x_0$, l'ordonnée ne changeant pas. Donc si $a > 0$, $2a$ dépliages vers la droite donnent comme abscisse $2a\ell + x_0$, et de même pour $a <$ en dépliant vers la gauche.

On fait de même pour les dépliages verticaux.
2. Le repère étant orthonormal, on a
$$\mathrm{d}(X_{ab}, D) = \frac{|y_0 + 2bL - p(x_0 + 2a\ell) - m|}{\sqrt{1 + p^2}} = \boxed{\frac{|y_0 - px_0 - m - 2ap\ell + 2bL|}{\sqrt{1 + p^2}}}.$$
3. On a pour $a, b \in \mathbb{Z}$, $2bL + 2ap\ell = 2L\left(b + a\frac{p\ell}{L}\right)$, donc $\boxed{G = 2LG_\omega}$, où $\boxed{\omega = \frac{p\ell}{L}}$. Cela prouve en particulier que G est un sous-groupe de $\mathbb{R}$.
4. Supposons $\omega \notin \mathbb{Q}$. Alors, G_ω est dense dans $\mathbb{R}$. En posant $t = \frac{y_0 - px_0 - m}{2L} \in \mathbb{R}$, il existe $a, b \in \mathbb{Z}$ tels que $|t - (a + b\omega)| < \frac{\varepsilon\sqrt{1 + p^2}}{2L}$ (car $\varepsilon\sqrt{1 + p^2}/(2L) > 0$). On en déduit que
$$|y_0 - px_0 - m - 2La - 2bp\ell| < \varepsilon\sqrt{1 + p^2}.$$
En posant $a' = b$ et $b' = -a$, on voit que $\mathrm{d}(X_{a'b'}, D) < \varepsilon$: on en déduit que si $\boxed{\frac{p\ell}{L} \text{ est irrationnel}}$, alors la trajectoire est dense.