Solution du petit problème: Groupes $\mathbb{Z}/n\mathbb{Z}$ et applications

Partie I: Etude des sous groupes de $(\mathbb{Z}, +)$

1. K étant un sous-groupe non réduit à $\{0\}$, il existe $k \in K$ tel que $k \neq 0$. Comme K est un sous-groupe de $(\mathbb{Z}, +)$ $-k \in K$ d'où nous pouvons supposer que $k > 0$ (quitte à remplacer k par $-k$). Aussi, $K \cap \mathbb{N}^*$ est-il un ensemble non vide: puisque c'est un sous-ensemble de $\mathbb{N}$, il admet un plus petit élément: soit donc n celui-ci.

2. Nous allons procéder par double inclusion (égalité d'ensembles):
   Si $i \in \mathbb{N}$, alors $i \times n = \underbrace{n + n + \ldots + n}_{i \ fois} \in K$ puisque K est stable par $+$. En remarquant que $-i \times n \in K$ (sous-groupe étant stable par passage au symétrique), nous en déduisons que $n\mathbb{Z} \subset K$.
   Réciproquement, soit $k \in K$. Effectuons la division euclidienne de k par n (remarquons que n est non nul puisque $n \in K \cap \mathbb{N}^*$). Il existe donc un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $k = qn + r$ avec $0 \leqslant r < n$. Donc $r = k - qn$: comme $k \in K$ et $n \in K$, nous en déduisons que $r \in K$. Si $r \neq 0$, alors $r \in K \cap \mathbb{N}^*$ et $r < n$ ce qui contredit la minimalité de n. Aussi, $r = 0$ et donc $k = qn \in n\mathbb{Z}$. On en déduit donc l'inclusion réciproque.

3. Nous venons de démontrer que tout sous-groupe de $(\mathbb{Z}, +)$ différent de $\{0\}$ était de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$. Comme $\{0\}$ est un sous-groupe de $(\mathbb{Z}, +)$ pouvant s'écrire $0\mathbb{Z}$, nous en déduisons que tout les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Partie II: Construction du groupe $\mathbb{Z}/n\mathbb{Z}$

1. La relation $\mathcal{R}$ est bien symétrique, puisque $\forall x \in \mathbb{Z}$, x a même reste dans la division euclidienne par n que x (sic!). Aussi, $x\mathcal{R}x$.
   Supposons que $x\mathcal{R}y$: aussi, x a même reste dans la division euclidienne par n que y d'où .... $y\mathcal{R}x$.
   Enfin, supposons que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors x et y ont même reste dans la division euclidienne par n, tout comme y et z ... on en déduit alors que x et z ont même reste dans la division euclidienne par n et donc $x\mathcal{R}z$.
   La relation $\mathcal{R}$ est donc bien une relation d'équivalence sur $\mathbb{Z}$.

2. Supposons que $x\mathcal{R}y$. Aussi, x et y ont même reste dans la division euclidienne par n. Ainsi, il existe $0 \leqslant r < n$ et $(q_1, q_2) \in \mathbb{Z}^2$ tels que $x = q_1 n + r$ et $y = q_2 n + r$. Il s'ensuit donc que $x - y = q_1 n - q_2 n = (q_1 - q_2)n \in n\mathbb{Z}$.
   Réciproquement, si $n|x-y$, alors soient (q_1, r_1) et (q_2, r_2) les couples quotient / reste de la division euclidienne de, respectivement, x et y par n. Aussi, $x = q_1 n + r_1$ et $y = q_2 n + r_2$. Nous avons alors $x - y = (q_1 - q_2)n + (r_1 - r_2)$. Comme $n|x-y$ (par hypothèse) et $n|(q_1 - q_2)n$, nous en déduisons que $n|r_1 - r_2$. Or, des encadrements $0 \leqslant r_1 < n$ et $0 \leqslant r_2 < n$, nous déduisons que $-n < r_1 - r_2 < n$. Le seul entier multiple de n compris strictement entre $-n$ et n étant 0, nous en déduisons que $r_1 - r_2 = 0$, soit $r_1 = r_2$. Aussi, $x\mathcal{R}y$.

3. (a) Nous savons que $x \equiv y \mod n$, c'est-à-dire que $n|x - y$. De même, $z \equiv t \mod n$ donc $n|z - t$. Il s'ensuit donc qu'il existe $k, k' \in \mathbb{Z}$ tels que $x - y = kn$ et $z - t = k'n$. En sommant, nous obtenons que $x + z - (y + t) = n(k + k')$ soit $n|(x + z) - (y + t)$ d'où $x + z \equiv y + t \mod n$.
   (b) Reprenons les notations de la question précédente. Nous avons alors $xz - yt = x(z - t) + xt - yt = x(z - t) + t(x - y)$. Comme $n|z - t$ et $n|x - y$, nous en déduisons que $n|xz - yt$ d'où $xz \equiv yt \mod n$.

4. Nous savons que $x\mathcal{R}y$ si et seulement si $n|x - y$ donc $y \in \overline{x}$ si et seulement si $x - y \in n\mathbb{Z}$, ou encore $y - x \in n\mathbb{Z}$, d'où $y \in x + n\mathbb{Z}$.
   L'inclusion réciproque est évidente.

5. (a) Soient $x, x' \in \mathbb{Z}$ tels que $\overline{x} = \overline{x'}$ et $y, y' \in \mathbb{Z}$ tels que $\overline{y} = \overline{y'}$. Nous devons montrer que $\overline{x + y} = \overline{x' + y'}$, ce qui résulte de la question **3.a**. En effet, $\overline{x} = \overline{x'}$ si et seulement si $x \equiv x' \mod n$.

(b) Soient $\overline{x}$, $\overline{y}$ et $\overline{z}$ trois éléments de $\mathbb{Z}/n\mathbb{Z}$. Nous avons alors

$$(\overline{x}+\overline{y})+\overline{z}=\overline{x+y}+\overline{z}=\overline{(x+y)+z}.$$

Par associativité de l'addition dans $\mathbb{Z}$, nous en déduisons que$(x+y)+z=x+(y+z)$ d'où il s'ensuit que

$$(\overline{x}+\overline{y})+\overline{z}=\overline{x+(y+z)}=\overline{x}+\overline{y+z}=\overline{x}+(\overline{y}+\overline{z})$$

Aussi, la loi somme sur $\mathbb{Z}/n\mathbb{Z}$ est bien associative.
Remaquons que l'associativité de cette loi est liée à l'associativité de la loi $+$ de $\mathbb{Z}$. On démontre de même que la somme dans $\mathbb{Z}/n\mathbb{Z}$ est commutative car la somme dans $\mathbb{Z}$ l'est.

(c) Comme $\overline{x}+\overline{y}=\overline{x+y}$, nous en déduisons que $\overline{0}$ est élément neutre de $\mathbb{Z}/n\mathbb{Z}$.
0 *est évidemment l'élément neutre de* $(\mathbb{Z},+)$*, mais notez que* $\overline{0}=n\mathbb{Z}$

(d) Nous remarquons que $\overline{x}+\overline{-x}=\overline{x+(-x)}=\overline{0}$ d'où l'inverse de $\overline{x}$ est $\overline{-x}$.
Remarquons que $\overline{-x}$ *a un sens (la classe de* $-x$*), donc on peut écrire* $-\overline{x}=\overline{-x}$*, mais que la loi de soustration n'existe par (non associative). Aussi, lorsque l'on écrit (même dans* $\mathbb{Z}$*)* $a-b$*, il faut comprendre* $a+(-b)$*. Notez aussi que le terme inverse est plutôt malheureux ici: on préfère opposé, ou symétrique (terme générique), car on réserve le terme inverse à une notation multiplicative*

(e) On a vérifié tous les conditions ... donc $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien.
Notez que l'on ne peut pas ici montrer que c'est un sous-groupe de quelqu'un, car il n'est a priori pas contenu dans un groupe connu!

Partie III: Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

1. Soient $x,y\in\mathbb{Z}$. Nous avons $\pi(x+y)=\overline{x+y}=\overline{x}+\overline{y}=\pi(x)+\pi(y)$. Donc π est bien un morphisme de groupes. Son noyau est $n\mathbb{Z}$ (puisque $\overline{0}=n\mathbb{Z}$). Enfin, elle est clairement surjective puisque si $\overline{x}\in\mathbb{Z}/n\mathbb{Z}$, alors $\pi(x)=\overline{x}$.

2. Montrons donc que l'image réciproque d'un sous-groupe par un morphisme de groupes est un sous-groupe (du groupe du départ). Déjà, $0\in K=\pi^{-1}(H)$ puisque $\pi(0)=\overline{0}\in H$ (en effet, H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ donc contient $\overline{0}$ l'élément neutre de $\mathbb{Z}/n\mathbb{Z}$).
Soit $x\in\pi^{-1}(H)$. Aussi, $\pi(x)=\overline{x}\in H$. Comme H est un sous-groupe, il est stable par passage au symétrique, d'où $\overline{-x}\in H$ et donc $-x\in\pi^{-1}(H)$.
Enfin, soit $x,y\in\pi^{-1}(H)$. Alors $\overline{x}\in H$ et $\overline{y}\in H$ donc comme H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$, il est stable par somme, et donc $\overline{x}+\overline{y}\in H$. Comme $\overline{x}+\overline{y}=\overline{x+y}$, nous en déduisons que $x+y\in\pi^{-1}(H)$ d'où $K=\pi^{-1}(H)$ est stable par loi interne.
Il s'ensuit donc que K est un sous-groupe de $(\mathbb{Z},+)$.

3. Nous savons par la question **I.3** que tous les sous-groupes de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$: aussi, notons $K=k\mathbb{Z}$ *(on évite d'utiliser la lettre* n *qui est réservée à* $\mathbb{Z}/n\mathbb{Z}$*).* On a donc $H=\pi(k\mathbb{Z})=<\overline{k}>$.

4. (a) Posons donc $Pgcd(x,n)=p$ et montrons que $<\overline{x}>=<\overline{p}>$. Puisque c'est une égalité de deux ensembles, nous allons procéder par double inclusion. Comme $<\overline{x}>$ est engendré par $\overline{x}$, il suffit de montrer que $\overline{x}\in<\overline{p}>$ pour prouver que $<\overline{x}>\subset<\overline{p}>$. p étant le $Pgcd$ de x et n, il existe deux entiers k_x et k_n tels que $x=k_xp$ et $n=k_np$.

$$\overline{x}=\overline{k_xp}=\underbrace{\overline{p}+\overline{p}+\ldots+\overline{p}}_{k_x\quad fois}=k_x\overline{p}\in<\overline{p}>$$

Reste donc à prouver l'inclusion réciproque. Nous savons, d'après l'identité de Bezout, qu'il existe u et v deux entiers tels que $ux+vn=p$, d'où en passant aux classes d'équivalences modulo n (ie. en composant par l'application π) nous en déduisons que $\overline{ux+vn}=\overline{p}$ soit $u\overline{x}=\overline{p}$ (puisque $\overline{n}=\overline{0}$). Il s'ensuit donc que $\overline{p}\in<\overline{n}>$ et par suite $<\overline{p}>\subset<\overline{x}>$.

(b) Rappelons que l'ordre d'un élément est défini par le cardinal du sous-groupe qu'il engendre. Aussi, $o(\overline{x}) = Card(< \overline{x} >)$). D'après l'égalité précédente, nous avons $o(\overline{x}) = o(\overline{p})$.
$o(\overline{p})$ est alors le plus petit entier strictement positif pour lequel $m\overline{p} = \underbrace{\overline{p} + \overline{p} + \ldots + \overline{p}}_{m \ \ fois} = \overline{0}$. Or, $0 < p < n$ d'où $o(\overline{p}) = n/p$ puisque $\frac{n}{p} \times p = n$.