Algèbre et Arithmétique 3
FEUILLE DE TD No 5

Exercice 2

1. Puisque $\bar{2}+\bar{2}+\bar{2}+\bar{2}+\bar{2} = \bar{10} = \bar{0}$, l'ordre de 2 est un diviseur de 5. Par ailleurs, pour tout k compris entre 1 et 4, une somme de k termes égaux à $\bar{2}$ n'est pas nulle dans $\mathbb{Z}/10\mathbb{Z}$. Donc l'ordre de $\bar{2}$ est exactement 5 (on aurait pu aussi dire que les seuls diviseurs de 5 sont 1 et 5, mais puisque $\bar{2} \neq \bar{0}$, l'ordre de $\bar{2}$ ne peut pas être 1, donc c'est 5).

2. L'ensemble $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ est inclus dans $\mathbb{Z}/12\mathbb{Z}$, est stable par l'addition et par le passage à l'inverse, donc c'est un sous-groupe de $\mathbb{Z}/12\mathbb{Z}$. On aurait pu aussi remarquer que c'est l'image de $3\mathbb{Z}$ par le morphisme canonique de passage au quotient $\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$. Or $3\mathbb{Z}$ est un groupe et l'image d'un groupe par un morphisme est un groupe, donc $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ est un sous-groupe de $\mathbb{Z}/12\mathbb{Z}$.

3. Un sous-groupe d'ordre 6 de $\mathbb{Z}/12\mathbb{Z}$ doit contenir 6 éléments. Le sous-groupe $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ convient.

4. L'ordre d'un sous-groupe doit diviser l'ordre du groupe d'après le théorème de Lagrange. Donc les seuls ordres a priori possibles des sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont 1, 2, 3, 6. Or on vérifie qu'il existe bien des sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ pour chacun de ces ordres : $\{\bar{0}\}$ est un sous-groupe d'ordre 1, $\{\bar{0}, \bar{3}\}$ est un sous-groupe d'ordre 2, $\{\bar{0}, \bar{2}, \bar{4}\}$ est un sous-groupe d'ordre 3, $\mathbb{Z}/6\mathbb{Z}$ est un sous-groupe (de lui-même) d'ordre 6.

5.a) Le groupe G_d doit contenir d éléments. Soit $\bar{a}$ la classe de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$. L'ensemble $\{\bar{0}, \bar{a}, 2.\bar{a}, \ldots, (d-1).\bar{a}\}$ convient puisqu'il contient d éléments et est bien un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.

5.b) Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Alors, d'après le théorème de Lagrange, l'ordre de tout élément $\bar{x}$ de H divise d, donc $d.\bar{x} = \bar{0}$. Comptons le nombre d'éléments $\bar{y}$ de $\mathbb{Z}/n\mathbb{Z}$ qui vérifient $d.\bar{y} = \bar{0}$. Puisque $d.\bar{y} = \bar{0}$, il existe $k \in \mathbb{Z}$ tel que l'égalité suivante $dy = kn$ ait lieu dans $\mathbb{Z}$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $y = k\frac{n}{d}$. Dans $\mathbb{Z}/n\mathbb{Z}$, les éléments de la forme $k\frac{n}{d}$ sont exactement les éléments de G_d, il en existe donc d. Or le groupe H est censé contenir d éléments. Donc les éléments de H sont exactement ceux de G_d. Donc $H = G_d$.

5.c) On vient ainsi de démontrer que si d est un diviseur de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Remarque : on note parfois $a\mathbb{Z}/n\mathbb{Z}$ le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, où $a = \frac{n}{d}$.

Exercice 3

On cherche dans un premier temps les morphismes de groupes, puis dans un deuxième, les morphismes d'anneaux, à chaque fois de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. On note par une barre les entiers vus dans $\mathbb{Z}/10\mathbb{Z}$ et par un point les entiers vus dans $\mathbb{Z}/n\mathbb{Z}$ de sorte que $\bar{10} = \bar{0}$ et $\dot{n} = \dot{0}$. Enfin, la notation $4.\bar{2}$ est l'addition $\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8}$, tandis que $\bar{4}.\bar{2} = \bar{8}$ est la multiplication dans $\mathbb{Z}/10\mathbb{Z}$.

Trouver les morphismes de groupes de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$

Analyse. Soit ϕ un morphisme de groupes de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Alors $\phi(\bar{0}) = \dot{0}$. Par ailleurs, $10.\phi(\bar{1}) = \phi(10.\bar{0}) = \dot{0}$. Notons $\dot{a} = \phi(\bar{1})$. Puisque $10.\dot{a} = \dot{0}$, il existe un entier k tel que $10a = kn$ dans $\mathbb{Z}$. Donc a est un entier vérifiant $a = \frac{kn}{10}$.

Synthèse. Soit a un entier vérifiant $a = \frac{kn}{10}$. Alors il existe un morphisme ψ de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ donné par $\psi(\bar{\ell}) = \ell.\dot{a}$. Cela définit bien une application de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ car si $\bar{m} = \bar{\ell}$, alors $m - \ell \in 10\mathbb{Z}$, donc $\ell.a - m.a \in 10a\mathbb{Z}$, mais $10a = kn$, donc $\ell.a - m.a \in kn\mathbb{Z} \subset n\mathbb{Z}$, donc $\ell.\dot{a} = m.\dot{a}$ Par ailleurs, la définition $\psi(\bar{\ell}) = \ell.\dot{a}$ nous garantie qu'il s'agit bien d'un morphisme de groupes, le seul qui vérifie $\Psi(\bar{1}) = \dot{a}$.

Conclusion. La donnée d'un morphisme de groupes de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est équivalente à celle d'un entier a pouvant être mis sous la forme $\frac{kn}{10}$ où k est un entier, où $\dot{a}$ est l'image de $\bar{1}$ par ce morphisme.

Remarque. Lorsque n et 10 sont premiers entre eux, les entiers a convenables sont de la forme $k'n$ où $k' \in \mathbb{Z}$, donc $\dot{a} = \dot{0}$. Donc le seul morphisme de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ lorsque n et 10 sont premiers entre eux est le morphisme trivial. A l'inverse, lorsque 10 divise n, il existe 10 morphismes de groupes de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Par exemple, si $n = 30$, on peut choisir l'entier a dans $3\mathbb{Z}$, et chaque entier de $3\mathbb{Z}$ compris entre 0 et 27 fournit un morphisme de groupes différent. Dernier exemple, Lorsque $n = 4$, a doit être un entier vérifiant $\frac{kn}{10}$ qui est égal à $\frac{2k}{5}$. Donc a appartient à $2\mathbb{Z}$. Donc on a deux morphismes de groupes possibles : celui où $\dot{a} = \dot{0}$ (le morphisme trivial) et celui où $\dot{a} = \dot{2}$.

Trouver les morphismes d'anneaux de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$

Analyse. Un morphisme d'anneaux est un morphisme de groupes pour l'addition qui en plus doit être compatible avec la multiplication et doit préserver l'élément neutre de la multiplication. Donc si ϕ est un morphisme d'anneaux de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, il faut que $\phi(\bar{1}) = \dot{a}$ où a est un entier tel qu'il existe $k \in \mathbb{Z}$ tel que $a = \frac{kn}{10}$, et par ailleurs, il faut que $\dot{a} = \dot{1}$, autrement

dit, il existe un entier ℓ tel que $a = \ell n + 1$. Pour qu'un tel a existe, il faut donc vérifier l'équation $\ell n + 1 = \frac{kn}{10}$ d'inconnues k et ℓ. Cette équation est équivalente à :

$$(10\ell - k)n = -10. \tag{1}$$

Cette équation n'a de solutions que si $n \in \{1, 2, 5, 10\}$. On a vu que dans chaque cas, $\dot{a} = \dot{1}$. Jusque là, nous avons vérifier que ces conditions sur n et sur ϕ au travers de a étaient des **conditions nécessaires**. Nous allons vérifié qu'elles sont suffisantes.

Synthèse. Soit $n \in \{1, 2, 5, 10\}$ et soit ϕ une application de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ telle que $\phi(\bar{1}) = \dot{a} = \dot{1}$. Par ailleurs, on impose aussi que $\phi(x.\bar{1}) = x\phi(\bar{1})$, autrement dit que $\phi(\bar{x}) = \dot{x}$. Cela détermine complètement l'application ϕ pourvu qu'elle soit bien définie. Or si $\bar{y} = \bar{x}$, on a $x - y \in 10\mathbb{Z}$, donc en particulier $x - y \in n\mathbb{Z}$ puisque n divise 10, donc $\dot{y} = \dot{x}$. Ainsi l'application ϕ est bien définie. C'est bien un morphisme de groupes : on l'a défini pour cela. Ce morphisme envoie bien $\bar{1}$ sur $\dot{1}$. Il reste juste à vérifier que pour tous $\bar{y}$, $\bar{x}$, on a $\phi(\bar{y}.\bar{x}) = \phi(\bar{y}).\phi(\bar{x})$. Or en notant z le produit xy dans $\mathbb{Z}$, on a $\phi(\bar{y}.\bar{x}) = \phi(\overline{xy}) = \phi(\bar{z}) = \dot{z}$ et par ailleurs, $\phi(\bar{y}).\phi(\bar{x}) = \dot{y}.\dot{x} = \dot{z}$. Donc il s'agit bien d'un morphisme d'anneaux.

Conclusion. On a ainsi exactement quatre morphisme d'anneaux de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ lorsque n parcourt $\mathbb{N}^*$: un pour chaque entier n de $\{1, 2, 5, 10\}$. De plus, ces morphismes sont donnés par la formule $\phi(\bar{x}) = \dot{x}$.