TD n°5. Théorèmes de factorisation, groupes cycliques

Exercice 1. Soit n et m deux entiers tels que m divise n.

a) On considère l'homorphisme $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})(m\mathbb{Z}/n\mathbb{Z})$. Montrer que cet homomorphisme est surjectif. Quel est son noyau ? En déduire qu'il y a un isomorphisme naturel $\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$.

b) Rappeler comment sont caractérisés les sous-groupes d'un groupe quotient. En déduire qu'il y a une bijection entre les diviseurs positifs de n et les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

c) Quels sont les entiers m tels que $cl(m) \in \mathbb{Z}/n\mathbb{Z}$ engendre $\mathbb{Z}/n\mathbb{Z}$?

Exercice 2. Soit p un nombre premier. On appelle p-groupe un groupe dans lequel l'ordre de tout élément est une puissance de p. Soit $(A, +)$ un p-groupe abélien fini.

1) Soit k un entier non multiple de p, et a un élément de A. Montrer que a et ka ont même ordre.

2a) A partir de maintenant, on fixe $a_0 \in A$ d'ordre maximal (parmi tous les éléments de A). On sait que l'ordre de a_0 est de la forme p^{n_0}. Soit A' le quotient $A/ < a_0 >$, et

$$\pi : A \longrightarrow A'$$

le morphisme quotient. Justifier que A' est encore un p-groupe abélien fini.

2b) Soit $a' \in A'$, d'ordre $p^{n'}$. On veut montrer qu'il existe $a \in A$, de même ordre que a', tel que $\pi(a) = a'$. Soit $b \in A$ arbitraire tel que $\pi(b) = a'$. Expliquer pourquoi il existe un entier n, et un entier k non multiple de p, tels que $p^{n'}b = p^n k a_0$.

2c) Si $p^{n'}b = 0$, on prend $a = b$ et c'est gagné. Sinon, montrer que $n \geq n'$.
Indication : Supposant $n < n'$, montrer que l'ordre de b est $n_0 + n' - n$. Pourquoi cela est-il absurde ?

2d) Montrer que $a := b - p^{n-n'} k a_0$ répond à la question posée en 2b).

3a) On se propose de démontrer qu'il existe des entiers positifs $n_1, ..., n_r$ tels que A est isomorphe au produit

$$\mathbb{Z}/p^{n_0}\mathbb{Z} \times \mathbb{Z}/p^{n_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z}.$$

On raisonne par récurrence sur le cardinal de A. Que se passe-t-il si ce cardinal est 1 ?

3b) Si le A n'est pas le groupe trivial, justifier que $|A'| < |A|$. Par récurrence, on peut donc supposer qu'il existe des entiers positifs $n_1, ..., n_r$ tels que

$$A' = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z}.$$

Pour $i = 1 \ldots r$, soit a'_i l'élément de A' dont les coordonnées sont toutes nulles, sauf la i-ième qui vaut $\overline{1}$. Justifier que, pour $i = 1 \ldots r$, il existe un élément a_i de A de même ordre que celui de a'_i, et tel que $\pi(a_i) = a'_i$.

3c) Montrer que le morphisme

$$\phi : \mathbb{Z}/p^{n_0}\mathbb{Z} \times \mathbb{Z}/p^{n_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \longrightarrow A,$$

$$e_i \mapsto a_i,$$

est bien défini et est un isomorphisme.

Exercice 3. Soit G un groupe et H un sous-groupe distingué de G.

a) Si K est un sous-groupe de G, quel est le noyau de l'application $K \to KH/H$? En déduire que $K/(K \cap H) \simeq KH/H$.

b) On suppose que H et G/H sont simples, c'est à dire qu'ils n'ont pas de sous-groupes distingués non triviaux.
Soit K un sous-groupe distingué de G différent de $\{e\}, H$ et G. En considérant le sous-groupe KH/H, montrer que $KH = G$.

c) Déduire des questions précédentes que $K \cap H = \{e\}$, puis que $K \simeq G/H$ et que $H \simeq G/K$

d) Montrer que $G \simeq (G/H) \times (G/K) \simeq K \times H$.

Exercice 4. a) Montrer que pour tout $n \in \mathbb{N}^*$, le groupe $\mathbb{Q}/\mathbb{Z}$ contient exactement un sous-groupe cyclique d'ordre n.

b) Soit $\alpha \in \mathbb{Q}/\mathbb{Z}$. Déterminer tous les sous-groupes cycliques de $\mathbb{Q}/\mathbb{Z}$ qui le contiennent.

c) Déterminer les homomorphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$.

d) Déterminer les homomorphismes de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$.