TD 3 – Groupes, anneaux, morphismes, etc.

Exercice 1. *Divers*

1. Quel est l'ordre de $[1]_n$ dans $(\mathbb{Z}/n\mathbb{Z},+)$? Et son ordre dans $(\mathbb{Z}/n\mathbb{Z}^\times,\times)$?
2. Calculer l'ordre de $[2]_7$ et de $[3]_7$ dans $\mathbb{Z}/7\mathbb{Z}^\times$. Lequel des deux est générateur ?
3. Soit $G=\mathbb{Z}/6\mathbb{Z}$ et $H=\{[0]_6,[3]_6\}$.
   - **i.** Montrer que H est un sous-groupe de G.
   - **ii.** Montrer que G/H est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.
4. Montrer que pour tout $n>1$, $n\mathbb{Z}$ est isomorphe à $\mathbb{Z}$.
5. Soit m et n premiers entre eux, et f la fonction de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, définie par $f([a]_n)=[ma]_n$. Montrer que f est un automorphisme.
6. Soit m et n deux entiers, $g=\text{PGCD}(m,n)$ et $h=\text{PPCM}(m,n)$ (défini par $h=mn/\text{PGCD}(m,n)$. Montrer que $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/g\mathbb{Z}\times\mathbb{Z}/h\mathbb{Z}$.

Exercice 2. *L'anneau $\mathbb{Z}[\sqrt{2}]$*

Soit $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2} : a,b\in\mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ un anneau.
2. On considère la fonction f de $\mathbb{Z}[\sqrt{2}]$ dans lui-même qui à $a+b\sqrt{2}$ associe $a-b\sqrt{2}$. Montrer que f est un automorphisme de $\mathbb{Z}[\sqrt{2}]$.
3. Pour $x\in\mathbb{Z}[\sqrt{2}]$, on pose $N(x)=x\cdot f(x)$. Montrer que N est un morphisme de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}$.
4. Montrer que x est inversible dans $\mathbb{Z}[\sqrt{2}]$ si et seulement si $N(x)=\pm1$. Donner des exemples d'éléments inversibles dans $\mathbb{Z}[\sqrt{2}]$.

Exercice 3. *Méthode de Newton*

Soit m et n deux entiers premiers entre eux, et u l'inverse de m modulo n. Soit $y\in\{0,\dots,m-1\}$ et $z\in\{0,\dots,n-1\}$. On pose

$$x=y+m\times(u(z-y)\bmod n).$$

1. Montrer que $x\in\{0,\dots,mn-1\}$.
2. Montrer que $x\equiv_m y$.
3. Montrer que $x\equiv_n z$.
4. En déduire que x est l'unique solution $<mn$ du système d'équations $x\equiv_m y$ et $x\equiv_n z$.
5. Résoudre le système $x\equiv_{19687} 18000$ et $x\equiv_{17} 13$.
6. Comment utiliser cette technique pour résoudre un système de plus de deux équations de congruence ?