DM Bonus – Compléments sur les groupes finis

1 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

On cherche à déterminer la structure du groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. On suppose connu[1] le caractère cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$ si p est un nombre premier.

1. Montrer que si p est un nombre premier et si $\alpha \geq 1$ est un entier naturel,
$$\left|(\mathbb{Z}/p^\alpha\mathbb{Z})^\times\right| = p^\alpha - p^{\alpha-1}.$$

1.1 Étude de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ pour $p \neq 2$ et $\alpha \geq 2$

Soient p un nombre premier impair et $\alpha \geq 2$ un entier naturel.

2. Montrer que pour tout $k \in \mathbb{N}^*$, $(1+p)^{p^k}$ s'écrit $1 + \lambda p^{k+1}$, avec $\lambda \wedge p = 1$.
3. En déduire que la classe de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^{\alpha-1}$.
4. Soit $x \in \mathbb{Z}$ dont la classe dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1$.
Montrer que la classe de x dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre un multiple de $p-1$.
5. En déduire l'existence de $y \in \mathbb{Z}$ dont la classe dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p-1$.
6. Montrer que la classe de $(1+p)y$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^\alpha - p^{\alpha-1}$.
En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

1.2 Étude de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$

Soit $\alpha \geq 3$ un entier naturel.

7. Montrer que $(\mathbb{Z}/2\mathbb{Z})^\times$ est réduit à un élément et que $(\mathbb{Z}/4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
8. Montrer que pour tout $k \in \mathbb{N}^*$, 5^{2^k} s'écrit $1 + \lambda 2^{k+2}$, avec λ un entier impair.
9. En déduire que l'ordre de la classe de 5 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est $2^{\alpha-2}$.
10. Montrer que l'application $\phi : \mathbb{U}_2 \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \to (\mathbb{Z}/2^\alpha\mathbb{Z})^\times, (\pm 1, \bar{k}) \mapsto \pm 5^k$ est bien définie et que c'est un isomorphisme de groupes.

[1] Ceci a été traité dans les notes de cours.

1.3 Quand $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

Soit $n \geq 2$ un entier, dont on note $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ la décomposition en facteurs premiers.

11. Montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est isomorphe à $\left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}\right)^\times$.

12. Soient $C_1, \ldots, C_m$ des groupes cycliques. Montrer que le produit $C_1 \times \cdots \times C_m$ est cyclique ssi les cardinaux $|C_1|$, ..., $|C_m|$ sont deux à deux premiers entre eux.

13. Déterminer les entiers n pour lesquels $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

2 Théorème de Cauchy

Soient G un groupe fini et p un diviseur premier de $|G|$. On cherche à montrer qu'il existe un élément x de G d'ordre p.

On note E l'ensemble des familles $(g_c)_{c\in\mathbb{Z}/p\mathbb{Z}}$ de G indexées par $\mathbb{Z}/p\mathbb{Z}$ et telles que $\prod_{k=0}^{p-1} g_{\overline{k}} = e_G$.

1. On définit une relation $\mathscr{R}$ sur E par :

$$(g_c)\,\mathscr{R}\,(g'_c) \iff \exists a \in \mathbb{Z}/p\mathbb{Z} : \forall c \in \mathbb{Z}/p\mathbb{Z}, g'_c = g_{a+c}.$$

   Montrer qu'il s'agit d'une relation d'équivalence sur E.

Si $(g_c) \in E$, on note $H_{(g_c)} = \left\{a \in \mathbb{Z}/p\mathbb{Z} \mid \forall c \in \mathbb{Z}/p\mathbb{Z}, g_{a+c} = g_c\right\}$.

2. Montrer que $H_{(g_c)}$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$.

3. En déduire l'alternative suivante :

   - Ou bien $H_{(g_c)} = \{\overline{0}\}$ et $\mathrm{cl}_{\mathscr{R}}\left((g_c)\right)$ est de cardinal p.
   - Ou bien $H_{(g_c)} = \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{cl}_{\mathscr{R}}\left((g_c)\right)$ est de cardinal 1.

4. En considérant la partition de E associée à $\mathscr{R}$, en déduire que le nombre de $\mathscr{R}$-classes d'équivalence de cardinal 1 est divisible par p.

5. En déduire que le nombre N d'éléments x de G d'ordre p vérifie $N \equiv -1\,[p]$.

   En particulier, il existe un élément d'ordre p dans G : c'est le théorème de Cauchy.