# THÉORÈME DE WEDDERBURN

On désigne par $\mathbb{Z}[X]$ l'ensemble des polynômes en l'indéterminée $X$ à coefficients entiers relatifs ; $\mathbb{Z}[X]$ est un anneau pour la somme et le produit des polynômes.
Toutefois, $Z$ n'étant pas un corps, les propriétés du cours ne s'appliquent pas à $\mathbb{Z}[X]$. En revanche, $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, avec $\mathbb{Q}$ qui lui est bien un corps.

## Partie I: Polynômes cyclotomiques

Soit $n \geqslant 1$. On note $V_n \subset \mathbb{U}_n$ l'ensemble des générateurs de $\mathbb{U}_n$ et on l'appelle aussi l'ensemble des racines primitives $n$-ième de l'unité. Et on définit le $n$-ième polynôme cyclotomique $\Phi_n$ par

$$\Phi_n = \prod_{\zeta \in V_n} (X - \zeta)$$

On note $\omega = e^{\frac{2i\pi}{n}}$, et pour tout $k \in [\![0, n-1]\!]$, $\omega_k = \omega^k$.

1. A quelle condition sur $k$, $\omega_k$ est-elle une racine primitive $n$-ième ?
2. Déterminer les racines primitives $n$-ièmes de l'unité pour $n = 2, 3, 4, 5, 6$.
3. Déterminer les coefficients de $\Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6$.
4. Déterminer $\deg \Phi_n$.
5. Montrer que pour tout $n \in \mathbb{N}^*$, $\quad X^n - 1 = \prod_{d|n} \Phi_d$.
6. Retrouver la valeur de la somme $\sum_{d|n} \varphi(d)$.
7. Soit $A, B \in \mathbb{Z}[X]$. Montrer que, si $B$ est unitaire, alors le quotient et le reste de la division euclidienne de $A$ par $B$ sont encore à coefficients entiers (donner un contre-exemple dans le cas où $B$ n'est pas unitaire).
8. En déduire que, pour tout $n \in \mathbb{N}^*$, $\Phi_n$ est à coefficients entiers.

## Partie II: Théorème de Wedderburn

Soit $(\mathbb{K}, +, \times)$ un anneau fini de cardinal $q \geqslant 3$ vérifiant $\mathbb{U}(\mathbb{K}) = \mathbb{K} \setminus \{0\}$. On se propose de montrer que $(\mathbb{K}, +, \times)$ est un corps, cela revient à démontrer que $(\mathbb{K}, +, \times)$ est commutatif.
Notons $Z = \{z \in \mathbb{K} \mid \forall x \in \mathbb{K},\ zx = xz\}$ le centre de $\mathbb{K}$. (On souhaite montrer que $Z = \mathbb{K}$).

9. Montrer que $Z$ est un sous-corps de $\mathbb{K}$ (forcément commutatif).
10. En déduire que $\mathbb{K}$ peut-être muni d'une structure d'espace vectoriel sur $Z$ ; et que donc si $p = \mathbf{Card}(Z)$, le cardinal de $K$ est de la forme $q = p^n$ avec $n \geqslant 1$. On souhaite montrer que $n = 1$.
11. Pour tout $a \in K$, notons $Z_a = \{g \in \mathbb{K} \mid ga = ag\}$ (le normalisateur de $a$).
    Expliquer que $Z_a$ est un sous-espace vectoriel de $\mathbb{K}$ et donc qu'il existe $d_a \geqslant 1$ tel que $\mathbf{Card}(Z_a) = p^{d_a}$.
    Par ailleurs ($\mathbb{K}$'.) est un groupe fini de cardinal $q - 1$. On définit une relation sur $\mathbb{K}^* = G$ :
    $$\forall (a, b) \in G^2,\ a \sim b \Longleftrightarrow \exists g \in G, b = gag^{-1}.$$
12. Montrer que $\sim$ est une relation d'équivalence sur $G$.
    Pour tout $a \in G$ on notera $\overline{a}$ la classe d'équivalence de $a$ dans $G$, et $H_a = \left\{g \in G \mid gag^{-1} = a\right\}$ (le stabilisateur de $a$). On notera $\widetilde{G}$ l'ensemble des classes d'équivalence.
13. Expliquer que $H_a = \mathbb{Z}_a^* = Z_a \setminus \{0\}$. En déduire $\mathbf{Card}(H_a)$.
14. Soit $a \in G$. Soit $b \in \widetilde{a}$ ; ainsi il existe $h \in G$ tel que $b = hah^{-1}$. $h$ étant ainsi fixé, montrer que pour tout $g \in G$, $gag^{-1} = b$ si et seulement si $g \in h.H_a$.
15. Montrer que $G = \bigcup_{b \in \widetilde{a}} \left\{g \in G \mid b = gag^{-1}\right\}$ et que cette union est disjointe. Déduire de la question précédente que chacune des parties de cette union a pour cardinal $\mathbf{Card}(H_a)$. En déduire que $\mathbf{Card}(H_a).\mathbf{Card}(\widetilde{a}) = \mathbf{Card}(G)$.
16. Dans le cas où $a \in Z^*$, donner $Z_a$, $H_a$ et $\widetilde{a}$ ?
17. Dans le cas général, comme $\mathbf{Card}(H_a)$ divise $\mathbf{Card}(G)$ en déduire que $d_a \mid n$ ; expliquer que si $a \notin Z^*$, $d_a \neq n$.

**Théorème de Wedderburn**

18. Expliquer que $\mathbf{Card}(G) = \sum_{\widetilde{a}\in\widetilde{G}} \mathbf{Card}(\widetilde{a}) = \mathbf{Card}(Z^*) + \sum_{\widetilde{a}\in\widetilde{G}, a\notin Z^*} \mathbf{Card}(\widetilde{a})$, et donc que :

$$p^n - 1 = p - 1 + \sum_{\widetilde{a}\in\widetilde{G}, a\notin Z^*} \frac{p^n - 1}{p^{d_a} - 1}$$

19. Par l'absurde si $n > 1$, en déduire que $\Phi_n(p) \mid (p-1)$. Expliquer que nécessairement $p = 2$ et que l'on aboutit à une contradiction.
20. Conclure.