Aix–Marseille Université 2018-2019

Mathématiques – M1

DEVOIR SURVEILLÉ N°2– ALGÈBRE ET GÉOMÉTRIE-2H

Exercice 1

Déterminer, dans $\mathbb{Q}[X]$, un polynôme annnulateur pour $\sqrt{3}+\sqrt[3]{2}$.

Exercice 2

Décrire le groupe des inversibles de $\mathbb{Z}/_{11\mathbb{Z}}$ et donner la liste des éléments d'ordre maximal.

Exercice 3

Pour tout $d \in \mathbb{N}^*$, on dit qu'une racine $d^{\text{ième}}$ de l'unité dans $\mathbb{C}$ est *primitive* si elle engrendre toutes les autres racines $d^{\text{ième}}$ par multiplication ; on note

$$\phi_d(X) := \prod_{\substack{\zeta\in\mathbb{C} \text{ racine } d^{\text{ème}} \\ \text{primitive de l'unité}}} (X-\zeta),$$

le $d^{\text{ième}}$ polynôme cyclotomique. On rappelle que $\phi_d(X) \in \mathbb{Z}[X]$ et que, pour tout $n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \phi_d(X)$.

Pour tout ensemble A contenant un élément noté 0, on notera $A^* := A \setminus \{0\}$.

Dans cet exercice, on ne suppose pas *a priori* qu'un corps est commutatif. Le but est de démontrer le théorème de Wedderburn, lequel affirme que tout corps fini est néanmoins commutatif. On considère donc un corps fini $\mathbb{F}$ et on suppose, par l'absurde, qu'il est non commutatif. On note $Z := \{x \in \mathbb{F} \mid \forall y \in \mathbb{F}, xy = yx\}$ le centre de $\mathbb{F}$ et $q := |Z|$.

1. (a) Montrer que Z est un sous-corps de $\mathbb{F}$ contenant au moins deux éléments.
   (b) Montrer que $\mathbb{F}$ est un Z–espace vectoriel.
   (c) En déduire que $|\mathbb{F}| = q^n$ avec $n \in \mathbb{N}^* \setminus \{1\}$.
2. On considère l'action de $\mathbb{F}^*$ sur lui-même par conjugaison.
   (a) Dans cette question, on fixe $x \in \mathbb{F}^*$ et on note $Z(x) := \{y \in \mathbb{F} \mid xy = yx\}$ le commutant de x.
      i. Montrer que $Z \subset Z(x)$ et en déduire que $|Z(x)| = q^{d_x}$ avec $d_x \in \mathbb{N}^*$.
      ii. Montrer que $\text{Stab}(x) \cup \{0\} = Z(x)$.
      iii. Montrer que $\text{Stab}(x)$ est un sous-groupe de $\mathbb{F}^*$ et en déduire que $q^{d_x} - 1$ divise $q^n - 1$.
      iv. Montrer que d_x divise n, avec $d_x = n$ si et seulement si $x \in Z^*$.
      v. On note $\omega(x)$ l'orbite de x. Montrer que $|\omega(x)| = \prod_{\substack{d \text{ divise } n \\ d \text{ ne divise pas } d_x}} \phi_d(q)$.
   (b) i. Montrer que $|\mathbb{F}^*| = |Z^*| + \sum_{\substack{\omega \text{ orbite} \\ |\omega|>1}} |\omega|$.
      ii. En déduire que $\phi_n(q)$ divise $q-1$.
3. (a) Soit $z \in \mathbb{C} \setminus \{1\}$ tel que $|z| = 1$. Montrer que $|q-z| > q-1 \geq 1$.
   (b) Conclure.