Théorème de Wedderburn

1) Soit $\mathrm{P} \subset \mathbf{M}_2(\mathbb{C})$ l'ensemble des matrices A antihermitiennes (${}^t\bar{\mathrm{A}} = -\mathrm{A}$) et de trace nulle, et soit $\mathbb{H}$ le sous-$\mathbb{R}$-espace vectoriel de $\mathbf{M}_2(\mathbb{C})$ engendré par P et la matrice unité $\mathbf{1}$. $\mathbb{H}$ est donc l'ensemble des matrices $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, avec $a, b \in \mathbb{C}$.

a) Soient $\mathrm{A}, \mathrm{B} \in \mathrm{P}$; montrer que $\mathrm{A}^2, \mathrm{B}^2$ puis $\mathrm{AB} + \mathrm{BA}$ sont dans $\mathbb{R}\mathbf{1}$ (appliquer le théorème de Cayley-Hamilton). En déduire que $\mathbb{H}$ est une sous-$\mathbb{R}$-algèbre de $\mathbf{M}_2(\mathbb{C})$.

b) Montrer que $\mathbb{H}$ est un corps ("corps des quaternions"), et admet une base (sur $\mathbb{R}$) formée de la matrice unité et des matrices

$$\mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad , \quad \mathbf{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad , \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

qui vérifient

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1} \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k} \ , \text{ etc.}$$

2) Soit K un corps fini. On se propose de prouver que K est commutatif ("théorème de Wedderburn").

a) On désigne par Z le centre de K, c'est-à-dire l'ensemble des éléments qui commutent avec tous les éléments de K. Montrer que Z est un corps (fini) commutatif.

b) On note q le cardinal de Z. Montrer que le cardinal de K est une puissance de q ; on le note q^n.

c) Soit $x \in \mathrm{K}$, et soit $\mathrm{Z}(x)$ l'ensemble des éléments de K qui commutent avec x. Montrer que $\mathrm{Z}(x)$ est un sous-corps de K qui contient Z. En déduire que l'ordre du groupe multiplicatif $\mathrm{Z}(x)^*$ est de la forme $q^d - 1$ et divise $q^n - 1$. Montrer que cela entraîne $d|n$ (considérer la division euclidienne de n par d).

d) En comptant les classes de conjugaison d'éléments de K^* ("équation aux classes"), montrer qu'on a

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d_i} - 1}$$

où les entiers d_i divisent strictement n.

On va montrer qu'une telle relation n'est possible que si $n = 1$ (et donc $\mathrm{K} = \mathrm{Z}$). On rappelle pour cela que le polynôme cyclotomique $\Phi_r(\mathrm{X}) \in \mathbb{Z}[\mathrm{X}]$ est défini par

$$\Phi_r(\mathrm{X}) = \prod_{\zeta \in \mathrm{P}_r} (\mathrm{X} - \zeta)$$

où P_r désigne l'ensemble des racines primitives r-ièmes de l'unité. On a donc

$$\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d(\mathrm{X}) \ .$$

e) Déduire de *d*) que l'entier $\Phi_n(q)$ divise $q - 1$. Montrer par ailleurs qu'on a $|\Phi_n(q)| > q - 1$ si $n > 1$, d'où une contradiction.

3) Soit K un corps (non nécessairement commutatif) de caractéristique $p > 0$, G un sous-groupe fini de K^*. Montrer que le sous-groupe additif de K engendré par G est un sous-anneau fini de K, puis que c'est un corps. Déduire du théorème de Wedderburn que G est cyclique.

Le résultat est-il encore vrai en caractéristique 0?